ARTICLE 19

DA CIBERSEGURANÇA À CIBERGUERRA

O DESENVOLVIMENTO DE POLÍTICAS DE VIGILÂNCIA NO BRASIL

EQUIPE ARTIGO 19

DIRETORA
Paula Martins

PROTEÇÃO E SEGURANÇA DA LIBERDADE DE EXPRESSÃO
Júlia Lima
Thiago Firbida
Alessandra Alves

DIREITOS DIGITAIS
Laura Tresca
Luiz Perin

ACESSO À INFORMAÇÃO
Joara Marchezini
Mariana Tamari
Bárbara Paes
Lia Logarezzi

CENTRO DE REFERÊNCIA LEGAL
Camila Marques
Raissa Maia
Mariana Rielli
Dennys Eduardo G. Camara

COMUNICAÇÃO
João Ricardo Penteado
Roberto Batista

ADMINISTRATIVO-FINANCEIRO
Regina Marques
Rosimeyri Carminati
Yumna Ghani

CONSELHOS ADMINISTRATIVO E FISCAL
Eduardo Pannunzio
Belisário dos Santos Júnior
Malak Poppovik
Luiz Eduardo Regules
Luciana Guimaraẽs
Marcos Fuchs
Heber Araújo
Thiago Donnini

1 – Introdução	06
2 – Intersecções entre o vigilantismo, cibersegurança, cibercrimes e ciberguerra	09
3 – A cultura de vigilância versus a proteção da privacidade no Brasil	15
3.1 Nasce um negócio	16
3.2 A proteção da privacidade no Brasil	17
3.3 Padrões Internacionais	18
4 – Respostas Brasileiras	21
4.1 Infraestrutura	21
4.2 Governança da Internet	23
4.3 Defesa Cibernética	26
5 – Panorama da Segurança Cibernética Brasileira	31
5.1 Ameaças e níveis de segurança no Brasil: avanços e retrocessos	33
5.2 Segurança da rede	34
5.4 Ciberguerra	39
6 – Considerações Finais	44
7 – Anexos	47
8 – Referências	74

SIGLAS

CIA	Central Intelligence Agency ou Agência Central de Inteligência
ABIN	Agência Brasileira de Inteligência
ANATEL	Agência Nacional de Telecomunicações
CALEA	The Communications Assistance for Law Enforcement Act ou Lei de Auxílio das Comunicações para a aplicação do Direito
CCOMGEX	Centro de Comunicações e Guerra Eletrônica do Exército Brasileiro
CDCiber	Centro de Defesa Cibernética
CDN	Conselho de Defesa Nacional
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CGI.br	Conselho Gestor da Internet no Brasil
CGSI	Comitê Gestor de Segurança da Informação
CIGE	Centro de Instrução de Guerra Eletrônica
CITEX	Centro Integrado de Telemática do Exército
CMID	Conselho Militar de Defesa
CPI	Comissão Parlamentar de Inquérito
CREDEN	Câmara de Relações Exteriores e Defesa Nacional
DENARC	Divisão Estadual de Narcóticos
DoS	Denial of Service ou Negação de Serviço
DPF	Departamento da Polícia Federal
EB	Exército Brasileiro
EscCom	Escola de Comunicações
EsIMEx	Escola de Inteligência Militar do Exército
ESUDE	Escola Sul-americana de Defesa
EUA	Estados Unidos da América
GSI-PR	Gabinete de Segurança Institucional da Presidência da República
HT	Hacking Team
ICANN	Internet Corporation for Assigned Names and Numbers ou Corporação da Internet para Atribuição de Nomes e Números
IDCIBER	Instituto de Defesa Cibernética
IP	Internet Protocol ou Protocolo de Internet
IPEA	Instituto de Pesquisa Econômica Aplicada
LAI	Lei de Acesso à Informação (Lei nº 12.527, de 2011)
MBL	Movimento Brasil Livre
MCI	Marco Civil da Internet (Lei nº 12.965, de 2014)
MD	Ministério da Defesa
Minicom	Ministério das Comunicações
MJ	Ministério da Justiça
MP	Ministério Público
MPF	Ministério Público Federal
MPOG	Ministério de Orçamento, Planejamento e Gestão
NETMundial	Encontro Multissetorial Global Sobre o Futuro da Governança da Internet
NIC.br	Núcleo de Informação e Coordenação do ponto BR
NSA	National Security Agency ou Agência de Segurança Nacional
NuComDCiber	Núcleo do Centro de Defesa Cibernética
NuENaDCiber	Núcleo da Escola Nacional de Defesa Cibernética
OCEO	Offensive Cyber Effect Operations ou Operações Cibernéticas Ofensivas
OEA	Organização dos Estados Americanos

ONU	Organização das Nações Unidas
OSINT	Open Source Intelligence ou Inteligência de Fontes Abertas
OTAN	Organização do Tratado do Atlântico Norte
PF	Polícia Federal
PMDB	Partido do Movimento Democrático Brasileiro
PR	Presidência da República
PSDB	Partido Social Democrático Brasileiro
PT	Partido dos Trabalhadores
PTTs	Pontos de troca de tráfego
RENASIC	Rede Nacional de Segurança da Informação e Criptografia
SCAe	Subgrupo de Cooperação Aeroespacial (UNASUL)
SCDC	Subgrupo de Cooperação de Defesa Cibernética (UNASUL)
SegCiber	Segurança Cibernética
Serpro	Serviço Federal de Processamento de Dados
SGTI	Secretaria de Logística e Tecnologia da Informação
SIC	Segurança da Informação e Comunicações
SNI	Serviço Nacional de Inteligência
TAC	Termo de Ajustamento de Conduta
Telebrás	Telecomunicações Brasileiras S.A.
TIC	Tecnologias da Informação e Comunicações
TNI	Tactical Network Injector
UNASUL	União de Nações Sul-Americanas
UnB	Universidade de Brasília
UNHRC	United Nations Human Rights Council ou Conselho de Direitos Humanos da ONU
USCYBERCOM	United States Cyber Command ou Comando Cibernético dos Estados Unidos
VANT	Veículo aéreo não-tripulado
VoIP	Voice over Internet Protocol ou Voz por IP

INTRODUÇÃO

A visão de um ambiente livre, plural e democrático é a tradicional imagem propagada da internet. Entretanto, por diversos interesses - notadamente os econômicos e políticos - muitas atividades feitas na Internet estão em permanente vigilância. Às vezes, com o consentimento do próprio usuário, quando da instalação de aplicativos, por exemplo. Outras vezes não.

Em junho de 2013, o jornalista Glenn Greenwald, do jornal britânico The Guardian publicou pela primeira vez reportagem sobre os documentos disponibilizados Edward Snowden, ex-técnico da CIA – Central Intelligence Agency. De acordo com as denúncias, o programa Prism[1] teria rastreado 2,3 bilhões de telefonemas e mensagens. E-mails, chats online e chamadas de voz dos serviços das maiores empresas presentes no ambiente da rede, como Apple, Facebook, Google, Microsoft, YouTube, Skype, AOL e Yahoo estavam na mira do monitoramento montado pela NSA – National Security Agency, que já era funcional havia dez anos. Snowden é, ainda hoje, acusado de espionagem pelo governo estadunidense e está em asilo político na Rússia[2].

Além de espionar a população americana, vários países da Europa e da América Latina foram alvos da ação. Entre os países espionados estava o Brasil. O denunciante demonstrou através de documentos vazados que o governo dos EUA, mais especificamente a NSA, estava inclusive fazendo o monitoramento de conversas de e-mail da presidenta Dilma Rousseff. De acordo com os vazamentos de Snowden, o Brasil ficou atrás apenas dos Estados Unidos em volume de monitoramentos e interceptações[3]. Alguns dos arquivos fazem parte de uma apresentação interna da NSA, denominada "filtragem inteligente de dados: estudo de caso México e Brasil" e foram divulgados por Greenwald[4]. Eles demonstram que a presidente Dilma Rousseff e seus principais assessores foram alvos específicos e diretos de espionagem da agência.

Tais denúncias tiveram ampla repercussão pública no Brasil, com extensa cobertura jornalística. Na época, criou-se uma expectativa de uma reação contundente por parte do governo brasileiro. A atitude mais imediata foi o cancelamento de uma missão brasileira aos Estados Unidos[5] e a promoção de investigações sobre as revelações. Inicialmente, as averiguações do Ministério da Defesa e das Forças Armadas do Brasil acabaram não encontrando indícios de invasão nos sistemas criptografados que contém as informações estratégicas do país[6]. Entretanto, as acusações tiveram grande influência no Congresso Nacional e em 10 de agosto de 2013 uma CPI - Comissão Parlamentar de Inquérito foi instaurada para investigar o suposto monitoramento em massa.

A CPI para apurar as denúncias da espionagem e da vigilância estadunidense no Brasil foi chamada de CPI da Espionagem. Durou sete meses e teve participação de 13 senadores entre titulares e suplentes. Segundo as conclusões da CPI, não foi possível determinar quais informações teriam sido violadas ou se efetivamente houve espionagem nos moldes das revelações feitas por Snowden, mas a CPI destacou que os indícios coletados apontavam nesta direção. A conclusão mais importante - e que legitimou a adoção de medidas práticas para o desenvolvimento de políticas no setor - foi a

1 O esquema de vigilância de comunicações online organizado pela NSA em parceria com Reino Unido, Canadá, Austrália e Nova Zelândia que armazenava sem autorização os dados das comunicações via internet entre pessoas, governos e empresas. O programa permitia aos funcionários da NSA a coleta de vários tipos de dados dos usuários em poder de sites e serviços de internet, incluindo histórico de pesquisas, conteúdo de e-mails, transferências de arquivos, vídeos, fotos, chamadas de voz e vídeo, detalhes de redes sociais, logins e quaisquer outros dados em poder das empresas de Internet. Para saber mais acesse: http://infograficos.estadao.com.br/public/especiais/snowden/quem-e-snowden.html

2 http://g1.globo.com/mundo/noticia/2014/08/snowden-recebe-permissao-de-residencia-por-3-anos-na-russia.html

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

4 http://g1.globo.com/politica/noticia/2013/09/documentos-da-nsa-apontam-dilma-rousseff-como-alvo-de-espionagem.html

5 http://politica.estadao.com.br/noticias/geral,dilma-cancela-viagem-aos-eua,1075730

6 http://oglobo.globo.com/mundo/governo-brasileiro-nao-ve-indicios-de-invasao-nos-sistemas-9033959

constatação de que há fragilidades na segurança digital brasileira e há necessidade de mais transparência e controle sobre as requisições de dados feitas no Brasil. Especificamente, o relatório final acabou por recomendar[7]:
- um maior investimento na área de inteligência e contra-inteligência por conta da vulnerabilidade observada atualmente na área;
- investimentos em tecnologia própria e nacional;
- capacitação de profissionais para atuação na área;
- a publicação do Plano Nacional de Inteligência pela Presidência da República;
- a criação de uma Agência Brasileira de Inteligência de Sinais, para operar no ambiente virtual e que tenha um caráter ofensivo[8];
- a aprovação da PEC nº67, de 2012, que eleva a atividade de inteligência ao nível constitucional, cria um sistema de brasileiro de inteligência com fiscalização do Poder Legislativo.

Aliado ao contexto de crescentes protestos sociais, a realização da Copa do Mundo e as Olimpíadas, tais reações resultaram na constituição de um amplo aparato estatal de vigilância da Internet no Brasil. O objetivo dessa publicação, portanto, é de demonstrar como se estruturou esse arcabouço estatal e o impacto de tais práticas para a liberdade de expressão no país. Assim, outras medidas adotadas após as revelações de Snowden e como evoluímos do debate da cibersegurança para a ciberguerra serão detalhadas a seguir.

A privacidade nas comunicações e no uso da rede é elemento importante para a liberdade de expressão, na medida em que determinadas mobilizações e articulações, sociais e políticas, requerem confidência entre os pares para que ocorram. Quando agentes ou instituições do Estado ou do governo empregam práticas de vigilância, eles limitam a livre comunicação de ideias. O constrangimento do livre pensamento coíbe qualquer tipo de apontamento de eventuais abusos dos mais diversos atores presentes na sociedade, ou até mesmo de um questionamento da ordem vigente. É necessário, portanto, garantir o direito à privacidade para que o direito à liberdade de expressão possa ser pleno.

7 http://www.senado.leg.br/atividade/rotinas/materia/getTexto.asp?t=149208&c=PDF&tp=1

8 No relatório, são apresentadas agências de inteligência de sinais pelo mundo e um aspecto destacado é o fato de que todas exercem atividades de inteligência - reunião de dados, inclusive protegidos, para produção de conhecimento - e contra-inteligência. Estados Unidos, Reino Unido, Canadá, Austrália e Nova Zelândia já investem na inteligência de sinais há pelo menos três décadas, com cooperação entre eles, na aliança conhecida como Five Eyes. Em alguns países, a atividade de inteligência de sinais associa-se à guerra eletrônica, absorvida em estruturas de defesa cibernética, geralmente no setor militar. Em outras nações, existem agências civis próprias para esse tipo de serviço. Uma terceira realidade são órgãos civis e militares de inteligência e defesa cibernética que convivem em uma mesma comunidade e se mesclam em certas missões. Para mais informações, acesse: http://www.senado.gov.br/noticias/jornal/emdiscussao/espionagem/materia.html?materia=cpi-pede-orgao-para-inteligencia-cibernetica.html

_INTERSECÇÕES ENTRE O VIGILANTISMO, CIBERSEGURANÇA, CIBERCRIMES E CIBERGUERRA

INTERSECÇÕES ENTRE O VIGILANTISMO, CIBERSEGURANÇA, CIBERCRIMES E CIBERGUERRA

A internet tornou-se essencial para boa parte das atividades que realizamos cotidianamente. Diversas operações diárias, individuais e coletivas, são realizadas ou facilitadas pela internet. Igualmente, a própria operação do Estado e a prestação de serviços públicos viram-se também impactadas pela rede. Por exemplo, os sistemas de energia, hidráulica, comunicação, segurança dos países são sumariamente controlados por meio dela. Isso os tornou incrivelmente eficientes, dinâmicos e ágeis em comparação a décadas passadas. O custo de tal prática, entretanto, é a dependência do pleno funcionamento do sistema online.

Neste contexto, alguns termos foram sendo criados e disseminados para referência a situações consideradas de risco para indivíduos, grupos, empresas, órgãos estatais etc. no mundo online.

A **cibersegurança** ou **segurança cibernética** pode ser definida como a proteção de sistemas, redes e dados no ciberespaço. Ataques cibernéticos sem o envolvimento de agentes estatais podem designar uma série de ações, como atividades criminosas, espionagem industrial, guerra econômica, entre outras. Essas ações não são facilmente rastreáveis, pois quem as realiza normalmente tem conhecimento técnico o suficiente para não deixar rastros[9]. É uma questão crítica não só para o Estado e empresas, mas também para cidadãos usuários da internet. Ações de prevenção e reação a tais incidentes normalmente ocorre no âmbito civil e privado.

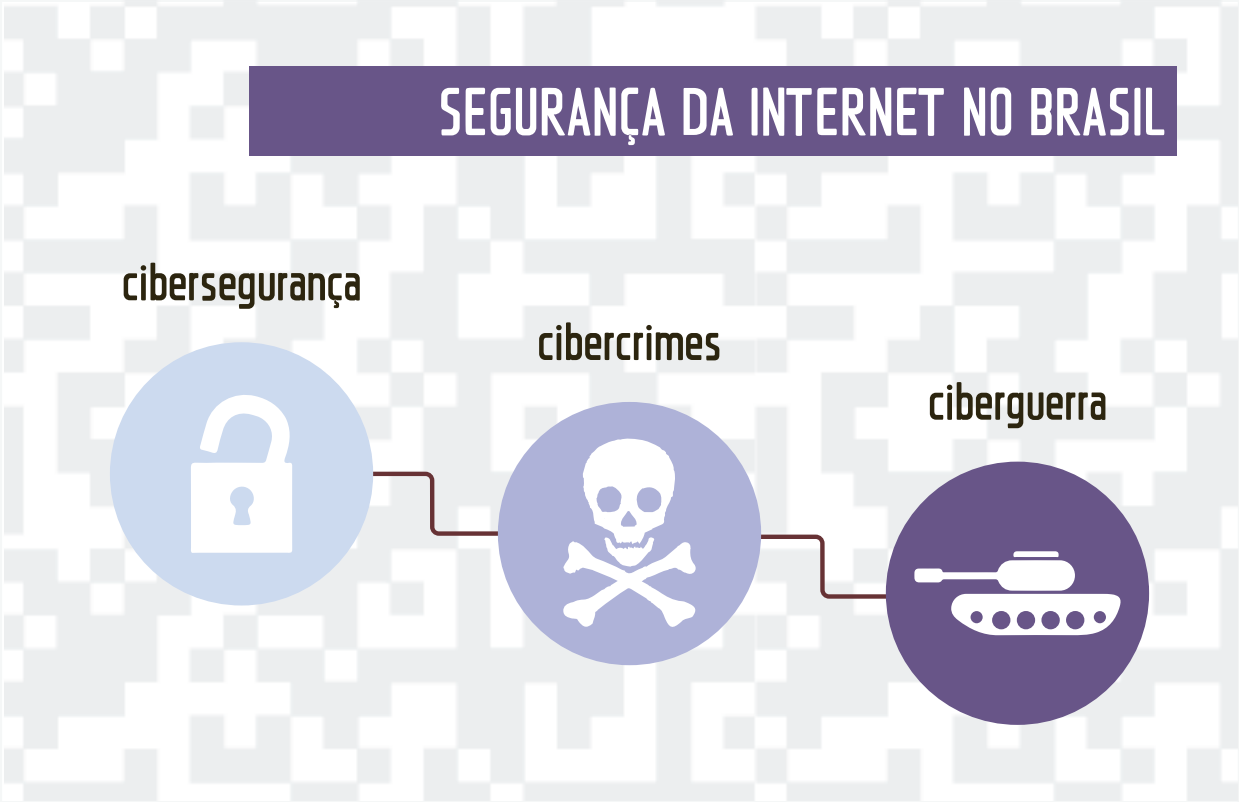
O escopo dos **cibercrimes** ou **crimes cibernéticos** se limita a atos proibidos por lei que fazem uso da internet. Portanto, devem ser responsabilidade das polícias e dos órgãos com capacidade investigativa do Estado. É necessário diferenciar que nem todo cibercrime é considerado uma ameaça estatal - que teria de ser uma ação configurada contra o Estado.

Existem inúmeras discussões sobre o significado de **ciberguerra** ou **guerra cibernética**, mas ela deve pode ser compreendida, de maneira geral, como um confronto via meios eletrônicos e informáticos – via internet - e que costumam ter como alvo infraestruturas críticas, notadamente bens de interesse público como redes de energia elétrica, de gás e de água, os serviços de transportes, os serviços de saúde e financeiros. Uma possível uma guerra cibernética entre governos, por exemplo, pode ocorrer por meio da instalação de softwares que podem causar danos físicos a sistemas de áreas críticas para um país[10]. Tais tipos de ataques se tornaram parte central da atuação e do planejamento estratégico de vários Estados do mundo, a ponto de criarem unidades de inteligência militar especializadas. As ações empregadas para prevenção e reação de tais ataques estão no âmbito da **ciberdefesa**.

---

9 Em março de 2014, aconteceu um grande ataque cibernético, considerado por muitos o maior já registrado até então. A internet no mundo inteiro teve a velocidade afetada por conta de uma briga entre o grupo privado Spamhaus, que luta contra o envio de spams e o provedor Cyberbank que abriga sites acusados de enviar esse tipo de mensagens. O Spamhaus teria bloqueado todos os servidores mantidos pela Cyberbank por considera-los perigosos. Por sua vez, o Cyberbank negou que tenha qualquer influência sobre o que ocorra com esses servidores e que a Sapmhaus estaria abusando de seu poder. Fato é que, após o bloqueio, ocorreram ataques DDoS (que derruba servidores com enormes quantidades de tráfego) massivos que prejudicaram todo o tráfego na rede, inclusive sites como o Netflix. Veja mais: http://www.bbc.co.uk/portuguese/ultimas_noticias/2013/03/130327_ataque_cibernetico_ji.shtml

10 Foi este o caso do Stuxnet, descoberto em 2010, quando foi descoberto um software instalado em uma usina nuclear iraniana programado pela inteligência americana que conseguia danificar o reator nuclear impedindo o processo de enriquecimento de urânio. Este caso, no entanto, é único na história até o momento, no qual um país consegue sabotar por meio do uso de um software uma usina energética de outro. Fonte: http://oglobo.globo.com/sociedade/tecnologia/novos-ciberguerreiros-do-pentagono-2943247



É importante frisar que os limites e parâmetros que serão adotados pelo Estado brasileiro parecem estar ainda em construção, com referências variadas em diversas publicações. De acordo com o Livro Verde da Segurança Cibernética no Brasil[11], publicado pelo Departamento de Segurança da Informação e Comunicações do então Gabinete de Segurança Institucional da Presidência da República[12], inicialmente, interpreta-se que o escopo de atuação da segurança cibernética compreende aspectos e atitudes tanto de prevenção quanto de repressão. E para a defesa cibernética entende-se que a mesma compreende ações operacionais de combates ofensivos. De acordo com publicações anteriores, o governo brasileiro através do IPEA[13] define defesa cibernética como o "(...) conjunto de ações defensivas, exploratórias e ofensivas, no contexto de um planejamento militar, realizadas no espaço cibernético, com as finalidades de proteger os sistemas de informação, obter dados para a produção de conhecimento de inteligência e causar prejuízos aos sistemas de informação do oponente (Brasil, 2011)". Já a ideia de segurança cibernética em nível estatal, diz respeito "(...) à proteção e garantia de utilização de ativos de informação estratégicos, principalmente os ligados às infraestruturas críticas da informação (...)" para controlar a infraestrutura crítica nacional abrangendo, inclusive a interação com órgãos privados envolvidos no funcionamento destas. Já segundo definição da Doutrina Militar de Defesa Cibernética, a guerra cibernética:

"Corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar, explorar, corromper, degradar ou destruir capacidades de comando e controle do adversário, no contexto de um planejamento militar de nível operacional ou tático ou de uma operação militar. Compreende ações que envolvem as ferramentas de TIC para desestabilizar os Sistemas de Tecnologia da Informação e Comunicações e Comando e Controle (STIC3) do oponente e defender os próprios STIC3. Abrange, essencialmente, as ações cibernéticas. A oportunidade para o emprego dessas

11 http://dsic.planalto.gov.br/documentos/publicacoes/1_Livro_Verde_SEG_CIBER.pdf - pg 19

12 Hoje uma secretaria subordinada à Casa Militar

13 www.ipea.gov.br/agencia/images/stories/PDFs/TDs/td_1850.pdf

ações ou a sua efetiva utilização será proporcional à dependência do oponente em relação às TIC."[14]

Todos estes termos tocam a questão do **vigilantismo**. O termo é usado aqui para se referir à pratica de operações de vigilância generalizada ou de massa, que muitas vezes são utilizadas de forma excessiva, ou mesmo ilegal, tanto por governos como por entes privados. O vigilantismo é uma ameaça à liberdade de expressão e outros direitos fundamentais, como a privacidade, por exemplo. Ele pode ocorrer tanto no âmbito da cibersegurança, cibercrime ou ciberguerra.

Uma guerra sem fronteiras

No momento em que as sociedades passam a depender de sistemas online para gerenciar energia, segurança, comunicação, agricultura, saúde pública e outros serviços públicos, qualquer possibilidade de interrupção torna-se um risco para a segurança nacional. A informação passa a ter uma importância estratégica ainda maior numa sociedade moderna.

Até o início do Século XX, os Estados tinham a terra e a água como domínios de guerra. Durante a II Guerra Mundial, o domínio vertical passou a ser incorporado pela aeronáutica. Já o domínio espacial apareceu na Guerra Fria. Durante os anos 80 e 90, com a disseminação dos computadores como resultado da revolução da microeletrônica, a informação passou a ser algo onipresente e essencial para as disputas entre sociedades. Para garantir o pleno funcionamento social, os Estados passaram a elaborar uma doutrina de segurança para o que é concebido como o quinto domínio da guerra, a cibernética, ou a dimensão da informação.

Em outubro de 2010, durante a administração de Barack Obama, entrou em operação o USCYBERCOM, o Comando Ciber do Exército dos Estados Unidos tendo como justificativa a proteção das redes militares e do governo contra ciberataques de outras nações. O novo comando absorveu as demais forças tarefas e outros grupos de trabalho do exército que existiam anos antes e teve inicialmente em sua direção o General Keith Alexander, na época também diretor da NSA[15]. O contexto mundial da criação do ciber comando era a onda de ciberataques ocorridos na Estônia[16], em 2007, e na Geórgia[17], em 2008, na qual a Organização do Tratado do Atlântico Norte (OTAN) interviu para defender as redes civis e militares dos países atacados. Em ambos os casos, se suspeita articulação ou mesmo apoio militar do governo russo aos ataques - os quais resultaram na interrupção dos sistemas de comunicação e bancário dos dois países por dias e até semanas.

No entanto, dada a própria organização da rede, ataques cibernéticos são difíceis de serem apurados para o apontamento da autoria. Da perspectiva de nações com o domínio de ciberguerra como China, Israel, Rússia e Estados Unidos, na verdade, isso pode configurar uma vantagem, uma vez que podem desenvolver suas atividades de espionagem e guerra econômica sem estarem diretamente envolvidos e, inclusive, negarem qualquer relação com o ocorrido (ver Operação Aurora[18] e Stuxnet[19]). Os casos de ciberataques não devem ser analisados como incidentes isolados, mas como a realização de uma doutrina específica e militarizada de ciberdefesa, a qual prevê o emprego de

14 Páginas 20-36 http://defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf

15 http://news.bbc.co.uk/2/hi/8511711.stm

16 http://www.theguardian.com/world/2007/may/17/topstories3.russia

17 http://www.telegraph.co.uk/news/worldnews/europe/georgia/2539157/Georgia-Russia-conducting-cyber-war.html

18 A Operação Aurora (2010) teve como alvo de ataques diversas empresas dos EUA, entre elas o Google, que teve sua propriedade intelectual roubada e acesso violado de contas de emails de ativistas de direitos humanos. Ver anúncio oficial do Google, "New approach to China", https://googleblog.blogspot.com/2010/01/new-approach-to-china.html

19 Ver nota 10.

ciberarmas e ciberataques para assegurar os objetivos nacionais[20]. Revelado em documento vazado por Edward Snowden, uma diretiva secreta sobre ciberdefesa elaborada durante a administração Obama define as chamadas Operações Cibernéticas Ofensivas ("Offensive Cyber Effect Operations", em inglês)[21], as quais:

"[As OCEO] oferecem capacidades únicas e não convencionais para o avanço dos objetivos nacionais dos Estados Unidos ao redor do mundo com pouco ou nenhum advertência viso ao adversário ou alvo e com efeitos potenciais que vão desde algo sutil até algo gravemente danoso. O desenvolvimento e a sustentação das capacidades de OCEO, no entanto, podem exigir de esforço e tempo considerável caso o acesso e as ferramentas para um alvo específico ainda não existam."

"O Governo dos Estados Unidos deverá identificar potenciais alvos de importância nacional onde as Operações Cibernéticas Ofensivas podem oferecer um balanço favorável entre a efetividade e o risco em comparação com os outros instrumentos de poder nacional, estabelecer e manter as capacidades de OCEO integradas conforme apropriadas com as outras capacidades ofensivas dos Estados Unidos, e executar essas capacidades de uma forma consistente com as disposições dessa diretiva"[22]

O emprego de segurança ofensiva para a realização de OCEOs implica no desenvolvimento, na compra de vulnerabilidades e na implementação de backdoors[23] nos softwares e hardwares para a criação de ciberarmas. Por um lado, ao caminharem nessa direção os Estados tornam o mundo menos seguro para todos, pois não só eles passam a colecionar vulnerabilidades críticas dos sistemas, como também possivelmente as nações adversárias, que são obrigadas a atacar com as mesmas "armas". Por outro, após a externalização da produção tecnológica mundial para a China, é alarmante observar a segurança dos equipamentos ali produzidos quando os outros países também implementam backdoors em suas tecnologias via ordens secretas ou mesmo por dispositivos legais como no caso do CALEA[24] nos Estados Unidos. Esse é um grave problema de confiança que atingiu as empresas do Vale do Silício após as revelações de Snowden e tem chamado a atenção dos militares brasileiros.

No entanto, mesmo a "vigilância passiva", isto é, a coleta em massa de dados por empresas e governos, tornou-se uma atividade crítica não só para o direito à privacidade, mas um risco à segurança nacional, pois uma vez que coletadas essas informações poderão ser extraídas pela inteligência de outros países diretamente dos serviços que realizaram o armazenamento. Atualmente, os países que adotam uma doutrina de segurança nacional que se vale de vigilância em massa e, consequentemente, da coleta de dados em massa, também colocam em risco a própria segurança do país. Como afirmou um especialista em segurança, "O novo mantra da cibersegurança: 'se você não pode proteger, não colete'"[25].

Essa conclusão pode ser extraída diante dos grandes vazamentos de banco de dados de saúde pública, do Social Security Number e de empresas aéreas dos Estados Unidos no início de 2015. Sob a condição de anonimato[26], analistas da inteligência dos Estados Unidos informaram que a China

20 Ver Bruce Schneier: CNN, 18 de junho de 2013, disponível em: http://edition.cnn.com/2013/06/18/opinion/schneier-cyber-war-policy/index.html

21 Documento vazado: http://www.theguardian.com/world/interactive/2013/jun/07/obama-cyber-directive-full-text

22 https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities

23 Apresentação na Trilha de Cibersegurança e Confiança no V Fórum da Internet no Brasil, disponível em https://www.youtube.com/watch?v=daGmaaTJMJw

24 https://www.eff.org/issues/calea

25 Richard Bejtlich, 03 de setembro de 2015, "New cybersecurity mantra: if you can't protect it, don't collect it".

26 "With a series of major hacks, China builds a database on Americans", The Washington Post, 05 de Junho de 2015, https://www.washingtonpost.com/world/national-security/in-a-series-of-hacks-china-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa--0ba3-11e5-95fd-d580f1c5d44e_story.html

passou a aumentar sua capacidade de coleta de inteligência criando um banco de dados dos americanos a partir dos dados vazados. Da perspectiva da inteligência chinesa, ao invés de usarem inteligência de sinais (SIGINT) ou humana (HUMINT) para recrutar, espionar ou sabotar, uma seleção de alvos muito mais sofisticada poderia ser feita através do cruzamento desses bancos de dados. Esse é um novo tipo de ameaça a segurança nacional, pois sua ameaça não é a interrupção de serviço, mas o seu perfeito funcionamento.

A noção de segurança de rede, portanto, parte do princípio de que praticamente todo movimento na esfera virtual repercute também fora dela. Os danos causados às redes são danos causados diretamente a quem as utiliza. Assim, o monitoramento da rede a fim de evitar incidentes de segurança tem objetivos legítimos e a ciberguerra não é um cenário ficcional. Inclusive, a proteção da segurança nacional é uma preocupação legítima e motivação para uma possível restrição à liberdade de expressão, prevista em tratados internacionais de direitos humanos, como a Convenção Americana de Direitos Humanos (ou Pacto de San José da Costa Rica), de 1969[27].

Diante desse cenário, em 2015, um Grupo das Nações Unidas de Especialistas Governamentais em Desenvolvimento no Campo das Comunicações e Telecomunicações no Contexto de Segurança Internacional lançou um relatório de consenso sobre as regras de comportamento no ciberespaço, especialmente durante tempos de paz[28]. Participaram do grupo de trabalho representantes de 20 nações. Entre outras recomendações, o relatório indica que os países não devem usar tecnologias de informação e comunicação para atacar infraestrutura crítica ou interromper os sistemas de informação dos serviços de emergência.

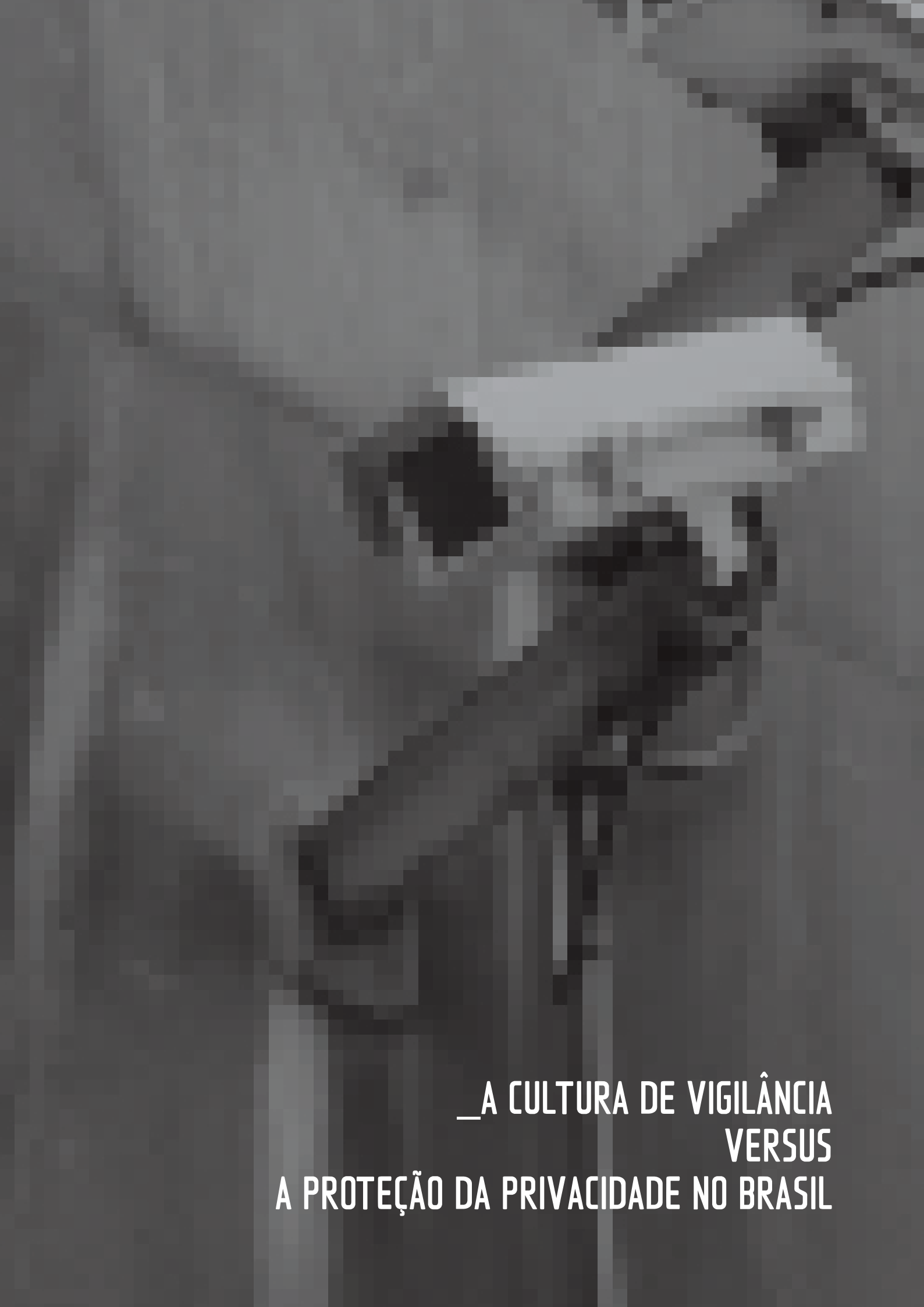
Há ainda outras iniciativas de acordos táticos como a Coalisão pela Liberdade Online - Freedom Online Coalition[29], que reúne 29 governos para a promoção da liberdade na Internet com uma abordagem multissetorial ou a recém-lançada Global Forum on Cyber Expertise[30], que reúne governos e empresários em torno das questões de cibercrimes e cibersegurança.

27 http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/anexo/and678-92.pdf

28 http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

29 https://www.freedomonlinecoalition.com/

30 http://www.thegfce.com/



_A CULTURA DE VIGILÂNCIA VERSUS A PROTEÇÃO DA PRIVACIDADE NO BRASIL

A CULTURA DE VIGILÂNCIA VERSUS A PROTEÇÃO DA PRIVACIDADE NO BRASIL

A cultura de vigilância no Brasil é histórica. Durante a ditadura (1964 – 1985), o expediente foi amplamente utilizado para combater a resistência ao regime. A doutrina militar orientou-se em encontrar e eliminar os perigos internos - os subversivos - transformando cidadãos em possíveis ameaças à segurança nacional. Era necessário vigiar os cidadãos, infiltrar militares nos círculos sociais e realizar trabalho de inteligência para detectar as novos potenciais perigos. Essa prática teve como órgão principal o Serviço Nacional de Inteligência - SNI.

O que se imaginou ser uma página do passado mostrou-se presente, novamente, no período democrático. A interceptação das comunicações foi uma exceção ao direito à privacidade admitida na Constituição Federal de 1988. Então, em 1996, a gestão presidencial de Fernando Henrique Cardoso elaborou a Lei 9.269 para regularizar essas exceções a fim de que o Brasil seguisse o mesmo rumo dos regimes democráticos e coibisse a prática herdada do período militar.

Mais de uma década após a regularização do grampo, entre 2007 e 2009, a Comissão Parlamentar de Inquérito sobre as "Escutas Telefônicas Clandestinas"[31]- conhecida como a CPI dos Grampos - foi responsável por fazer uma radiografia sobre a situação das interceptações telefônicas no país[32]. Segundo o levantamento inicial, em 2007, foram operacionalizadas 409.000 interceptações no Brasil. Neste número contabilizava a quantidade de pedidos judiciais feitos para um mesmo número, uma vez que a interceptação judicial é válida por um período (15 dias), a cada nova prorrogação foi contado como uma nova interceptação. Após reconsiderar o método, contabilizando o mesmo número de telefone, independente do prazo e das prorrogações legais da interceptação, o número de interceptações no país passou para 375.643 no ano de 2007. Em 2008, o número total de interceptações no país foi de 358.839. Na época, o país foi chamado de República dos Grampos ou Grampolândia[33].

A CPI mapeou e trouxe à luz diversas práticas ilegais que ocorriam nas interceptações como, por exemplo, a prática da "barriga de aluguel", na qual os números de telefones de outras investigações eram enxertados no pedido judicial de quebra de sigilo de investigação não relacionada. Como não há revisão ou processo de checagem dos números pela autoridade judicial, aproveitava-se assim de um pedido legal para executar uma operação ilegal. Ainda foi apurado o vazamento dos áudios e das transcrições dos grampos para os jornais[34], tendo como origem a falta de cadeia de custódia e a não restrição de acesso aos áudios, ou seja, um técnico forense poderia copiar os áudios para seu computador pessoal.

Hoje, apesar de legalmente estabelecidos, os grampos continuam uma prática institucionalizada do Estado brasileiro, através das polícias e do Ministério Público. O uso interceptação de comunicações privadas de forma sistemática para a resolução de casos policiais, apesar de muitas vezes legítima e autorizada por um juiz, é demasiadamente disseminada no país e muitas vezes privilegiada em detrimento de outras formas de investigação. Não só parece haver muita flexibilidade do Judiciário

31 A comissão foi estabelecida após as denúncias feitas pela revista Veja, edição 2.022, nº 33, de 22 de agosto de 2007, num controverso episódio resultante da Operação Satyagraha conhecido como o "grampo sem áudio" entre o Ministro do Supremo Tribunal Federal, Gilmar Mendes, e o senador Demóstenes Torres.

32 As notas taquigráficas assim como o relatório final da CPI dos Grampos: http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/53a-legislatura-encerradas/cpiescut/relatorio-final-aprovado-1

33 http://www.gazetadopovo.com.br/vida-publica/bem-vindo-a-grampolandia-b606ggp62q8zv1mffuja94hn2

34 É importante diferenciar estes vazamentos seletivos daquilo que é feito por organizações de whistleblowers como WikiLeaks e The Intercept, pois, nestes é possível a opinião pública ter acesso tanto a análise feito pelo jornalista quanto ao material fonte, podendo então realizar sua própria análise dos documentos.

para analisar os pedidos, mas também um claro exagero das autoridades competentes na busca por esse tipo de provas. A situação já foi inclusive motivo de discussão que teve como pivô o Ministério Público no ano de 2013[35]. Delegados da Polícia Federal afirmavam que estavam preocupados com o "uso descontrolado" da ferramenta.

Para evitar potenciais abusos desses atos, devem ser considerados os direitos humanos fundamentais e dos preceitos do Código de Processo Penal. Ademais, os pedidos de quebra de sigilo, principalmente os telemáticos, também devem ser analisados diante dos limites de necessidade e proporcionalidade.

Nasce um negócio

É importante observar que o grande número de escutas telefônicas só foi possível na conjunção de dois fatores: em primeiro, a herança de uma prática histórica de um regime não democrático no país, isto é, a ditadura e a espionagem dos cidadãos; e, segundo, a digitalização das comunicações, o que implica na diminuição do trabalho humano para a gravação, transcrição dos áudios e busca do material de interesse. O que era realizado por trabalho manual, ou seja, necessitava de agentes escutando, anotando e analisando os áudios, agora esse processo é completamente digitalizado e automatizado por software. A digitalização da comunicação tornou barato o custo da vigilância.

A venda de soluções de segurança para indivíduos como o uso de softwares antivírus e similares durante muito tempo foi um bom nicho de mercado. Hoje, além do mundo corporativo, há um novo mercado representado na figura dos Estados e das suas organizações para a aplicação da lei. Começa a aparecer uma procura maior por parte do aparato estatal de programas, equipamentos e dispositivos capazes de protegê-los e de outro lado interceptar comunicações telemáticas na internet e até mesmo infectar dispositivos como celulares. Produtos e serviços são apresentados e criados especificamente para os desafios e necessidades destes agentes estatais[36]. Nasce, assim, um novo consumidor e uma nova oferta de produtos.

No âmbito da CPI dos Grampos, o Guardião, da empresa Dígitro, o Sombra e outros produtos para interceptação utilizadas pelas polícias judiciárias e pelo Ministério Público também foram apresentados em sessões restritas e analisados pelos deputados, os quais chegaram a visitar a sede da Dígitro, em Santa Catarina. Embora esses serviços sejam "grampos passivos", isto é, dependem da cooperação das operadoras de telefonia móvel, a CPI, à época, observou a ausência de legislação que regule a venda e acesso aos produtos de interceptação.

Hoje em dia, os grampos foram devidamente regulamentados e fazem parte de um mercado que tem como consumidor as autoridades com capacidade investigatória no Brasil. A empresa Dígitro inclusive divulgou comunicado[37] reiterando alguns pontos para esclarecer sua atuação e venda, como:

"- A Operadora não intercepta "alvos" sem autorização judicial.
- A Justiça não concede Alvarás para entidades privadas ou pessoas.
- As operações investigativas são normalmente acompanhadas pelo Ministério Público.
- A Dígitro não vende o Guardião para entidades não habilitadas — e só entidades de Estado são habilitadas. Cada equipamento tem número de série. A distribuição é controlada. Não existe a hi-

35 http://colunaesplanada.blogosfera.uol.com.br/2013/03/26/sistema-guardiao-e-o-motivo-da-briga-entre-policia-e-mp/

36 Um exemplo é o smartphone brasileiro 'anti-espião', que vem com aplicativo de mensagens criptografadas. O Ministério da Justiça comprou em julho de 2014 licenças para colocar o app nos smartphones de 11,5 mil de agentes de inteligência -- 6 mil já o utilizam. Mais informações em: http://g1.globo.com/tecnologia/noticia/2015/03/smartphone-brasileiro-anti-espiao-veta-camera-e-gps-pela-seguranca.html

37 http://www.digitro.com/pt/comunicado/

pótese de uso "avulso" do equipamento. A implantação e operação só são possíveis com técnicos preparados e treinados para esse fim."

A novidade é que a situação parece ter se ampliado para o meio digital, tendo em vista o acesso e disseminação do uso de sistemas como o Guardião para interceptações de voz de maneira sistematizada e otimizada. Neste ponto, existe controvérsia se a lei de interceptação telefônica se aplicaria ou não aos meios digitais, já que atualmente ela já é utilizada para ligações de voz por IP (VoIP). Outros tipos de captura, como por exemplo de tráfego de dados, não necessariamente se enquadrariam na categoria, mas a lei já é utilizada para tanto[38].

Não há regulamentação, porém, para a possibilidade de venda da tecnologia para outros países e a crescente necessidade de realizar grampos pelas polícias e pelo Ministério Público brasileiro chamaram a atenção de países vizinhos. Empresas como a Dígitro começaram a exportar tecnologia brasileira de interceptações semelhantes ao Guardião. Um exemplo que se tornou público foi o caso uruguaio, onde o governo negou-se a fornecer informações a respeito da compra da ferramenta[39]. Ademais, a tecnologia vem sendo empregada pelas polícias uruguaias sem que exista uma regulamentação clara para essa prática naquele país.

A proteção da privacidade no Brasil

No que tange especificamente à privacidade, o Brasil ainda carece de uma lei de proteção de dados pessoais. Contudo, não é verdade que existe um completo vazio regulatório sobre a questão no Brasil. Existem legislações dispersas e diferentes que trazem alguma garantia à privacidade, sem abranger o tema por completo. Entre estas, destacam-se a Lei de Cadastro Positivo (Lei nº 12.414, de 2011), a Lei de Acesso à Informação (Lei nº 12.527, de 2011), o Marco Civil da Internet (Lei nº 12.965, de 2014), além de alguns dispositivos constitucionais genéricos, como os artigos 5.º, 10.º e 12.º da Constituição.

A Lei de Cadastro Positivo, por exemplo, regulamenta a formação e consulta a bancos de dados pessoais ou jurídicos para formação de conjuntos de dados financeiros ou históricos de crédito. Nela já há a garantia à privacidade no tratamento desses dados. Além disso, ela regula a objetividade, veracidade, clareza e facilidade de compreensão para a coleta dos dados que são utilizados para avaliar a situação econômica do titular. A lei garante também o acesso a todos os dados armazenados, além da responsabilidade sobre a atualização e correção de informações obtidas.

Já a Lei de Acesso à Informação, em seu artigo 31, também regula como será feito o tratamento das informações pessoais. Nela, são mencionadas a necessidade de transparência, respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. Outro ponto importante é a garantia da restrição de acesso por parte de agentes públicos sem autorização para tanto, a não ser que sejam cumpridos alguns requisitos básicos relacionados à necessidade, interesse público, cumprimento de ordens judiciais e proteção de direitos humanos. Além disso, há a regulamentação sobre o fornecimento para terceiros mediante assinatura de termo de responsabilidade que deixe claro os objetivos do requerente, bem como as suas obrigações conforme a lei.

Entre 2008 e 2012, a sociedade civil organizada brasileira mobilizou-se contra o vigilantismo na Internet proposto pela então chamada Lei Azeredo, um projeto de lei sobre cibercrimes. O movimento foi bem sucedido e o projeto, quando aprovado, já estava praticamente esvaziado de sentido[40].

38 http://www.cartacapital.com.br/tecnologia/o-grampo-de-dados-e-legal-no-brasil-6792.html

39 http://www.dw.com/en/surveillance-and-human-rights-in-the-digital-age/a-18399282

40 Registra-se que as Leis de cibercrimes aprovadas no Brasil e incorporadas ao Código Penal têm dispositivos prejudiciais à

De outro lado, como reação ao debate penal, iniciou-se a discussão do Marco Civil da Internet, com ampla possibilidade de participação social na formulação do projeto de lei. Adotada em 2014, a Lei traz garantias gerais importantes para a proteção da privacidade online. De acordo com o artigo 7, os contratos de prestação de serviço na internet devem ser bem claros com relação à proteção, coleta, armazenamento e tratamento dos dados. Além disso, há ênfase na questão da proibição da cessão de informações a terceiros sem autorização prévia. O consentimento expresso é reforçado e exige destaque do assunto nas cláusulas contratuais. A exclusão dos dados dos usuários deve ser garantida àqueles que decidirem apagar seus dados após o término de relação entre as partes. Entre outras garantias, a lei estabelece que o acesso a dados armazenados, de fluxo de informações e comunicações privadas somente poderá ocorrer mediante autorização judicial. Contudo, ainda há pontos muito importantes que devem estar previstos em um futuro marco regulatório para proteção de dados pessoais.

Padrões internacionais

Em 2009, o relator especial da ONU para promoção e proteção dos direitos humanos e liberdades fundamentais, Martin Scheinin, argumentou que "Estados podem fazer uso de medidas de vigilância específicas desde que seja um caso específico de interferência, com base em um mandado emitido por um juiz na mostra de causa provável ou motivos razoáveis"[41]. Não se trata, portanto, de vigilância em massa.

Em seu relatório de 16 de maio de 2011[42], o então Relator Especial da ONU sobre a Liberdade de Opinião e Expressão, Frank La Rue, expressou suas preocupações de que:

> "A Internet também apresenta novas ferramentas e mecanismos através dos quais tanto o Estado quanto os agentes privados podem monitorar e coletar informações sobre as comunicações e atividades dos indivíduos na Internet. Tais práticas podem constituir uma violação do direito à privacidade dos usuários da Internet e, ao minar a confiança das pessoas e da segurança na Internet, impedir o livre fluxo de informações e ideias online."

O Relator Especial da Liberdade de Expressão observou ainda que:

> "O direito à privacidade pode estar sujeito a restrições ou limitações em certas circunstâncias excepcionais. Isso pode incluir medidas estatais de vigilância para fins de administração de justiça criminal, prevenção do crime ou no combate ao terrorismo. No entanto, tal interferência é permitida apenas se os critérios para limitações permissíveis sob a lei internacional de direitos humanos forem cumpridos. Assim, deve haver uma lei que defina claramente as condições em que o direito dos indivíduos à privacidade possa ser limitado em circunstâncias excepcionais e as medidas de usurpar este direito sejam tomadas com base em uma decisão específica por uma autoridade do Estado expressamente autorizada por lei a fazê-lo, geralmente o Judiciário, com a finalidade de proteger os direitos dos outros, como por exemplo, assegurar provas para evitar a execução de um crime e deve respeitar o princípio da proporcionalidade."

Contudo, após as revelações de Edward Snowden ficou claro que os governos têm atuado nas redes majoritariamente através de práticas vigilantistas principalmente com finalidades políticas e econômicas.

---

liberdade de expressão, como uma possível criminalização de práticas cotidianas, mas não contém mais a previsão de vigilância em massa.

41 Relatório do Relator Especial sobre a promoção e proteção dos direitos humanos e liberdades fundamentais, enquanto contesta o terrorismo, A/HRC/13/37, 28 de dezembro de 2009

42 http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

Nesse contexto, em defesa da privacidade de todas as pessoas online, 420 organizações sociais, em conjunto com juristas do mundo inteiro, endossaram 13 Princípios Internacionais sobre a Aplicação Dos Direitos Humanos na Vigilância Das Comunicações[43]. O objetivo do documento é balancear quando se faz necessário e é proporcional alguma medida de vigilância e contra-atacar práticas de vigilância em massa sem limites. Os Princípios são:

1. Legalidade, por se entender que qualquer tipo de limitação aos direitos humanos deva estar disposta na lei de maneira clara, precisa e com flexibilidade para revisões periódicas;
2. Fim Legítimo, para que medidas só possam ser impostas por autoridades estatais específicas, com interesse definido e sem nenhuma forma discriminatória possível;
3. Necessidade, em que o Estado sempre tenha que justificar que uma violação através da vigilância seja estrita comprovadamente necessária para atingir um fim legítimo;
4. Adequação, a fim de que instâncias de Vigilância das Comunicações autorizadas por lei devam ser apropriadas para a realização Fim Legítimo identificado;
5. Proporcionalidade, fazendo com que a sensibilidade da informação e a gravidade da infração aos direitos humanos sejam levadas em consideração, atendendo minimamente à diretrizes pré-estabelecidas;
6. Autoridade Judicial Competente, que tenha a capacidade e o conhecimento necessário e seja imparcial e independente, não tendo vínculo das autoridades que realizam a Vigilância das Comunicações;
7. Devido Processo Legal, assegurando que o Estado garanta os procedimentos que interferem nos direitos humanos sejam feitos de acordo com a lei;
8. Notificação do Usuário, dentro de tempo suficiente, permitindo recurso e outras medidas;
9. Transparência, para que o uso e o escopo das leis esteja o mais acessível possível à sociedade, através do fornecimento do maior número de informações sobre os pedidos de vigilância;
10. Escrutínio Público, com o estabelecimento de mecanismos de fiscalização independentes que tenham amplo e apropriado acesso às ações do Estado para, inclusive, avaliá-lo no uso da Vigilância das Comunicações;
11. Integridade das Comunicações e Sistemas, garantindo que sistemas de segurança não sejam comprometidos em decorrência de constrangimento estatal, como a criação de obrigações de retenção de dados;
12. Salvaguardas para a Cooperação Internacional, onde o padrão mais seguro em uma situação que leis de mais de um Estado possam ser aplicadas, como em uma busca de assistência de prestadores de serviço estrangeiros, seja privilegiado;
13. Salvaguardas Contra Acesso Ilegítimo e o Direito a Medidas Eficazes, a fim de que seja promulgada uma legislação que criminalize a vigilância das comunicações com sanções civis e criminais, além de garantir proteção para denunciantes e reparações para afetados.

A ARTIGO 19 entende que toda e qualquer política de segurança que envolva práticas de vigilância devem basear-se nesses Princípios a fim de não incorrer em violações dos direitos humanos.

A seguir, analisaremos como o Estado e o governo brasileiro regiram as denúncias de Snowden, para poder avaliar se tais diretrizes e ações tomadas fazem sentido à luz de tais princípios e do direito internacional.

43 https://pt.necessaryandproportionate.org/text

_RESPOSTAS BRASILEIRAS

RESPOSTAS BRASILEIRAS

Uma das consequências das denúncias de Edward Snowden, portanto, foi o reconhecimento que o Brasil deveria melhorar a segurança da Internet no país. Para isso, o governo brasileiro estruturou ações muito além dos tradicionais incidentes de segurança[44] e em pelo menos três frentes diferentes: infraestrutura, governança da internet e defesa.

Infraestrutura

O Brasil vai construir um cabo submarino de fibra óptica interligando o país com o continente europeu. Atualmente, cerca de 80% do tráfego de internet brasileiro passa pela infraestrutura estadunidense antes de ir para outros continentes, como Europa e Ásia. O governo justifica a iniciativa com base na possibilidade de otimização da transmissão de dados através da diminuição de latência (tempo de resposta das transmissões), o que acarretaria na diminuição dos custos[45] e permitirá que o Brasil e demais países da América do Sul tenham acesso direto a alguns dos maiores Pontos de Troca de Tráfego (PTTs) do mundo, localizados em Frankfurt, Amsterdã, Londres e Paris, ampliando a oferta de capacidade de tráfego internacional. O cabo deverá entrar em operação em 2017, de acordo com a Telebrás, que deverá ter a parceria da empresa espanhola Islalink, com previsão de investimentos de US$ 185 milhões.[46].

Tal ação também tem, entretanto, consequências na multilateralidade da infraestrutura, hoje extremamente centralizada nos EUA[47]. Ou seja, o teor é de viés político e de afirmação do país no cenário da governança da internet global, principalmente no aumento de relações com os europeus com a criação de novas possibilidades, como o barateamento da vinda de provedores de internet Europeus para o Brasil. O fator segurança é bastante questionável, já que o fato das informações não passarem mais majoritariamente pelo território norte-americano não significaria que alguém não poderia interceptá-lo em outro ponto da rede, já que a internet funciona de maneira interligada[48].

Não por acaso, uma das polêmicas durante as discussões do Marco Civil da Internet foi a respeito da localização dos servidores de conteúdos. Uma das propostas determinava que os dados deveriam ser hospedados totalmente em território nacional. Argumentou-se, logo após as revelações de Snowden, que seriam medidas de segurança necessárias para proteger a privacidade das informações de cidadãos brasileiros contra a espionagem da NSA. Mas, dado o contexto, o real objetivo era apenas o de obter jurisdição sobre dados de empresas estadunidenses hospedados no exterior. Até a aprovação da lei, as autoridades investigatórias brasileiras sempre tiveram dificuldade em

---

44 Como por exemplo, DoS -- Denial of Service, invasão ou scan.

45 http://www.cartacapital.com.br/tecnologia/novo-cabo-submarino-entre-brasil-e-europa-deve-baratear-internet-689.html

46 http://www.telebras.com.br/inst/?p=6285

47 http://www.comunicacoes.gov.br/sala-de-imprensa/todas-as-noticias/institucionais/35876-joint-venture-construira-cabo-submarino-ligando-o-continente-sul-americano-a-europa

48 Centralizar ou limitar a interconexão internacional e processamento local de dados ou requisição de retenção foram apontados como exemplos de fragmentação induzida por governos, na publicação "Fragmentação Internet: Uma visão geral", escrita por William J. Drake, Vinton G. Cerf, Wolfgang Kleinwächter. Acesse em: http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

obter registros de navegação de empresas estrangeiras. A preocupação com o rastreamento de comunicação e necessidade de identificação de autores e da sistemática de alocação de blocos de endereços IP identificável a determinados países é bastante problemática, porque ignora a eficiência e arquitetura da rede ao buscar a facilitação de localização de tráfego de roteamento, resolução de endereços e atribuição de nomes, numeração e endereçamento. Não obstante, tal ideia seria bastante custosa aos provedores de serviços por obrigá-los a ter seus dados armazenados em dois lugares diferentes, o que poderia acabar onerando o consumidor final. Tal fato também tem consequências graves para a privacidade dos usuários que tem seus dados armazenados. Se os diversos bancos de dados que estão no mundo já estão sujeitos aos mais variados tipos de ataques, a duplicação das informações poderia aumentar ainda mais a vulnerabilidade do que foi armazenado[49].

A ideia de forçar por meio da lei a criação de datacenters nacionais recebeu fortes críticas por parte da sociedade civil - incluindo a ARTIGO 19 - e não permaneceu na lei aprovada. Entretanto, foi criada a exigência de guarda de logs de acesso e logs de aplicações, por um ano e seis meses respectivamente, que podem ser consideradas exageradas. Tais determinações estão presentes nos artigo 13 e 15 do Marco Civil da Internet e provavelmente são uma das questões mais controversas dentro da lei. Apesar da pressão de parte da sociedade civil para que essa parte do texto não fosse aprovada, a influência dos órgãos de investigação (polícias e Ministério Público) para a guarda desses dados por maior tempo e em maior quantidade fez com que a lei fosse aprovada com tal redação.

Outra medida adotada decorrente das denúncias[50] foi a implementação do provimento de um serviço desenvolvido em software livre para e-mails, desenvolvido pelo Serpro[51] e conhecido como Expresso Livre[52]. Com isso, o Serpro entrou em evidência com o anúncio da presidente Dilma Rousseff de que seria feita a implementação de um sistema seguro para proteger os e-mails do Governo Federal[53]. Na época, diversas outras iniciativas, como maior uso de ferramentas com software livre, também foram anunciadas como uma das soluções para questões de segurança relacionadas à espionagem e monitoramento[54] que eclodiram no Brasil em 2013.

Passada a insatisfação inicial, o serviço deverá ser abandonado em breve. Em setembro de 2015, o Ministério do Planejamento, Orçamento e Gestão decidiu contratar os serviços da empresa Microsoft[55]. Para além das diversas implicações de segurança da informação que representa o uso de uma ferramenta estrangeira para a comunicação institucional, conforme as revelações sobre a NSA, também é afetada a política de uso e fomento de plataformas abertas. Tal ação do governo demonstra que as recomendações destes padrões, advindas do texto do Marco Civil da Internet, pouco importaram para a decisão da Secretaria de Logística e Tecnologia da Informação (SGTI) do Ministério.

---

49 http://www.bbc.com/portuguese/noticias/2013/10/131030_marco_civil_mm_dg

50 http://www.cartacapital.com.br/internacional/dilma-rousseff-foi-espionada-pelos-eua-6006.html

51 O Serpro, ou Serviço Federal de Processamento de Dados, é uma empresa pública brasileira, vinculada ao Ministério da Fazenda. É a maior empresa pública de Tecnologia da Informação da América Latina e uma das maiores do setor no mundo. Foi criada em 1964 com o objetivo de dar agilidade a setores estratégicos da Administração Pública brasileira e presta serviços de TI e Comunicações para estes.Um dos investimentos da empresa está ligado ao desenvolvimento de soluções com Software Livre .

52 http://softwarelivre.org/expresso-livre

53 http://g1.globo.com/politica/noticia/2013/10/dilma-diz-que-e-mail-do-governo-tera-protecao-contra-espionagem.html

54 http://info.abril.com.br/noticias/seguranca/2013/07/software-livre-pode-evitar-espionagem-avalia-serpro.shtml

55 http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=40688&sid=10

Governança da internet

No âmbito da governança da internet, o Brasil liderou a crítica ao vigilantismo americano no contexto internacional. Em discurso de abertura na Assembleia Geral da ONU, em setembro de 2013, a Presidente Dilma Rousseff vocalizou a indignação das práticas de vigilância em massa[56]:

"Lutei contra o arbítrio e a censura e não posso deixar de defender de modo intransigente o direito à privacidade dos indivíduos e a soberania de meu país. Sem ele – direito à privacidade – não há verdadeira liberdade de expressão e opinião e, portanto, não há efetiva democracia. Sem respeito à soberania, não há base para o relacionamento entre as nações", disse.

A presidenta propôs a implementação de mecanismos multilaterais capazes de garantir os seguintes princípios: 1. Liberdade de expressão, privacidade do indivíduo e respeito aos direitos humanos; 2. Governança democrática, multilateral e aberta; 3. Universalidade que assegura o desenvolvimento social e humano e a construção de sociedades inclusivas e não discriminatórias; 4. Diversidade cultural, sem imposição de crenças, costumes e valores; e 5. Neutralidade da rede, ao respeitar apenas critérios técnicos e éticos, tornando inadmissível restrição por motivos políticos, comerciais e religiosos.

Com o cenário favorável, o país se mobilizou e passou a articular propostas para incidir no cenário da governança da internet[57]. Em 18 de dezembro de 2013, conseguiu aprovar uma resolução sobre privacidade na Assembleia Geral da ONU[58]. A resolução reafirma a privacidade com direito humano e condena as práticas de espionagem e interceptação de comunicações em escala massiva. Embora o documento aprovado não tenha a força de uma norma, é útil para demonstrar a importância do assunto e é porta de entrada para futuras discussões que possam levar a resoluções de cunho normativo mais forte. Ainda, em fevereiro de 2014, realizou em parceria com outras missões no Seminário sobre o Direito à Privacidade na Era Digital, em Genebra.

Já em março de 2015, foi aprovada pelo Conselho de Direitos Humanos da ONU a criação da Relatoria Especial sobre o Direito à Privacidade[59]. A criação da instituição é uma reação à crescente mobilização contra a vigilância em massa praticada por governos e empresas, além de outras viola-

56 http://blog.planalto.gov.br/na-onu-dilma-propoe-governanca-global-para-internet/

57 As revelações de Snowden trouxeram desafios quanto ao futuro da governança da internet. Vale destacar dois principais: 1.Repensar formas de encriptação para que as comunicações virtuais não sejam tão suscetíveis à interceptação tanto pelo governo norte-americano como por empresas. Os documentos vazados comprovaram que, sem encriptação, não há privacidade da Internet. Ademais, hoje em dia, os meios de encriptação ainda são pouco difundidos. Restringem-se basicamente à comunidade acadêmica e aos ativistas digitais que têm conhecimento da estrutura de poder por trás da Internet há tempos.

2. Descentralizar o pleno poder dos EUA sobre a Internet, a começar pela remoção da ICANN da influência do United States Department of Commerce. A Internet Corporation for Assigned Names and Numbers (ICANN), subordinada aos EUA, é responsável pela distribuição de números de "Protocolo de Internet" (IP), pela designação de identificações de protocolo, pelo controle do sistema de nomes de domínios de primeiro nível com códigos genéricos (gTLD) e de países (ccTLD), além de funções de administração central da rede de servidores. Atualmente, o controle físico da Internet se concentra nos EUA. A subordinação de um órgão de alcance mundial, com responsabilidades e capacidades tão elevadas a um único Estado pode denotar, na realidade, a subordinação do meio virtual. O governo americano já anunciou que pretende descentralizar o controle sobre a ICANN, mas as propostas para isso variam. Alguns defendem a manutenção da estrutura nos EUA, mas com mudanças profundas na gestão, enquanto outros defendem a mudança da estrutura física para outro país, mais neutro, como por exemplo, a Suíça. O grupo de transição inclusive conta com presença de brasileiros, levando em consideração que o país não só sediou o evento NetMundial, bem como assume papel de protagonismo nas discussões de governança da internet nos espaços internacionais. Integram o Grupo de Coordenação Hartmut Glaser (CGI.br, pela Address Supporting Organization - ASO), Demi Getschko (CGI.br, pela Internet Society) e Jandyr Ferreira dos Santos (MRE, pelo Comitê de Assessoramento Governamental, o GAC).

Para saber mais, acesse: https://pressfreedomfoundation.org/encryption-works

http://www.teletime.com.br/28/05/2014/chehade-diz-que-nova-governanca-da-icann-sera-colaborativa-e-descentralizada/tt/379242/news.aspx

58 http://internacional.estadao.com.br/noticias/geral,proposta-brasileira-contra-espionagem-digital-e-aprovada-na-onu,1110227

59 http://oglobo.globo.com/sociedade/tecnologia/onu-indica-relator-especial-para-investigar-espionagem-violacoes-privacidade-digital-15709089

ções à privacidade, que passarão a ser alvo de um monitoramento sistemático e independente. O direito à privacidade era até hoje um dos poucos direitos que ainda não haviam merecido a criação de uma Relatoria Especial na ONU. O mandato do relator é capaz de monitorar as atividades de vigilantismo dos Estados, tarefa que muitas vezes inexiste em nível nacional, mesmo em democracias consideradas bem estabelecidas.

O Brasil também presidiu o Grupo das Nações Unidas de Especialistas Governamentais em Desenvolvimento no Campo das Comunicações e Telecomunicações no Contexto de Segurança Internacional, com participação de representantes de 20 nações. Lançado um relatório de consenso[60], ele traz regras mínimas de comportamento no ciberespaço, especialmente durante tempos de paz.

Além disso, o país foi um dos principais convocadores do NETMundial - Encontro Multissetorial Global Sobre o Futuro da Governança da Internet[61], realizado em abril, na cidade de São Paulo para a elaboração de um documento sobre o futuro da governança da Internet. O documento final cita a necessidade da proteção à privacidade em oposição às práticas de vigilância em massa:

O direito à privacidade deve ser protegido. A isso se inclui a não sujeição à vigilância arbitrária ou ilegal, coleta, tratamento ou uso de dados pessoais. O direito à proteção da lei contra tais interferências deve ser garantido.

Procedimentos, práticas e legislação a respeito de vigilância das comunicações, suas interceptações e coletas de dados pessoais, incluindo vigilância em massa, interceptação e coleta, devem ser revisados. Isso deve se dar através de um viés que apoie o direito à privacidade por meio da garantia e implementação efetiva de todas as obrigações sujeitas às leis internacionais dos direitos humanos (NETMundial Multistakeholder Document, pg. 4, tradução nossa).

O evento também teve grande importância considerando-se processos de reformulação da governança da internet por meio da possível adoção do modelo multissetorial. A maior consequência até 2016 foi a concordância da diretoria da ICANN de que o compromisso de respeitar os direitos humanos deve fazer parte de estatutos da organização, além da promoção de avanços e melhorias na accountability de sua atuação[62].

No âmbito do Mercosul, a regulamentação da internet com ênfase nos aspectos de segurança cibernética começou a ser discutida em julho de 2013 com a aprovação da "Decisão sobre o Repúdio à Espionagem por parte dos Estados Unidos da América nos Países da Região"[63]. Em agosto de 2013, representantes do bloco reuniram-se com o Secretário Geral da ONU, Ban Ki-moon, para expressar a insatisfação e a preocupação com relação às práticas de vigilantismo[64]. Duas novas reuniões em setembro e novembro, na Venezuela, reafirmaram o posicionamento do bloco e houve a renovação do comprometimento a fim de criar uma instância permanente para tratar de assuntos relacionados à segurança na internet e telecomunicações[65].

---

60 http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174

61 http://netmundial.br/pt/

62 https://www.article19.org/resources.php/resource/38249/en/icann-board-ag

63 Veja a resolução completa: http://www.mercosur.int/innovaportal/file/4677/1/decisao_espionagem_pt.pdf

64 http://www.bbc.co.uk/portuguese/noticias/2013/08/130730_patriota_eua_mdb_pu.shtml

65 Veja os resultados da Reunião de Autoridades e Experts em Segurança Informática e das Telecomunicações do MERCOSUL: http://www.recyt.mincyt.gov.ar/files/ActasComisionSocinfo/Acta2013_02/Anexo_V_Resultados_Reunion_de_Autoridades.pdf

Veja Comunicado Conjunto: http://goo.gl/0irP0p

Mais especificamente na UNASUL, em setembro de 2013, o Ministro da Defesa, Celso Amorim, já aventava e reafirmava a possibilidade e a vontade do governo brasileiro em formar uma Comissão de Assessoria Militar, que tivesse como prioridade justamente o fortalecimento do sistema de proteção de defesa cibernética[66]. Em fevereiro de 2014, o projeto para a criação da Escola Sul-Americana de Defesa (Esude) foi aprovado na organização internacional. A ideia extrapola o tema da segurança cibernética, mas também o trata de forma prioritária, sendo que a primeira atividade do plano de ação da UNASUL (item 1a) no ano de 2014 é a realização de um Seminário Internacional de Defesa Cibernética com o objetivo de gerar capacidades para enfrentar desafios impostos por ameaças cibernéticas e informáticas no campo da defesa. Além disso, o Plano de Ação, no item 3b, deseja manter o Grupo de trabalho constituído por especialistas com o propósito de apresentar o projeto, o desenvolvimento e a produção de um sistema regional de aeronaves não tripuladas, chamado VANT REGIONAL[67].

Entretanto, a articulação até o momento mais concreta foi com a vizinha Argentina, na ocasião da visita do Ministro da Defesa deste país ao Brasil também em novembro de 2013, quando uma agenda bilateral de cooperação no âmbito da defesa cibernética foi iniciada. Da reunião, saiu o acordo de que militares argentinos viriam ao Brasil no ano de 2014 para participarem de curso sobre o tema junto com seus pares brasileiros. Em março, outro encontro entre autoridades da defesa brasileiras e argentinas tratou da institucionalização do Subgrupo de Cooperação de Defesa Cibernética (SCDC) e o Subgrupo de Cooperação Aeroespacial (SCAe).

Para além da articulação regional, as declarações resultantes das reuniões de cúpula do BRICS[68] recorrentemente estão afirmando que existe uma preocupação destes países como uso da internet e TICs para fins de crime organizado transnacional, desenvolvimento de instrumentos ofensivos e realização de atos de terrorismo, tal como ocorreu com os documentos de Fortaleza e de Ufá. Concretamente, houve a criação de um grupo de trabalho para tratar de questões como o compartilhamento de informações, coordenação contra cibercrimes e projetos de desenvolvimento e pesquisa na área. Especificamente a Rússia está ampliando a cooperação militar com o Brasil. Fora os outros tipos de intercâmbio de tecnologias militares também envolvidos nos acordos, os dois países estabeleceram em outubro de 2013 a criação de um grupo de trabalho para tratar de questões de Defesa Cibernética, identificado como um problema que tem de ser estudado dados os potenciais riscos.[69]

Internamente, o governo acelerou a tramitação do Marco Civil da Internet, que estava sob análise da Câmara de Deputados desde 2011[70]. O texto aprovado traz garantias importantes ao direito à privacidade. Ele está protegido, por exemplo, pela condicionalidade do acesso à informação de comunicações de terceiros, que só poderá ser dar via ordem judicial. O artigo 7 dispõe de questões importantes sobre dados pessoais, proibindo a coleta de dados sem autorização prévia do usuário e o seu compartilhamento com terceiros sem prévio aval. Também está previsto um mecanismo de exclusão de dados de usuários que optarem por não utilizar mais determinado aplicativo. Além disso,

66 http://politica.estadao.com.br/noticias/geral,unasul-precisa-fortalecer-defesa-cibernetica-diz-amorim,1074415

67 Link para o Plano de Ação: http://www.ceedcds.org.ar/Portugues/09-Downloads/Port-PA/PORT-Plan-de-Accion-2014.pdf

68 BRICS é um acrônimo que se refere aos países (o grupo BRICS: Brasil, Rússia, Índia, China e África do Sul), que juntos formam um grupo político de cooperação.

69 http://www.brasil.gov.br/defesa-e-seguranca/2013/10/brasil-e-russia-decidem-ampliar-cooperacao-em-defesa

70 Ele foi formulado a partir de um grande processo colaborativo na internet iniciado em 2009 pela Secretária de Assuntos Legislativos do Ministério da Justiça em parceria com a Fundação Getúlio Vargas. Mais de duas mil sugestões de vários setores da sociedade foram recebidas e debatidas na constituição do texto da lei. No Congresso Nacional, ele passou por novas rodadas de consultas online e audiências públicas. O amplo processo participativo foi fundamental para que a sociedade civil organizada tivesse legitimidade para apoiar a resistência a certas negociações típicas do Congresso Nacional brasileiro.

o documento final assegura outros pontos importantes, como o respeito à liberdade de expressão online, a neutralidade de rede, a não responsabilização de provedores por conteúdos e a obrigação de criação de uma agenda que garantam a discussão progressiva do uso e desenvolvimento da rede.

Outra consequência das denúncias foi o fortalecimento da legitimidade do CGI.br - Comitê Gestor da Internet no Brasil perante o governo especialmente pelo seu caráter multissetorial. O CGI.br foi criado com a atribuição de estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil e diretrizes para a execução do registro de Nomes de Domínio, alocação de Endereço IP (Internet Protocol) e administração pertinente ao domínio ".br". Também promove estudos e recomenda procedimentos para a segurança da Internet e propõe programas de pesquisa e desenvolvimento que permitam a manutenção do nível de qualidade técnica e inovação no uso da Internet. Ainda, busca promover a qualidade técnica, a inovação e a disseminação dos serviços ofertados, além de iniciativas importantes, como o Fórum da Internet no Brasil, para a disseminação de conhecimento sobre as redes. Possui em seus quadros nove representantes do governo federal, quatro do setor empresarial, quatro do terceiro setor, três da comunidade científica e tecnológica e um representante de notório saber em assuntos de internet.

Com o avanço das discussões sobre privacidade na internet após as denúncias de Snowden, não só a população começou a se atentar mais com relação às violações que ocorrem no Brasil, principalmente com vazamentos de dados pessoais. Foi unânime nas análises pós-aprovação do Marco Civil que o Brasil ainda precisava criar um marco legal para a maneira com que os dados pessoais dos usuários de internet, mas também fora dela, são utilizados[71].

Os debates sobre a legislação de proteção a dados pessoais no Brasil tiveram início já em 2010, quando o Ministério da Justiça realizou um debate público via uma plataforma na internet. Em janeiro de 2015, atento às demandas da sociedade, o Ministério da Justiça lançou um novo debate público, já que a proposição por parte do Executivo de um marco legal para o tema vinha se arrastando há anos. No entanto, até hoje o processo não foi finalizado, apesar de ter sido apresentado pelo Ministério da Justiça e enviado para a Casa Civil. Após os trâmites internos do governo, o projeto deverá ser apresentado ao Congresso. Quando aprovada, a lei poderá finalmente coibir abusos daqueles que utilizam dados pessoais inadequadamente.

Defesa cibernética

As iniciativas de defesa cibernética brasileira antecederam as denúncias de Edward Snowden. Após o estabelecimento do USCYBERCOM, o comando militar de defesa cibernética dos Estados Unidos, os militares brasileiros se viram numa situação que precisavam se atualizar em relação ao contexto internacional e passaram a incorporar a doutrina de cibersegurança. Inicialmente, em 2010, foi criado o Núcleo do Centro de Defesa Cibernética (NuCDCiber) no Exército para coordenar e executar um projeto de estrutura sobre a área cibernética, o desenvolvimento de um Centro de Defesa Cibernética, planejar e executar a segurança cibernética, coordenar a Rede Nacional de Segurança da Informação e Criptografia, entre outras responsabilidades. Essas atividades foram alocadas para diferentes órgãos dentro do Exército como o Centro de Comunicações e Guerra Eletrônica do Exército Brasileiro (CCOMGEX), Centro Integrado de Telemática do Exército (CITEX) e o Centro de Defesa Cibernética. Em novembro de 2012, foi fundado o Centro de Defesa Cibernética (CDCiber), vinculado ao Ministério da Defesa (MD). Isso implicou na alteração a estrutura regimental da Marinha, Exército e Aeronáutica (Decreto nº 7.809) e, posteriormente, atribir a responsabilidade pela

71 http://tecnologia.uol.com.br/noticias/redacao/2015/05/11/apesar-de-pioneirismo-com-marco-civil-brasil-peca-na-protecao-de-dados.htm

coordenação e integração da defesa cibernética junto ao MD (Portaria nº 3.028). Resumidamente, o CDCiber é criado para o país realizar ações ofensivas, defensivas e exploratórias, isto é, de ataques online até mitigar ações de sabotagens e espionagem.

Após as revelações de Snowden, de maneira imediata, houve algumas reestruturações e investimentos no CDCiber foram anunciados, como o aumento do corpo de oficiais e compra de equipamentos[72]. O centro recebeu R$ 400 milhões até 2015 para investimentos em seus projetos[73]. Além disso, houve a criação de uma Escola Nacional de Defesa Cibernética[74]. O projeto entrou em vigor em 2015 como o Instituto de Defesa Cibernética (IDCIBER), vinculado à UnB[75]. Também, houve a implementação do Núcleo da Escola Nacional de Defesa Cibernética (NuENaDCiber), dentro do Comando Militar do Planalto (CMP). O primeiro teve como objetivo a criação dos cursos de ensino a distância (EAD), que buscam desvincular o papel de capacitar recursos humanos para a atuação de defesa cibernética no país, deixando o CDCiber com a única prerrogativa de atuar em operações de guerra cibernética. Segundo o próprio IDCIBER em sua página menciona, "desde sua concepção, tem como responsabilidade contemplar também, o acesso à Lista de Discussão e à Ferramenta de Cooperação (Twiki) da Rede Nacional de Excelência em Segurança da Informação e Criptografia (RENASIC) e às bibliotecas digitais de interesse das Forças Armadas".

No mesmo período, em julho de 2015, em conjunto com o Núcleo da Escola Nacional de Defesa Cibernética (NuENaDCiber), foi criado o Núcleo do Comando de Defesa Cibernética (NuComDCiber) também dentro do CMP, ambos com instalações provisórias.

A Escola, após a construção de suas instalações, deverá começar a contar com atividades presenciais. O NuComDCiber é também subordinado ao CDCiber e conta com o exercício de militares das três Forças: Exército, Marinha e Aeronáutica. Tem como objetivo integrar atividades para operações conjuntas com o objetivo de controle operacional.

Veja abaixo todos os projetos que estão sendo desenvolvidos nessa área, com os respectivos responsáveis:

Projeto	Responsabilidade
Organização do Centro de Defesa Cibernética	CDCiber
Planejamento e Execução da Segurança Cibernética (Escudo Cibernético)	CITEx
Estrutura de Apoio Tecnológico e Desenvolvimento de Sistemas	CDS
Estrutura de Pesquisa Científica na Área Cibernética	IME

72 http://politica.estadao.com.br/noticias/geral,exercito-se-arma-para-defender-o-espaco-cibernetico-brasileiro,729291

73 Fonte: https://medium.com/brasil/por-dentro-do-cdciber-o-centro-de-defesa-cibernetica-do-exercito-brasileiro-40ce637d119

74 Fonte: http://www.brasil.gov.br/defesa-e-seguranca/2014/02/brasil-tera-escola-nacional-de-defesa-cibernetica

75 Fonte: http://www.idciber-eb.unb.br/

Estrutura de Capacitação e de Preparo e Emprego (Força Cibernética)	CCOMGEX
Arcabouço Documental	CDCiber
Estrutura para Produção do Conhecimento Oriundo da Fonte Cibernética	CIE
Gestão Pessoal	CDCiber
Rede Nacional da Segurança da Informação e Criptografia (RENASIC)	CDCiber
Rádio Definido por Software (RDS)	CTEx

Fonte:http://www.defesa.gov.br/arquivos/ensino_e_pesquisa/defesa_academia/cedn/viii_cedn/cibercidviiicedn.pdf

A mesma portaria que criou os núcleos supracitados[76], citada na Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal[77], ainda revela que existe "ênfase na implantação e a consolidação do Sistema de Homologação e Certificação de Produtos de Defesa Cibernética, o apoio à pesquisa e ao desenvolvimento de produtos de defesa cibernética, bem como a criação do Observatório de Defesa Cibernética".

Tal documento ainda revela que a Segurança da Informação e Comunicações (SIC) e a Segurança Cibernética (SegCiber) são a base da Defesa Cibernética, objetivando impedir ações contra os interesses do país e da sociedade. Tais ações buscam resultar em "benefícios para a sociedade, tais como proteção da privacidade, transparência, democratização do acesso a informação e salvaguarda dos ativos de informação sigilosos."

Uma das metas é interessante para resumir o objetivo do documento de estratégia e, portanto, o caminho e o foco do governo brasileiro com relação à defesa cibernética:

> "É essencial avançar na articulação para o fortalecimento e aceleração da implantação do ecossistema digital (SIC+SegCiber+Empresas+ICT) com a finalidade de apoiar o desenvolvimento de tecnologias de SIC e de SegCiber, a exemplo de soluções de reconhecimento de artefatos maliciosos e outras ferramentas cibernéticas, alavancando a criação do mesmo e promovendo maior sinergia com o ecossistema da defesa cibernética. Para tanto, faz-se necessário aprimorar os mecanismos de fomento e de financiamento que favoreçam parcerias entre o setor privado e as universidades e institutos de pesquisa, para o desenvolvimento e a produção de soluções de SIC e de SegCiber."

Ainda é importante ressaltar que o comando de tais operações é de responsabilidade do "órgão central", que no caso é o GSI atualmente vinculado Casa Militar, com assessoramento de um Comitê Gestor de Segurança da Informação (CGSI) e colaboração dos órgão competentes específicos.

76 Portaria Normativa MD 2.777, de 27 de outubro de 2014, disponível em http://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=28/10/2014&jornal=1&pagina=7&totalArquivos=56

77 http://dsic.planalto.gov.br/documentos/publicacoes/4_Estrategia_de_SIC.pdf

Entretanto, o esforço de integrar atividades e atuar mais no ambiente da rede já é conhecido desde julho de 2013, quando em reportagem amplamente divulgada pela imprensa, o general José Carlos dos Santos, oficial do Exército à frente do CDCiber, revelou que o Centro estava realizando acordos com os Ministérios da Justiça e da Defesa com o objetivo "de coordenar e integrar os esforços da segurança cibernética desses grandes eventos", através do monitoramento de fontes abertas, como as redes sociais. Tal ação coordenada seria apenas uma "atribuição temporária", aparentemente visando grandes eventos, como foi o caso da Copa do Mundo, em 2014, e da visita do Papa, em 2013[78].

No contexto da Copa do Mundo, a ARTIGO 19 enviou pedidos de informação ao exército, mencionando a reportagem e solicitando mais informações sobre o monitoramento das redes sociais, bem como a utilização do Sistema Guardião, a ferramenta de investigação que realiza monitoramento de dados e gravações de voz, para análise de autoridades com poder de polícia[79]. Em resposta aos pedidos, o Exército não se manifestou a respeito do monitoramento online durante a Copa e ainda negou a utilização do Sistema Guardião[80], apesar da existência da notícia e da declaração do próprio general do Exército.

A partir das poucas informações obtidas, a seguir, apresentaremos a seguir um panorama de como da segurança cibernética brasileira está estruturada para além do âmbito do Exército, chegando no âmbito de competência do Ministério da Justiça que refere-se às agências de aplicação da lei, como o Ministério Público e as Polícias.

O caso das rondas virtuais

Esse contexto associado à realização de megaeventos, como a Copa do Mundo de Futebol e as Olimpíadas, ensejou a compra de diversos equipamentos e softwares para garantir a segurança dos eventos[81]. Pouco se sabe se estas tecnologias estão sendo utilizadas com propósitos específicos e salvaguardas com respeito aos direitos humanos fundamentais dos cidadãos. Tampouco há informação suficiente disponível sobre a finalidade ou o grau de proteção dos bancos de dados que são criados pelo uso das mesmas.

Diversas matérias jornalísticas[82] sugerem que, para além da segurança pública, tais equipamentos e serviços de inteligência estão sendo utilizados, por exemplo, para vigilância na rede de movimentos sociais a fim de se evitar protestos como os que existiram no país em 2013 – em grave violação ao direito humano de liberdade de expressão e liberdade de manifestação. Indícios apontam que, apesar de o governo brasileiro ter começado a sofrer com o vigilantismo estatal de outros Estados, suas práticas internas tem o mesmo fim – influenciar em fatores políticos e econômicos.

Durante os protestos em resposta à realização da Copa do Mundo no Brasil, em 2013 e 2014, diversos foram os critérios que os policiais usaram para definir quais seriam os sujeitos alvo de suas

78 Fonte: http://g1.globo.com/tecnologia/noticia/2013/07/exercito-monitorara-redes-sociais-durante-visita-do-papa-e-copa-de-2014.htm

79 http://www.digitro.com/pt/index.php/component/content/article/89Itemid=1

80 http://www.artigo19.org/centro/esferas/detail/657

81 http://apublica.org/2013/09/copa-brasil-vira-mercado-prioritario-da-vigilancia/

82 http://sao-paulo.estadao.com.br/noticias/geral,abin-monta-rede-para monitorarinternet,1044500http://brasil.estadao.com.br/noticias/geral,exercito-brasileiro-cria-orgao-para-monitorar-manifestacoes,1536422

investigações no contexto destas grandes manifestações públicas ocorridas no período.

O inquérito policial que levou a prisão ou perseguição de mais de 20 manifestantes no Rio de Janeiro, por exemplo, revela que grande parte da investigação foi feita através do monitoramento de redes sociais e que os argumentos oferecidos para apresentar uma pessoa como suspeita eram baseados, muitas vezes, em comentários, fotos, tags e redes de amizade do Facebook[83].

As denúncias e as intimações feitas no âmbito do inquérito, eram respaldadas por informações coletadas nas chamadas "Rondas Virtuais"[84], em que a polícia fazia uma varredura e analisava não só os perfis pessoais das pessoas consideradas suspeitas, mas também de parentes, amigos e amigas, ou meros contatos do Facebook que se ligavam a elas a partir de comentários, curtidas, ou marcações feitas em posts e fotos relacionadas aos temas das manifestações.

Tais práticas denunciam como as polícias civis costumam agir em investigações desse tipo. A informação reunida foi proveniente de perfis públicos e com baixo nível de privacidade e que teriam facilitado a busca dos policiais.

De acordo com o inquérito é impossível determinar se o método utilizado foi apenas esse ou se também fez-se uso de perfis falsos, com solicitações de amizade a usuários investigados para analisar informações não públicas, prática que, inclusive, já foi publicamente combatida pelo Facebook [85].

Além do monitoramento de dados disponíveis nas redes sociais, houve, na mesma investigação, dezenas de pedidos de grampos telefônicos prontamente atendidos pelos juízes e pelas operadoras de telefonia. Também graves foram os pedidos de quebra de sigilo de dados cadastrais de ao menos 46 perfis, 1 grupo e 3 páginas do Facebook, nos seguintes termos: "(...) dados cadastrais contendo Logs de criação e acesso, com data, hora e referência horária, IP, e-mail principal e secundário, telefones de confirmação, bem como demais informações constantes no banco de dados (cartões de crédito, se o perfil administra alguma página etc) (…)" que tinham como objetivo identificar possíveis ligações com partidos políticos, principalmente no financiamento das ações políticas e dos materiais utilizados.

Também foram identificados pedidos de quebra de sigilo telemático das comunicações feitas por mensagens privadas no Facebook incluindo dados como "texto, imagens, arquivos de áudio, localização etc", registrados a partir de março de 2013 até a "data de deferimento da medida". Não foi possível, porém, saber se tais pedidos foram atendidos pelas empresas que atuam na internet.

---

83 A Agência Pública teve acesso ao inquérito e ressaltou esses aspectos nesta reportagem: http://apublica.org/2015/05/um-preso-politico-no-brasil-democratico/

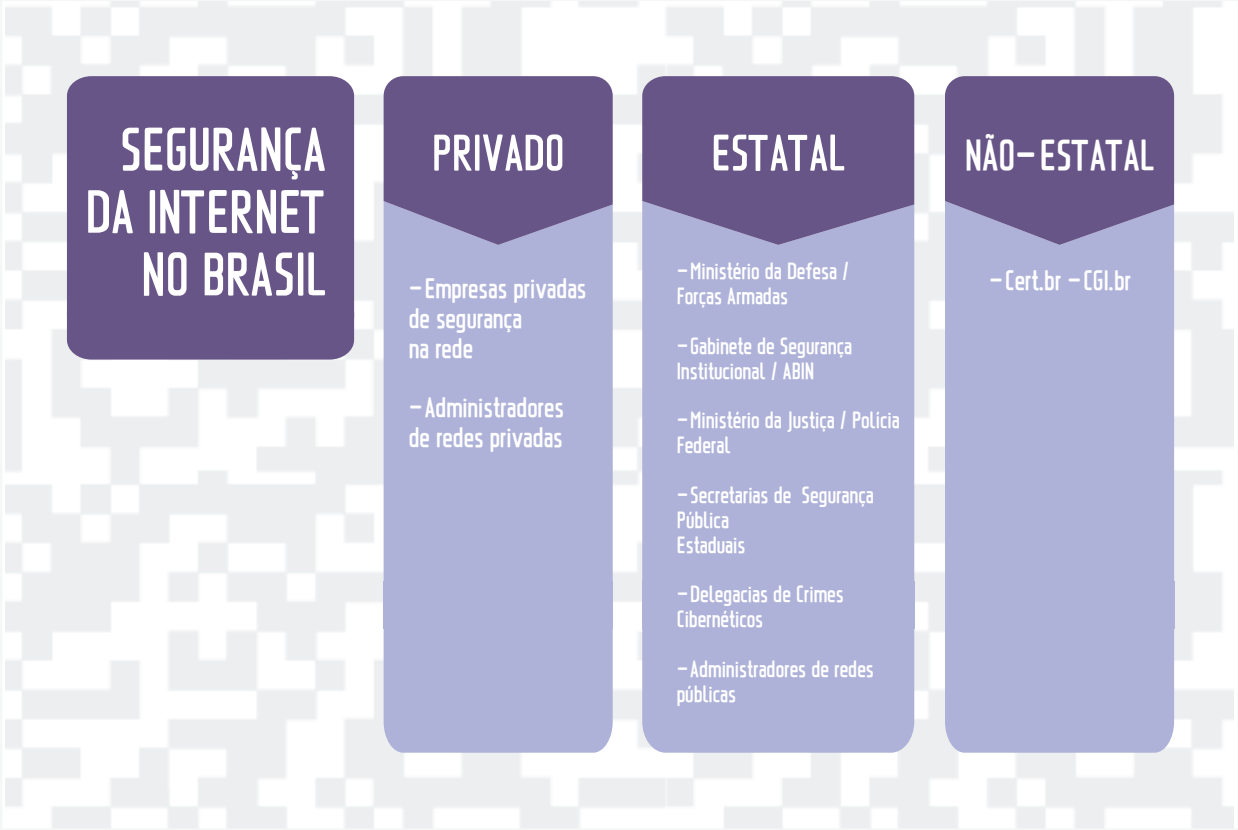
84 "Ronda Virtual"é basicamente o trabalho manual de checar perfis de pessoas que estão associadas a páginas que apoiavam os protestos e eventualmente faziam apologia à depredação de patrimônio, contra policiais, etc. A prática já foi apresentada em outros casos em que a polícia se manifestou (e.g. http://oglobo.globo.com/sociedade/oab-rj-aciona-ministerio-publico-estadual-policia-civil-para-investigar-paginas-consideradas-racistas-13953005)

85 http://www.huffingtonpost.com/james-parsons/facebooks-war-continues-against-fake-profiles-and-bots_b_6914282.html

_PANORAMA DA SEGURANÇA CIBERNÉTICA BRASILEIRA

PANORAMA DA SEGURANÇA CIBERNÉTICA BRASILEIRA

A política de segurança cibernética no Brasil tem suas funções compartilhadas entre alguns órgãos estatais e não-estatais. Os principais órgãos do governo federal que têm atuado na segurança das redes são: CDCiber, Polícia Federal e ABIN. Em âmbito estadual, são recorrentes relatos de monitoramentos de diversos tipos da rede por Secretarias de Segurança Pública Estaduais, Delegacias de Crimes Cibernéticos e Polícia Civil (Veja anexo as descrições das instituições e seus papeis). Para além dos órgãos estatais, existem atores não-estatais que vigiam a rede com o declarado objetivo de proteção à segurança. Vão desde empresas privadas de serviços de segurança online até administradores de redes. Entre os atores não-estatais destaca-se a atuação do CERT.br, vinculado ao Comitê Gestor da Internet no Brasil – CGI.br.

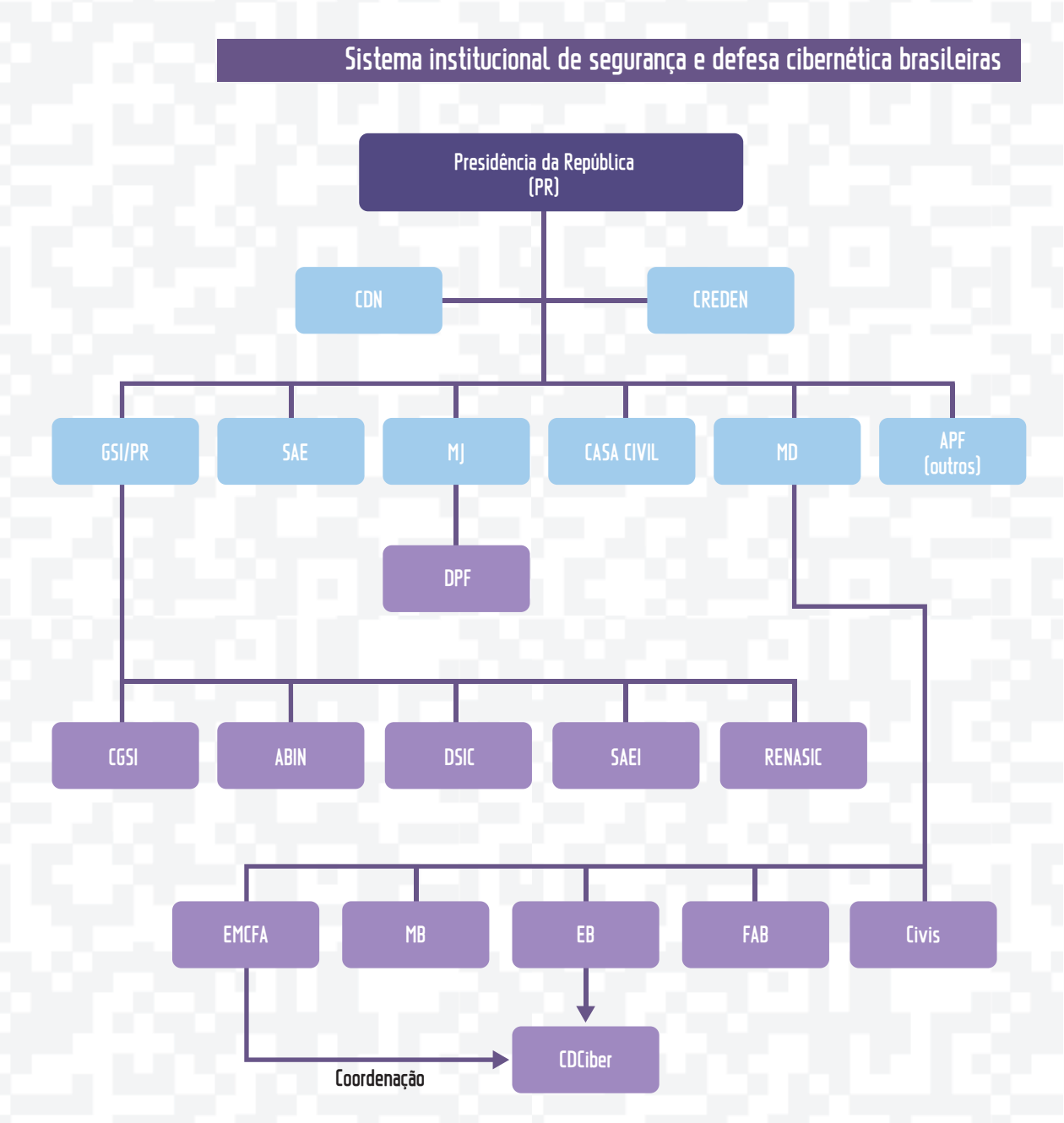


Fonte: http://www.ipea.gov.br/agencia/images/stories/PDFs/TDs/td_1850.pdf

A função de prevenção quanto a de repressão de potenciais ataques através da rede é responsabilidade do Gabinete de Segurança Institucional da Presidência da República (GSI), recentemente incorporado à Secretaria de Governo, e seus órgãos vinculados como a ABIN. Já as ações operacionais de combates ofensivos ficam a cargo do Ministério da Defesa, mais especificamente do Exército, com o CDCiber. A Polícia Federal também tem um papel importante na área criminal.

Para exercer suas funções, os órgãos estatais brasileiros adotaram práticas de vigilância na rede. Um dos sistemas de monitoramento da Internet mais usados pelos órgãos brasileiros é o OSINT - Open Source Intelligence, que é a coleta e processamento de dados que estão disponíveis de forma aberta. A ABIN, por exemplo, admite o uso para coleta e reunião de dados inclusive em seu site institucional[86]. A inteligência obtida por fontes abertas incluem vários provedores diferentes de informação, como a mídia tradicional, redes sociais, blogs, sites de compartilhamento de vídeo,

86 http://www.abin.gov.br/modules/mastop_publish/?tac=Fontes_abertas_e_Intelig%EAncia_de_Estado



observação de imagens de satélite e afins, trabalhos acadêmicos, etc. Este é um dos métodos de monitoramento utilizados pelos órgãos de segurança de todo o mundo, tendo sido melhor apresentado para agentes de segurança brasileiros no período que antecedeu a Copa do Mundo[87].

Ameaças e níveis de segurança no Brasil: avanços e retrocessos

Os ataques cibernéticos ocorrem em pelo menos três âmbitos e correspondem a diferentes tipos de reações, soluções e respostas. Partimos de uma situação em que os indivíduos tinham que se conscientizar ao usar sistemas informatizados e adotar medidas de cibersegurança. Passamos por um debate público forte sobre cibercrimes, com ampla resistência por parte de organizações da sociedade civil (debate que sempre volta à tona) contra práticas de vigilantismo. Agora, estamos em um estágio em que falamos de ciberguerra de maneira totalmente obscura, sem acesso mínimo

87 http://www.defesanet.com.br/eventos/noticia/14147/Especialista-em-seguranca-recomenda-para-a-Copa-do-Mundo--%E2%80%9CPrever-para-prover%E2%80%9D/

a informações por parte das autoridades públicas. Evoluímos do debate da cibersegurança para a ciberguerra. Ou seja, há uma tendência de militarização de um problema que deveria permanecer a ser enfrentado prioritariamente na esfera civil. Veja abaixo como estão organizadas ações em cada um desses âmbitos no Brasil.

Segurança da rede

No Brasil, quem trata das questões relacionadas a incidentes de segurança em âmbito nacional é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil - CERT.br. O centro tem como objetivo detectar e reunir estatísticas sobre ataques e incidentes de segurança na internet ocorridas no Brasil. Além disso, também tem a responsabilidade de dar visibilidade e disseminar conteúdo, inclusive educativo, sobre as questões de segurança na internet a partir da análise dos dados estatísticos públicas recolhidas e da correlação com os incidentes de segurança no Brasil, como por exemplo o ataque de malwares e vírus de computador diversos.

As atividades do CERT.br ainda envolvem desde suporte aos processos de recuperação e análise de ataques e de sistemas comprometidos, a articulação entre os setores variados da internet do Brasil para estabelecer boas práticas e cooperação de segurança. Ademais, o órgão atua diretamente na cibersegurança da rede brasileira, já que precisa detectar a ocorrência de ataques e incidentes no Brasil através da distribuição de uma rede de honeypots, ou iscas, para atrair ataques dos mais diversos.

Na área de educação, o CERT.br possui cartilhas temáticas[88]que envolvem os diversos assuntos relacionados à segurança da internet. A Cartilha de Segurança para Internet contém recomendações e dicas sobre como um usuário comum pode otimizar a segurança durante a navegação. São 14 temas divididos em capítulos: 1. segurança na internet; 2. golpes na internet; 3. ataques na internet; 4. códigos maliciosos (malware); 5. spam; 6. outros riscos; 7. mecanismos de segurança; 8. contas e senhas; 9. criptografia; 10. uso seguro da internet; 11. privacidade; 12. segurança de computadores; 13. segurança de redes; e 14. segurança de dispositivos móveis.

Anos atrás, o Brasil figurava entre os países que mais recebiam e-mails maliciosos do mundo. Em busca de soluções para o problema, depois de sete anos de negociação com operadoras, provedores Internet, Minicom, Anatel e Ministério da Justiça, o Comitê Gestor da Internet anunciou em 2013 que as teles iriam fechar o acesso dos usuários residenciais banda larga fixa e 3G à porta 25, que é muito utilizada para o disparo de mensagens indesejadas.[89] Após a implementação, o país rapidamente saiu do ranking dos 10 países mais sujeitos a envio de spam[90]. Entretanto, o mesmo não pode ser aplicado ao número de incidentes (ataques) reportados ao CERT.br no ano de 2014.

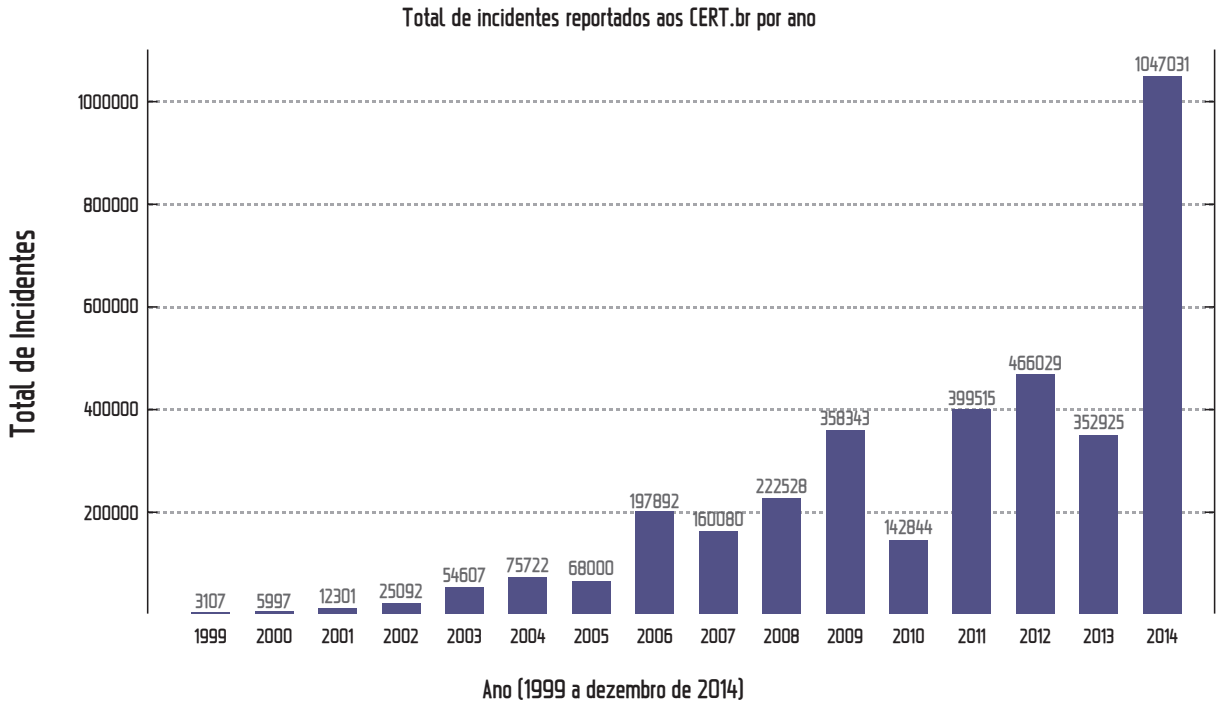
A tabela abaixo revela como aumentou o número de ataques reportados. Dentre esses ataques, destacam-se as fraudes e tentativas de fraude, os scans, varreduras para identificação de computadores ativos e, portanto, potenciais alvos, e os DoS, ataques de negação que tem como objetivo derrubar um serviço, um computador ou uma rede[91].

88 http://cartilha.cert.br/

89 http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=32179&sid=4

90 https://tecnoblog.net/127232/brasil-ranking-spam/

91 http://www.cert.br/stats/incidentes/2014-jan-dec/tipos-ataque-acumulado.html



Fonte: http://www.cert.br/stats/incidentes/

Tal constatação ensejou o debate de crimes praticados na internet, como fraudes, invasões e derrubadas de redes. Notou-se a necessidade de trazer soluções para o problema. Então, partiu-se de um cenário em que os indivíduos tinham que se conscientizar ao usar sistemas informatizados, relacionada diretamente à noção de segurança cibernética, promovida pelo CERT.br, e passou-se a um debate público forte sobre cibercrimes.

Cibercrimes

Para a questão de cibercrimes, o Brasil já possui Leis específicas. Uma delas entrou em debate quando apresentada em 1999, a Lei 12735 conhecida como Lei Azeredo, alvo de inúmeras controvérsias e discussões na Câmara e sancionada com apenas dois artigos dos quatro que resistiram. A outra é a Lei 12737, que ficou conhecida como Lei Carolina Dieckmann, sancionada sem vetos. Ambas foram publicadas no Diário Oficial da União em dezembro de 2012, automaticamente passando a figurar no Código Penal brasileiro como nossas primeiras legislações de combate a crimes na internet[92].

Com a justificativa de combater os crimes na rede, começou-se um movimento de enquadrar crimes na internet, como os de discurso de ódio, como cibercrimes. O que difere bastante do uso de ferramentas específicas para invasão e realização de fraudes dentro da rede. Tal discurso contaminou o debate no Brasil a ponto de culminar numa crescente tentativa legislativa de ligar os dois fatores e criar novas leis para punir "crimes na internet", sempre com a justificativa do anonimato e do aumento de casos.

Os exemplos começaram há muito tempo, quando o Orkut foi a primeira rede social a se popularizar no Brasil. Criado em 2004 e desenvolvido pelo Google, inicialmente como um produto "beta"

92 As leis estabelecem penas e multas para questões como violação de mecanismos de segurança de equipamentos de informática para obtenção de segredos comerciais, industriais e conteúdo privado, além de controle remoto não autorizado de dispositivo invadido. A pena é aumentada em caso de divulgação, comercialização ou transmissão dos dados obtidos. Além disso, para prevenir danos a usuários de computador e outros dispositivos, também serão punidos aqueles que produzirem, venderem ou difundirem programas que são destinados a invasão de computadores, com agravante de pena nos casos de prejuízos econômicos ou danos contra autoridades públicas.

e com o conteúdo acessível apenas para os membros participantes, os quais precisavam ser convidados para ingressar na plataforma. Ano após ano o número de usuários brasileiros no Orkut foi crescendo até conquistar mais de 50% do tráfego do site. Mas, desde 2005, a Polícia Federal e o Ministério Público Federal passaram a realizar diversas ações, inclusive ameaçando fechar o serviço no Brasil, para obrigar a empresa a ceder os dados de contas e comunidades que estariam cometendo crimes de ódio e pedofilia.

Em resposta, por conta dos dados serem hospedados nos servidores do Google nos Estados Unidos e, então, estarem sujeitos as leis daquele país, o presidente do Google Brasil afirmou que não poderia ceder mais informações. Essa disputa levou cerca de dois anos, após muita pressão política e jurídica, como a CPI da Pedofilia, em que por fim o Google assinou um Termo de Ajustamento de Conduta (TAC) com o Ministério Público Federal[93], e, entre outras coisas, concedeu acesso especial para a Polícia Federal na plataforma.

A negação dos pedidos em alguns casos e a cooperação noutros, tem criado uma série de atritos principalmente com a polícia judiciária brasileira. Em fevereiro de 2015, o deputado Sibá Machado protocolou na Câmara dos Deputados, o pedido de abertura de uma CPI para apurar: a operação IB2K (2014) da Polícia Federal, os índices do relatório da Central Nacional de Denúncias de Crimes Cibernéticos (2013/2014), além das perdas no país por crimes cibernéticos e o vazamento de fotos íntimas[94]. Assim foi aprovada pelo presidente da Câmara, Eduardo Cunha, a CPI dos Cibercrimes[95] em julho.

Uma das preocupações na época da sua criação era de que a CPI passasse a investigar a chamada "guerrilha do PT na internet" a respeito da campanha eleitoral em 2014. Na 23º reunião da CPI, passou a convocar figuras públicas do debate político online, com representantes do Movimento Brasil Livre (MBL), perfil Dilma Bolada, entre outros. Embora a conclusão dessa CPI esteja além deste relatório, é importante destacar como o conceito de cibercrimes, por sua própria indefinição, transformou-se num embate político eleitoral entre oposição e governo para apurar a origem de pagamentos para blogueiros, perfis e páginas em redes sociais. Nota-se, portanto, mais uma adição à noção dos cibercrimes.

Denota-se, então, que para o senso comum qualquer crime que aconteça com o advento da internet é um cibercrime. Porém é extremamente perigoso ir por esse caminho já que as ferramentas, tanto cibernéticas quanto jurídicas, para tratar desses problemas são diferentes. Enquanto os cibercrimes de fato apenas ocorrem por causa da existência da internet e de sistemas automatizados, os crimes de discurso de ódio e outros tipos de crimes (como estelionato) apenas usam a internet como plataforma, já são ilícitos tipificados em nossas leis.

O debate de que alguma vigilância seria necessária para combater crimes na internet sempre teve ampla resistência no Brasil por parte de organizações da sociedade civil. O problema é ainda maior quando começa a surgir discursos que evocam o militarismo para lidar com problemas de esfera civil e privada, já que a ideia de que proteger todo um país, inclusive cidadãos e empresas, começa a ser relacionada a soberania nacional, com o objetivo de garantir a "prosperidade" da nação[96].

---

93 TAC MPF e Google: http://www.prsp.mpf.mp.br/prdc/prdc/prdc-informa/informativo-no8/acordo-poe-fim-a-disputa-judicial--entre-mpf-e-google

94 http://gizmodo.uol.com.br/o-que-sera-cpi-dos-crimes-ciberneticos/

95 http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/

96 http://www.dw.com/pt/pol%C3%ADticas-de-defesa-priorizam-cada-vez-mais-seguran%C3%A7a-cibern%C3%A9tica/a-5756123

Segurança Ofensiva[97]

As implementações técnicas de padrões de segurança refletiu na capacidade dos peritos forenses brasileiros. Na 12º reunião da CPI dos Cibercrimes[98], realizada em setembro de 2015, representantes do Instituto Nacional de Criminalística, da Associação Brasileira de Criminalística e da Polícia Federal abordaram as dificuldades que estavam tendo para obter provas através da quebra do sigilo das comunicações como, por exemplo, do aplicativo WhatsApp:

"Eles promovem um software que, quando instalado no seu aparelho — e vamos supor que o senhor vai mandar uma mensagem para o Deputado Jean — , a mensagem sai criptografada do seu celular, passa pelo servidor da empresa, criptografado a 128 bits, a 256 bits, e só o Deputado Jean, com a chave dele, vai conseguir abrir aquela mensagem. Se você fizer a interceptação, você vai interceptar um dado criptografado, e, hoje, com um dos melhores quebradores de senha, pode levar 100 anos para descobrir o que você mandou para ele. Hoje é o ambiente, e o ambiente leva ao anonimato, e anonimato em segurança pública só significa uma coisa: impunidade." (Bruno Telles, Presidente da Associação Brasileira de Criminalística).

> "Bom, com relação às ordens judiciais, se o WhatsApp entrega decifrado ou não decifrado, disso eu falei. O Facebook, o detentor de direitos, tem a obrigação de atender às nossas normas. Se ele entrega cifrado ou não entrega cifrado — as procuradoras aqui já falaram, entendeu? — Eu vou repetir as palavras dele: "Eles querem entregar cifrados". Agora, o conceito de interceptação, o conceito que a Lei nº 9.296... Você imagine se a lei fosse prevista para eu entregar uma coisa que não seja possível visualizar! Seria como interceptar um telefone e ter essas conversas criptografadas e enviar para você: "Ó, pegue aí e veja o que você consegue fazer". Então, é isso que estão fazendo com a gente. Isso dificulta o nosso processo? Dificulta. A Polícia Federal tem várias metodologias que contornam algumas criptografias, alguns tipos — não vou revelar aqui os métodos que ela utiliza. Mas, enfim, a legislação brasileira deve ser cumprida. O WhatsApp, o Facebook, todas as redes sociais devem responder de acordo com a nossa legislação. Se eles não estão cumprindo — os senhores aqui já têm ciência, não são só palavras minhas, são palavras de outros palestrantes que já passaram por aqui, inclusive membros do Ministério Público —, então, vocês têm que fazer valer. Eu acho que os senhores têm prerrogativa para isso e têm força para isso." (André Abreu Magalhães, Perito da Polícia Federal)

Tornou-se de conhecimento público, através do vazamento dos e-mails, que a Polícia Federal estava contratando os serviços da empresa italiana Hacking Team (HT)[99]. A HT foi fundada em 2003, como uma empresa de consultoria de segurança, tendo como capital inicial €223.572,00 e como sócio majoritário David Vincenzetti. Ao longo dos anos, a empresa passou além de oferecer serviços como teste de penetração e auditoria para a venda de malware para governos ao redor do mundo, inclusive de países que são internacionalmente conhecidos por violarem o direito a liberdade de expressão.

A segurança ofensiva é sustentada por Vincenzetti como o futuro para a interceptação das comunicações, uma vez que tanto os usuários quantos os provedores de conteúdo passaram a criptografar os dados. Em outra mensagem disponibilizada, ele afirma que mesmo se o futuro dessa criptoguerra

97 Segurança ofensiva é uma abordagem proativa e de oposição para proteger sistemas informáticos, redes e indivíduos de ataques. As medidas de segurança ofensivas são focadas em buscar os responsáveis pelos ataques e, em alguns casos, a tentativa de desabilitar ou, pelo menos, interromper suas operações, ao invés de aguardar passivamente ataques e efetivar uma defesa.

98 Notas taquigráficas - 12 reunião (15/09/2015)http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/documentos/notas-taquigraficas/nt150915-crc-sem-revisao

99 Todos os pedidos de informações feitos pela ARTIGO 19 sobre o assunto foram negados.

em andamento tenha como resultado a implementação de um novo CALEA, isto é, um mecanismo jurídico para a implementação de um dispositivo de interceptação nas tecnologias de comunicação criptografadas no Ocidente, a HT não sairia de cena, pois os "infratores" mudariam para uma tecnologia feita em outro país [100].

Basicamente, o produto principal da HT é uma suíte de invasão desenvolvida a partir de vulnerabilidades não divulgadas publicamente nos sistemas operacionais. Através da engenharia social, isto é, da ação do alvo clicar e executar o programa malicioso, é possível contaminá-lo, extrair os dados, interceptar áudios e vídeos de conversas, acionar a câmera de vídeo, infectar outros computadores, descobrir sua localização e inclusive ser removido sem deixar rastros no dispositivo da vítima. Como algumas dessas vulnerabilidades acabaram sendo corrigidas pelas empresas dos softwares, é necessário comprar ou encontrar novas vulnerabilidades. Um estudo sobre o mercado das vulnerabilidades utilizadas pela HT a partir dos e-mails vazados foi feito[101] e mostra que o preço pago por cada vulnerabilidade variava entre US$ 39 mil a US$ 45 mil.

Sob o codinome Brenda, a Polícia Federal estabeleceu um contrato com a HT para a implementação de um projeto piloto no início 2015, após a aprovação de uma emenda na Lei 13.097 que dispensa a licitação para a contratação de serviços técnicos especializados destinados à polícia judiciária para o rastreamento e obtenção de provas. Ela se refere à aquisição de equipamentos sensíveis e necessários à investigação policial e modifica o art. 3o da Lei 12.850, de 2 de agosto de 2013, que diz respeito aos meios de obtenção de provas policiais para as investigações, passando a vigorar com o seus parágrafos 1º e 2º com a seguinte redação:

> "§1º Havendo necessidade justificada de manter sigilo sobre a capacidade investigatória, poderá ser dispensada licitação para contratação de serviços técnicos especializados, aquisição ou locação de equipamentos destinados à polícia judiciária para o rastreamento e obtenção de provas previstas nos incisos II e V.
> §2º No caso do § 1o, fica dispensada a publicação de que trata o parágrafo único do art. 61 da Lei no 8.666, de 21 de junho de 1993, devendo ser comunicado o órgão de controle interno da realização da contratação."

Os incisos citados do Art. 3º dizem respeito a: II - captação ambiental de sinais eletromagnéticos, ópticos ou acústicos; e V - interceptação de comunicações telefônicas e telemáticas, nos termos da legislação específica.

Atuando através de uma empresa representante no Brasil, a Yasnitech, a proposta executada era de R$ 25 mil reais/mês por 3 meses para 10 agentes e todos os softwares necessários. O hardware necessário, aluguel da rede de anonimato e conexão à Internet foram de responsabilidade da PF. Houve um interesse especial na aquisição da solução da HT para a invasão de dispositivos móveis como os smartphones. Para o projeto piloto foi concedida uma autorização judicial para 17 alvos que utilizavam smartphones.

Caso o projeto tivesse um resultado satisfatório, o contrato seria expandido para 100 agentes e teria como expectativa o retorno financeiro de € 1.200,000, colocando o Brasil como um dos maiores clientes da empresa em 2015. Além da suíte principal da HT, a Polícia Federal também adquiriu um Tactical Network Injector (TNI) para inserir pacotes maliciosos no tráfego de rede de um alvo. Em termos práticos, caso um alvo esteja usando o computador conectado numa rede pública, como a de um hotel, é possível que a PF injete tráfego para que o computador acesse uma página falsa e baixe um programa malicioso.

100 https://www.wikileaks.org/hackingteam/emails/emailid/179629

101 https://tsyrklevich.net/2015/07/22/hacking-team-0day-market/

Outros clientes brasileiros também foram prospectados como a Polícia Civil e a Polícia Militar de São Paulo. Embora a última instituição não tenha papel de polícia judiciária, ela poderia adquirir o produto da HT para investigar casos de crimes de internos, julgados dentro do âmbito da Justiça Militar que foi argumentado no pedido de informações feito pela ARTIGO 19 (ver em Anexos). Além delas, o produto foi apresentado para a ABIN, DENARC, Secretaria de Segurança Pública de São Paulo, o Exército Brasileiro, o Ministério Público Federal, a Polícia Militar de Brasília, de Minas Gerais, do Rio Grande do Sul, a Secretaria de Estado da Segurança do Paraná, Secretaria de Estado da Fazenda do Espírito Santo, entre outros. Porém, o único contrato firmado no primeiro semestre de 2015 foi com a Polícia Federal.

Ainda não se sabe quem são os autores do vazamento dos dados e todas as vulnerabilidades utilizadas para seus produtos foram arrumadas pelos fabricantes de softwares. Até a data do vazamento, a Polícia Federal indicava que seguiria utilizando o produto da HT e não compraria a solução das empresas de segurança ofensiva concorrentes como o FinFisher, da Gamma Group, a qual também teve seus dados vazados em 2014.

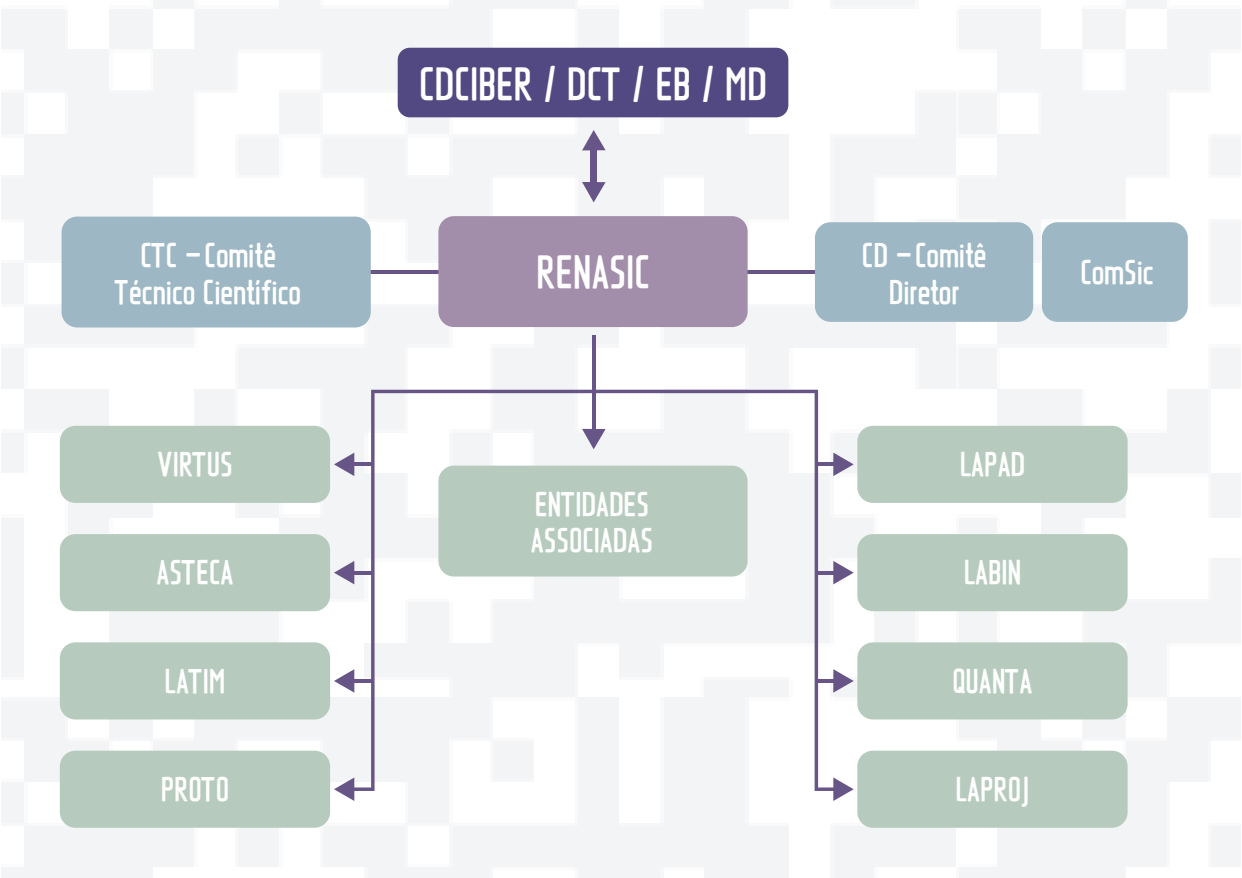
Ciberguerra

Há quatro níveis de decisão na estratégia de ciberdefesa brasileira. O plano político, o qual é definido a segurança cibernética pelo Gabinete de Segurança Institucional e depende diretamente da Administração Pública Federal. O plano estratégico, a defesa cibernética é definida pelo Ministério da Defesa, mas também interage com o GSI. E, no plano tático e operacional, a guerra cibernética é componente de cada uma das Forças Armadas.

No nível político compõe o Sistema de Segurança e Defesa Cibernética os seguintes órgãos: ABIN, ANATEL, Câmara de Relações Exteriores e Defesa Nacional (CREDEN), Casa Civil da Presidência da República, CGI.br, Conselho de Defesa Nacional (CDN), Departamento da Polícia Federal, Departamento de Segurança da Informação e Comunicações (DSIC), GSI-PR e SERPRO. No nível estratégico, as decisões do Ministro da Defesa são assessoradas pelo Comandante da Aeronáutica, do Exército, Marinha, do Conselho Militar de Defesa (CMiD). O CDCiber é de responsabilidade do Exército Brasileiro, mas de operação conjunta com a Marinha e a Aeronáutica. Desta forma, ele passa a organizar os destacamentos militares - para atuar no nível operacional e tático -, centralizar as cooperações internas e externas no âmbito cibernético e também manter as relações entre o campo da segurança da informação e a defesa nacional.

Um exemplo dessa cooperação mista promovida pelo Exército é a RENASIC, Rede Nacional de Segurança da Informação e Criptografia, que foi criada em 2008 e passou a ser coordenada pelo CDCiber. A RENASIC é responsável pelo estudo, análise e desenvolvimento de "infra-estrutura comum que inclui:"- ferramentas para a avaliação dos algoritmos de criptografia; ambientes de avaliação para hardware e software criptográficos; instrumentação física e lógica para análise de ataques secundários (side-channel atacks), suas respectivas contramedidas, além de ferramentas para avaliação dos esquemas de defesa cibernética e forense computacional."[102] A composição da RENASIC não é exclusivamente militar, pelo contrário, é uma área de intercâmbio entre entidades governamentais e privadas, universidades e instituições nacionais e internacionais.

102 http://www.renasic.org.br/institucional



Fonte: http://www.renasic.org.br/images/content/RENASIC_Organograma.png

Quadro Resumido dos Níveis		
Político	Segurança Cibernética	Gabinete de Segurança Institucional
Estratégico	Defesa Cibernética	Ministério da Defesa
Operacional Tático	Guerra Cibernética	Componentes das forças armadas

De acordo com a Doutrina Militar de Defesa Cibernética[103], a defesa cibernética possui três tipos de ações: ataque (negação, interrupção, destruir), defesa (neutralização e mitigação) e exploração, que consiste na obtenção e coleta de informações de interesse. As ações dependem do nível político. É o Ministério de Defesa que estabelece níveis de alerta cibernético durante as operações, como a proteção de grande evento, ou mesmo nas atividades diárias. Há cinco níveis: Branco / Baixo, Azul / Moderado, Amarelo / Médio, Laranja / Alto, Vermelho / Muito Alto. No nível baixo, quando as ameaças conhecidas não impactam nos interesses do MD. Já no nível muito alto, é quando forças hostis interrompem as infraestruturas críticas de informação com alto impacto e sem estimativa de tempo para o cumprimento da missão.

103 Páginas 20-36 http://defesa.gov.br/arquivos/legislacao/emcfa/publicacoes/doutrina/md31_m_07_defesa_cibernetica_1_2014.pdf

Nível de Alerta		Significado / Interpretação (*)[104]
Cor	Nome	
Branco	Baixo	- Aplicável quando as ameaças cibernéticas percebidas não afetam o Espaço Cibernético de interesse do MD e das FA. - Situação normal ou rotineira, considerando o histórico. - Probabilidade de concretização de ameaças cibernéticas baixa, considerando o histórico.
Azul	Moderado	- Aplicável quando as ameaças cibernéticas percebidas afetam o Espaço Cibernético de interesse do MD e das FA, sem comprometer as infraestruturas críticas da Informação. - Probabilidade de concretização de ameaças cibernéticas entre baixa e média, considerando o histórico.
Amarelo	Médio	- Aplicável quando ações cibernéticas hostis afetam o Espaço Cibernético de interesse, sem comprometer as infraestruturas críticas da informação. - Aplicável quando houver a percepção de ameaças cibernéticas contra as infraestruturas críticas da informação. - Probabilidade da concretização de ameaças cibernéticas entre média e alta, considerando o histórico.
Laranja	Alto	- Aplicável quando as ações cibernéticas hostis degradam alguma Infraestrutura Crítica da Informação. - Probabilidade de concretização de ameaças cibernéticas entre média e alta, considerando o histórico. - Infraestrutura Crítica da Informação atingida, porém com possibilidade de restabelecimento das condições de segurança ou dos serviços em tempos aceitáveis para o cumprimento da missão. - Infraestrutura Crítica da Informação atingida com impacto entre médio e alto, considerando o histórico.
Vermelho	Muito alto	- Aplicável quando ações cibernéticas hostis exploram ou negam a disponibilidade das infraestruturas críticas da informação. - Probabilidade de concretização de ameaças cibernéticas muito alta, considerando o histórico. - Infraestrutura Crítica da Informação atingida com impacto alto ou superior, considerando o histórico.

Fonte: Páginas 27 e 28 da "Doutrina Militar de Defesa Cibernética"[104]

104 Observações:

Os especialistas em ciberguerra são formados em técnicas ofensivas, defensivas e de inteligência, respectivamente por três órgãos do Exército: Centro de Instrução de Guerra Eletrônica (CIGE), Escola de Comunicações (EscCom) e Escola de Inteligência Militar do Exército (EsIMEx). Os cursos possuem a duração de 24 semanas, divididos em duas fases: a primeira, de oito semanas de ensino à distância e a segunda, reservada apenas para os aprovados, é presencial no CIGE e têm a duração de 16 semanas. Em algum tempo, a consolidação da Escola Nacional de Defesa Cibernética deverá desenvolver a capacidade de formar a maioria dos militares que atuarão no setor.

Essa estrutura de composição híbrida entre militares e empresas também pode ser vista durante os mega-eventos como a Rio +20 (2012), Copa das Confederações (2013), Copa da FIFA (2014), e, possivelmente em breve, as Olimpíadas (2016). Os eventos têm servido como momentos para adquirir hardware, software, treinamento e troca de experiência e cooperação na área entre outros países e com outras empresas. De acordo com a já supracitada Estratégia de SIC brasileira, uma passagem revela como a segurança cibernética perpassa tais eventos. Os grandes eventos são identificados da seguinte maneira, revelando-se quase um laboratório da experiência do governo na área:

> "O cenário de realização de grandes eventos no Brasil (2013 a 2016) ressalta tais preocupações e serve de oportunidade para a conformação de uma situação benéfica, alavancando os compromissos com a SIC e com a SegCiber pactuados e reforçados na direção de que haja capacidade efetiva do governo de catalisar e estimular ações em prol dos diferentes tópicos que perpassam e sustentam tais áreas de atuação."

O CDCiber, por meio do Destacamento de Guerra Cibernética, publicamente participou das seguintes ações:
- Operação Anhanduí (2011)
- Operação Amazônia (2012)
- Operação Atlântico III (2012)
- Rio +20 (2012)
- Operação da Jornada Mundial da Juventude (2013)
- Operação Ágata (2013)
- Operação Laçador (2013)
- Copa das Confederações de Futebol (2013)
- Copa do Mundo de Futebol (2014)

Publicamente, a atuação do CDCiber na Copa do Mundo teve como resultados e destaques:

Resultados	Destaques
O emprego de 112 militares e civis	Vazamento de informações da rede do Itamaraty
79 pessoas capacitadas	Comprometimento de conta do Twitter da Polícia Federal
2 cursos de capacitação	Ataques à página do Exército
12 novas vulnerabilidades alertadas	

- os enunciados da coluna "Significado/Interpretação" representam possíveis cenários, propositadamente simplificados para fins de clareza e síntese; para classificar o nível, pode-se tomar uma ou mais das possibilidades discriminadas em cada uma das linhas da coluna "Significado/Interpretação"; os cenários possíveis são inúmeros e as possibilidades registradas neste documento constituem um núcleo básico, que pode ser desdobrado e enriquecido conforme a aplicação dos níveis e planejamentos de situações específicas reais ou simuladas; quando se enuncia que uma ameaça "afeta" o Espaço Cibernético, subentende-se que uma ou mais das ameaças percebidas se concretizam e causam um impacto correspondente.

Fonte: Gal Cam, disponível em: cert.br/forum2014/slides/ForumCSIRTs2014-CDCiber.pdf
fonte: http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/credn/eventos/2014/seminario-os-projetos-estrategicos-das-forcas-armadas-contribuicao-ao-desenvolvimento-nacional/mesa-2-general--de-divisao-paulo-sergio-melo-de-carvalho-chefe-do-centro-de-defesa-cibernetica-do-exercito-cd-ciber/view

É com muita atenção que a sociedade deve observar as atuações do governo e do Exército nos grandes eventos com relação à segurança cibernética e ações de ciberdefesa. As Olimpíadas do Rio deverão ser o grande laboratório do esforço reconhecido pela divulgação da Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal. A atuação na Copa do Mundo torna o cenário ainda mais alarmante, tendo em vista as atuações de apoio do Exército em manifestações civis.

Tendência: monitoramento de mídias sociais

O monitoramento de mídias sociais a fim de avaliar a imagem dos governos e governantes nessas plataformas parece ter se tornado método recorrente de qualquer gestão pública. Entretanto, no final do ano de 2014, a prática tomou outra dimensão e parece ter adquirido o caráter de mapeamento de grupos ideológicos na internet.

Em dezembro de 2014, a então Secretaria de Direitos Humanos informou que iniciaria um monitoramento de discurso de ódio na internet[105]. A busca ativa de discursos de ódio se daria pelo uso de um software que coleta dados e identificar redes responsáveis. A tônica da legislação brasileira, como previsto pelo Marco Civil da Internet, é de proteção à privacidade, de forma que um monitoramento indiscriminado, com caráter investigativo, além de violar a presunção de inocência, significaria acesso a informações dos usuários sob a justificativa da busca por atividade ilícita. Entretanto, o que revela a intenção de mapeamento de grupos ideológicos nas redes sociais é o contexto da criação e anúncio do projeto, profundamente contaminado pelo debate eleitoral das eleições de 2014, que acabava por criar um ambiente virtual hostil tanto para o governo situacional quanto para a oposição.

Agora, em novembro de 2015, o Ministério das Mulheres, Igualdade Racial e Direitos Humanos que agora centraliza as pautas de direitos humanos sinaliza que a aplicação não foi deixada de lado. Fazendo uso dos recentes casos e discussões sobre racismo e machismo na internet e em redes sociais, o agora denominado "Monitor de Direitos Humanos Criado pelo Laboratório de Estudos em Imagem e Cibercultura da Universidade Federal do Espírito Santo (UFES) voltou à pauta[106].

A tendência de vigiar e controlar as redes, portanto, precisa ser ressaltada. Ainda que seja no caso de monitoramentos que ocorram com informações que o próprio usuário deixa públicas, é importante considerar que nos ambientes offline o monitoramento de cidadãos requer um aval judicial, fazendo ainda uma analogia ao caso das "Rondas Virtuais". Se a ferramenta "Monitor de Direitos Humanos" vier a ser implementada, é extremamente necessário que sejam praticados os mais altos níveis de transparência e controle social, indo muito além do disponível na política institucional, principalmente no uso que o Estado fará dos dados.

105 http://www.brasil.gov.br/cidadania-e-justica/2014/12/governo-vai-usar-software-contra-crimes-de-odio-na-internet

106 http://www.ebc.com.br/cidadania/2015/11/aplicativo-vai-monitorar-mensagens-de-odio-e-racismo-nas-redes-sociais

CONSIDERAÇÕES FINAIS

A ARTIGO 19 avalia que as instituições estatais que estão incumbidas de atuar no âmbito da ciberdefesa brasileira ainda estão em processo de adaptação e construção. Entretanto, a mistura conceitual de crimes que ocorrem na Internet com as ações de espionagem e ciberataques fez com o que o país adotasse medidas caras, ineficientes e potencialmente violadoras da privacidade.

As respostas brasileiras às denúncias de espionagem feitas por Snowden ou ocorreram forma isolada ou chegaram ao ponto de serem antagônicas. Isso é muito visível na dimensão política internacional, com o caso da realização do NETMundial e o discurso da presidente na ONU e, por outro, no plano militar o fortalecimento do CDCiber ou ainda os dispositivos jurídicos de retenção de dados no Marco Civil da Internet. Ao procurar evitar ciberataques de outras nações, investiu-se numa resposta militar, com a adesão da doutrina da guerra cibernética - o que acarretou na militarização de conflitos sociais e na corrida em adquirir capacidades de ciberguerra com a fabricação ou aquisição de ciberarmas. O desenvolvimento e exploração de vulnerabilidades deve ser uma solução integrada aos desenvolvedores de softwares, isto é, uma vez descoberta uma falha ela deverá ser reportada aos desenvolvedores[107]. O Brasil não pode passar a coletar e acumular "exploits" para utilizar contra outras nações. Descobrir uma falha e transformá-la numa ciberarma é tornar a sua própria infraestrutura vulnerável.

As práticas contraditórias do governo brasileiro com relação ao vigilantismo não só se revelam pela legislação ou política internacional, mas também em diversas práticas das polícias e do judiciário. Recentemente, até no executivo, com o abandono do uso de ferramentas desenvolvidas nacionalmente e com código aberto. Na prática, as respostas às denúncias de Edward Snowden pouco adiantaram para alertar o poder público a respeito da segurança cibernética, já que o Brasil não necessariamente evoluiu um aparato voltado à cibersegurança, mas está fortalecendo um verdadeiro sistema para a ciberguerra.

Não pode ser visto como corriqueiro o fato de o Exército Brasileiro desenvolver um aparato de ciberdefesa com eventual capacidade de monitoramento de comunicações sem a transparência que se espera em uma sociedade democrática. Tampouco é aceitável que o Ministério da Defesa estabeleça padrões de atuação em manifestações considerando como inimigos movimentos sociais e a população civil que sai às ruas exercendo o pleno direito de liberdade de expressão e manifestação.

Ainda, é necessário não criminalizar a autodefesa dos usuários e dos provedores de serviços online como o emprego de criptografia forte e o anonimato[108]. Também não é aceitável que um suspeito seja forçado a produzir provas contra si e contribuir para sua própria condenação, com a obrigação de desencriptar entrando com sua própria senha, com base em uma ordem judicial - o que é uma prática que está ficando cada vez mais comum em todo o mundo. A vigilância faz com que indivíduos procurem ferramentas seguras para troca de informações e opiniões. Outros procuram segurança adicional no anonimato. Assim, como o direito à privacidade e à liberdade de expressão, a criptografia e o anonimato são importantes para os defensores de direitos humanos, os denunciantes, jornalistas e ativistas.

---

107 A ideia de divulgação responsável (responsible disclosures) de vulnerabilidades envolve ponderar os impactos nos usuários de um determinado sistema, hardware, software ou serviço. Difere da divulgação completa, que pode acarretar em eventuais consequências para os usuários se por ventura alguém resolver explorar a falha no período em que o problema ainda estiver sendo resolvido. Ao mesmo tempo, por motivos de transparência, o público deve estar ciente da falha, evitando uma falsa sensação de segurança, mas apenas publicizar a vulnerabilidade sem contactar os responsáveis para buscar uma solução conjunta pode não ser a melhor opção. Nestes casos, todas as partes interessadas concordam em estabelecer um período de tempo para que a vulnerabilidade seja corrigida pelo desenvolvedor antes da publicação dos detalhes.

108 Carta Aberta aos Líderes do Mundo, endossando a não flexibilização dos padrões de criptografia por meio de legislação e outras políticas https://www.securetheinternet.org/?lang=pt-br

No entanto, a solução técnica passa por um entrave político global. Não há um alinhamento ou mesmo interesse em acabar ou evitar que a vigilância em massa seja possível no país, pois não é politicamente unânime que a sua existência seja nociva para o desenvolvimento da humanidade. Pelo contrário, ela é justificada pelos seus defensores e varia de acordo com os contextos locais: os dissidentes ao regime na China, os criminosos no Brasil, os terroristas no Oriente Médio, a pedofilia e crimes sexuais no Reino Unido e na Austrália.

Considerando-se os 13 Princípios Internacionais sobre a Aplicação dos Direitos Humanos na Vigilância das Comunicações, é possível afirmar que o Brasil está longe de realizá-los por completo. Com relação à **legalidade** se observa que pelo Marco Civil da Internet, o conteúdo das comunicações está protegido no artigo 7°, II, que fala da inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial. Entretanto, existe controvérsia se a lei de interceptação telefônica se aplicaria ou não aos meios digitais, já que atualmente ela já é utilizada para ligações de voz por IP (VoIP). Outros tipos de captura, como por exemplo de tráfego de dados, não necessariamente se enquadrariam na categoria, mas a lei já é utilizada para tanto. Embora se construa uma narrativa de fim legítimo relacionado à segurança nacional, o que se observa na prática é a vigilância com o objetivo de obter controle sobre os movimentos sociais, a fim de se evitar principalmente protestos legítimos. É notável, por exemplo, no caso dos 23 processados pelos protestos durante a realização da Copa do Mundo, quando os sigilos telefônicos dos investigados foi quebrado com base em indícios superficiais de investigações feitas em páginas do Facebook. É possível observar, inclusive, a abordagem política presente nos julgamentos de valor feitos pelas forças policiais e que, mesmo amparadas por decisões judiciais, não levam o princípio de fim legítimo em consideração. Também podemos afirmar que não estão sendo observados os princípios de **necessidade** e **adequação**. Por exemplo, as notícias de compra de softwares de invasão de dispositivos pela Polícia Federal, além de inapropriadas perante as instâncias que poderiam autorizá-la, não parecem necessárias ou adequadas para o fim que se pretende obter. Práticas de violação de sigilo de comunicações devem ser entendidas como a última alternativa e tem de ser comprovadamente necessárias para atingir um fim legítimo. Ainda, muitas vezes são medidas não proporcionais a direitos fundamentais como o direito à privacidade e liberdade de expressão e à própria sensibilidade do objeto da violação. O que se nota é que embora geralmente estejam amparadas por medidas expedidas por **autoridade judicial competente**, a autorização é feita de maneira questionável, sem revisão devidamente criteriosa e balanceamento de direitos. Ainda, é possível considerar que a produção de provas via rondas virtuais, por exemplo, não segue o **devido processo legal**, por se basearem em juízos de valor dos investigadores, através de suposições e análise de conteúdo que, por exemplo, pode ser irônico ou satírico. A **notificação do usuário** de que pode ser investigado, em geral, não ocorre. Mais do que isso, por vezes, terceiros com quem se mantém diálogos online e não são alvo de investigação acabam sendo monitorados e começam a participar das investigações policiais sem que tenham conhecimento. No caso das Rondas Virtuais, quando pessoas que apareciam em fotos dos acusados automaticamente entravam no escopo da investigação da polícia. O mais grave de tudo é a falta de **transparência**. Escondem-se informações sob o pretexto da segurança nacional e, inclusive, existe a prática de produzir legislação que acaba apoiando esse mecanismo, como a isenção de processo de licitação para a compra de equipamento "sensível" e "necessário" à investigação policial, no artigo 3° da Lei no 12.850. Como consequência, não estão sujeitos ao **escrutínio público** todos os casos que envolvem o uso de equipamentos que envolvem investigações "sensíveis" e relacionadas à segurança nacional. A tendência é que, com a pressão dos órgãos de investigação, cada vez mais essas práticas sejam legitimadas por meio de legislação. A **integridade das comunicações e sistemas** também estão ameaçadas com a criação de obrigações de retenção de dados considerada abusiva no Marco Civil da Internet. A guarda de registros de conexão no Artigo 13 obriga os serviços de provimento de internet a guardarem dados dos usuários por um ano, enquanto o Artigo 15 obriga a guarda de registros de acesso dos usuários por parte dos serviços e aplicações de internet por seis

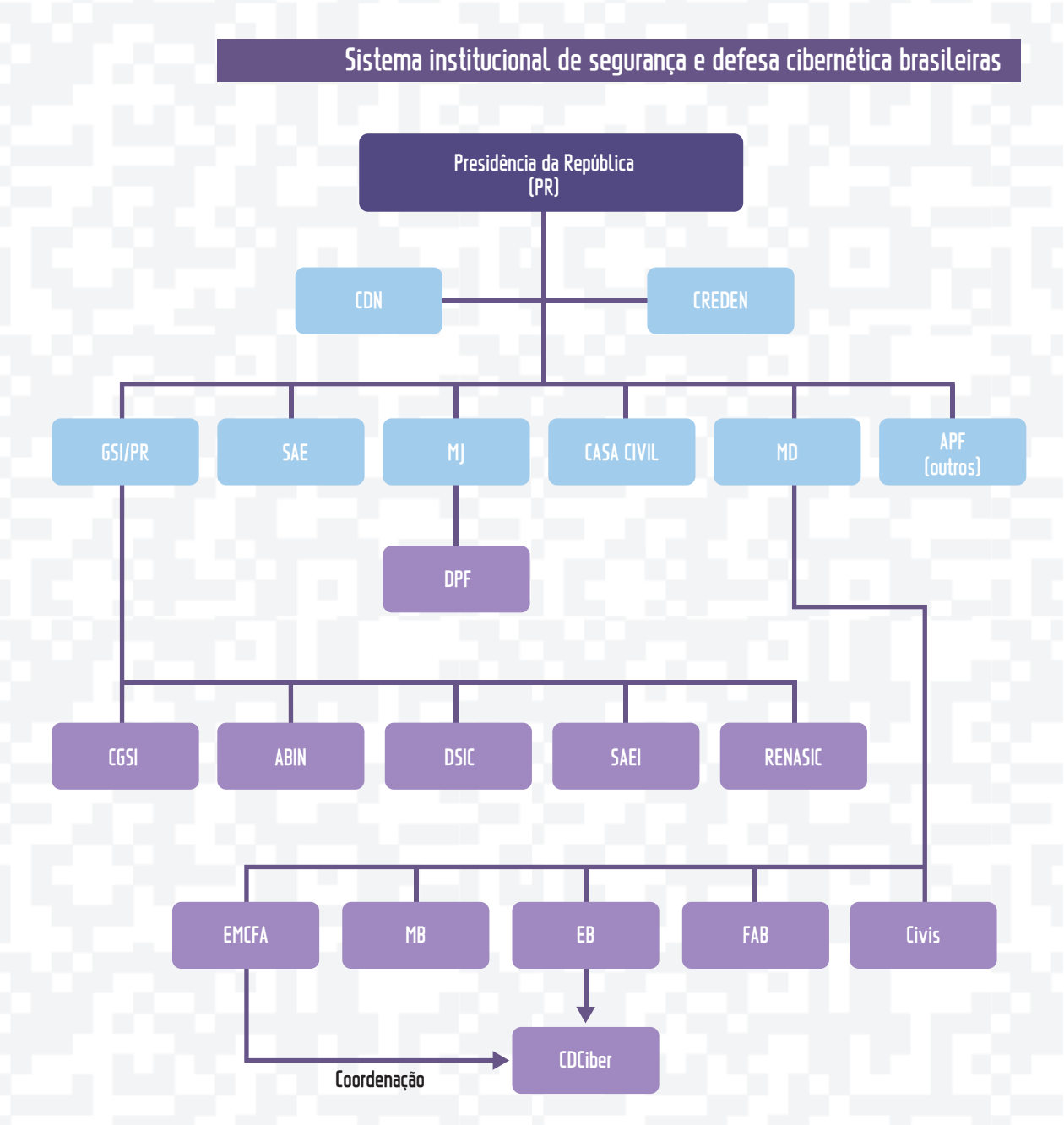
meses. A guarda de tantos dados por tanto tempo só aumenta a possibilidade de abusos por parte do Estado e, até mesmo, de que tais dados sejam violados por terceiros. E nas relações internacionais não está claro o mecanismo adotado de **salvaguardas para a cooperação *internacional***. *Sem uma lei de proteção de proteção de dados pessoais, ainda não há ainda legislação que criminalize a vigilância das comunicações com sanções civis e criminais, além de garantir proteção para denunciantes e reparações para afetados.* Por fim, as **salvaguardas contra acesso ilegítimo e o direito a medidas *eficazes*** também estão prejudicadas sem uma lei de proteção de dados pessoais.

Assim, nossa preocupação principal é que o Brasil, na implantação dessas políticas, acabe por repetir os mesmos erros de países como os EUA, que constituíram serviços de inteligência que violam sistematicamente os direitos à privacidade e à liberdade de expressão. Para que haja controle social sobre o que acontece no desenvolvimento dessas capacidades, é necessário que o governo seja mais transparente com relação às informações de protocolos, procedimentos, operações e poderio. Não se deve aceitar a justificativa de segurança nacional, já que não se buscam detalhamentos de eventuais operações, mas sim números que permitam à sociedade avaliar a capacidade de guerra e segurança cibernética. Acesso à informação é um dos passos imprescendíveis para observância do respeito a direitos fundamentais, em especial a liberdade de expressão e privacidade.

ANEXOS

Organismos brasileiros de segurança e defesa cibernética

Nos próximos itens do documento, abordaremos as atuais funções e atividades das instituições responsáveis pela segurança cibernética.



Fonte: http://www.ipea.gov.br/agencia/images/stories/PDFs/TDs/td_1850.pdf

Ministérios da Justiça e da Defesa

O Ministério da Justiça e da Defesa são os principais responsáveis a nível nacional segurança pública e as maiores somas destinadas à aquisição de equipamentos de segurança partem do orçamento destes órgãos. Na Copa do Mundo, por exemplo, o investimento total na área de segurança foi de R$ 1,9 bilhão, 1,2 bi do Ministério da Justiça e R$700 mi do Ministério da Defesa. Entre os investimentos dessas instituições estão robôs antibombas, imageadores aéreos para helicópteros e plataformas de observação elevada, que captam imagens de diversos ângulos e as transmitem em tempo real para os centros de controle[109]. A maior contribuição atribuída pelos Ministérios ao esquema de segurança montado para a Copa foi a integração que promoveria entre os órgãos policiais no âmbito regional e nacional.

Forças Armadas

Terra, ar e mar não são mais os únicos espaços de ação das Forças Armadas. O ambiente cibernético tornou-se uma quarta dimensão de atuação para as instituições militares. Todas as unidades: Marinha, Aeronáutica e Exército possuem equipes de defesa cibernética. Em 2011 – ou seja, antes das denúncias de Edward Snowden - foi fundado sob coordenação do Exército, o CDCiber[110]. A instituição coordena e integra as ações das unidades, além de contar com um simulador de guerra cibernética, o SIMOC, produzido pela empresa nacional Rustcon e um laboratório de análises de artefatos maliciosos. De início, o discurso imperante para a necessidade do CDCiber era o da ciberguerra e a necessidade de uma maior proteção dos sistemas cibernéticos nacionais contra ameaças estrangeiras.

Contudo, em 2013, o CDCiber agiu com outra finalidade: montou um esquema de vigilância, utilizando o software nacional Guardião, da empresa Dígitro. O centro de operações do CDCiber em Brasília contou com 50 militares que, durante o período da Copa das Confederações de intensa agitação popular tiveram por objetivo identificar os líderes das manifestações[111]. A Polícia Federal atuou conjuntamente ao CDCiber. O general José Carlos Santos, responsável pela unidade em 2013, afirmou que em nenhum momento esse monitoramento invadiu as contas de usuários e que pararam logo após a Copa das Confederações. O general também afirmou que o Exército receberia até 2015 uma verba de R$400 milhões especificamente para tratar da segurança cibernética[112].

Vale registrar que a Marinha, por sua vez, também atuou no esquema de segurança da Copa do Mundo. Suas cinco aeronaves não tripuladas sobrevoaram a região dos estádios para realizar um mapeamento e ajudar na identificação de suspeitos. As câmeras instaladas nessas aeronaves têm alta resolução e conseguem identificar rostos facilmente.

É interessante notar o caráter policialesco que as Forças Armadas assumiram durante um período de "necessidade" - o que tem sido cada vez comum, já que exemplos não faltaram na contenção de manifestações nas ruas das cidades-sede da Copa do Mundo durante todo o evento, com o objetivo de se prevenir de determinadas situações nos protestos. A ARTIGO 19 avalia que há uma tendência a situação se mantenha e o CDCiber continue exercendo um papel de destaque nos esquemas de

---

109 http://www.justica.gov.br/noticias/integracao-das-forcas-policiais-e-investimento-em-seguranca-serao-os-grandes-legados-da-copa

110 http://www.dct.eb.mil.br/

111 http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=34302#.U_ZER6ObDIU

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

segurança no país. Por exemplo, o órgão ministrou cursos de preparação para oficiais que trabalharam nas cidades-sede e estabeleceu uma parceria com o Serpro (Serviço Federal de Processamento de Dados) para combater possíveis ataques[113].

Polícia Federal

A Polícia Federal é a responsável em nível nacional pela proteção contra os crimes cibernéticos. Sendo sua missão na área: "Coordenar e executar a reação a ações ilícitas criminais praticadas contra a Segurança da Informação e Comunicação da APF (Informação e Ativos da Informação) para permitir a responsabilização criminal dos autores dos delitos" (grifo nosso)[114]. O órgão policial conta com um Centro de Monitoramento do Serviço de Repressão a Crimes Cibernéticos desde 2011, em Brasília. Sua principal função é proteger as mais de 320 redes do Governo Federal dos milhares de ataques que elas recebem por hora, com o objetivo de proteger os dados sensíveis do governo e dos cidadãos.

No entanto, com a realização da Copa do Mundo nota-se uma mudança no caráter puramente de REAÇÃO das atividades empreendidas pela PF na campo cibernético: "De acordo com o delegado Tarcísio Jansen, da Polícia Civil, equipes do serviço de inteligência terão auxílio da Polícia Federal para monitorar sites de relacionamentos e páginas da internet. O objetivo é antecipar possíveis manifestações e identificar os líderes."[115]. Ou seja, a Polícia Federal atuou também proativamente, em busca de possíveis suspeitos.

Na Copa, foi montado o pelo Centro de Cooperação Policial Internacional (CCPI), uma integração entre as forças de segurança dos países participantes da Copa do Mundo sob o comando da Secretaria Extraordinária de Segurança para Grandes Eventos (Sesge), do Ministério da Justiça. Conforme o SESGE afirma[116], o CCPI tem a função de gerenciar as informações relacionadas aos antecedentes criminais, à nacionalidade e a autenticidade de documentos de estrangeiros que ingressem no Brasil, de listas de passageiros, dentre outras informações disponíveis e que sejam de interesse operacional. Ele também concentrou informações relativas às ocorrências e os incidentes envolvendo torcedores estrangeiros.

Além dessas medidas, a Polícia Federal dispõe de duas aeronaves não tripuladas que já foram utilizadas em operações contra narcotráfico por exemplo[117]. Há possibilidades de que esses drones, assim como os da FAB, tenham sido utilizados para a vigilância nos estádios da Copa[118]. Esse tipo de equipamento possui tecnologia de vigilância de alta capacidade, podendo mapear uma área extensa com detalhamento de imagens capaz de identificar rostos.

---

113 http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=36857&sid=18

114 http://www.eceme.ensino.eb.br/ciclodeestudosestrategicos/index.php/CEE/XICEE/paper/viewFile/27/41

115 http://www.adpf.org.br/adpf/admin/painelcontrole/materia/materia_portal.wsp?tmp.edt.materia_codigo=6712#.U4YbX_ldV40

116 http://sesge.mj.gov.br/?p=3026

117 http://oglobo.globo.com/rio/veiculo-aereo-nao-tripulado-ajudou-prender-chefe-do-trafico-da-mare-12012255

118 http://g1.globo.com/brasil/noticia/2014/03/fab-compra-novo-drone-para-vigiar-estadios-durante-copa-do-mundo.html

Casa Militar (Gabinete de Segurança Institucional) e ABIN

Fonte: Casa Militar

O Gabinete de Segurança Institucional era o órgão que detinha a responsabilidade de dar assistência e assessoramento em questões militares e de segurança à Presidência. Também tinha a responsabilidade de garantir pleno exercício das funções do cargo, segurança pessoal e dos ambientes frequentados. Ele está subdivido em diversos segmentos e frentes. A ABIN é a agência de inteligência do governo brasileiro e estava no mesmo nível de outras Secretarias que respondiam direto ao GSI-PR.

Em outubro de 2015, a secretaria acabou sendo integrada a um novo ministério, resultado da fusão entre os antigos ministérios de Relações Institucionais, Micro e Pequena Empresa e da Secretaria-Geral, além de algumas atribuições do Gabinete de Segurança Institucional, como o controle da ABIN, formando a Secretaria do Governo. Ao mesmo tempo, o gabinete tem seu nome modificado e, de acordo com a Medida Provisória nº 696, de 02 de outubro de 2015, passou a chamar-se Casa Militar. A casa militar passa, portanto, a ter entre suas atribuições a assistência e coordenação junto ao governo em assuntos militares e de segurança, além de garantir a segurança da presidência.

A Agência Brasileira de Inteligência - ABIN[119] foi fundada em 1999 e é responsável por planejar, executar, coordenar, supervisionar e controlar as atividades de inteligência do país. A agência teve um aumento seu orçamento em de cerca de 300% em 10 anos, considerando o orçamento de R$124,5

119 http://www.abin.gov.br

milhões da agência em 2003 e o de R$500 milhões em 2013[120]. Deste último montante, cerca de R$ 56 milhões são direcionados diretamente às ações de inteligência desenvolvidas. Após a reforma de ministérios de 2015, a ABIN passou a ser controlada pela Secretaria de Governo da Presidência da República.

Durante a Copa das Confederações e as manifestações de junho de 2013, a ABIN passou a ser constantemente citada nos noticiários nacionais, notadamente pelo sistema Mosaico[121]. O monitoramento das redes sociais causou incômodo e represálias da opinião pública[122], além de chacotas nas redes sociais pela crença na incapacidade da agência em realizar tal tarefa. A finalidade do sistema Mosaico foi comparada do programa Prism da NSA[123]. Não há informações mais claras sobre o início das atividades de monitoramento das redes pela agência, se ela teria começado a monitorar com a emergência das manifestações ou já o fazia antes e se, após a grande onda de agitação popular, a ABIN cessou com a prática ou a manteve.

Polícia Militar

No Brasil, a Polícia Militar - PM tem papel de polícia administrativa dentro de cada estado da federação. Cabe à PM o policiamento ostensivo e preventivo, bem como a manutenção da ordem pública. No Distrito Federal, por exemplo, a Polícia Militar monitorou redes sociais e listas de e-mails no início das manifestações de julho de 2013, com o intuito de estimar a quantidade de pessoas que iriam às manifestações[124], prática que tem se mostrado sistemática depois desse período. O uso desses monitoramentos vem se intensificando e a PM tem usado as redes para planejar e coordenar suas ações. Nos mesmos protestos de 2013, por exemplo, a PM de Goiás realizou o mesmo trabalho da ABIN no monitoramento das redes sociais utilizando um programa que selecionava palavras-chave para a identificação de manifestantes[125]. A PM de São Paulo também filmou manifestantes durante os protestos, sendo que o destino das imagens nunca foi esclarecido[126].

Vigilantismo na Copa do Mundo

A realização da Copa do Mundo em 2014 acendeu um alerta para a repetição das atividades de monitoramento, com o agravante de que as leis e uma estrutura específica de segurança foram implementadas para o evento futebolístico.

A Lei geral da Copa é o regime legislativo especial sob o qual foi regido o evento da Copa do Mundo no Brasil, aprovado em 2012. Todo o processo foi questionado e criticado por ceder à Fifa poder abusivo[127]. Movimentos sociais fizeram uma série de reclamações quanto ao projeto e ao papel subserviente à Fifa que o governo brasileiro desempenhou em todo o processo de elaboração legislativa. Dentre os vários abusos estão: os novos tipos penais e as restrições à liberdade de expressão e à criatividade brasileira. Por exemplo, chargistas, imprensa e toda a

120 http://www.contasabertas.com.br/website/arquivos/584

121 http://sao-paulo.estadao.com.br/noticias/geral,abin-monta-rede-para-monitorar-internet,1044500

122 http://pt.globalvoicesonline.org/2013/06/21/monitoramento-abin-redes-sociais

123 http://gizmodo.uol.com.br/o-que-e-prism

124 http://g1.globo.com/distrito-federal/noticia/2013/06/pm-do-df-monitora-redes-sociais-para-se-antecipar-manifestacoes.html

125 http://www.tvsd.com.br/noticias/jmd/policia-militar-monitora-as-redes-sociais

126 http://www.cartacapital.com.br/blogs/caixa-preta/pm-finge-que-filmagens-de-protestos-feitas-por-policiais-nao-existem-3192.html

127 http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/Lei/L12663.htm

torcida que usar os símbolos da Copa do Mundo pertencentes à FIFA poderiam ser processados (Artigos 31 a 34)[128].

Essa legislação afetou o modo de operação das forças de segurança. Diferentemente do que acontece em jogos da CBF – Confederação Brasileira de Futebol, a segurança nos estádios da Copa e nos seus arredores, os escritórios da FIFA/COL, hotéis das seleções e da FIFA, campos oficiais de treinamento e centro de treinamento de seleções foi feita por agências privadas de segurança. A interação entre forças públicas e privadas ainda é algo obscuro, não houve parâmetros para saber em que medida isso funcionou ou não, sendo esse um dos desafios apontados no planejamento estratégico de segurança para a Copa do Mundo FIFA Brasil 2014[129]. Pergunta-se quais foram os limites impostos às agências privadas escaladas para fornecer a segurança da Copa. Elas puderam realizar algum tipo de monitoramento ou vigilância sob as pessoas que assistiram aos jogos da Copa? Com quais equipamentos? Será que pessoas suspeitas tiveram seus perfis analisados e tiveram a entrada barrada nos jogos?

O emprego de segurança privada em espaços públicos, como vimos recentemente no Brasil para grandes eventos, permite que a segurança não seja distribuída de forma igualitária, focada em delitos menores, além da busca e repressão de mercados informais, em prol de agentes privados específicos e seus interesses. Nesses casos, é praxe que quaisquer potenciais ameaças de segurança e outras violações que, apesar de baseadas em protocolos, acabam advindo de julgamentos subjetivos dos agentes de segurança.

A aliança entre a privatização de espaços públicos em nome de eventos, ainda que dentro de leis controversas[130], com o experimento de vigilância e monitoramento de entes privados para a manutenção da ordem e dos seus interesses é potencialmente perigosa. A admissão de que instituições privadas sejam responsáveis pela segurança de brasileiros e estrangeiros é uma aposta governamental que reflete uma tendência mundial de privatização da segurança. Essa desvinculação do aparato estatal de uma de suas funções mais elementares pode causar grandes problemas na responsabilização dos erros e abusos que podem ocorrer. Assim como toda terceirização, a segurança privada permite aos governos que a contratam se eximir das culpas que lhe recairiam, caso a segurança fosse pública.

Um dos exemplos foi o dos gastos com câmeras de segurança para os estádios de mais de R$80 milhões. Não houve, entretanto, garantia de que as imagens coletadas seriam apagadas pela FIFA depois[131]. Não obstante, os gastos públicos[132] com segurança e o emprego também de forças públicas como polícias e seus batalhões especiais, exército, força nacional e agências de vigilância e monitoramento para a realização de um evento privado torna toda questão bastante controversa. O legado em muitas áreas com aumento de tecnologias de repressão, vigilância e monitoramento adquiridas para a Copa do Mundo é extremamente preocupante na continuidade das relações do governo brasileiro com sua população, já que é mera compra e existência desses equipamentos já justifica seu uso.

---

128 http://www.portalpopulardacopa.org.br/index.php?option=com_k2&view=item&id=230:lei-geral-da-copa-um-%E2%80%9C-chute-no-traseiro%E2%80%9D

129 Planejamento Estratégico na íntegra http://goo.gl/r3djMC

130 http://esportes.estadao.com.br/noticias/futebol,fifa-nao-vai-aceitar-mudancas-na-lei-geral-da-copa,1052121

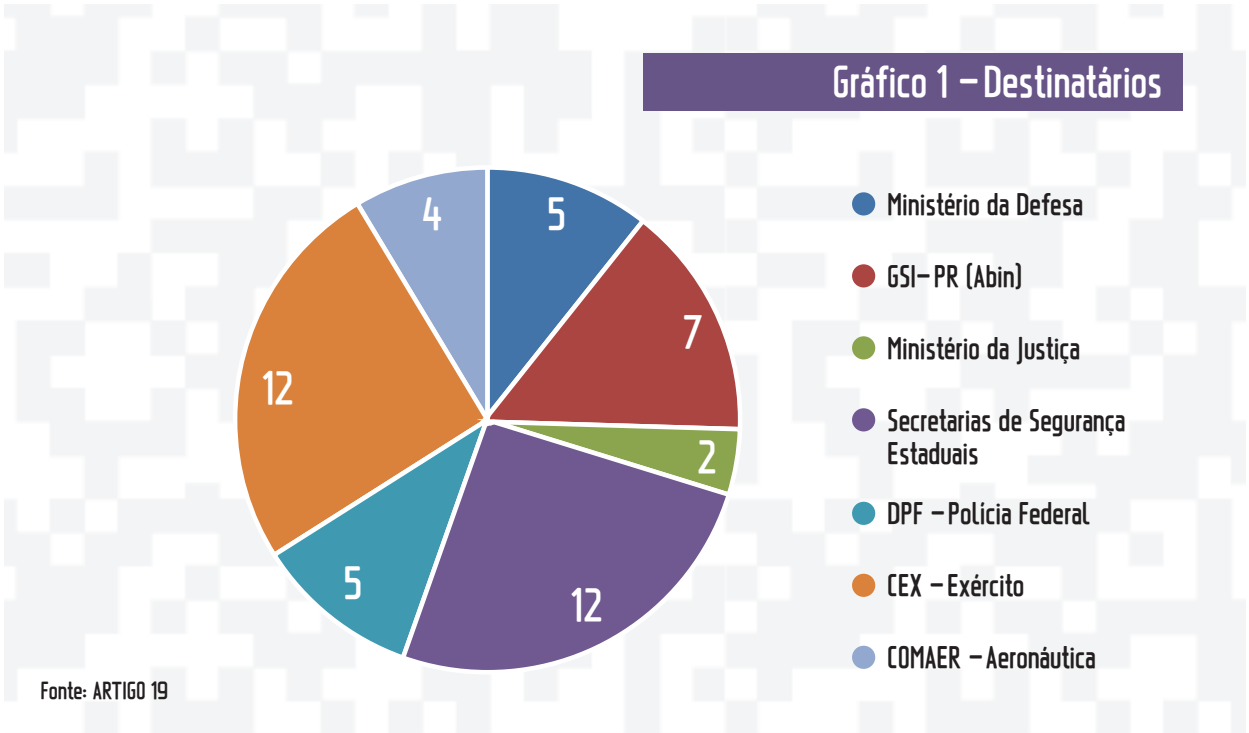
131 http://www.cartacapital.com.br/sociedade/o-rio-que-viola-os-direitos-humanos

132 http://exame.abril.com.br/brasil/noticias/seguranca-da-copa-tera-170-mil-agentes-e-plano-contra-violencia-em-protestos

Pedidos de informação

A ARTIGO 19 e parceiros realizaram 47 pedidos de informação a órgãos públicos no Brasil, entre 30 de maio de 2014 a 8 de agosto de 2014, a fim de aprofundar como funcionam as políticas de vigilância no país. Os órgãos destinatários dos pedidos de informação foram: Ministério da Defesa, Ministério da Justiça, Gabinete de Segurança Institucional da Presidência da República, Comando do Exército, Comando da Aeronáutica, Departamento da Polícia Federal e Secretarias Estaduais de Segurança Pública dos 12 Estados que sediaram partidas na Copa do Mundo. Veja abaixo a quantidade enviada a cada órgão:

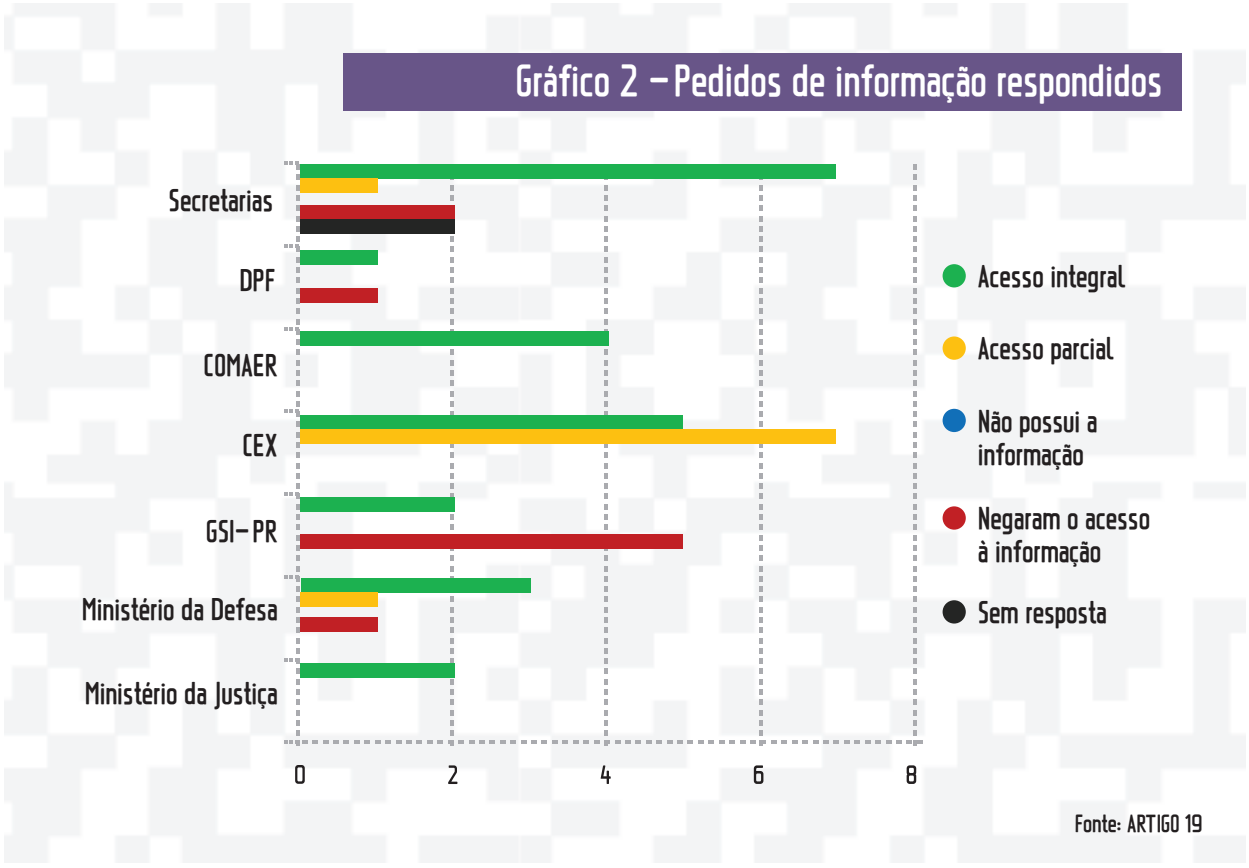
A ARTIGO 19 e parceiros realizaram 47 pedidos de informação a órgãos públicos no Brasil, entre 30 de maio de 2014 a 8 de agosto de 2014, a fim de aprofundar como funcionam as políticas de vigilância no país. Os órgãos destinatários dos pedidos de informação foram: Ministério da Defesa, Ministério da Justiça, Gabinete de Segurança Institucional da Presidência da República, Comando do Exército, Comando da Aeronáutica, Departamento da Polícia Federal e Secretarias Estaduais de Segurança Pública dos 12 Estados que sediaram partidas na Copa do Mundo. Veja abaixo a quantidade enviada a cada órgão:



Para as Secretarias de Segurança Estaduais foram enviados 12 pedidos de informações iguais, sobre a destinação e uso dos equipamentos de segurança que receberam durante a realização da Copa do Mundo. O Comando do Exército recebeu 10 solicitações que versavam sobre monitoramento online, questões de vigilância e ciberguerra, em geral a respeito das movimentações, relações e treinamentos dos órgãos do CEX com outros atores. Para o Ministério da Justiça, foram enviadas pergunta relativa aos imageadores comprados para a Copa do Mundo e sobre o monitoramento desempenhado durante a Copa do Mundo. No âmbito do Gabinete de Segurança Institucional da Presidência da República, as perguntas se voltaram, em geral, ao monitoramento durante a Copa e o funcionamento dos Centros Integrados de Controle criados para o evento. Também versaram sobre relações desempenhadas pela Agência Brasileira de Inteligência (ABIN), agência submetida

ao GSI-PR, com plataformas monitoradas. O Comando da Aeronáutica foi questionado a respeito de questões de vigilância durante a Copa do Mundo e também sobre seus Veículos Aéreos Não Tripulados (VANTs). Os VANTs também foram tema dos questionamentos ao Departamento da Polícia Federal, que também recebeu perguntas sobre monitoramento e relacionamentos.

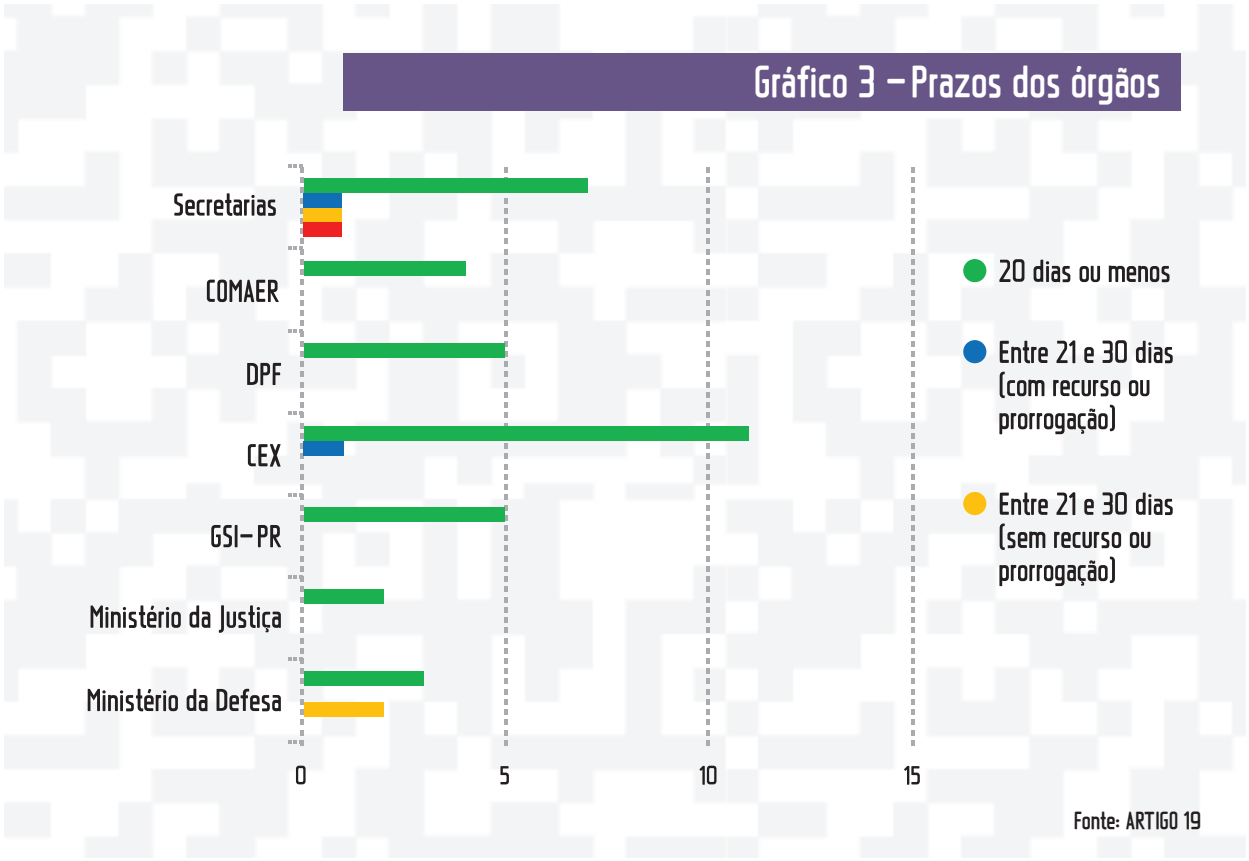
Dos 47 pedidos de informação, 44 foram respondidos e três ainda aguardam respostas e, dado o tempo passado, pode-se inferir que não serão respondidos. Entre os respondidos, 10 negaram o acesso à informação. A principal alegação foi proteção da segurança nacional e a garantia da liberdade da nação. Seis deram acesso parcial a informações solicitadas e 27 acesso integral. A ARTIGO 19 não apresentou recursos às respostas que já foram recebidas:



O Ministério da Defesa, apesar de ter respondido a maioria das questões, foi o único órgão que efetivamente negou acesso à informação, além de ter uma ocorrência maior de acesso parcial às informações. O Ministério da Justiça forneceu acesso integral a todas informações solicitadas. Já o Comando de Exército, deu acesso integral na maioria dos casos e parcial em alguns outros. Já em relação aos Estados, a resposta das Secretarias atendeu integralmente aos pedidos de informação.

O prazo legal, estabelecido em Lei[133], foi cumprido na maioria dos casos em que recebemos respostas, inclusive tendo sido respondidos em menos de 20 dias. Veja a seguir o desempenho de cada órgão:

133 É estabelecido o prazo de 20 dias da data do pedido. As únicas ressalvas se dão nos casos de os pedidos terem sido efetuados depois das 19h de um determinado dia útil ou no caso de o prazo final coincida com um final de semana ou feriado. Em ambos, o prazo é prolongado para o próximo dia útil. Os órgãos também podem pedir uma prorrogação de 10 dias do prazo mediante uma justificativa expressa, aumentando para 30 dias o limite. Após esse prazo de 30 dias, levando em conta as ressalvas, a resposta é considerada atrasada.



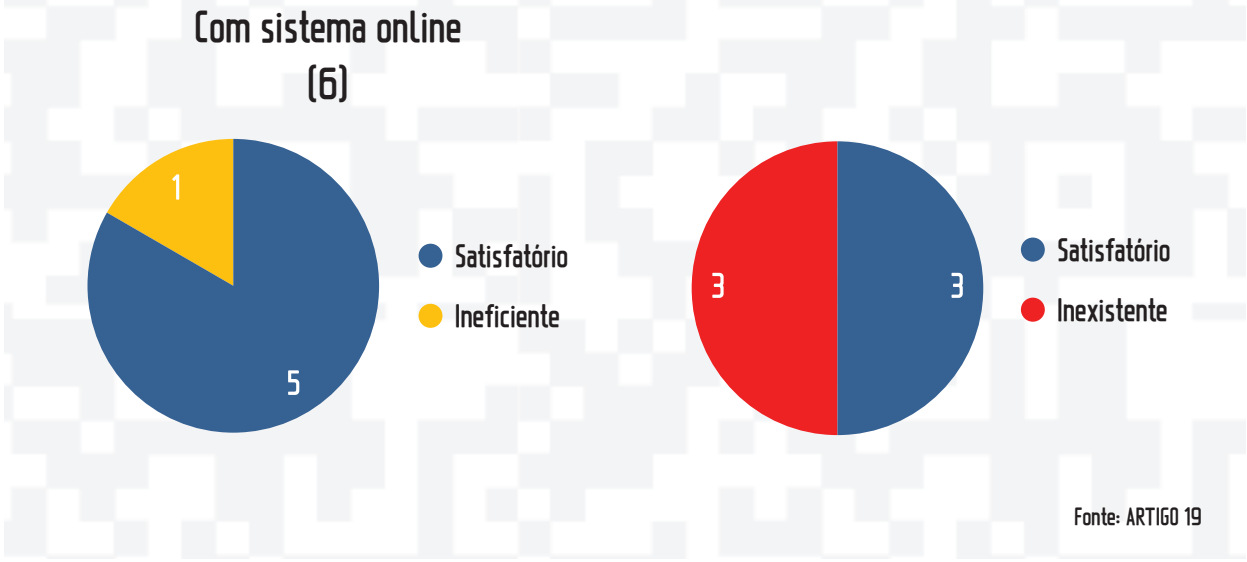
O Comando do Exército respondeu todos os pedidos de informações em menos de 20 dias. Já o Ministério da Justiça respondeu a um pedido em menos de 20 dias, enquanto outro tomou 21 dias, sem que tivesse sido pedida a prorrogação legal do prazo. O Ministério da Defesa agiu da mesma maneira em dois pedidos, respondendo-os em mais de 20 dias, porém menos de 30. Entretanto, respondeu a maioria dos pedidos em menos de 20. Dentre as secretarias estaduais, três delas responderam dentro do prazo legal.

Em geral, sistemas online podem ser considerados uma boa prática de acesso à informação. Entretanto, a existência de uma página para um sistema online de atendimento não significa, necessariamente, que o atendimento vá ser eficiente, já que o sistema pode ser limitado ou confuso. Porém, há situações em que não há sistematização, mas o atendimento pode ser igualmente eficiente via respostas de e-mail. O que se deve evitar são situações em que nem sequer há resposta ou mesmo casos em que inexiste um contato para a efetuação do pedido de informação.

Uma das dificuldades encontradas para fazer pedidos de informações sobre as políticas de segurança implementadas nos Estados de realização da Copa do Mundo foi falta de sistemas online ou sistemas ineficientes[134]. Veja a seguir as condições dos sistemas encontradas:

134 A discriminação da existência de um sistema online ou não se dá pela identificação de uma sistematização, ou página, especificamente criada para a resposta de pedidos de informação, contando com respostas automáticas e/ou posteriores.

Gráfico 4 – Estados e sistema online de Acesso à Informação



Foram encontrados seis Estados sem sistema online para realização de pedidos de informações. Entretanto, em três casos, o mecanismo via e-mail disponível foi bastante satisfatório. Em outros três Estados, porém, simplesmente não está claro o procedimento para a realização de pedidos de informações, apesar da LAI já ter sido aprovada há dois anos. Enquanto isso, dos outros seis Estados com sistema online de pedidos de informação, apenas um deles apresentou algum tipo de problema, sendo classificado como insatisfatório.

Considerou-se satisfatório o sistema que tem regras claras de funcionamento, expressas em alguma área acessível no site do Governo do Estado ou de sua respectiva Secretaria. Um sistema online foi considerado ineficiente a partir do momento em que, apesar de sua existência, existiam limitações a um determinado tipo pedido ou outras restrições. Quando não há sistema online, o atendimento aos pedidos se mostrou satisfatório quando houve transparência quanto ao procedimento necessário e a partir do momento em que há resposta imediata do órgão receptor, confirmando o recebimento e a abertura da ocorrência. Um sistema inexistente se dá quando não há maneira de se requerer pedidos de informação pela internet e/ou não há nenhum tipo de procedimento ou informação referente à Lei de Acesso à Informação e de como registrar um pedido. Veja a situação nos Estados de realização da Copa do Mundo:

Tabela 1 – Sistema online de acesso à informação X eficiência no atendimento

Estado	Existência de Sistema Online	Eficiência no atendimento
Amazonas	Não	Não
Bahia	Sim	Sim
Ceará	Não	Não
Distrito Federal	Sim	Sim

Mato Grosso	Não	Sim
Minas Gerais	Sim	Sim
Paraná	Sim	Sim
Pernambuco	Não	Sim
Rio de Janeiro	Não	Não
Rio Grande do Norte	Não	Não
Rio Grande do Sul	Sim	Sim
São Paulo	Sim	Sim

Fonte: ARTIGO 19

Os Estados do Amazonas, Rio de Janeiro e Rio Grande do Norte não contam com sistema online e nem com nenhuma menção à processualística de como fazer um pedido de informação online. Para obter informações sobre como enviar um pedido para as Secretarias foi necessário ligar e obter um endereço direto de e-mail. Já o caso do Rio de Janeiro é diferente, já que há um processo definido de efetuação de pedidos de informação no Estado e está expresso no endereço online de algumas das Secretarias, mas não há menção ao processo para a Secretaria de Segurança Pública. No site da Polícia Militar, entretanto, há o mesmo processo disponível para as outras Secretarias. No entanto, esse processo demanda a apresentação do formulário pessoalmente no respectivo órgão, além de a necessidade da assinatura de um termo de responsabilidade perante a utilização das informações solicitadas.

Já Ceará, Mato Grosso e Pernambuco descrevem em seus sites claramente o processo para envio de pedidos de informação, apesar de não terem um sistema online para facilitar o processo via o próprio site. Nos três casos o pedido tem de ser feito via e-mail para a Ouvidoria do Estado onde, após confirmação de recebimento, é gerado um protocolo de atendimento.

Bahia, Distrito Federal, Minas Gerais, Paraná, Rio Grande do Sul e São Paulo contam com um portal de acesso para efetuação de pedidos com base na LAI. Todos funcionam bem, com geração de protocolo automático ou envio deste por e-mail. Porém, o sistema do Estado da Bahia é, de certa forma, limitante, já que é necessário definir uma temática pré-estabelecido dentre uma lista de inúmeros separados por área. Se for necessária a apresentação de uma pergunta que foge aos temas definidos, é necessário escolher algum que se aproxime e depois fazer uma complementação do pedido.

Descrição das respostas recebidas

O Ministério da Justiça, em geral, forneceu boas respostas aos nossos pedidos de informações, com acesso integral às informações pedidas.

Já o Ministério da Defesa se comportou de maneira difusa. As respostas às perguntas, quando respondidas, são feitas de maneira d sucinta e clara. Entretanto, quando o pedido é negado ou alguma informação não é passada de maneira integral, as justificativas são extensas, vagas e evasivas.

Por sua vez, o Serviço de Informações ao Cidadão do Exército Brasileiro respondeu de maneira bastante satisfatória algumas de nossas perguntas inclusive fazendo uso de respostas já redigidas anteriormente para completar novas. Porém, algumas das respostas evitaram profundidade a respeito do perguntado, fazendo uso de exemplificações. Dessa forma, responderam algumas de maneira incompleta, dando acesso parcial.

As Secretarias de Segurança Pública estaduais que já responderam aos pedidos de informação forneceram acesso integral a solicitações. Através de serviço que conta com um sistema online, Minas Gerais e Rio Grande do Sul responderam rapidamente ao questionamento, só diferindo um pouco na forma de responder que foi bastante sucinta no caso de Minas Gerais e muito bem elaborada no caso do Rio Grande do Sul. Já o Estado do Ceará respondeu a solicitação através de e-mail, de forma rápida e concedendo acesso integral à informação.

Com relação aos outros órgãos, ainda aguardamos as respostas para análise. Confira abaixo como foram respondidas cada uma das perguntas realizadas:

Tabela 2 – Destinatários, perguntas realizadas e qualidade das respostas

	Órgão	Avaliação da resposta	Pergunta
1	Ministério da Defesa	O MD respondeu com atraso de 5 dias do primeiro prazo legal, dando acesso integral e resposta satisfatória. Apesar de não terem indicado o órgão que possui as informações sobre a aquisição dos imageadores, o MD responde o que lhe cabe "oficialmente", portanto, a resposta é válida.	Qual será a destinação dos 33 imageadores aéreos comprados pelo MD após a Copa do Mundo? Qual será a frequência de uso? Para quais finalidades serão usados?
2	Ministério da Defesa	Através do CEX, foi respondido dentro do prazo legal prorrogado. O acesso foi parcial, uma vez que as perguntas foram respondidas uma a uma, mas o protocolo foi mencionado, mas sem fornecer acesso a ele.	Sobre a criação da nova 4ª Subchefia do Comando de Operações Terrestres (COTER), e com base na notícia do jornal O Estado de São Paulo, de 31 de julho de 2014 sobre este fato (link: http://brasil.estadao.com.br/noticias/geral,exercito-brasileiro-cria-orgao-para-monitorar-manifestacoes,1536422), pergunto: 1)O Ministério da Defesa já realizava algum tipo monitoramento anteriormente? Se sim, como se dava esse monitoramento? 2)Quais os métodos de vigilância e monitoramento que serão empregados? Quais os sistemas de vigilância e monitoramento que serão utilizados? 3)O Ministério da Defesa tem ciência de todos os métodos de vigilância e monitoramento utilizados pelos órgãos que farão a alimentação de inteligência da 4ª Subchefia do COTER? Se sim, quais são esses métodos?

			4)Qual protocolo será seguido para requerimento de informações dos diversos membros do Sisbin, que farão a alimentação da inteligência do órgão? 5)Qual é a amplitude de atuação do órgão? O que ele especificamente terá como responsabilidade? Quais são as possibilidades de ações concretas?
3	Ministério da Defesa	A resposta do MD foi dentro do prazo, porém negando o acesso. As justificativas foram evasivas, e alegaram que há a necessidade de sigilo em vista da proteção da sociedade e dos interesses do Brasil.	Quais os protocolos seguidos pelo MD o monitoramento OSINT online e de redes sociais? Quais os critérios necessários para que seja autorizado o monitoramento de um alvo específico em OSINT pela internet?
4	Ministério da Defesa	O MD, através do CEX respondeu após 5 dias do prazo legal. Mesmo assim, a resposta deu acesso integral à informação e foi completa e bem formulada.	Quais são os critérios para considerarmos um estado iminente de guerra cibernética?
5	Ministério da Defesa	Respondido dentro do prazo, a resposta deu acesso integral, com redação satisfatória.	O Ministério da Defesa tem parceria com o CGI.br? Se sim, quais atividades foram desenvolvidas? O Ministério da Defesa tem parceria com o Nic.br? Se sim, quais atividades foram desenvolvidas?
6	Ministério da Justiça	A pergunta foi encaminhada ao DPF e, apesar de um dia de atraso do primeiro prazo legal, o acesso foi integral e a resposta foi satisfatória e esclarecedora.	Como será realizado o monitoramento dos torcedores pelo Centro de Cooperação Policial Internacional (CCPI)? Quantos integrantes de forças de segurança estrangeiras atuarão no CCPI? De que países? Qual o protocolo de atuação desses agentes estrangeiros?
7	Ministério da Justiça	O MJ respondeu dentro do prazo, com formulação e explicação completas. O acesso foi integral.	Quais as instâncias de decisão sobre os alvos do monitoramento online e as plataformas monitoradas?
8	GSI-PR	Acesso negado. Justificativa de que as informações solicitadas encontram-se sob restrição de acesso, por classificação em grau de sigilo, conforme a legislação vigente.	Agentes de inteligência receberam treinamento de empresas estrangeiras para os equipamentos de segurança que foram utilizados durante a Copa do Mundo? Quantos foram esses treinamentos? Para o uso de quais tipos de equipamentos os agentes foram treinados?
9	GSI-PR	Acesso negado. Justificativa de que as informações solicitadas encontram-se sob restrição de acesso, por classificação em grau de sigilo, conforme a legislação vigente.	A respeito dos Centros Integrados de Comando e Controle de Belo Horizonte, Brasília, Cuiabá, Curitiba, Fortaleza, Manaus, Natal, Porto Alegre, Recife, Rio de Janeiro, Salvador e São Paulo, que

			operaram durante a Copa do Mundo, pergunto: 1) Quais foram os treinamentos realizados no âmbito da Abin para capacitação do seu pessoal para atuação nos Centros Integrados de Comando e Controle? Quais foram as datas dos treinamentos, os currículos e a quantidade de funcionários treinados? 2) Houve treinamento realizado pela IBM, ou demais empresas de tecnologia envolvidas na fabricação dos equipamentos dos Centros Integrados de Comando e Controle para oficiais da Abin ou demais agentes de segurança que atuarão nestes centros? Quais cursos foram oferecidos e em que datas?
10	GSI-PR	Acesso negado. Justificativa de que as informações solicitadas encontram-se sob restrição de acesso, por classificação em grau de sigilo, conforme a legislação vigente.	A respeito dos Centros Integrados de Comando e Controle de Belo Horizonte, Brasília, Cuiabá, Curitiba, Fortaleza, Manaus, Natal, Porto Alegre, Recife, Rio de Janeiro, Salvador e São Paulo, que operaram durante a Copa do Mundo, pergunto: Quantos integrantes da ABIN, da Polícia Federal e de polícias militares estaduais fizeram parte dos Centros Integrados de Comando e Controle durante a Copa do Mundo? Quais foram os cargos ocupados por oficiais da ABIN nos Centros Integrados de Comando e Controle?
11	GSI-PR	Acesso negado. Justificativa de que as informações solicitadas encontram-se sob restrição de acesso, por classificação em grau de sigilo, conforme a legislação vigente.	A respeito dos Centros Integrados de Comando e Controle de Belo Horizonte, Brasília, Cuiabá, Curitiba, Fortaleza, Manaus, Natal, Porto Alegre, Recife, Rio de Janeiro, Salvador e São Paulo, que operaram durante a Copa do Mundo, pergunto: 1) Quais as principais operações de OSINT que foram desenvolvidas pelos integrantes da ABIN durante a Copa do Mundo? Qual é o escopo e duração dessas atividades? 2) A ABIN adquiriu softwares de monitoramento online e de redes sociais nos últimos 3 anos? Quais os softwares adquiridos e os contratos de compra? 3) A ABIN adquiriu equipamentos de monitoramento físico nos últimos 3 anos?

			Quais os equipamentos que foram adquiridos e os contratos de compra? 4) Qual o destino dos equipamentos e softwares adquiridos por evento da Copa do Mundo, após o período da Copa?
12	GSI-PR	Acesso negado. Justificativa de que as informações solicitadas encontram-se sob restrição de acesso, por classificação em grau de sigilo, conforme a legislação vigente.	1) Quais os protocolos seguidos pela ABIN para o monitoramento OSINT online e de redes sociais? Quais os critérios necessários para que seja autorizado o monitoramento de um alvo específico em OSINT pela internet? 2) Quando iniciou-se este tipo de trabalho de monitoramento? 3) Quais as instâncias de decisão sobre os alvos do monitoramento online e as plataformas monitoradas?
13	GSI-PR	A ABIN deu acesso integral à informação, respondendo de maneira sintética às questões, sem entrar em detalhamentos.	Como é o relacionamento da ABIN com as plataformas monitoradas (Facebook, Twitter, Goole)? Existe cooperação dessas empresas no monitoramento ou cessão de informações dos usuários?
14	GSI-PR	Acesso Integral às informações pedidas.	1) A Abin tem parceria com o CGI.br? Se sim, quais atividades foram desenvolvidas? 2) A Abin tem parceria com o NIC.br? Se sim, quais atividades foram desenvolvidas? 3) A Abin trabalha ou já trabalhou em parceria com o CDCiber? Se sim, quais atividades foram desenvolvidas?
15	Comando do Exército	Com exceção da primeira e da última pergunta, o exército respondeu de forma completa a satisfatória todas as outras. Ambas fizeram menção indireta à Copa do Mundo, mas em nenhuma das respostas o evento foi citado. A última pergunta foi ignorada. Acesso parcial, com resposta insuficiente.	1) O exército possui veículos aéreos não tripulados ou tem planos para comprá-los? Se sim, eles foram utilizados durante a Copa do Mundo? 2) Quantas pessoas trabalham no CDCiber? Há planos de aumento no efetivo? 3) Qual é o orçamento do CDCiber? 4) Qual foi o aumento no número de funcionários destinados para as atividades de inteligência e segurança durante a Copa do Mundo? 5) Qual é o destino dos funcionários e do equipamento do CDCiber após a Copa do Mundo?
16	Comando do Exército	Resposta veio em 8 dias e foi bem formulada pelo CEX. Além disso, o acesso à informação foi integral.	Quantos treinamentos foram realizados em decorrência do acordo de cooperação entre Serviço Federal de Processamento de Dados (Serpro) e o Centro de Defesa Cibernética do Exército Brasileiro (CDCiber) firmado em maio de 2014? Qual é o objetivo dos treinamentos?

17	Comando do Exército	A resposta veio dentro do prazo, mas o acesso foi parcial. Apesar de longa, a resposta não foi exatamente à pergunta do pedido, o que a tornou evasiva.	Quais as instâncias de decisão sobre os alvos do monitoramento online e as plataformas monitoradas?
18	Comando do Exército	Após recurso, CEX respondeu que não havia negado pedido e que havia respondido. Mas, para complementar a resposta, respondeu a todos os questionamentos de maneira clara. Acesso integral.	O exército faz parcerias com empresas privadas no setor de inteligência do CDCiber? Com que empresas? O que está sendo desenvolvido a partir destas parcerias?
19	Comando do Exército	CEX respondeu em oito dias. O acesso foi parcial já que parte das perguntas não foi respondida.	Quais empresas trabalham no desenvolvimento de software junto ao exército no setor de análise de risco e vulnerabilidade de sistemas cibernéticos? Quais os projetos em andamento?
20	Comando do Exército	CEX respondeu de maneira clara e rápida. Acesso foi integral.	1)O exército tem ou teve parceria com a empresa BluePex? Quais as ações já realizadas entre o exército e a referida empresa? 2)O exército tem ou teve parceria com a empresa Decatron? Quais as ações já realizadas entre o exército e a referida empresa?
21	Comando do Exército	O pedido de informação foi respondido em oito dias. A primeira pergunta foi bem respondida. Na segunda, não houve especificidade a respeito de quanto foi destinado a cada órgão e nem todos eles, mas foi esclarecido que é distribuído por todos. A terceira pergunta seguiu a mesma linha, exemplificando alguns dos tipos de gastos sem destrinchar todos os projetos. A quarta pergunta foi respondida usando como base a mesma resposta dada pelo CEX, quando encaminhada pelo MD, a respeito de Guerra Cibernética (n. 60502000941201428). O acesso foi parcial, com resposta insuficiente.	1) Em 2012, o General do Exército Brasileiro José Carlos dos Santos, oficial responsável pelo CDCiber à época, disse que o governo iria investir cerca de R$400 milhões para se manter seguro na Guerra Cibernética. Esta quantia foi investida de fato? Se não, qual foi o valor investido no período conseguinte? 2) Qual foi a sua distribuição entre os órgãos do exército? 3) O dinheiro foi gasto em equipamentos? Quais? 4) O General ainda se refere à retribuição de ofensivas caso o país seja atacado. De que maneira isso se daria?
22	Comando do Exército	O pedido de informação foi respondido em oito dias. As duas perguntas feitas foram bem respondidas e, novamente, para responder a segunda, foi usada a fundamentação	1) O exército adquiriu o SIMOC (Simulador de Operações de Guerra Cibernética) da empresa Rustcon? Quais as principais ações possibilitadas por este software? Quais os tipos de treinamento já desenvolvidos neste simulador?

		do pedido de Guerra Cibernética (n. 60502000941201428). O acesso foi integral.	2)Estamos em um estado iminente de guerra cibernética? Quais são os indícios de que isso esteja acontecendo?
23	Comando do Exército	O exército respondeu a primeira pergunta de forma integral, mas deixou de responder as seguintes. Acesso parcial.	1)Quando foi adquirido o software Guardião, da brasileira Dígitro? A partir de que data o software Guardião passou a ser utilizado? 2)Quando iniciou-se o monitoramento das redes sociais? A prática é perene ou se delimita a momentos de manifestação social? 3)Em que situações se justifica o monitoramento das redes sociais? 4)O Exército se utilizou do software durante a Copa do Mundo?
24	Comando do Exército	O CEX respondeu dentro do prazo e, das três perguntas feitas, só respondeu objetivamente a primeira delas. Ou seja, o acesso foi parcial à informação requerida.	Qual tipo de cooperação que existe entre CERT.br e o CCONGEx? O CCONGEx atua focado somente em incidentes de segurança que estão relacionados ao governo? Qual o critério de classificação para definir o que está relacionado ao governo?
25	Comando do Exército	O CEX respondeu ao questionamento de forma completa e bem redigida, apesar de fazer uso de colagem de respostas anteriores novamente. Acesso integral à informação.	1) Quais os protocolos seguidos pelo Exército para o monitoramento OSINT online e de redes sociais? Quais os critérios necessários para que seja autorizado o monitoramento de um alvo específico em OSINT pela internet? 2) Quando iniciou-se este tipo de trabalho de monitoramento? 3) Quais as instâncias de decisão sobre os alvos do monitoramento online e as plataformas monitoradas? 4) O Exército tem permissão para monitoramento online através de softwares espiões ou invasores? Quais os critérios para que esses softwares sejam utilizados?
26	Comando do Exército	O exército respondeu ao questionamento negando os fatos apontados na reportagem. O acesso foi integral, com resposta insatisfatória.	Reportagem do portal G1 (http://g1.globo.com/tecnologia/noticia/2013/07/exercito-monitorara-redes-sociais-durante-visita-do-papa-e-copa-de-2014.html) garante que o exército faz monitoramento de redes sociais através de um software da empresa Dígitro. 1)Qual o nome do software mencionado, disponibilizado pela empresa Dígitro para uso do exército? Quando foi adquirido? 2)Quando iniciou-se o monitoramento das redes sociais? A prática é perene ou se delimita a momentos de manifestação social?

			3)Em que situações se justifica o monitoramento das redes sociais? 4)O Exército se utilizou do software durante a Copa do Mundo?
27	Comando da Aeronáutica	A resposta do COMAER veio completa, citando inúmeras leis e para responder uma das perguntas. As outras foram bem respondidas e bem redigidas. O acesso foi integral.	1) Sabendo que a FAB adquiriu recentemente um veículo aéreo não tripulado para captação de imagens por câmeras de alta definição, gostaria de saber qual a lei que regula a captação de imagens por tais veículos no Brasil? A regulamentação para captação de imagens é a mesma em áreas públicas e áreas privativas? 2) As imagens capturadas são armazenadas? Por quanto tempo? 3) Qual o procedimento de vigilância feito pelos veículos aéreos não tripulado durante a Copa, além do acompanhamento de delegações "sensíveis" e autoridades com risco de segurança? Eles fizeram o acompanhamento das manifestações de rua? Com que objetivo?
28	Comando da Aeronáutica	O COMAER respondeu dentro do prazo ao pedido de informação. Uma pergunta foi bem respondida, porém a outra foi evasiva e insatisfatória, apesar de responder ao questionamento. Acesso integral.	1) Medidas de segurança para a Copa incluíram o uso de veículos aéreos não tripulados? Em que cidades? Com que tarefas específicas? 2) Foram utilizados para garantir a segurança em manifestações de rua? De que forma?
29	Comando da Aeronáutica	A resposta veio dentro do prazo e as perguntas foram bem respondidas, de forma completa, dando acesso integral à informação.	1) De quantos veículos aéreos não tripulados a FAB dispõe atualmente? Quais são os seus modelos? 2) Há plano para aquisição de mais equipamentos assim nos próximos 3 anos? De quais modelos? 3) A que uso esses equipamentos serão dedicados? Eles foram utilizados na Copa do Mundo de 2014? Se sim, qual será a destinação de depois da Copa?
30	Comando da Aeronáutica	A resposta veio dentro do prazo e as perguntas foram bem respondidas, de forma completa, dando acesso integral à informação.	1) Qual o valor dos Drones recentemente adquiridos pela FAB? Quais os contratos de compra? 2) Existe um protocolo/normativa para o uso desse tipo de equipamento pela FAB? 3) Qual o custo de manutenção dos drones atualmente operados pela FAB?

31	DPF - Polícia Federal	O pedido foi indeferido usando o Artigo 23, VIII – "comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações." Acesso negado, apesar de questões similares tenham sido feitas ao COMAER e respondidas de forma integral.	1) Quantos drones a Polícia Federal dispõe atualmente? Em que operações eles são atualmente empregados? Quando foram adquiridos? Por qual valor? Quais os contratos de compra? 2) Existe um protocolo ou normativa para o uso desse tipo de equipamento pela PF? 3) Qual o custo de manutenção dos drones atualmente operados pela PF?
32	DPF - Polícia Federal	O pedido foi indeferido usando o Artigo 23, VIII – "comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações." Acesso negado, apesar de questões similares tenham sido feitas ao COMAER e respondidas de forma integral.	Houve aquisições de drones pela PF especificamente para a Copa do Mundo? Quais os modelos, valores e contratos de compra? Qual foi a destinação desses equipamentos assim que o evento se encerrou?
33	DPF - Polícia Federal	O acesso foi negado. Pedido indeferido com base no Artigo 22 da LAI, fazendo menção posterior aos artigos 1° e 3° da Lei n.° 9.883/99 que criou o SISBIN.	1) Quais os protocolos seguidos pela PF para o monitoramento OSINT online e de redes sociais? Quais os critérios necessários para que seja autorizado o monitoramento de um alvo específico em OSINT pela internet? 2) Quando iniciou-se este tipo de trabalho de monitoramento? 3) Quais as instâncias de decisão sobre os alvos do monitoramento online e as plataformas monitoradas?
34	DPF - Polícia Federal	O acesso foi negado. Pedido indeferido com base no Artigo 22 da LAI, fazendo menção posterior aos artigos 1° e 3° da Lei n.° 9.883/99 que criou o SISBIN.	Como é o relacionamento da PF com as plataformas monitoradas (Facebook, Twitter, Google)? Existe cooperação dessas empresas no monitoramento ou cessão de informações dos usuários?
35	DPF - Polícia Federal	A Polícia Federal respondeu dentro do prazo, de forma solícita. As perguntas foram bem respondidas e o acesso foi integral.	1) A PF tem parceria com o CGI.br? Se sim, quais atividades foram desenvolvidas? 2) A PF tem parceria com o NIC.br? Se sim, quais atividades foram desenvolvidas?
36	Secretaria de Segurança Pública do RS	A Secretaria do RS respondeu, via e-mail, de forma clara e objetiva à questão colocada, dando acesso integral à informação.	É fato público a aquisição de imageadores térmicos aéreos pelo Ministério da Justiça para uso durante a Copa do Mundo e, também, que esses imageadores foram repassados aos Estados que foram sede durante a Copa do Mundo. 1)Os imageadores já foram utilizados em manifestações públicas durante a Copa do Mundo?

			2)Qual será a frequência de uso desses imageadores por parte do Estado do Rio Grande do Sul? 3)Para quais finalidades serão usados? 4) Serão usados em manifestações públicas?
37	Secretaria de Segurança Pública de SP	As respostas das perguntas vieram através do SIC da Polícia Militar do Estado. Apesar de dentro do prazo, foram mal formuladas, dando informações insuficientes e não respondendo diretamente aos questionamentos As respostas foram insuficientes e o acesso foi parcial.	É fato público a aquisição de imageadores térmicos aéreos pelo Ministério da Justiça para uso durante a Copa do Mundo e, também, que esses imageadores foram repassados aos Estados que foram sede durante a Copa do Mundo. 1)Os imageadores já foram utilizados em manifestações públicas durante a Copa do Mundo? 2)Qual será a frequência de uso desses imageadores por parte do Estado de São Paulo? 3)Para quais finalidades serão usados? 4) Serão usados em manifestações públicas?
38	Secretaria de Segurança Pública de MG	A resposta veio através da Controladoria Geral do Estado veio de forma completa e o Acesso foi integral.	É fato público a aquisição de imageadores térmicos aéreos pelo Ministério da Justiça para uso durante a Copa do Mundo e, também, que esses imageadores foram repassados aos Estados que foram sede durante a Copa do Mundo. 1)Os imageadores já foram utilizados em manifestações públicas durante a Copa do Mundo? 2)Qual será a frequência de uso desses imageadores por parte do Estado de Minas Gerais? 3)Para quais finalidades serão usados? 4) Serão usados em manifestações públicas?
39	Secretaria de Segurança Pública do PR	A Assessoria da PM do Estado do Paraná respondeu ao pedido dentro do prazo estabelecido. Deu respostas completas, apesar de serem breves. Acesso integral.	É fato público a aquisição de imageadores térmicos aéreos pelo Ministério da Justiça para uso durante a Copa do Mundo e, também, que esses imageadores foram repassados aos Estados que foram sede durante a Copa do Mundo. 1)Os imageadores já foram utilizados em manifestações públicas durante a Copa do Mundo? 2)Qual será a frequência de uso desses imageadores por parte do Estado do Paraná? 3)Para quais finalidades serão usados? 4) Serão usados em manifestações públicas?
40	Secretaria de Segurança Pública do DF	A Ouvidoria da Polícia Civil do DF respondeu ao questionamento. A resposta veio em 22 dias e o acesso foi integral.	É fato público a aquisição de imageadores térmicos aéreos pelo Ministério da Justiça para uso durante a Copa do Mundo e, também, que esses imageadores foram

			repassados aos Estados que foram sede durante a Copa do Mundo. 1)Os imageadores já foram utilizados em manifestações públicas durante a Copa do Mundo? 2)Qual será a frequência de uso desses imageadores por parte do Distrito Federal? 3)Para quais finalidades serão usados? 4) Serão usados em manifestações públicas?
41	Secretaria de Segurança Pública do MT	Não respondido.	É fato público a aquisição de imageadores térmicos aéreos pelo Ministério da Justiça para uso durante a Copa do Mundo e, também, que esses imageadores foram repassados aos Estados que foram sede durante a Copa do Mundo. 1)Os imageadores já foram utilizados em manifestações públicas durante a Copa do Mundo? 2)Qual será a frequência de uso desses imageadores por parte do Estado do Mato Grosso? 3)Para quais finalidades serão usados? 4) Serão usados em manifestações públicas?
42	Secretaria de Segurança Pública do PE	Após resposta exigindo a apresentação de assinatura da responsável pela Artigo 19, foi apresentado recurso declarando a prática como ilegal e reiterando o pedido de informação. Após 5 dias a Secretaria de PE respondeu, dando acesso integral à informação pedida.	É fato público a aquisição de imageadores térmicos aéreos pelo Ministério da Justiça para uso durante a Copa do Mundo e, também, que esses imageadores foram repassados aos Estados que foram sede durante a Copa do Mundo. 1)Os imageadores já foram utilizados em manifestações públicas durante a Copa do Mundo? 2)Qual será a frequência de uso desses imageadores por parte do Estado de Pernambuco? 3)Para quais finalidades serão usados? 4) Serão usados em manifestações públicas?
43	Secretaria de Segurança Pública da BA	Secretaria respondeu aos questionamentos, porém de forma extremamente direta e curta. Acesso integral.	É fato público a aquisição de imageadores térmicos aéreos pelo Ministério da Justiça para uso durante a Copa do Mundo e, também, que esses imageadores foram repassados aos Estados que foram sede durante a Copa do Mundo. 1)Os imageadores já foram utilizados em manifestações públicas durante a Copa do Mundo? 2)Qual será a frequência de uso desses imageadores por parte do Estado da Bahia? 3)Para quais finalidades serão usados? 4) Serão usados em manifestações públicas?

44	Secretaria de Segurança Pública do CE	Secretaria respondeu rapidamente, de forma simples e rápida e sem detalhamentos. O Acesso foi integral.	É fato público a aquisição de imageadores térmicos aéreos pelo Ministério da Justiça para uso durante a Copa do Mundo e, também, que esses imageadores foram repassados aos Estados que foram sede durante a Copa do Mundo. 1)Os imageadores já foram utilizados em manifestações públicas durante a Copa do Mundo? 2)Qual será a frequência de uso desses imageadores por parte do Estado do Ceará? 3)Para quais finalidades serão usados? 4) Serão usados em manifestações públicas?
45	Secretaria de Segurança Pública do AM	Não respondido.	É fato público a aquisição de imageadores térmicos aéreos pelo Ministério da Justiça para uso durante a Copa do Mundo e, também, que esses imageadores foram repassados aos Estados que foram sede durante a Copa do Mundo. 1)Os imageadores já foram utilizados em manifestações públicas durante a Copa do Mundo? 2)Qual será a frequência de uso desses imageadores por parte do Estado do Amazonas? 3)Para quais finalidades serão usados? 4) Serão usados em manifestações públicas?
46	Secretaria de Segurança Pública do RN	Não respondido.	É fato público a aquisição de imageadores térmicos aéreos pelo Ministério da Justiça para uso durante a Copa do Mundo e, também, que esses imageadores foram repassados aos Estados que foram sede durante a Copa do Mundo. 1)Os imageadores já foram utilizados em manifestações públicas durante a Copa do Mundo? 2)Qual será a frequência de uso desses imageadores por parte do Estado do Rio Grande do Norte? 3)Para quais finalidades serão usados? 4) Serão usados em manifestações públicas?
47	Secretaria de Segurança Pública do RJ	Secretaria respondeu que não pode permitir o acesso pela internet. Decreto estadual só permite que acesso se dê através da entrega de formulário disponível no site, devidamente assinado, além de um termo de responsabilidade	É fato público a aquisição de imageadores térmicos aéreos pelo Ministério da Justiça para uso durante a Copa do Mundo e, também, que esses imageadores foram repassados aos Estados que foram sede durante a Copa do Mundo. 1)Os imageadores já foram utilizados em manifestações públicas durante a Copa do Mundo?

		sobre as informações que estão sendo pedidas, o que está em desacordo com a Lei Federal. Acesso negado.	2)Qual será a frequência de uso desses imageadores por parte do Estado do Rio de Janeiro? 3)Para quais finalidades serão usados? 4) Serão usados em manifestações públicas?

Fonte: ARTIGO 19

Análise das informações recebidas

Os órgãos consultados variaram bastante nas respostas quanto à qualidade e à transparência a respeito de alguns temas específicos. É interessante notar, inclusive, padrões de temáticas que não são respondidos ou, quando são, tem respostas evasivas e questionáveis. As respostas ainda levantam diversos tipos de questões sobre as diretrizes do governo brasileiro nas questões de vigilância cibernética e territorial, cibersegurança e controle social.

A seguir, apresentamos uma pequena análise das respostas recebidas. A íntegra das respostas você encontra no site.

Ministério da Justiça

Quando perguntado a respeito dos imageadores térmicos aéreos comprados para a Copa do Mundo, o Ministério da Justiça confirmou e esclareceu a quantidade e destino dos equipamentos: 13, sendo dois para o Rio de Janeiro e um para cada um dos outros 11 Estados sede. Além disso, informou sobre o seu uso em grandes eventos, considerado uma vantagem tática aérea que visa propiciar uma melhor tomada de decisões aonde for empregado, ou seja, maior controle sobre qualquer forma de manifestação social, grandes eventos e inclusive operações de polícia.

Nossa outra solicitação, encaminhada ao Departamento da Polícia Federal (DPF), fazia menção aos Centros de Cooperação Policial Internacional (CCPI), responsáveis pelo monitoramento de torcedores na Copa do Mundo. Para a resposta, foram apresentadas notícias postadas no site do DPF que apresentaram respostas aos questionamentos[135]. Ademais, a resposta foi complementada com a origem dos 205 policiais que viriam ao Brasil durante a Copa, fazendo questão de esclarecer que não seriam detentores de poder de polícia dentro do território nacional.

Ministério da Defesa

Quando perguntando sobre protocolos e critérios em ações de monitoramento OSINT (Open Source Intelligence)[136], o Ministério da Defesa respondeu com argumentações difusas, apelando para questões de interesses nacionais para finalmente se negar a responder integralmente ao pedido[137]. A

135 http://www.dpf.gov.br/agencia/noticias/2014/06/centro-de-cooperacao-policial-reune-250-policiais-de-todo-o-mundo http://www.dpf.gov.br/agencia/noticias/2014/06/pf-inaugura-centro-de-cooperacao-policial-internacional-para-a-copa

136 OSINT é o termo em inglês usado para descrever a inteligência, no sentido de informações, obtida através dados disponíveis para o público em geral, como a internet e mídias tradicionais.

137 As informações solicitadas não correspondem à hipótese de sigilo imposta pelo Ministério da Defesa, uma vez que sua profundidade não compromete atividades específicas de segurança ou inteligência. Procedimentos gerais, protocolos e critérios são informações de controle social - atividade que qualquer instituição pública está sujeita. Não poderiam, portanto, classificar todas as informações relacionadas ao

negação do pedido de informação reforça como é nebulosa a questão do monitoramento de redes na Internet.

Contudo, há afirmações na resposta que levantam questionamentos quanto aos objetivos deste tipo de ação, identificando supostos "interesses do país" como justificativa para monitorar o espaço cibernético e como forma de garantir a "liberdade de ação" da população dentro desse espaço. É interessante notar os traços de vigilantismo na resposta, quando o Ministério da Defesa afirma que "depende diretamente do grau de conscientização alcançado junto às organizações e pessoas acerca do valor da informação que detêm ou processam". A subjetividade contida em uma suposta "conscientização" sobre o que cada um pode ou deve acessar na internet é, de certa forma, alarmante e coloca na mão de órgãos governamentais com diretrizes de ação que não são de conhecimento público a definição sobre o que é de "interesse nacional" e o que pode e deve ser monitorado. Finalmente, com a negação do pedido baseada, segundo a redação da resposta, na "proteção da sociedade" fica clara a orientação do Ministério da Defesa nas questões de vigilância.

Comando do Exército (CEX)

O Comando do Exército esclareceu quais são os critérios para considerarmos um estado iminente de guerra cibernética. De acordo com órgão, a definição de "guerra" é uma ação beligerante entre dois Estados. No Brasil, a declaração e autorização de guerra competem ao Congresso Nacional. Portanto, o estabelecimento dessa condição depende da decisão em nível político e, para demonstrar o processo de tomada de decisão, uma ilustração é apresentada da seguinte maneira

Nível de decisão	Designação	Designação
Político	Segurança cibernética	Gabinete de Segurança Institucional (GSI)
Estratégico	Defesa cibernética (CDCiber)	Ministério da Defesa (MD)
Operacional	Guerra cibernética	Guerra cibernética
Tático		

Fonte: Comando do Exército, tabela contida em resposta do pedido de informação n. 60502000941201428

Como observado, o Centro de Defesa de Cibernética do Ministério da Defesa e do Comando do Exército integra o segundo nível de decisão, o Estratégico. Assim, no primeiro nível de decisão encontra-se o Político, submetido à Presidência da República. Já o terceiro nível entram os níveis operacionais e táticos, já no contexto de uma eventual Guerra Cibernética.

Quando perguntados sobre quais as instâncias de decisão sobre os alvos do monitoramento online e as plataformas monitoradas, o Comando do Exército responde que são adotados em procedimentos internos, mais especificamente no "cumprimento da legislação em vigor", se referindo à Portaria Nº 3.405, do Ministro da Defesa, de 21 de dezembro de 2012, que é consoante com o Decreto da Presidência da República nº6.703, de 18 de dezembro de 2008 que define as diretrizes da política de defesa nacional. Tal resposta, entretanto, é vaga, sem indicação objetiva dos órgãos envolvidos.

O questionamento sobre definição de alvos de seu órgão de defesa cibernética, o CDCiber, também é respondido com a evidente intenção em não determinar responsabilidades sobre as deci-

tema OSINT, mas apenas aquelas estritamente necessárias para garantir a segurança pública. O pedido de informação fundamentou-se no fato de que monitoramentos podem estar sendo usados para cercear a livre manifestação de pensamento e opinião.

sões. Dessa maneira, partem da definição de sua finalidade com a apresentação da legislação, com definições de sua missão e objetivo, para basear suas atividades cotidianas, mostrando claramente a orientação alinhada à resposta do Ministério da Defesa nas orientações vigilantistas.

De tais respostas, depreende-se que a decisão de monitoramentos de eventuais ataques na Internet é uma decisão política, de alto nível, apenas implantada de maneira estratégica pelo CDCiber. Não é possível saber, contudo, quais os limites de ação do CDCiber e nem qual a interpretação do órgão sobre o que influencia na liberdade de ação no espaço cibernético.

O exército brasileiro se negou veementemente a admitir que realizou ou realiza monitoramentos online de redes sociais, movimentos sociais e afins. Mesmo com o envio de notícias, que estão em sua maioria supracitadas, em que diversas vezes o exército é citado realizando algum tipo de monitoramento online, as respostas foram diretas e claras: não há monitoramento por parte do exército. Pode-se inferir, portanto, que ou a mídia está agindo de maneira equivocada nas suas fontes ou que o Comando do Exército está ocultando estas questões. O problema é que fizeram questão de responder a todos os questionamentos, ao invés de se negarem a ceder a informação com base em algum suposto sigilo. É difícil de acreditar que a mídia esteja equivocada, quando até o General do CDCiber dá uma entrevista confirmando as ações do órgão[138]. Indo além, a criação de órgãos como a 4ª Subchefia do COTER indica a crescente atuação do exército no controle social do cenário brasileiro. Com o objetivo preventivo de garantir maior "controle situacional" de operações de contenção de distúrbios, o órgão recebe dados de todos os órgãos que integram o Sistema de Inteligência Brasileiro (Sisbin). O CEX se negou, contudo, a admitir a realização de monitoramentos de movimentos sociais. É interessante notar, também, a temporalidade das movimentações do exército brasileiro, já que a 4ª Subchefia do COTER surgiu no contexto pós-Copa, quando diversas manifestações sociais ainda ocorriam ao redor do país.

Gabinete de Segurança Institucional

O principal responsável pela inteligência do país, através da subordinação da ABIN, se negou a responder cinco dos sete pedidos de informação feitos. As duas únicas respostas foram curtas e apenas negações de questões pontuais relacionadas a parcerias e relacionamento com empresas e outros órgãos. As questões que entraram nos méritos de monitoramento, protocolos, treinamento de agentes e destacamentos para as operações durante a Copa do Mundo foram enquadradas no argumento de que essas informações são sigilosas conforme a legislação vigente.

Para o GSI também foram feitos questionamentos referentes aos Centros Integrados de Comando e Controle, mas nenhuma questão que fez menção a estes foi respondida. Analisando a conjuntura recente, os Centros Integrados de Comando e Controle podem ser considerados o carro-chefe da segurança pública do novo período de governo da reeleita presidenta Dilma Rousseff, fato que já vinha sendo sinalizado desde o final da Copa do Mundo. Isso se daria inicialmente através da implementação dos centros nas 27 capitais e mudanças na constituição, a fim de garantir maior atuação do Governo Federal na segurança pública nacional e integração em ações de segurança dentro do território[139].

138 http://g1.globo.com/tecnologia/noticia/2013/07/exercito-monitorara-redes-sociais-durante-visita-do-papa-e-copa-de-2014.html

139 http://veja.abril.com.br/noticia/brasil/dilma-quer-centros-integrados-de-seguranca-nas-27-capitaishttp://www1.folha.uol.com.br/poder/2014/10/1534145-dilma-fala-em-mudar-constituicao-para-ampliar-papel-federal-na-seguranca.shtml

140 http://veja.abril.com.br/noticia/brasil/dilma-quer-centros-integrados-de-seguranca-nas-27-capitaishttp://www1.folha.uol.com.br/poder/2014/10/1534145-dilma-fala-em-mudar-constituicao-para-ampliar-papel-federal-na-seguranca.shtml

O simples fato de ser uma política de governo deveria garantir que a população pudesse ter acesso aos tipos de operações que estes centros já desenvolvem e pretendem desenvolver. É importante notar também que sistematicamente as ações no âmbito federal foram no sentido de dar apoio em questões de monitoramento. Dessa forma, é importante que mais atenção seja dada a estes Centros, já que dão diversos sinais de que serão empregados em diversas ações de vigilância e monitoramento.

Comando da Aeronáutica

O comportamento do COMAER na redação das respostas foi bastante satisfatório e transparente. Concedeu acesso integral aos pedidos e as respostas foram bem redigidas, com exceção de um pedido em que a resposta de algumas perguntas foi evasiva, porém é possível considerar que o acesso foi integral. Revelaram que Aeronaves Remotamente Tripuladas foram sim usadas em eventos relacionados à Copa do Mundo, além de qualquer operação de apoio. Além disso, informaram todas as aeronaves que a aeronáutica possui além dos seus valores, no total de atuais três e ainda informou que novas aquisições devem ser feitas nos anos conseguintes, o que deve aumentar o poderio brasileiro de vigilância ostensiva.

Departamento da Polícia Federal

A Polícia Federal se negou a dar acesso aos pedidos de informação que tocaram em questões de monitoramento, drones e protocolos. Se limitaram a responder dois dos cinco pedidos. Dois destes foram indeferido com base no Artigo 23, VIII da LAI:

> "(...) comprometer atividades de inteligência, bem como de investigação ou fiscalização em andamento, relacionadas com a prevenção ou repressão de infrações."

Estes pedidos foram negados apesar do fato de que o COMAER respondeu com solicitude à questões similares sobre veículos aéreos não-tripulados. É um indício de que esses órgãos estão trabalhando com diretivas e níveis de privacidade diferentes.
Já o outro pedido negado, relacionado a protocolos de monitoramento, se baseou no Artigo 22 da LAI relacionando-o com ditames da Lei n.º 9.883/99, que criou o SISBIN – Sistema Brasileiro de Inteligência, que é responsável pelo processo de obtenção, análise e disseminação da informação e inteligência brasileiro.

Questões relacionadas ao relacionamento da entidade com empresas privadas e redes sociais foram respondidas rapidamente, revelando que a PF não tem parcerias para investigação com empresas como Google e Facebook. Além disso, expuseram a participação da PF dentro do Comitê Gestor da Internet e do Núcleo de Informação e Coordenação do Ponto BR.

Novamente as questões de monitoramento e vigilância a nível federal são tratadas com sigilo, reforçando a ideia de que o governo brasileiro está agindo deliberadamente para expandir suas operações nesse sentido.

Secretarias Estaduais de Segurança Pública dos Estados

Foram efetuados pedidos de informação aos 12 Estados que sediaram partidas na Copa do Mundo, com o intuito de questionar a respeito do uso dos imageadores recebidos por para uso no evento e seu legado. Parte das perguntas já havia sido feita ao Ministério da Justiça e, dessa forma, os Estados que responderam ao pedido seguiram uma linha de conteúdo similar. É interessante notar que algumas respostas vêm mais definidas e respeitando o ordenamento da pergunta, enquanto outras são respondidas sem necessariamente definir bem qual pergunta em específico está sendo feita. Ademais, algumas Secretarias demonstram mais solicitude em responder as perguntas de forma completa e clara, enquanto outras são mais diretas e tendem a resumir muito mais a resposta.

Todos responderam que confirmam o uso do equipamento durante operações na Copa do Mundo, além disso houve um discurso homogêneo no sentido de melhorar a eficácia da ação em terra de diversos tipos de operações de garantia de ordem pública. Outros diversos usos foram citados partindo desde patrulha, monitoramento e apoio à segurança de eventos públicos até uso para monitoramento de trânsito e ambiental.

Vale menção à resposta dada pela Secretaria de Segurança Pública de Minas Gerais, em que a pergunta sobre o uso do equipamento em manifestações públicas foi respondida de forma minimalista com a frase "respondido na pergunta anterior". Esta resposta dá a entender que o termo "manifestações públicas" se iguala à "atividades relacionadas ao exercício da polícia ostensiva e preservação da ordem pública". Ou seja, tratando manifestações públicas sempre como potencial ameaça à ordem e dando a entender que o uso será constante nesse tipo de situação. Em contraste à essa resposta, a Secretaria de Segurança Pública do Rio Grande do Sul preferiu ser mais cautelosa, afirmando que "o emprego dependerá da avaliação técnica, a ser procedida caso a caso pelas polícias, essencialmente para a proteção da vida".

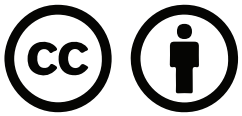
A Secretaria de São Paulo, através da Polícia Militar do Estado de São Paulo, demonstrou muita má vontade nas respostas, concedendo apenas acesso parcial às questões que foram extremamente mal formuladas e redigidas, criando a necessidade de pesquisa dos termos e siglas empregados e, ainda assim, não responderam às perguntas solicitadas. Apesar de confirmarem o recebimento do imageador, se limitaram em todas as perguntas a delimitar como competência das operações do Grupamento de Rádio Patrulha Aérea "João Negrão".

A aquisição de imageadores pelo Ministério da Justiça, repassados aos estados, reitera novamente o desejo do governo federal de ser mais atuante na segurança pública do país como um todo. Além disso, vale ressaltar o caráter recorrente de investimento em equipamentos de vigilância e monitoramento dos espaços físicos brasileiros, capazes de garantir maior eficiência na garantia da ordem. É neste sentido que surge o conflito, justamente com o potencial de uso desses instrumentos para coibir, dispersar e punir manifestações sociais. Através da resposta de muitos dos estados é possível aferir que serão usados para tanto.

REFERÊNCIAS

(DA CRUZ JUNIOR, S. C. A Segurança e Defesa Cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o Espaço Virtual. Brasília, 2013. Disponível em: <http://www.ipea.gov.br/agencia/images/stories/PDFs/TDs/td_1850.pdf>)
http://g1.globo.com/politica/noticia/2014/04/relatorio-final-da-cpi-da-espionagem-aponta-que-brasil-esta-vulneravel.html
http://g1.globo.com/politica/noticia/2013/09/senado-instala-cpi-para-investigar-espionagem-dos-eua-no-brasil.html
http://memoria.ebc.com.br/agenciabrasil/noticia/2013-11-05/cpi-da-espionagem-quer-explicacoes-sobre-841-antenas-dos-eua-no-brasil
http://www.contasabertas.com.br/website/arquivos/584
http://www.contasabertas.com.br/website/arquivos/7943
http://www.abin.gov.br/
http://www3.transparencia.gov.br/TransparenciaPublica/jsp/execucao/execucaoPorNatDespesa.jsf
http://convergenciadigital.uol.com.br/cgi/cgilua.exe/sys/start.htm?infoid=32182&sid=18#.U1_cavldV40
http://www.dct.eb.mil.br/index.php/2013-02-01-13-23-38
http://www.defesanet.com.br/cyberwar/noticia/15155/Governo-ainda-nao-prioriza-seguranca-da-informacao/
http://portal.mj.gov.br/main.asp?ViewID=%7B496D429E-9716-4514-A5FF-E68B415B3608%7D&params=itemID=%7B52DDC406-26C3-4E2B-80A1-CA8B8BFBDCC3%7D;&UIPartUID=-%7B2868BA3C-1C72-4347-BE11-A26F70F4CB26%7D
http://www.defesanet.com.br/cyberwar/noticia/5954/cdciber---centro-de-defesa-cibernetica-inicia-em-junho-
http://www.defesanet.com.br/cyberwar/noticia/14936/CPI-Espionagem-apresenta-Relatorio/
http://www.defesanet.com.br/cyberwar/noticia/15155/Governo-ainda-nao-prioriza-seguranca-da-informacao/
http://www.defesanet.com.br/cyberwar/noticia/1632/CDCiber---Na-guerra-cibernetica--Brasil-adota-estrategia-do-contra-ataque
http://www.defesanet.com.br/cyberwar/noticia/14856/Rustcon---Apresenta-Simulador-de-Operacoes-de-Guerra-Cibernetica/
http://www.revistaforum.com.br/quilombo/2014/01/15/ministerio-da-defesa-aprova-documento-tipico-de-ditadura-militar/
http://memoria.ebc.com.br/agenciabrasil/noticia/2013-02-19/cardozo-diz-que-sinesp-e-um-dos-maiores-legados-de-sua-gestao
http://memoria.ebc.com.br/agenciabrasil/noticia/2013-12-11/ministerio-da-justica-lanca-sistema-que-integra-dados-sobre-seguranca-publica-no-pais
http://www.tecmundo.com.br/brasil/40261-brasil-vai-usar-drones-para-reforcar-seguranca-durante-a-copa-do-mundo.htm
http://www.estadao.com.br/noticias/nacional,documento-da-abin-desmente-ministro-e-confirma-a-vigilancia-de-sindicalistas,1018582,0.htm
http://www.tecmundo.com.br/tecnologia-militar/37801-exercito-deve-receber-r-400-milho-

es-para-prevencao-de-guerra-cibernetica-.htm
file:///C:/Users/Marcelo/Downloads/Port%20%20185%20-%20Curso%20de%20Guerra%20Cibern%C3%A9tica%20para%20Sargentos.pdf
http://www.ccomgex.eb.mil.br/index.php/pt_br/noticias/guerra-cibernetica/risco-cibernetico
http://www.ensino.eb.br/exibeDetalhesCurso.do?curso=683&detalhes=true#como_fazer_sua_inscricao
http://www.bluepex.com.br/blog/?p=323
http://www.decatron.com.br/index.php/o-que-fazemos/
http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document
http://archive.today/7ZIY1#selection-675.49-675.118
http://www.eceme.ensino.eb.br/ciclodeestudosestrategicos/index.php/CEE/XICEE/paper/viewFile/27/41
http://www.adpf.org.br/adpf/admin/painelcontrole/materia/materia_portal.wsp?tmp.edt.materia_codigo=6712#.U4YbX_ldV40
http://www.ip-watch.org/2014/01/08/un-general-assembly-adopts-resolution-on-privacy-and-surveillance/
http://www.portal2014.org.br/noticias/13142/SEGURANCA+NA+COPA+DO+MUNDO+TERA+AUXILIO+INTERNACIONAL.html
http://www.portal2014.org.br/noticias/13312/SEGURANCA+PARA+A+COPA+TEM+157+MIL+AGENTES+E+INVESTIMENTO+DE+R+19+BI.html
http://www.direitoacomunicacao.org.br/content.php?option=com_content&task=view&id=9942
http://olhardigital.uol.com.br/noticia/o-brasil-esta-preparado-para-uma-guerra-virtual/33307
http://sidusmaximusti.blogspot.com.br/2013/03/saiba-como-o-brasil-se-protege-de.html
http://g1.globo.com/politica/noticia/2014/04/relatorio-final-da-cpi-da-espionagem-aponta-que-brasil-esta-vulneravel.html
http://www.ipea.gov.br/agencia/images/stories/PDFs/TDs/td_1850.pdf
http://www.sae.gov.br/site/wp-content/uploads/relatorio_XIIIENEE_ebook.pdf



ARTIGO 19
Defendendo liberdade de expressão e informação

Rua Joao Adolfo, 118 – Cj. 802
CEP: 01050-020 – Centro
São Paulo - SP

Tel: +55 11 3057-0042
http://www.article19.org
https://www.facebook.com/artigo19brasil


ARTICLE19