Artigos Selecionados REDE 2017
I Encontro da Rede de Pesquisa em Governança da Internet
Rio de Janeiro, 14 de Novembro de 2017

A MÍDIA NA GOVERNANÇA MULTISSETORIAL DA INTERNET:

Reflexões após três meses de clipping sobre cibersegurança na mídia *on-line* brasileira

Antonio Gomes de Jesus Neto
Mestre em Geografia Humana pela Universidade de São Paulo (USP)
Assistente de Comunicação na Rede ANSP (An Academic Network at São Paulo)
antoniogjneto@yahoo.com.br

RESUMO

As discussões sobre governança pautam-se, geralmente, no embate entre Estados e corporações. Crescentemente, porém, fala-se de um poder midiático que também governa, e frequentemente esquece-se do papel da ciência nesta composição. A partir disto, considerando a importância que a cibersegurança tem ganhado na política internacional e nacional, realizou-se durante três meses no projeto acadêmico Rede ANSP um levantamento sistemático de reportagens (*clipping*) sobre a temática na mídia *on-line* brasileira. Tal exercício permitiu identificar e articular os principais agentes envolvidos na governança da cibersegurança, bem como refletir sobre o papel da mídia na governança multissetorial da Internet.

PALAVRAS-CHAVE: cibersegurança; governança; mídia; psicosfera; ransomware.

Sugestão de citação (ABNT): SOBRENOME, Nome. **Título do artigo**. I ENCONTRO DA REDE DE PESQUISA EM GOVERNANÇA DA INTERNET, NOVEMBRO DE 2017. Disponível em: <endereço na web>. Acesso em: mês. ano.

INTRODUÇÃO

Há quase 15 anos atrás, Luker e Peterson (2003) já identificavam a reação mais usual da comunidade acadêmica à questão da cibersegurança: para os acadêmicos, não havia nada nos seus computadores que interessasse a um *hacker*, e além disso o ambiente acadêmico seria um ambiente aberto por excelência. O problema, diziam os autores à época, é que não seriam exatamente os dados e informações acadêmicas o objetivo principal desses *hackers*, mas a grande oferta de dispositivos potentes, conectados e desprotegidos que podem ser utilizados para a realização de ciberataques.

Em estudo bem mais recente, a Cisco (2017) reitera os potenciais perigos de uma "cultura acadêmica" (de livre acesso e compartilhamento) à segurança digital de universidades e instituições afins, mas também desmistifica a ideia de Luker e Peterson (2003) de que os dados e informações acadêmicas não estariam sob ameaça cibernética. No estudo, calcula-se que a incidência de *ransomwares*[1] no setor de educação é três vezes mais frequente do que no setor de saúde, e 10 vezes mais frequente do que no setor financeiro, e também são apresentadas notícias recentes da mídia sobre vazamentos de milhões de dados sigilosos de estudantes paulistas em 2017 e adulteração de notas por parte de estudantes mineiros entre 2014 e 2015.

Dada esta urgência em colocar a cibersegurança na ordem do dia para a comunidade acadêmica, a Rede Acadêmica do Estado de São Paulo (conhecida como Rede ANSP, cuja sigla vem do inglês "an Academic Network at São Paulo")[2], enquanto provedora de acesso à Internet às instituições acadêmicas do Estado de São Paulo, e enquanto projeto acadêmico financiado pela Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), elegeu-a como preocupação central no ano de 2017. Tal preocupação, dentre outras atividades, estimulou um levantamento bibliográfico sobre o assunto e "ligou as antenas" para a temática ao longo de todo o ano, não se restringindo apenas às publicações acadêmicas.

Na mídia internacional, desde a eleição de Donald Trump à presidência dos EUA, em 2016, as discussões sobre cibersegurança e política começaram a convergir e ganhar notoriedade, tanto com a divulgação de uma suposta interferência russa nos resultados do pleito[3], quanto com a suspeição de uma invasão sem precedentes da privacidade dos cidadãos eleitores em suas redes sociais para angariar votos

1 S*oftwares* maliciosos que "sequestram" dados de dispositivos conectados à Internet exigindo em troca um "resgate" (*ransom,* em inglês) em criptomoedas, como o bitcoin, para serem acessados novamente.

2 Para mais informações, consultar seu sítio eletrônico disponível no seguinte endereço: www.ansp.br.

(KROGERUS; GRASSEGGER, 2017). No Brasil, reportagens sobre a venda de dados particulares de cidadãos por parte do setor público começam a ser veiculadas (PASTI; PITA, 2017), bem como sobre a interferência de algoritmos na campanha eleitoral de 2018 (MONTEIRO, 2017), fazendo com que, ao menos na mídia, a combinação entre cibersegurança e governança já seja pauta recorrente e cada vez mais importante.

Em meio a estas discussões, em maio de 2017 um evento fundamental relacionado à temática surgiu na mídia de maneira avassaladora, funcionando como um disparador para a pesquisa ora apresentada. Com o advento do *ransomware* que ficou conhecido como WannaCry[4], e com sua ampla cobertura midiática, iniciou-se na Rede ANSP um levantamento sistemático de reportagens (método conhecido como *clipping*) sobre cibersegurança na mídia *on-line* brasileira. Ao longo de três meses, tal exercício permitiu conhecer as principais pautas, os interesses envolvidos e, sobretudo, o papel específico da mídia na discussão sobre a cibersegurança, configurando-a, aparentemente, como um agente central e pouco considerado nas atuais discussões sobre a governança multissetorial da Internet.

O argumento central do presente trabalho está divido em três partes, partindo de uma discussão teórica mais ampla para depois apresentar alguns dados empíricos coletados, e então esboçar uma avaliação crítica do papel da mídia na governança da cibersegurança. No primeiro item, a proposta é apresentar um quadro teórico aproximando as discussões sobre cibersegurança, governança e mídia, embasando assim a leitura a ser feita das reportagens jornalísticas levantadas e apresentadas no segundo item da argumentação. A premissa básica é a de que a mídia não é um agente neutro nas discussões sobre cibersegurança, e que as pautas e narrativas verificadas durante o exercício de *clipping* são guiadas por interesses específicos que, por sua vez, guiam o debate mais geral sobre a questão. Assim, na terceira e última parte do argumento esboça-se uma análise crítica da articulação entre a mídia dita hegemônica e os interesses do setor privado da tecnologia da informação, configurando o que se denominou aqui de “psicosfera corporativa da cibersegurança”.

---

3 Baseada em *hacking* de e-mails e vazamento de dados sigilosos do governo estadunidense. Para mais informações consultar: “Por que os serviços de inteligência dos EUA acham que a Rússia interferiu na eleição de Trump”. BBC Brasil, 07 jan. 2017. Disponível em: <http://www.bbc.com/portuguese/internacional-38525951>. Acesso em: 12 dez. 2017.

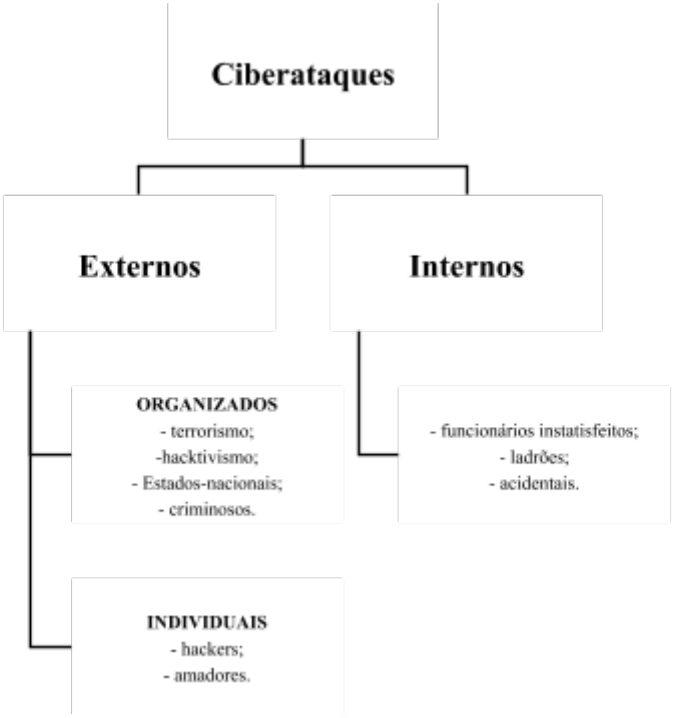
4 Denominação que, além de significar algo como “quero chorar” em português, é uma pequena abreviação do nome do *software* malicioso (um *worm*) que o disseminou: o WannaCryptor.

DESENVOLVIMENTO

Cibersegurança, governança e a mídia: as bases teóricas do *clipping*

Foi apenas no final dos anos 1980 que as primeiras discussões sobre cibersegurança vieram à tona, a partir de sucessivas e distintas invasões computacionais, as quais se convencionou chamar “ciberataques”. Pensando nas motivações por trás destes, Han e Dongre (2014) esboçaram uma tipologia que compreende práticas como espionagem, *hacktivismo*[5]*,* terrorismo, sabotagem, crimes financeiros e motivações individuais, conforme mostra a Figura 1. Em relatório recente, a Verizon (2016) estimou que 89% das atuais ameaças cibernéticas consistem em espionagem e/ou motivações financeiras.

Figura 1: As principais motivações por trás dos ciberataques



Fonte: Adaptado e traduzido de Han e Dongre (2014)

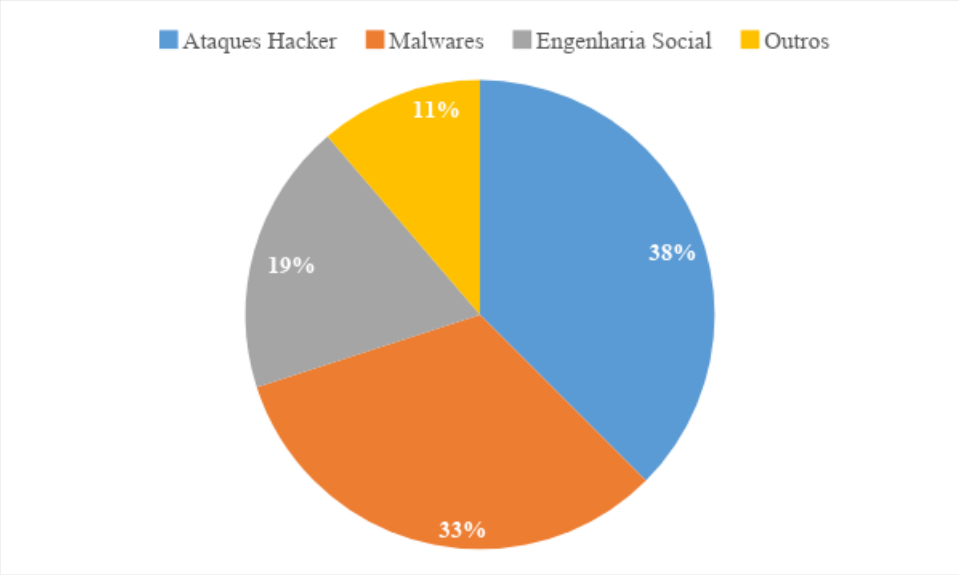
Quanto aos métodos de ciberataques em si, o relatório da Verizon (2016) organizou-os em três grandes categorias, a saber: ataques *hacker, malwares* e engenharia social[6]*.* Ataques *hacker* e *malwares,* que juntos correspondem atualmente a 70% das ameaças (Gráfico 1), diferem basicamente na combinação entre ações

5 Uma junção entre a prática de *hacking* (ação de ataque por parte de um *hacker*) e o ativismo, ou seja, utilizar ferramentas de *hacking* para transformar a sociedade de acordo com os ideais pregados por aquele(s) que executa(m) o(s) ataque(s).

6 No original, em inglês: *hacking*, *malwares* e *social engeneering*, respectivamente.

humanas diretas e ações automatizadas: nos *malwares,* a ação humana consiste fundamentalmente na criação e difusão de *softwares* maliciosos, mas o ataque em si é realizado pelo próprio aplicativo[7]; já no caso dos ataques *hacker*, apesar de geralmente apoiados em ferramentas automatizadas, a ação humana é sempre seu componente principal. A terceira categoria, a de engenharia social, consiste em uma forma de roubar informações confidenciais por meio da interação social, podendo ser, até mesmo, sem recurso a nenhum código ou conhecimento de tecnologia da informação[8].

Gráfico 1: Principais métodos de ciberataques em 2016



Fonte: Verizon (2016)

Pensar a cibersegurança não apenas em seus aspectos técnicos, mas também "como espaço de políticas" (KURBALIJA, 2016, p. 92), exige, contudo, traduzir essa discussão especializada para uma linguagem acessível à sociedade civil, para que ela possa ser debatida em termos de governança - que no caso da Internet é, hoje, baseada no princípio do multissetorialismo (KURBALIJA, 2016)[9]. Para que isso ocorra, são necessárias a criação e difusão de um ambiente dialógico que legitime sua importância e oriente determinadas ações de equacionamento do problema, tornando

7 É nesta categoria que se encaixam os *ransomwares,* como o WannaCry, cujos tipos cresceram 752% em 2016 (TREND MICRO, 2016).

8 Dentre os tipos de engenharia social, destaca-se o método de *phishing*, que traduzindo para o português seria algo como "pescar" ou "jogar uma isca". De maneira geral, práticas de *phishing* envolvem meios de obter informações como senhas ou dados pessoais confidenciais por meio de e-mails ou mensagens falsas em redes sociais, onde "joga-se uma isca" para ver se o usuário "cai no golpe" e cede essas informações.

a cibersegurança, portanto, uma discussão política.

A este ambiente de produção de sentidos, pertencente ao reino das ideias, o geógrafo Milton Santos (1996) denominou “psicosfera”, em complemento ao que seria a dimensão técnica da discussão – a “tecnosfera”. A psicosfera, porém, tem desde um caráter local (transmitido verbal e presencialmente) até o global, cujo alcance varia de acordo com o poder de difusão de informações do transmissor. Neste sentido, ao discutir a ideia de globalização, Santos (2000) fala de uma “violência da informação”, na qual um discurso hegemônico produz um sentido pretensamente universal das ideias, conferindo-lhe um poder igualmente global. Dentre outros agentes, o autor parece falar, também, da mídia.

Ainda que refletindo especificamente sobre o caso estadunidense, Herman e Chomsky (1998) elaboraram um instrumental teórico robusto para explicitar de que maneira a mídia se relaciona com o poder, sistematizando um “modelo de propaganda” com pontos importantes para a discussão ora proposta. Em primeiro lugar, os autores veem os veículos midiáticos hegemônicos como grandes corporações, muitas vezes parte de grandes conglomerados que visam exclusivamente o lucro, em um sistema financiado majoritariamente pela venda de espaços de publicidade. Assim, as pautas veiculadas pela Mídia não teriam o pretenso papel de informar a população, mas sim de responder aos interesses corporativos dela e de seus patrocinadores. Neste sentido, Herman e Chomsky (1998) dizem que a Mídia hegemônica não questiona o poder, mais sim endossa-o, e por sua íntima relação com ele veicula apenas aquilo que lhe interessa, fabricando consensos que formarão a opinião pública e guiarão as decisões políticas, ao invés de investigá-las.

Mesmo com outros agentes tendo também seu quinhão no debate sobre a governança multissetorial (KURBALIJA, 2016), tais decisões políticas parecem ainda ser protagonizadas por Estados e corporações, mas mesmo essa dualidade público-privada começa a apresentar uma possível mudança de status. Se durante muito tempo o debate sobre governança tinha o Estado como personagem central, Antas Junior (2005, p. 65) discorre sobre uma “regulação híbrida do território”, na qual os Estados repartem “porção significativa dessa responsabilidade com grandes corporações transnacionais”. Tal ideia parte, portanto, do princípio de que os agentes estatais e as corporações dividem esta tarefa regulatória, mas atualmente autores como Dowbor (2017, p. 55) entendem que as “estruturas de articulação intercorporativas [...] muito se assemelham a governos no sentido de exercício de

9 De maneira resumida, uma governança multissetorial seria aquela em que diferentes agentes (ou setores) seriam responsáveis por dialogar politicamente em relação a algum assunto de interesse comum, como a Internet. Os agentes do multissetorialismo são usualmente divididos em: governos, setor privado, terceiro setor, comunidade técnica/científica e sociedade civil.

poder político direto", e por isso já se fala em termos de uma "governança corporativa"[10].

Como tais corporações dependem de uma psicosfera robusta para validar seu paradigma de governança, é possível supor, baseado em Herman e Chomsky (1998), uma aliança de interesses entre elas e a mídia na criação desta psicosfera. Trazendo a discussão para o atual cenário de ameaças cibernéticas, e considerando o poder das grandes corporações de tecnologia da informação no mundo contemporâneo, a mídia hegemônica construiria então uma "psicosfera corporativa de cibersegurança"[11] que fabricaria consensos discursivos na opinião pública, endossando os interesses destas corporações. É diante deste quadro teórico que buscou-se ler as reportagens e pautas levantadas no *clipping* sobre cibersegurança realizado ao longo de três meses na mídia *on-line* brasileira.

O *clipping* em si: eventos e pautas principais ao longo de três meses

O dia 12 de maio de 2017 foi um ponto de inflexão na discussão midiática sobre cibersegurança. Foi neste dia que, a princípio timidamente, começaram a ser veiculadas na mídia nacional e internacional as primeiras informações sobre um ciberataque em escala mundial que, aparentemente, havia sequestrados dados e paralisado parcialmente as operações de centenas de empresas e órgãos governamentais em vários países. Em pouco tempo, o *ransomware* que ficou amplamente conhecido como WannaCry tomou conta dos noticiários pela ameaça que representava para o mundo da Internet, e com seu advento decidiu-se monitorar esta cobertura midiática não apenas para entender o que se passava, mas também para perceber de que maneira a discussão sobre cibersegurança era realizada para além de um seleto grupo de especialistas no assunto. Para tal, o primeiro passo era delimitar os veículos midiáticos que seriam monitorados.

O principal desafio na escolha destes foi manter um equilíbrio entre a chamada mídia hegemônica brasileira, que pelo seu alcance aparece como fundamental na criação e manutenção de uma psicosfera de cibersegurança, e alguns veículos midiáticos mais críticos e/ou independentes[12], que forneceriam um possível contraponto às discussões e opiniões mais consensuais. Em relação à primeira, a escolha de portais como UOL, G1 e R7, bem como jornais e revistas impressos com

10 Antas Jr (2005) fala de "hegemonia corporativa", possibilitando uma discussão sobre se a expressão "governança corporativa" representaria uma mudança real de paradigma, ou se apenas resgataria o vocabulário neoliberal do final dos anos 1980 e início dos 1990.

11 Adaptando a ideia de Santos (1996)

12 Não necessariamente contra-hegemômicos.

versões *on-line* bastante relevantes[13], parecem dar conta dos grandes grupos que encabeçam a lista do estudo "Quem controla a mídia no Brasil?"[14]. Dentro destes grandes portais (mas não só), procurou-se também levantar reportagens em veículos *on-line* dedicados à tecnologia, que trariam uma contribuição mais especializada à discussão, como: UOL Tecnologia, Convergência Digital e Olhar Digital (os três dentro do portal UOL); TechTudo (G1); Baboo (R7) e Tecmundo (independente destes grandes portais). Para contrapor esse discurso hegemônico sobre cibersegurança, foram selecionados também veículos teoricamente mais críticos, tanto em versões *on-line* de jornais e revistas impressos – como o jornal El País[15] e a revista Carta Capital -, quanto em portais exclusivamente *on-line* que funcionam de maneira mais independente, como é o caso dos portais Outras Palavras e Nexo.

Assim, em resumo, foram 17 os veículos selecionados, entre hegemônicos, especializados, críticos e/ou independentes: UOL, G1, R7, UOL Tecnologia, Convergência Digital (UOL), Olhar Digital (UOL), TechTudo (G1), Baboo (R7), Tecmundo, Folha de São Paulo, O Estado de São Paulo, Valor Econômico, El País, Carta Capital, Veja, Outras Palavras e Nexo.

Inicialmente pensado para acompanhar apenas a cobertura do *ransomware* WannaCry, verificou-se durante a execução do *clipping* que a cibersegurança adquirira importância crescente na pauta semanal destes veículos, de modo que paralelamente ao *clipping* relacionado ao WannaCry iniciou-se também um *clipping* semanal de notícias sobre cibersegurança nos veículos escolhidos, com 12 semanas (ou três meses) de duração. Com os dois exercícios em andamento, em cerca de 45 dias um novo *ransomware,* noticiado como Petya/NotPetya[16], entrou em pauta na mídia, cuja cobertura também foi contemplada por um terceiro trabalho de *clipping*. Cada um destes três esforços (WannaCry, *clipping* semanal e Petya/NotPetya) teve, porém, durações e metodologias próprias, que foram resumidos na Tabela 1:

13 Como os jornais Folha e Estado de São Paulo, o jornal Valor Econômico e a revista Veja.

14 Realizado pela ONG internacional Repórteres Sem Fronteiras e pelo coletivo brasileiro Intervozes, o "Media Ownership Monitor Brazil" pode ser acessado detalhadamente em https://brazil.mom-rsf.org/br/.

15 Que apesar de ser um jornal espanhol, produz hoje conteúdo relevante em seu portal brasileiro, do qual se coletou as reportagens contabilizadas neste *clipping*.

16 Assim estranhamente batizado pela semelhança com um *ransomware* chamado Petya, surgido e desaparecido em 2016, e que para diferenciá-lo deste ficou conhecido como Not Petya (ou ExPetr).

Tabela 1: Trabalhos, métodos e períodos de *clipping* sobre cibersegurança na mídia *on-line* brasileira

Evento/Trabalho	Método	Semanas (2017)											
		1	2	3	4	5	6	7	8	9	10	11	12
WannaCry	Narrativo	12/5			12/6								
Clipping Semanal	Palavras-chave/Pautas	17/5											11/8
Petya/NotPetya	Minuto-a-minuto						27/6	9/7					

Fonte: Elaboração própria

No primeiro *clipping,* relacionado ao *ransomware* WannaCry, realizou-se um método “narrativo”, organizando as reportagens a partir do cruzamento das datas de publicação com os temas abordados, visando entender a construção do discurso midiático hegemônico sobre os ciberataques provocados por este *ransomware*. Já no segundo trabalho, de *clipping* semanal, elegeram-se algumas palavras-chave de pesquisa, combinando conhecimento prévio sobre o assunto com experiências empíricas de trabalho, quais sejam: *hacker,* vírus, *malware, phishing, ransomware,* cibersegurança, ciberataque e cibernético. A partir das reportagens levantadas, seguiu-se um esforço, semelhante ao anterior, de classificação de pautas, mas agora com o intuito de entender similaridades e diferenças na pauta cotidiana sobre cibersegurança. Por fim, quando do advento do ciberataque Petya/NotPetya, repete-se a experiência narrativa realizada com o WannaCry, mas a avalanche inicial de notícias relacionadas ao evento acaba direcionando a organização das reportagens em um método “minuto-a-minuto”, ou seja, diário, mostrando a importância que, rapidamente, a cibersegurança adquiriu na pauta da mídia *on-line* brasileira pesquisada.

Durante a ocorrência do WannaCry, foram levantadas 106 reportagens em apenas um mês, organizadas inicialmente em 18 pautas específicas, posteriormente reorganizadas em outras quatro pautas gerais, como se vê na Tabela 2. Após uma apresentação inicial aparentemente neutra de *fatos e dúvidas*, identificam-se os *personagens* envolvidos no evento do WannaCry: entre um jovem britânico – funcionário de uma empresa estadunidense – que “desarmou” a ameaça, um grupo *hacker* que assumiu a autoria, e uma rotineira suspeição ao governo norte-coreano, transparece um embate discursivo e geopolítico em que a Agência Nacional de Segurança dos EUA (NSA), o governo chinês e outros agentes são manipulados de acordo com a orientação política do veículo midiático.

Tabela 2: Pautas e contagem de reportagens sobre o *ransomware* WannaCry (12/05 a 12/06/2017)

Pautas gerais	Pautas específicas (18 no total)	Reportagens
Fatos e dúvidas	Surgem as primeiras notícias: o que aconteceu, o que se sabe?	4
	Algumas explicações: o que é um ransomware? O que são Bitcoins?	4
	Os mapas e o alcance mundial do WannaCry	3
	A contabilização dos estragos	5
CURVA TEMPORAL: O WannaCry parece perder força		3
Personagens	Vitima ou (ir)responsável? O envolvimento da NSA	3
	Aparece o 'herói"!	4
CURVA TEMPORAL: A possível volta do WannaCry		4
Personagens	A China entra em cena	2
Análises e Consequencias	Afinal, o WannaCry conseguiu o que queria?	4
	A comunidade se preocupa com a cibersegurança	6
Personagens	Suspeita-se do culpado de sempre: a Coréia do Norte	7
	WannaCry, Windows e a pirataria na China, Rússia e Índia	5
Análises e Consequências	Passada a tempestade, hora de entender o que aconteceu	8
	E agora, o que fazer?	11
CURVA TEMPORAL: Passando o bastão: um novo ciberataque em curso		13
Análises e Consequências	O mundo pós-WannaCry	10
Personagens	Novos e velhos culpados voltam à pauta	7

Fonte: Elaboração própria

Desponta-se, assim, uma disputa narrativa "oculta" levada a cabo pelos veículos de mídia, desaguando na terceira grande pauta geral, das *análises e consequências* do ciberataque – intercalada temporalmente com a dos *personagens*. Frequentemente considerada "neutra", é nesta pauta que a mídia fabrica consensos discursivos hegemônicos (HERMAN; CHOMSKY, 1998), guiando a psicosfera da cibersegurança via "opinião de especialistas". Entre estas três pautas principais – "fatos e dúvidas", "personagens", "análises e consequências*"* –*,* surge periodicamente uma pauta denominada *curva temporal*, que mostra o movimento do evento em perspectiva cronológica: rapidamente o WannaCry parece perder força, ressurgindo dias depois até que um novo ciberataque[17] parece tomar seu lugar na pauta midiática. É aqui, aliás, que é publicado o maior número de reportagens por pauta, dados também apresentados e destacados na Tabela 2.

Disparado pelo esforço de *clipping* do WannaCry, o *clipping* semanal de notícias sobre cibersegurança tem, no final do evento anterior, um ponto de inflexão (Gráfico 2). Se, até o final das ocorrências do WannaCry, o número de reportagens semanais sobre cibersegurança raramente passa de 80, na semana subsequente elas se aproximam de 100, chegando ao pico de 123 na 11ª semana. Com 1.090 reportagens levantadas em 12 semanas, o esforço de sistematização destas em

17 Batizado de Adylkuzz.

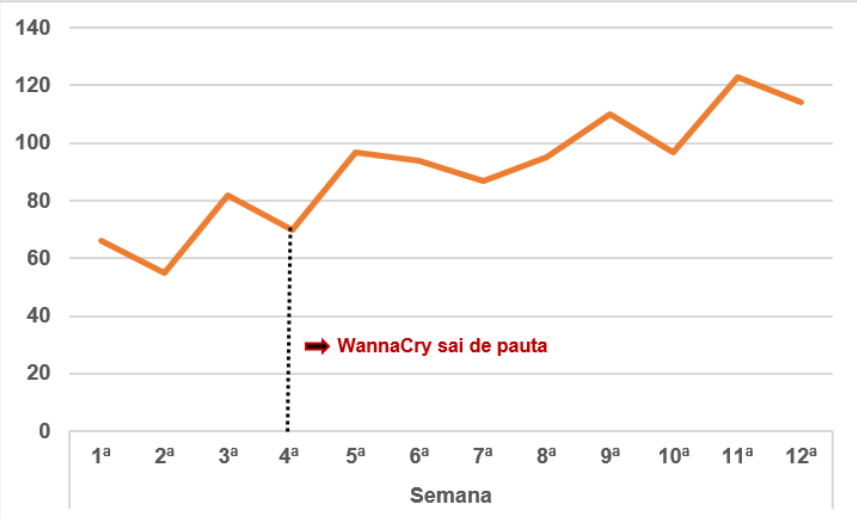
pautas procurou recorrências e efemérides no atual cenário da cibersegurança no Brasil, de modo que cinco pautas estão presentes em todas as semanas de *clipping.* Pautas como “análises gerais” e “dicas e ferramentas de segurança” reforçam o já citado papel da mídia *on-line* na construção da psicosfera brasileira de cibersegurança, e reportagens sobre “dados, privacidades, vigilância e espionagem” são praticamente diárias, envolvendo geralmente Estados e corporações de tecnologia da informação[18]. Na pauta “ciberataques semanais” parece clara a ameaça representada por *ransomwares, phishing* e ataques DDOS[19]. Fechando a lista das principais pautas estão as reportagens sobre “moedas virtuais”, que na esteira dos *ransomwares* que as utilizam como pagamento de resgate, surgem ao mesmo tempo como ameaça à estabilidade da segurança cibernética no Brasil e como possibilidade tecnológica de segurança para os bancos e o mercado financeiro.

Na metade do *clipping* semanal (6ª semana), o *ransomware* Petya/NotPetya vira pauta na mídia *on-line* brasileira, saindo, contudo, na mesma velocidade frenética com que entra. Com uma explosão de notícias no primeiro dia de aparição (44, ao todo), em pouco tempo este número despenca (como pode ser visto no Gráfico 3), tendo desaparecido da pauta em 13 dias com 115 reportagens publicadas no total – mais, portanto, do que o WannaCry, em menos da metade do período. Mesmo assim, o Petya/NotPetya serviu, como seu antecessor, para alavancar ainda mais o número de reportagens levantadas no *clipping* semanal, colocando de uma vez por todas a cibersegurança na ordem do dia da mídia *on-line* brasileira.

18 Tais como governos de Brasil, China, EUA, Israel, Reino Unido e Rússia, bem como as empresas Avast, Facebook, Google, Kaspersky e Microsoft.

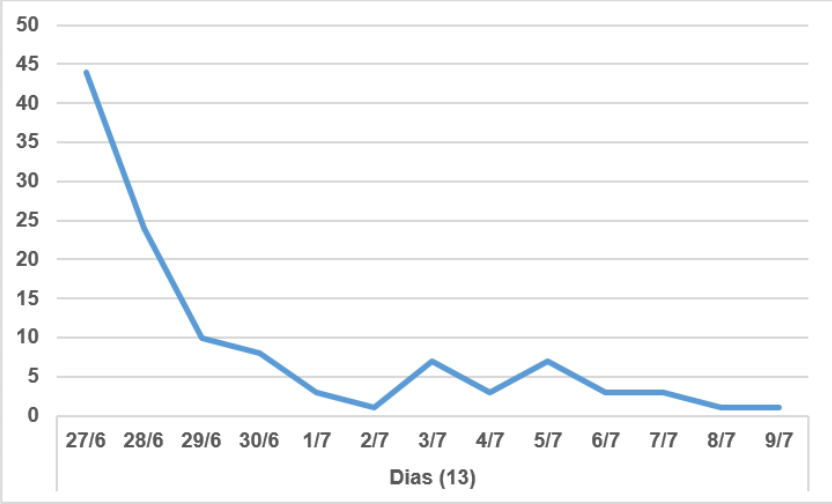
19 Os ataques DDOS (ou *distributed denial of service,* em inglês) são os chamados “ataques de negação de serviço”, quando uma grande quantidade de dispositivos (geralmente *hackeados* e controlados por um computador-mestre) acessa, ao mesmo tempo, determinado servidor *web* para tornar seus recursos indisponíveis por sobrecarga.

Gráfico 2: Reportagens publicadas sobre cibersegurança no *clipping* semanal (17/05 a 11/08/2017)



Fonte: Elaboração própria

Gráfico 3: A queda brusca e diária de notícias sobre o *ransomware* Petya/NotPetya em 13 dias (27/06 a 09/07/2017)



Fonte: Elaboração própria

De maneira geral, os *ransomwares* WannaCry e Petya/NotPetya guardam entre si semelhanças e diferenças. De maneira semelhante, ambos os ataques tiveram como fonte principal um *exploit*[20] do Windows conhecido como *Eternal Blue,* descoberto pela Agência Nacional de Segurança dos EUA (NSA) e vazado pelo grupo *hacker* Shadow Brokers. Além disso, ambos supostamente não conseguiram arrecadar o esperado em *bitcoins* exigidos para resgate – ainda que se questione se

20 Uma vulnerabilidade de *software*.

seria este o principal objetivo de sua ação –, e durante os dois eventos governos e corporações trocaram acusações sobre a responsabilidade pelo ocorrido. Somando-se WannaCry e Petya/NotPetya, foram afetadas empresas privadas como a espanhola Telefónica, a francesa Renault e a estadunidense FedEx, bem como instituições públicas brasileiras (o Tribunal de Justiça e o Ministério Público do Estado de São Paulo, o INSS e o Hospital do Câncer de Barretos), britânicas (sobretudo o serviço de saúde), russas (bancos e ministérios) e alemãs (a empresa ferroviária nacional). Dentre as principais diferenças entre ambos, destacam-se uma maior abrangência geográfica do Petya/NotPetya e, sobretudo, uma diferença criptográfica básica: no caso do WannaCry, apenas a criptografia do arquivo afetado era alterada, enquanto no caso do Petya/NotPetya, setores-chave do disco eram danificados, fazendo alguns especialistas considera-lo não apenas um *ransomware,* mas um *malware* destruidor de dados sem recuperação (PRESCOTT, 2017).

Para além de uma contabilização de notícias e de um entendimento dos fatos, constatou-se também durante os exercícios de *clipping* uma questão fundamental relacionada ao papel da mídia na governança da Internet: frequentemente, uma mesma reportagem foi publicada, senão literalmente, mas com pequenas mudanças, por diversos veículos da mídia *on-line* brasileira, repetição explicada nos próprios cabeçalhos das reportagens. Grandes agências transnacionais e internacionais[21] (grandes corporações midiáticas) distribuem uma quantidade relevante de pautas a serem publicadas na mídia *on-line* brasileira, projetando na psicosfera de cibersegurança brasileira um discurso hegemônico externo sobre o assunto e dificultando a criação de discursos, teorias e políticas nacionais sobre a questão. É sobre a atuação destas agências transnacionais e internacionais de notícias na governança da cibersegurança (e da Internet) no Brasil, articuladas com os veículos midiáticos hegemônicos nacionais, que se debruçará o último item deste trabalho.

A mídia e a psicosfera corporativa de cibersegurança: um agente da governança?

Apesar de robusto e contemporâneo, o instrumental teórico de Herman e Chomsky (1998) utilizado até aqui, relacionando mídia e poder, não é necessariamente uma abordagem inovadora. Albuquerque (2009), por exemplo, retoma a epistemologia desta ideia e busca identificar algumas particularidades

21 Pasti (2013) entende como transnacionais as agências que, embora consideradas empresas globais, mantém uma forte ligação com seus países-sede, como a Agence France-Presse (AFP, da França) e a Thomsons-Reuters (articulando Inglaterra, Canadá e EUA). No caso das internacionais, apesar de não abordadas pelo autor, pode-se considerar aquelas de alcance global ligadas diretamente com seu Estado de origem, como a agência pública britânica British Broadcasting Corporation (BBC).

nacionais da discussão: na tradição liberal britânica, a mídia é entendida como um contra-poder que questiona as decisões políticas e serve aos cidadãos[22]; na tradição estadunidense, ela é mais um ramo (do inglês “branch”) do governo; e no Brasil, para o autor, ela seria um superpoder “transcendental e moderador”. Em todos os casos, porém, é possível identificar uma mesma tradição em relacionar mídia e poder, sendo este o ponto de partida para entender seu lugar na governança da cibersegurança.

Apesar de declaradamente entender a mídia como o contra-poder da tradição liberal britânica, Galan-Gamero (2013) reconhece, porém, que a origem do que hoje se convencionou chamar de mídia remete a ideia, datada do século XVI, de “comércio de informações”[23]. Apesar de um interstício onde o autor defende que a mídia tenha se tornado um serviço de informação aos cidadãos, hoje, com a fusão dos meios de comunicação possibilitados pela Internet (texto, imagem, áudio e vídeo), fundiram-se também os veículos em grandes grupos midiáticos e/ou agências transnacionais e internacionais de notícias, retomando assim o viés eminentemente comercial dos primórdios da imprensa.

Segundo Pasti (2013, p. 31), as agências transnacionais de notícias “existem há quase dois séculos e desde o início de sua atuação vêm exercendo funções de comando nos círculos de notícias ao redor do mundo”. Nascidas “da necessidade de informações imediatas sobre a situação nos demais locais para a realização das atividades financeiras (NABARRO; SILVA, 2012, p. 67)”, tais agências sempre estiveram imiscuídas com o poderio econômico de sua época, mantendo relações estreitas com seus Estados de origem. Agências transnacionais, como a AFP e a Thomson-Reuters, e internacionais, como a BBC, “possuem redes próprias de escritórios e jornalistas, coletam informações de lugares distribuídos pelo mundo e vendem notícias às principais empresas de mídia, a governos, a investidores e a outros agentes (PASTI, 2013, p. 32)”, dotando-as, assim, de grande poder ao produzir uma psicosfera de dimensões globais.

Ao longo do exercício de *clipping* sobre cibersegurança que orienta este trabalho, é considerável a quantidade de reportagens produzidas, e muitas vezes publicadas em mais de um veículo de mídia *on-line* no Brasil, por estas agências citadas. É possível ter uma dimensão quantitativa destas reportagens na Tabela 3:

---

22 Noção mais difundida, e diametralmente oposta à argumentação de Herman e Chomsky (1998).

23 Entendimento reiterado e aprofundado no documentário “O Mercado de Notícias”, de Jorge Furtado.

Tabela 3: Quantidade de reportagens produzidas por diferentes agências internacionais de notícias durante os exercícios de *clipping* realizados de 12/05 a 11/08/2017

Agências	*Clipping* semanal		WannaCry	Petya/NotPetya
	Notícias	Multi-veículos	Notícias	Notícias
Reuters	82	26	7	11
BBC	10	8	4	0
AFP	8	0	4	0
Outras*	10	0	0	0

*Bloomberg, Financial Times, Deutsche Welle, New York Times, Folhapress, EFE, Dow Jones

Fonte: Elaboração própria

Dada a discussão estabelecida sobre a atuação da mídia como um agente do poder – independente do papel que se atribui a ela -, e dada a relevância destas grandes corporações midiáticas[24] na produção de conteúdo sobre cibersegurança na mídia *on-line* brasileira, é possível inferir que a mídia hegemônica cria, muitas vezes referendando um discurso externo, uma "psicosfera corporativa de cibersegurança" na Internet brasileira. Nesta psicosfera, cujas pautas "condicionam o debate público, a política e a cultura (PASTI, 2013, p. 151)", Estados como China e Rússia, e mesmo o governo dos EUA, são geralmente os únicos mencionados em casos de vigilância e espionagem, isentando as grandes corporações de suas responsabilidades[25].

Nas pautas principais e emergentes identificadas ao longo do *clipping* semanal, fica clara também a convergência entre o conteúdo publicado e os interesses corporativos desses grandes conglomerados de tecnologia da informação. Como afirma Pasti (2013, p. 148), "os agentes midiáticos, em especial as agências, inserem na psicosfera valores, preocupações e pautas ligadas [...] aos interesses de agentes hegemônicos — que são seus clientes", e portanto, "para além de uma leitura reducionista ou conspiratória, é necessário compreender que trata-se de um mercado de notícias, movido pelos interesses econômicos (e políticos) desses agentes (p. 147)".

Assim, as "dicas e ferramentas de segurança", quase invariavelmente, apontam como solução algum produto ou serviço oferecido por uma empresa de tecnologia da informação, que apesar de aparentemente servir às necessidades dos usuários de Internet, é na verdade uma forma bem clara de publicidade, como Galan-Gamero (2013) reconhece existir desde os primórdios da imprensa. Da mesma forma, as "análises gerais" realizadas por "especialistas" geralmente depositam as esperanças

24 Apesar do caráter público da BBC.

25 Em contraposição à mais conhecida noção de vigilância e espionagem exclusivamente estatal, Zuboff (2015) cunhou o conceito de "capitalismo de vigilância", onde a extração e análise de dados coletados por corporações como o Google são também mecanismos de vigilância e espionagem que ameaçam seriamente a privacidade dos usuários de Internet.

sobre o desenvolvimento técnico realizado pelo setor privado, e quando os Estados entram em cena, são geralmente criticados por suas falhas, raras vezes discutindo-se a responsabilidade das corporações de tecnologia da informação neste cenário de ameaças cibernéticas. Igualmente, a preocupação parece muito maior nas reportagens em que as ameaças recaem sobre os prejuízos financeiros que as empresas podem sofrer. No caso de reportagens em que as desenvolvedoras têm seus dispositivos de IoT[26] hackeados, ou as prestadoras de serviços *on-line* têm seus dados vazados, a preocupação é maior do que nos casos em que os usuários (enquanto cidadãos, e não consumidores) têm sua privacidade ameaçada.

No caso do *clipping* sobre os *ransomwares* WannaCry e Petya/NotPetya, a ameaça financeira representada pelo sequestro de dados, mais do que alavancar a quantidade de reportagens publicadas sobre cibersegurança, alavancou sobretudo uma (necessária, diga-se de passagem) economia de proteção que beneficia a indústria de segurança cibernética, com reiteradas análises sobre a vulnerabilidade digital de empresas, instituições e usuários, reforçando a necessidade de se investir em *softwares* e dispositivos mais protegidos. Assim, e pensando novamente na psicosfera como um ambiente de produção de sentidos, a iconografia desta cobertura midiática sobre os *ransomwares* ilustra, como na Figura 2, uma ameaça distópica e sombria, aparentemente descolada da realidade, fazendo com que a audiência da mídia *on-line* brasileira seja envolta pela necessidade de segurança de uma maneira bastante maniqueísta e um tanto superficial.

Figura 2: Iconografia do *clipping* sobre os *ransomwares* WannaCry e Petya/NotPetya

Fonte: Elaboração própria a partir das reportagens levantadas

Desta maneira, alimentada por agências de notícias internacionais e por conglomerados midiáticos nacionais (os grupos que “controlam a mídia” no Brasil), a

26 Internet of Things, em inglês, ou Internet das Coisas, em português.

mídia *on-line* brasileira hegemônica atua como um agente quase “oculto” da governança da cibersegurança no país, fabricando consensos discursivos através da criação de uma psicosfera que, pela proximidade com as corporações de tecnologia da informação, funciona como um dos pilares da chamada governança corporativa. Neste sentido, no caso da governança da cibersegurança (que pode ser ampliada para a governança multissetorial da Internet de modo geral), a mídia não seria o contra-poder da tradição liberal britânica, nem um ramo do governo como na tradição estadunidense, mas sim endossaria um poder corporativo através da formação transversal da opinião pública na Internet, aproximando, portanto, as discussões de Herman e Chomsky (1998), Dowbor (2017) e Albuquerque (2009).

CONCLUSÕES (E REFLEXÕES)

Obviamente não se questiona aqui a indiscutível preocupação com as atuais ameaças cibernéticas por parte de todos os setores que compõem a governança da Internet, desde os Estados e corporações, passando pela comunidade científica até (e principalmente) os próprios usuários. O objetivo neste trabalho é, sobretudo, chamar a atenção para a urgência em se considerar a mídia como mais um destes agentes na governança multissetorial da Internet, com funções e responsabilidades próprias, e que, no caso da cibersegurança, com o avanço da noção de governança corporativa, atua, junto ao setor privado, para criar uma psicosfera que muitas vezes vilaniza ou culpabiliza outros agentes.

A despeito da função que se atribua a ela, historicamente a mídia sempre foi entendida como uma forma de manifestação de poder, e ao longo dos diferentes exercícios de *clipping* realizados pareceu explícito o seu alinhamento com os interesses das corporações de tecnologia da informação em relação às discussões sobre cibersegurança. Desde as análises de especialistas, passando pelas dicas e ferramentas sugeridas, pelas narrativas construídas em torno dos eventos de *ransomware*, até chegar às articulações mais estruturais da mídia hegemônica e das grandes agências de notícias, em vários aspectos identificados nas reportagens levantadas é possível verificar uma convergência discursiva entre o que interessa a essas corporações e o que diz a mídia *on-line* brasileira (sobretudo a hegemônica). Assim, longe de ser um agente neutro na governança da cibersegurança, a psicosfera corporativa que essa mídia hegemônica constrói tem um papel fundamental nas disputas narrativas (e consequentemente políticas) com outros setores envolvidos na questão, como os governos, a comunidade científica e a sociedade civil. Assim, faz-se coro aqui à discussão sobre a necessidade de regulação da mídia, que ao contrário de uma censura, apenas responsabilizaria os veículos midiáticos pelo poder que

indiscutivelmente eles possuem de formar a opinião pública.

Para além da mídia, porém, certamente os outros agentes da governança multissetorial da Internet precisam assumir suas responsabilidades perante o atual cenário de ameaças cibernéticas. Considerando a informação como um dos principais, senão o principal ativo de poder contemporâneo (BESSA, 2014), como, então, equacionar a enorme e crescente quantidade de dados e algoritmos em posse de corporações privadas a uma ainda necessária regulação estatal? É possível uma maior transparência em relação ao teor e ao uso destes elementos que colocam em risco a privacidade e a segurança dos usuários da Internet, tal como colocado por Zuboff (2015)?

Quanto à comunidade científica, o principal desafio parece, também, o equacionamento entre um discurso especializado que vê no desenvolvimento técnico a panaceia para a contenção de ciberataques e um discurso crítico que, sem esquecer a dimensão técnica do problema, também não perde de vista as relações de poder envolvidas neste desenvolvimento. Neste sentido, iniciativas acadêmicas multissetoriais como a Rede ANSP (que além da academia, trabalha também conjuntamente com os setores público e empresarial) são um modelo interessante para discutir a cibersegurança no âmbito científico, levando em consideração, com uma visão mais crítica e totalizante, as dimensões políticas e técnicas da questão.

Por fim, frequentemente ignorados como responsáveis pela difusão e contenção de ciberataques e indiscutivelmente visados como alvo de espionagem, vigilância e vazamento de dados, a maior capacitação dos próprios usuários da Internet parece fundamental para uma maior capilaridade das estratégias de cibersegurança. Em um mundo onde o acesso a informações em rede é cada vez mais ubíquo e presente no dia-a-dia da população mundial, habilidades em linguagem de programação – cruciais para o entendimento do que as ameaças cibernéticas representam – não podem mais ser consideradas tarefas de especialistas, e sim incorporadas ao cotidiano mais banal dos usuários da Internet. Só assim a compreensão da criptografia e das suas potencialidades como protetora da privacidade dos cidadãos poderão ser plenamente exploradas, sem que para isso os usuários sejam dependentes de soluções comerciais elaboradas pelo setor privado e difundidas pela mídia como parte das estratégias de *marketing* ligas à publicidade e à propaganda.

REFERÊNCIAS

ALBUQUERQUE, Afonso de. As três faces do Quarto Poder. **ENCONTRO ANUAL DA COMPÓS**, XVIII, 2009, Belo Horizonte. *Anais...* Belo Horizonte : PUC-MG, 2009. p. 1-13.

ANTAS JUNIOR, Ricardo Mendes. **Território e regulação: espaço geográfico, fonte material e não-formal do direito**. São Paulo : Humanitas, 2005.

BESSA, Jorge. **O escândalo da espionagem no Brasil: o caso Snowden**. Brasília : Thesaurus, 2014.

BRITISH BROADCASTING CORPORATION (BBC). Por que os serviços de inteligência dos EUA acham que a Rússia interferiu na eleição de Trump. **BBC Brasil**, 07 jan. 2017. Disponível em: <http://www.bbc.com/portuguese/internacional-38525951>. Acesso em: 12 dez. 2017.

CISCO. **Cibersegurança no setor de Educação no Brasil**. 2017. Disponível em: <https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/witb/1514454/PDF.pdf>. Acesso em 28 set. 2017.

DOWBOR, Ladislau. **A era do capital improdutivo: a nova arquitetura do poder – dominação financeira, sequestro da democracia e destruição do planeta**. São Paulo : Outras Palavras & Autonomia Literária, 2017.

GALAN-GAMERO, Javier. Cuando el 'cuarto poder' se constituye em cuarto poder: propuestas. **Palabra Clave**, v. 17, n. 1, p. 150-185, mar. 2014.

HAN, Chen; DONGRE, Rituja. Q&A: what motivates cyber-attackers? **Technology Inovation Management Review (TIM Review), Carleton University, Ottawa**, v. 4, n. 10, p. 40-42, out. 2014. Disponível em <https://timreview.ca/sites/default/files/article_PDF/HanDongre_TIMReview_October2014.pdf>. Acesso em 16 set. 2017.

HERMAN, Edward; CHOMSKY, Noam. **Manufacturing consent: the political economy of the mass media.** New York : Pantheon Books, 1998.

KROGERUS, Mikael; GRASSEGGER, Hannes. Big data: toda democracia será manipulada? **Outras Palavras**, 05 fev. 2017. Disponível em: <http://outraspalavras.net/posts/big-data-toda-democracia-sera-manipulada/>. Acesso em 12 dez. 17.

KURBALIJA, Jovan. **Uma introdução à Governança da Internet**. São Paulo : Comitê Gestor da Internet no Brasil, 2016.

LUKER, Mark; PETERSEN, Rodney. **Computer and network security in higher education.** Washington, DC : Educause, 2003. Disponível em: < https://library.educause.edu/resources/2003/1/computer-and-network-security-in-higher-education>. Acesso em: 16 set. 2017.

MONTEIRO, Renato. A perigosa caixa preta dos algoritmos e a campanha eleitoral de 2018. **El País**, São Paulo, 12 out. 2017. Disponível em: <https://brasil.elpais.com/brasil/2017/10/11/opinion/1507749770_561225.html>. Acesso em: 12 dez. 2017.

NABARRO, Wagner; SILVA, Adriana. Informação e território: a Agence France Press no Brasil. **Boletim Campineiro de Geografia (BCG)**, v. 2, n. 1, p. 63-85, 2012.

PASTI, André. **Notícias, informação e território: as agências transnacionais de notícias e a circulação de informações no território brasileiro**. 2013. 237 f. Dissertação (Mestrado em Geografia), Instituto de Geociências, Universidade Estadual de Campinas, Campinas, 2013).

_____; PITA, Marina. A cidade é nossa. E os dados? **Carta Capital**, 27 set. 2017. Disponível em: <https://www.cartacapital.com.br/blogs/intervozes/a-cidade-e-nossa-e-os-dados>. Acesso em: 12 dez. 2017.

PRESCOTT, Roberta. Petya: o mais novo inimigo. **Revista Abranet**, São Paulo, ano VI, ed. 21, p. 26, jun./ago. 2017.

SANTOS, Milton. **A natureza do espaço: técnica e tempo, razão e emoção**. São Paulo : Hucitec, 1996.

_____. **Por uma outra globalização: do pensamento único à consciência universal**. Rio de Janeiro : Record, 2000.

TREND MICRO. **TrendLabs 2016 security roundup: a record year for enterprise threats**. 2016. Disponível em: <https://documents.trendmicro.com/assets/rpt-2016-annual-security-roundup-a-record-year-for-enterprise-threats.pdf>. Acesso em: 15 set. 2017.

VERIZON. **Data breach investigations report. 89% of breaches had a financial or espionage motive**. 2016. Disponível em: <https://regmedia.co.uk/2016/05/12/dbir_2016.pdf>. Acesso em: 15 set. 2017.

ZUBOFF, Shoshana. Big other: surveillance capitalism and the prospects of an information civilization. **Journal of Information Technology**, v. 30, p. 75-89, 2015.