ISSN: 2525-457X
Análise Estratégica
v. 32, n.1, dez./fev. 2024

UMA ANÁLISE PRELIMINAR DO AMBIENTE INFORMACIONAL CONTEMPORÂNEO NO BRASIL

A PRELIMINARY ANALYSIS OF THE CONTEMPORARY INFORMATION ENVIRONMENT IN BRAZIL

EUGENIO DINIZ

RESUMO

Realiza-se uma análise do ambiente informacional brasileiro contemporâneo, como uma espécie de diagnóstico preliminar. Embora esse ambiente seja robusto em vários aspectos, algumas vulnerabilidades potenciais são identificadas, e são consideradas algumas alternativas de enfrentamento existentes.

Palavras-chave: Ambiente informacional contemporâneo; Ambiente informacional brasileiro; Alfabetização midiática; Análise de infraestrutura

ABSTRACT

An analysis of the contemporary Brazilian information environment is carried out, as a kind of preliminary diagnosis. Although this environment is robust in many respects, some potential vulnerabilities are identified, and some existing coping alternatives are considered.

Keywords: Contemporary information environment; Brazilian information environment; Media literacy; Infrastructure analysis

O AUTOR

Professor do Departamento de Relações Internacionais da Pontifícia Universidade Católica (PUC-MG). Diretor Executivo e fundador da Synopsis - Inteligência, Estratégia, Diplomacia. É membro do International Institute for Strategic Studies - IISS (Londres) e da International Association for Security and Intelligence Studies - INASIS. É pesquisador 1C do Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq). Pesquisador contratado do Núcleo de Estudos Prospectivos do Centro de Estudos Estratégicos do Exército (NEP-CEEEx) no ciclo 2023-2024.

1 INTRODUÇÃO

Neste ensaio, visa-se a uma identificação das características do ambiente informacional contemporâneo, de maneira similar a uma análise diagnóstica, de modo a permitir a apresentação de sugestões para o enfrentamento de desafios na eventualidade de ocorrência de situações de confrontação. Esse tipo de diagnóstico é comumente apontado como a primeira tarefa de processos de levantamento de sugestões relativas a infraestruturas críticas nos guias de melhores práticas1. Viabilizar a comunicação dos brasileiros entre si, das lideranças políticas e dos comandantes entre si e com a sociedade brasileira em geral, permitindo aos brasileiros informarem-se e, eventualmente, identificarem e protegerem-se contra informações falsas é um tipo de capacidade crítica em tempos normais, e ainda mais em tempo de guerra. Principalmente em tempo de guerra, mas também em situações de maior confrontação em tempo de paz, é necessário assegurar ao máximo essa capacidade de comunicação, bem como contrarrestar esforços hostis de interferência nessa comunicação. A primeira seção traz uma análise mais geral do ambiente informacional brasileiro contemporâneo, a segunda seção enfoca elementos constitutivos de sua dimensão física, a terceira seção está concentrada na dimensão informacional e a quarta seção na dimensão cognitiva. A última seção é dedicada às considerações finais.

Uma ressalva: o emprego dos termos "dimensão física", "dimensão informacional" e "dimensão cognitiva" não significa que sejam necessariamente adequados, ou os mais adequados; mas, como não seria pertinente discutir essa adequação aqui, optou-se por emprega-los como vêm sendo discutidos, conforme analisado em outros ensaios (Diniz, 2023a; 2023b).

2 O AMBIENTE INFORMACIONAL BRASILEIRO CONTEMPORÂNEO

Pode-se dizer que, no Brasil, temos um ambiente informacional plenamente contemporâneo, basicamente maduro, com todas as suas principais características[2]:

- De acordo com os dados da Pesquisa Nacional por Amostragem Domiciliar (PNAD) Contínua, no quarto trimestre de 2021, dos aproximadamente 72.900.000 domicílios brasileiros, aproximadamente 69.496.000 (95,3%) tinham acesso à televisão[3]; mesmo no meio rural, a taxa atinge 90,8%. Por Grandes Regiões, o acesso é menor nos meios rurais das regiões Norte (82,79%) e Nordeste (89,41%);
- 26,56% dos aproximadamente 72.900.000 domicílios brasileiros tinham acesso a serviços de TV por assinatura[4], na maior parte nas zonas urbanas (28,13% dos domicílios, contra 16,16% nas zonas rurais). Também aqui a variação regional é grande: enquanto 34,62% dos domicílios urbanos da Região Sudeste tinham TV por assinatura, apenas 15,47% dos domicílios urbanos da Região Nordeste dispunham desses serviços; 26,58% dos domicílios rurais da Região Sudeste tinham TV por assinatura, contra apenas 10,12% dos domicílios rurais da Região Norte;

[1] V., p. ex., Western Australian Auditor General (2023).

[2] Para a caracterização do ambiente informacional contemporâneo, v. Diniz (2023a; 2023b).

[3] Dados disponíveis em https://sidra.ibge.gov.br/tabela/7167#resultado, acesso em 3 de outubro de 2023.

[4] Dados disponíveis em https://sidra.ibge.gov.br/tabela/7287#resultado, acesso em 3 de outubro de 2023.

- No mesmo período, utilizava-se a Internet em aproximadamente 65.620.000 (90,01%) domicílios, mas, nesse caso, a discrepância entre os meios urbano e rural era maior: enquanto a Internet era utilizada em 92,31% dos domicílios urbanos, nos rurais, a utilização caía para 74,73% – novamente, a utilização era menor nas zonas rurais das regiões Norte (58,56%) e Nordeste (73,88%)[5];

- Especialmente interessante, porém, é o fato de que, nos aproximadamente 65.620.000 domicílios em que se acessa a Internet, em 99,5% dos casos, houve acesso por telefone móvel celular – e praticamente sem diferenças entre as Grandes Regiões ou entre as zonas rurais e urbanas: a variação foi de 99,25% no meio rural na Região Sul a 100% no meio rural da Região Centro-Oeste. Já o acesso por microcomputador ou *tablet* ocorreu em 44,27% dos domicílios, aí predominando amplamente as zonas urbanas[6];

- Porém, é necessário um certo cuidado com relação ao dado acima, pois, apesar de haver acesso por celular à Internet em praticamente todos os domicílios com Internet, em muitos casos, esse acesso por celular é feito somente por meio de acesso fixo; dos aproximadamente 65.620.000 domicílios em que há acesso à Internet, o acesso por rede de telefonia celular móvel ocorre em aproximadamente 51.950.000 domicílios (79,16%) do total – e *somente por telefonia móvel* em aproximadamente 10.072.000 (15,35%) domicílios. A banda larga fixa está presente em 54.794.000 (83,50%) dos domicílios, e em 43.312.000 (66,00%) foram identificados acessos tanto por banda larga fixa quanto por banda larga móvel[7];[8]

- Estima-se que, em janeiro de 2023, havia aproximadamente 152,4 milhões de usuários de plataformas de mídias sociais no Brasil, número equivalente a 70,6% da população brasileira e a 83,8% do total de usuários de Internet no Brasil[9].

Do ponto de vista do consumo de informações, a pesquisa *Reuters Institute Digital News Report 2022* (Reuters Institute for the Study of Journalism, 2022), em 2022, 83% dos brasileiros obtinham notícias na Internet (incluindo portais de notícias e plataformas de mídias sociais), sendo que 64% as obtinham em mídias sociais plataformas de mídias sociais eram as fontes principais; os canais de TV (aberta e por assinatura) eram fontes para 55% dos brasileiros (contra 75% em 2013); e apenas 12% da população obtinha informações em mídia impressa (contra 50% em 2013). A principal forma de acesso à informação digital é o celular (75% do público, contra 23% em 2013), seguido dos microcomputadores (24% em 2022, contra 83% em 2013) e dos *tablets* (8% em 2022, contra 14% em 2013).

Em 2022, 48% do público tinha confiança geral nas notícias, pondo o Brasil em 14º lugar entre os países pesquisados; particularmente interessante, porém, é o contraste com apenas

[5] Dados disponíveis em https://sidra.ibge.gov.br/tabela/7307#resultado, acesso em 3 de outubro de 2023.

[6] Dados disponíveis em https://sidra.ibge.gov.br/tabela/7311#resultado, acesso em 3 de outubro de 2023.

[7] Dados disponíveis em https://sidra.ibge.gov.br/tabela/7311#resultado, acesso em 3 de outubro de 2023.

[8] As informações sobre acesso à Internet do IBGE convergem com as registradas pela União Internacional das Telecomunicações: https://www.itu.int/en/ITU-D/Statistics/Dashboards/Pages/Digital-Development.aspx, acesso em 3 de outubro de 2023.

[9] De acordo com https://datareportal.com/reports/digital-2023-brazil, acesso em 3 de outubro de 2023. Observe-se, porém, que esse número não é exatamente de indivíduos distintos – pode haver indivíduos com vários perfis diferentes em cada plataforma, por exemplo. Mais esclarecimentos estão disponíveis em https://datareportal.com/notes-on-data.

um ano antes (54%, o que punha o Brasil em 7º lugar entre os países pesquisados, de acordo com Reuters Institute for the Study of Journalism, 2021 – a edição anterior do relatório) e 62% em 2015. Curiosamente, em 2021, apenas 34% do público confiava nas notícias obtidas em plataformas de mídias sociais; mas, ao mesmo tempo, 47% compartilhavam notícias por essas plataformas, ou por aplicativos de mensagem, ou por correio eletrônico; em 2022, 46% compartilhavam notícias por essas vias. Ainda mais paradoxalmente, dentre as seis fontes consideradas mais confiáveis pelos brasileiros, quatro são de telejornais da TV aberta e seus portais na Internet, um é o portal de um jornal impresso (considerado mais confiável que o próprio jornal), sendo que o conjunto representado por jornais (impressos) locais e regionais ocupava o segundo lugar (61% confiavam nesse canal).

Portanto, o ambiente informacional brasileiro apresenta múltiplos canais, desde os tradicionais e centralizados – com destaque para as grandes emissoras de TV de sinal aberto, cuja cobertura abrange praticamente todo o país, e para os grandes jornais com suas páginas na Internet, invariavelmente permitindo algum tipo de acesso gratuito a alguma informação como as da "primeira página", atualizadas continuamente ao longo do dia –, passando pelos mais personalizados, como as TVs por assinatura, que incluem os canais dedicados exclusivamente a notícias; passando ainda pelas diversas páginas na Internet com acesso a informações, inclusive amplo acesso à informação produzida por órgãos e agências governamentais, mas incluindo também empresas, organizações não-governamentais (ONGs), blogues e páginas pessoais de comentaristas profissionais e amadores; e, por fim, às diversas plataformas de mídias sociais[10]. Assim, há múltiplas maneiras pelas quais agências governamentais podem comunicar-se com os cidadãos, e estes comunicarem-se entre si. Um aspecto interessante é a robusta credibilidade das notícias veiculadas por emissoras de TV e suas versões digitais; outro é o contraste entre a comparativamente baixa credibilidade atribuída às informações obtidas por mídias sociais e a disposição em compartilhá-las. Os dados sugerem, entretanto, uma forte e crescente centralidade do acesso à Internet por telefonia móvel para as comunicações e para o acesso a notícias e informações.

2.1 DIMENSÃO FÍSICA

Atualmente, o Brasil tem 92.334[11] estações de rádio-base (ERBs, ou seja, as "torres de celular"); destas, porém, 3.478 são "2G" (segunda geração de serviços de telefonia móvel) e só permitem chamadas telefônicas e mensagens de texto SMS, e não permitem acesso à Internet; portanto, 88.856 estações permitem o acesso dos telefones celulares à Internet, a portais de notícias, a plataformas de mídias sociais e aos aplicativos de mensagens pelas quais a informação circula na rede mundial de computadores. Esses números deverão aumentar significativamente ao longo do processo de implementação da malha de serviços de telefonia móvel de quinta geração ("5G"). É inviável, tanto técnica quanto economicamente, aumentar significativamente a segurança física dessas instalações – as antenas têm que ficar expostas para poderem captar e transmitir. Do ponto de vista da segurança desse tipo de componente da infraestrutura física do ambiente informacional, para além de delimitação do perímetro, câmeras e algumas poucas restrições de acesso pouco sofisticadas, sua

[10] Não foi possível obter dados atualizados sobre os domicílios com acesso a rádio. Os dados mais recentes a que tivemos acesso são de 2011, quando 83,80% dos domicílios tinham acesso ao rádio (91,25% da Região Sul; 65,04% na Região Norte). Fonte: Antonik (2013).

[11] Fonte: https://www.telecocare.com.br/mapaerbs/ERBs_Ago23.zip, acesso em 3 de outubro de 2023; dados atualizados até agosto de 2023.

preservação depende fundamentalmente de redundância e dispersão. Sob esse aspecto, essa rede de ERBs é bastante robusta[12].

Outro aspecto relevante dessa robustez é a redução da dependência com relação a fornecedores – tanto empresas quanto países quanto, numa questão tão sensível, alinhamentos políticos internacionais. Também sob esse aspecto, essa rede pode ser considerada bastante robusta: estima-se que aproximadamente metade dos equipamentos utilizados na prestação de serviços de telefonia móvel é fornecida pela chinesa Huawei, ao passo que o restante é dividido principalmente entre a Nokia, da Finlândia (cuja adesão à Organização do Tratado do Atlântico Norte – OTAN foi aprovada recentemente), e a Ericsson, da Suécia (cuja adesão à OTAN está sendo negociada) (IISS, 2023). Também do ponto de vista da cadeia de suprimentos, a malha brasileira é bastante robusta.

O aspecto seguinte são as conexões com a Internet, propriamente ditas. Do ponto de vista da infraestrutura física, os elementos principais a considerar são os *Internet Exchange Points* (IXPs), em que as redes de servidores dos provedores de Internet se conectam uns com os outros; e os cabos submarinos de Internet, que viabilizam essas conexões entre servidores pelos diversos continentes. De acordo com o *IXP Database*[13], o Brasil tem 46 IXPs. Aqui parece haver alguma vulnerabilidade: embora os IXPs estejam distribuídos por 25 Unidades da Federação[14], com boa dispersão espacial ao longo do território, na maior parte das UFs (16) há apenas um IXP – ou seja, pouquíssima redundância. Aqui, parece haver espaço para medidas relacionadas à proteção física: os números são comparativamente pequenos e as conexões se dão mediante cabos em *switches*. Não há impedimentos técnicos nem econômicos significativos.

Quanto aos cabos submarinos[15], há 16 no Brasil. Um deles (o *Brazilian Festoon*) conecta diretamente apenas cidades brasileiras[16], mas uma delas é o Rio de Janeiro, que está conectado a outros 7 cabos ligados ao exterior, e outra é Salvador, conectada a dois outros cabos. Outros 15 cabos conectam o Brasil ao exterior, o que, à primeira vista, fornece alguma redundância[17]; entretanto, no Brasil, esses cabos estão conectados a apenas quatro cidades: Fortaleza, Salvador, Rio de Janeiro e Praia Grande. Embora seja inviável proteger fisicamente os cabos submarinos ao longo de toda a sua extensão, esse não é o caso de seus pontos de chegada em terra.

Não foi possível obter dados sistemáticos sobre a infraestrutura física para transmissões de TV (aberta e por cabo) nem para radiodifusão. Entretanto, sabe-se que essas redes são bem distribuídas, com várias torres de transmissão e de retransmissão espalhadas por todo o país. Embora a importância desses serviços para a obtenção de informações pelo público tenha declinado drasticamente, eles permanecem bastante importantes em pelo menos dois aspectos: (i) como já mencionado, as informações difundidas por esses veículos (principalmente as emissoras de TV) são as mais respeitadas, em geral, pela população brasileira; (ii) dada a sua ampla presença em todo o território, servem como uma espécie de capacidade informacional de reserva – desse ponto de vista, conferem algum grau

[12] Isso pode facilmente ser observado olhando-se o mapa interativo disponível em https://www.telecocare.com.br/mapaerbs/index.php, acesso em 3 de outubro de 2023.

[13] Disponível em https://ixpdb.euro-ix.net/en/, acesso em 4 de outubro de 2023; dados atualizados em 4 de outubro de 2023.

[14] Não há IXPs no Amapá e em Rondônia.

[15] Dados disponíveis em https://www.submarinecablemap.com/landing-point/rio-de-janeiro-brazil, acesso em 4 de outubro de 2023.

[16] Aracaju (SE), Atafona (no município de São João da Barra, RJ), Ilhéus (BA), João Pessoa (PB), Macaé (RJ), Maceió (AL), Natal (RN), Porto Seguro (BA), Recife (PE), Salvador (BA), Sítio (município de Arraial do Cabo, RJ), São Mateus (ES) e Vitória (ES).

[17] A Índia, por exemplo, está conectada a 22 cabos submarinos; a África do Sul está conectada a 10 cabos submarinos; a Argentina a 8.

de profundidade[18] à capacidade informacional brasileira, principalmente como canal alternativo de comunicação entre agências governamentais e a população, que pode ser muito valiosa em caso de guerra, por exemplo. Essa capacidade mostrou-se muito útil à Rússia no que concerne a suas ações na Ucrânia[19]. Sim, na Rússia, ao que consta, a influência do governo sobre as organizações e os veículos de mídia seria muito maior que no Brasil; por outro lado, como mostrado anteriormente, as grandes organizações de notícias são, no geral, bastante respeitadas pela população, o que torna mais críveis as informações veiculadas por elas.

Mas, possivelmente, o elemento mais importante a conferir profundidade à capacidade comunicacional brasileira é a comunicação por satélites. Como é amplamente sabido, o sistema de comunicações Starlink[20], da SpaceX, vem provendo o acesso à Internet na Ucrânia, tanto à população em geral quanto ao governo e às forças ucranianas; por outro lado, parece que, em pelo menos uma circunstância, o serviço teria sido negado à Ucrânia pelo próprio Elon Musk, por uma discordância sua quanto a uma possível ação das forças ucranianas e suas eventuais possíveis consequências (Pennington; Lyngaas, 2023). Evidentemente, não se trata de discutir aqui a pertinência das atitudes do principal decisor da SpaceX, e nem a adequação nem os riscos da suposta ação ucraniana que aquele teria alegadamente querido evitar. Os pontos aqui são: (i) um governo e suas forças armadas ficaram totalmente dependentes de uma empresa privada de outro país – no limite, na verdade, a decisão final parece ter sido de um único indivíduo – para que suas forças possam atuar contra uma força hostil; e (ii) um cidadão privado de outro país pôde interferir diretamente na capacidade de atuação das forças ucranianas contra as forças russas.

O Brasil tem hoje 7 satélites de comunicação ativos[21]. Um deles, o SkyBrasil-1, transmite apenas programas de TV para uma empresa, a DirecTV. Outro, o Satélite Geoestacionário de Defesa e Comunicações Estratégicas (SGDC-1) – que é um arranjo, originalmente, entre o outrora Ministério da Ciência, Tecnologia, Inovação e Comunicação (MCTIC), a Telebrás, o Ministério da Defesa, a Agência Espacial Brasileira (AEB) e o Instituto Nacional de Pesquisas Espaciais (INPE) – utiliza a Banda Ka, que possibilita acesso à conexão de banda larga em todos os locais do país, e a Banda X, para comunicações militares. Os demais são operados pela Embratel Star One, hoje controlada pela Claro, do México. Um deles, o Star One D1, é dedicado à telefonia celular e à transmissão de dados em altíssima velocidade; o Star One C4 é dedicado exclusivamente à TV; o Star One C2 é dedicado a telefonia, TV, rádio, transmissão de dados e Internet; o Star One C3 a TV, Internet e telefonia; e o Star One D2, além de transmissões de TV e telefonia, também transmite na Banda X, para comunicações militares. Além disso, está prevista a obtenção e lançamento de mais um Satélite Geoestacionário de Defesa e Comunicações Estratégicas – o SGDC-2 (Henry, 2019). Do ponto de vista do equipamento, à primeira vista, o Brasil pareceria bem servido; entretanto, o fato de que cinco dos satélites sejam operados por uma empresa sediada no México pode significar uma vulnerabilidade.

Essa possível vulnerabilidade inclui também o fato de que os teleportos de Guaratiba, Tanguá, Mosqueiro, Manaus e João Pessoa também são operados pela Embratel Star One. Porém, nesse

[18] No sentido de "defesa em profundidade"

[19] Não estão em discussão aqui o mérito ou a qualidade das informações veiculadas; referimo-nos aqui apenas à capacidade, por parte das autoridades russas, de veicular a informação desejada a seu público.

[20] Sobre a SpaceX e o Starlink, v. a excelente matéria de Vaiano (2023).

[21] Os dados sobre satélites foram obtidos de https://www.ucsusa.org/resources/satellite-database; de https://www.embratel.com.br/satelites/nossa-frota; e https://www.gov.br/aeb/pt-br/programa-espacial-brasileiro/satelites. Todos foram acessados pela última vez em 3 de outubro de 2023.

caso, como essas instalações estão fisicamente em território brasileiro, há uma margem de manobra maior das autoridades para lidar com elas – dependendo da disponibilidade de pessoal técnico. Ainda assim, trata-se de um aspecto a levar em consideração[22]. Sob esse ponto de vista, uma vez que o acesso aos satélites é feito por meio dessas instalações, essa margem de manobra contribui para reduzir o risco de interferência externa nesse acesso em situações de maior tensão. Evidentemente, a pequena quantidade e a importância dessas instalações fazem com que sua proteção física e as barreiras contra acessos indevidos sejam considerações importantes.

Os satélites, em si mesmos, porém, são relativamente pouco vulneráveis à ação destrutiva hostil. Como estes se encontram em órbita geoestacionária, entre 35.700 e 35.800 km de altitude[23], não são vulneráveis à ação de mísseis antissatélites de combustível sólido; por sua vez, os de combustível líquido são de ação mais lenta e, em princípio, podem ser mais facilmente destruídos ainda em solo – tudo dependerá, evidentemente, da existência da capacidade de fazê-lo. Quanto a danos físicos, em princípio, podem ser vulneráveis à ação de satélites antissatélites, ou "satélites assassinos", mas cuja presença nas proximidades das órbitas dos seus alvos pode ser monitorada[24]. O principal risco é a interceptação da transmissão dos satélites, no âmbito das medidas, contramedidas e contracontramedidas eletrônicas[25].

Dos 72.900.000 domicílios brasileiros, 21,58% dispõem de antenas parabólicas para recepção de sinal de satélite, sendo que 50,96% dos domicílios rurais têm antenas parabólicas – 58,90% dos domicílios rurais da Região Centro-Oeste e 56,12% dos domicílios rurais da Região Nordeste[26]. Entretanto, essas antenas são necessárias para a recepção do sinal de TV por satélite; os acessos à telefonia móvel e à Internet não dependem delas. Assim, a penetração e a capilaridade das antenas parabólicas para captação do sinal de TV por satélite constituem uma maneira adicional pela qual seria possível continuar informando a sociedade brasileira, com interferência externa, em princípio, limitada.

Tudo somado, portanto, pode-se dizer que, em princípio, a disponibilidade de comunicação por satélites confere robustez e profundidade à capacidade informacional brasileira, com considerável autonomia. Especialmente importante, em caso de guerra, é a capacidade do sistema de comunicação por satélites disponível aos brasileiros de realizar comunicações militares pela Banda X, ou seja, de viabilizar atividades de comando e controle das Forças Armadas, o que é uma consideração importante para as atividades informacionais em situações de guerra.

2.2 Dimensão Informacional

Do ponto de vista da chamada "dimensão informacional", o panorama não parece muito favorável.

No final de 2020, o mercado brasileiro de computação em nuvem era dominado pelas seguintes empresas, todas elas sediadas no exterior: a Amazon Web Services (AWS), com 53,7% do

[22] A nosso ver, é surpreendente que a análise feita pelo *International Institute for Strategic Studies (IISS, 2023)* não atribua importância a essa vulnerabilidade potencial.

[23] Em comparação, os satélites Starlink estão todos na Órbita Terrestre Baixa (LEO), com perigeus de 258 a 570 km e apogeus de 280 a 575 km.

[24] Para mais informações sobre satélites, v. Welti (2012).

[25] Para assuntos relacionados a medidas, contramedidas e contracontramedidas eletrônicas relacionadas à comunicação via satélite, v. Adamy (2021).

[26] Fonte: https://sidra.ibge.gov.br/tabela/7288#resultado, acesso em 3 de outubro de 2023.

mercado; a Microsoft, com 15,8%; a Huawei, com 7,7%; a IBM, com 3,3%; o Google, com 3,1%; e a Oracle, com 2,2%, sendo o restante (aproximadamente 14,2%) dividido entre outras empresas menores (BNamericas, 2021). De outra perspectiva, 78,1% da computação em nuvem no Brasil são controlados por empresas sediadas nos EUA, sendo que a AWS sozinha controla mais da metade desse mercado. Isso inclui a hospedagem de domínios na Internet, tanto de empresas quanto de pessoas. Uma boa parte dos blogues mais respeitados – inclusive de entidades ligadas a universidades e instituições de pesquisa, mas também de veículos jornalísticos – está hospedada em servidores ligados àquelas empresas; mas também em bancos saúde e, inclusive, governamentais. Muitos dos serviços de hospedagem de domínios mais conhecidos também usam, na verdade, os serviços de nuvem daqueles provedores.

O risco aí envolvido é imenso, e não apenas uma possibilidade abstrata. Em 9 de janeiro de 2021, por exemplo, a AWS informou à plataforma de mídia social Parler que deixaria de hospedá-la a partir de pouco antes da meia-noite de 10 de janeiro de 2021 – ou seja, pouco mais de 24 horas, e num fim de semana, o que dava pouca margem de manobra para que a plataforma encontrasse novas alternativas de hospedagem. A Parler nunca se recuperou desse episódio. Não havia inadimplência por parte da plataforma; segundo a AWS, sua decisão baseava-se na avaliação de que teria havido aumento significativo de conteúdo violento na plataforma, o que contrariaria as condições de serviço da plataforma (Fung, 2021; Paczkowski; Mac, 2021))[27]. Aqui, não se está discutindo o mérito da decisão da AWS: o que está em tela é que provedores de serviços de computação em nuvem podem retirar conteúdos inteiros da Internet (no caso, incluindo o conteúdo produzido e circulado por usuários) praticamente imediatamente.

O problema é que, nesse caso, os usuários e clientes escolhem, direta ou mediante intermediários, os serviços daqueles provedores por razões como confiabilidade, segurança e preço. Como a base de clientes é muito grande, o custo total daquela confiabilidade e daquela segurança (múltiplos servidores, múltiplos *datacenters* e *datawarehouses*, pessoal técnico altamente capacitado etc.) tem ganhos de escala muito significativos, tornando as alternativas muito dispendiosas – o que faz com que as vantagens dos incumbentes aumente muito, criando assim um círculo que lhes é favorável, mas prejudicial ao surgimento de alternativas.

Esse é um gargalo crítico no ambiente informacional brasileiro. A única maneira de contorná-lo parece ser dispor de capacidade própria de armazenamento em nuvem em larga escala, de modo a prover alguma redundância para, em caso de situações mais tensas, permitir uma rápida migração de domínios – pelo menos, alguns dos mais críticos, como, por exemplo, comunicações, governos, bancos e serviços de saúde – para novos servidores. O problema óbvio é que o custo dessa infraestrutura alternativa seria elevado, e possivelmente exigiria alguma forma de subsídio ou de custeio público. Trata-se, portanto, de um problema complexo, que transcende considerações técnicas e econômicas para tornar-se um problema importante de políticas públicas.

Um outro aspecto relevante é a importância das plataformas de mídias sociais para a troca de informações, mas também para o acesso a notícias e para a comunicação das autoridades para com a população. Como já visto, por mais que haja uma desconfiança maior do público com relação à informação que circula nessas plataformas, o fato é que boa parte da informação – inclusive o conteúdo produzido pelos veículos jornalísticos em que a população mais confia – é acessada pelo público por meio delas. De acordo com o *Reuters Institute Digital News Report 2022*, 64% dos brasileiros acessam

[27] Cabe lembrar que isso ocorreu logo depois dos acontecimentos no Capitólio em 6 de janeiro de 2021.

conteúdo noticioso pelas plataformas de mídia social e aplicativos de mensagem, da seguinte maneira: YouTube (43%)[28], WhatsApp (41%), Facebook (40%), Instagram (35%), Twitter (renomeado para X) (13%); e TikTok (12%). Como o YouTube é controlado pela Alphabet Inc. (grupo que controla também todos os serviços Google – motor de busca, Google Drive, Google Sala de Aula etc.) e WhatsApp, Facebook e Instagram são todos controlados pela Meta, constata-se imediatamente que apenas duas empresas, ambas sediadas nos EUA, têm ampla capacidade de, pelo menos durante algum tempo – nos meses iniciais de uma guerra, por exemplo –, controlar o acesso dos brasileiros à informação.

De fato, há indícios de que, ao que parece, na busca por conter a proliferação de informações errôneas (*misinformation*) ou deliberadamente falsas (*disinformation*), algumas plataformas excluíram, bloquearam ou interferiram na circulação de mensagens cujo conteúdo foi, posteriormente, corroborado, ou, pelo menos, considerado plausível – por exemplo, as notícias referentes ao conteúdo armazenado no computador portátil de Hunter Biden, antes da eleição de seu pai, o atual presidente Joe Biden (decisão considerada errada, depois da eleição, pelo então *CEO* do Twitter, Jack Dorsey); ou críticas feitas por pesquisadores renomados a políticas adotadas durante a Covid-19 (independentemente de terem sido confirmadas ou não). Outro exemplo, pertinente para a discussão feita aqui, foi a decisão da controladora do YouTube de bloquear, em todo o mundo, o acesso a canais das organizações de mídia ligadas ao governo russo (Dave, 2022). De novo, o ponto aqui não é o mérito dessas decisões, mas o simples fato de que elas podem ser tomadas.

O desafio aqui é significativo. Quando da ação russa para anexar a Crimeia, em 2014, os ucranianos puderam migrar da VKontakte (plataforma de mídia social russa que, até então, era de longe o sítio mais acessado na Ucrânia) porque estavam disponíveis alternativas amplamente acessíveis que, naquele contexto, não lhes eram hostis – ou seja, Facebook, Twitter, YouTube etc. Mas, na eventualidade de uma atitude menos favorável por parte dessas plataformas e aplicativos em alguma situação em que o Brasil se veja envolvido, em princípio, não haveria alternativas facilmente disponíveis. Apenas no caso de aplicativos de mensagem, haveria a alternativa mais conhecida do Telegram, que tem reputação de independência, inclusive com relação ao governo da Rússia, seu país de origem. Há outros menos conhecidos, mas com boa reputação entre usuários, como Signal. Na esfera governamental, há ainda o aplicativo de mensagens utilizado pela Agência Brasileira de Inteligência (Abin), que é o Athena[29]. Mas, no caso das plataformas de mídia social, até onde seja de nosso conhecimento, não há alternativas de grande porte – pelo menos de amplo conhecimento no Brasil – aos serviços prestados pelas plataformas mencionadas anteriormente, que possam tornar-se alternativas óbvias rapidamente, para as quais haveria migração em massa. As alternativas mais óbvias ao YouTube seriam o Vimeo (estadunidense) e o Rumble (canadense), além do TikTok (chinês) – este último só para vídeos curtos. Essa é uma grande vulnerabilidade do ambiente informacional atualmente vigente no Brasil.

Esse desafio é composto pelo fato de que, como já visto, os celulares predominam amplamente como modo de acessar a Internet no Brasil, mesmo pelos serviços de acesso fixos. A Samsung e a Motorola, que dominam o mercado de celulares no Brasil, (41, 61% e 20,46%, respectivamente, de acordo com Bonaventura, 2023), utilizam o sistema operacional Android, da Alphabet, ao passo que os celulares da terceira colocada, a Apple (18,74% do mercado brasileiro), utilizam sistema operacional próprio, o IoS. Até mesmo os celulares da chinesa Xiaomi usam um

[28] Isso é interessante, pois parece sugerir que mesmo os telejornais alcançam a população, em alguma medida, por meio da Internet, e não pelos sinais de TV aberta ou por assinatura.

[29] Sobre o Athena, v. https://www.gov.br/abin/pt-br/assuntos/tecnologia/athena, acesso em 2 de outubro de 2023.

sistema operacional, o MIUI, que é baseado no Android. Mesmo que surgisse um aplicativo de plataforma de mídia social mais independente, ele dependeria, em alguma medida, da anuência das controladoras dos sistemas operacionais. Também aqui, a experiência do Parler é reveladora. Na mesma época em que a AWS encerrou a hospedagem da plataforma, a Google Store (Android) e a Apple Store (IoS) deixaram de oferecer seu aplicativo. Com isso, o Parler podia ser baixado e instalado, mas não seria mais atualizado automaticamente em nenhum celular baseado no Android e no IoS.

A avaliação deste autor é que essa conjugação entre a centralidade das plataformas de mídia social e aplicativos de mensagem acessados por celular para a obtenção de notícias por parte dos cidadãos brasileiros e a ausência de alternativas óbvias àquelas plataformas e aos sistemas operacionais dos celulares é hoje, de longe, a maior vulnerabilidade do ambiente informacional no Brasil, e a mais difícil de se enfrentar.

Entretanto, do ponto de vista da chamada dimensão informacional, ela não é a única vulnerabilidade. Evidentemente, há todos os outros riscos relacionados à segurança cibernética e assuntos relacionados. Em larga medida, isso é responsabilidade das empresas e organizações. Porém, há dois aspectos que é necessário ter em conta. Um deles é a escassez de profissionais qualificados na área, mesmo entre os profissionais da área conhecida como "tecnologia da informação" (TI): este seria um dos setores com maior carência de profissionais qualificados, atrás apenas de profissionais de cuidados pessoais (IISS, 2023, p. 16; OAS, 2020, p. 18). O outro é o que poderíamos chamar de baixa consciência da importância da segurança cibernética entre os usuários de Internet no Brasil, em geral (OAS, 2020, p. 15), inclusive junto a lideranças políticas, empresariais e até mesmo profissionais de TI.

A carência de profissionais qualificados em segurança cibernética põe em risco a disponibilidade e a integridade de informações para o público em geral e até mesmo para os públicos internos das organizações, o que pode comprometer o acesso a serviços e bens críticos; pode também tornar disponíveis a agentes, organizações, agências ou mesmo forças adversas informações valiosas – organizacionais e pessoais – que podem ser usadas para desvantagem do Brasil; isso pode ser feito a partir de diversos tipos de programas nocivos (conhecidos como *malwares*), mas também de procedimentos de *phishing*, engenharia social e semelhantes, pelos quais se podem obter informações importantes, com destaque para credenciais de acesso a dados sensíveis que poderão então ser obtidos, adulterados ou mesmo negados a seus usuários legítimos. Quanto ao público em geral, essa falta de atenção a procedimentos de cibersegurança pode levar até mesmo ao compartilhamento, por ingenuidade, de informações importantes ou que podem levar a outras informações importantes; também pode levar à obtenção de informações sobre as credenciais de acesso a informações sensíveis, próprias dos indivíduos ou mesmo de organizações a que pertencem; mas também podem levar à indisponibilidade do provimento de serviços por organizações por meio da captura dos computadores individuais para a realização de ataques de negação de serviço (DoS, do inglês *denial of service*) e de negação distribuída de serviços (DDoS, do inglês *distributed denial of service*), que sobrecarregam os servidores das organizações-alvos com solicitações de acesso em volume tal que seus sistemas não as podem processar, impedindo o seu funcionamento normal.

Conquanto importantes, enfrentar essas duas vulnerabilidades seria, em princípio, menos complicado. Nada impede que incentivos públicos e privados sejam alocados para a formação acelerada de profissionais de segurança da informação, *desde que haja, no público em geral e nas lideranças políticas, empresariais e sociais, consciência da centralidade e da urgência do enfrentamento do problema*. Sendo assim, seria de máxima importância o estabelecimento de programas e iniciativas de conscientização sobre o assunto, de amplo alcance, e o fortalecimento e expansão de iniciativas já existentes.

Porém, há outras providências que podem ser tomadas no âmbito dos poderes públicos no sentido de aumentar a segurança da informação no Brasil. IISS (2023) traz um excelente inventário de várias iniciativas tomadas ou em curso no Legislativo e no Executivo em âmbito federal, e não precisamos retomá-las aqui[30]. É importante ter em mente, porém, que esses esforços vêm produzindo frutos:

> "O Brasil fez avanços notáveis na melhoria da segurança cibernética no âmbito do governo federal ao longo dos anos, como fica evidente no último Global Cybersecurity Index da União Internacional de Telecomunicações, que mostrou sua ascensão do 70º lugar em 2018 para o 18º em 2020, ficando em primeiro lugar entre os Estados latino-americanos. Porém, o grau de segurança cibernética ainda é inadequado tendo em vista o desenvolvimento desigual da segurança cibernética por toda a sociedade." (IISS, 2023, p. 17).

2.3 Dimensão Cognitiva

Porém, na ausência de colapso da capacidade informacional decorrente de atividades nas dimensões física e informacional, resta ainda avaliar as atividades no âmbito da chamada "dimensão cognitiva" do ambiente informacional.

Como apontado em texto anterior (Diniz, 2023b), dadas as características mais gerais do ambiente informacional contemporâneo, no que concerne à sua chamada "dimensão cognitiva", as atividades comunicacionais de maior envergadura, frequentemente designadas como "comunicações estratégicas", poderiam caracterizar-se, basicamente, por:

- Amplo esforço dos Estados em atingir seus próprios públicos de modo a, reforçando suas narrativas, mitos, afinidades, maximizar a observância dos comportamentos desejados e minimizar comportamentos indesejados;
- Amplo esforço no sentido de divulgar informações favoráveis junto a seu próprio público – o que poderia incluir a multiplicação de mensagens com informações selecionadas, incompletas, e eventualmente distorcidas ou falsas, bem como o emprego de *bots*;
- Amplo esforço de *negação de capacidade informacional* (*information denial*) ao adversário, o que, do ponto de vista da dimensão cognitiva, significaria tentar impedir a veiculação de informações indesejadas em qualquer tipo de mídia junto a seu público (ou seja, censura);
- Esforços de confrontar informações divulgadas pelos adversários, principalmente as falsas ou exageradas, que pudessem lhe trazer algum tipo de vantagem;
- Pouco esforço no sentido de confrontar diretamente os quadros interpretativos de públicos adversários;
- Esforços no sentido de divulgar, seletivamente, junto aos públicos adversários, informações verdadeiras e significativas que pudessem efetivamente minar as percepções daqueles públicos, ou, em períodos iniciais curtos, até mesmo informações falsas.

[30] V. também ITU (2023).

Ainda como mostrado em Diniz (2023b), foi possível identificar vários desses comportamentos tanto nas relações entre Rússia e Ucrânia, desde o período da anexação da Crimeia pela Rússia, em 2014-2015, quanto no período entre 2015 e 2022 (antes da invasão da Ucrânia pela Rússia) e, posteriormente, desde a invasão da Ucrânia. Entretanto, nem todos os tipos de esforços possíveis mencionados acima têm méritos, seja do ponto de vista valorativo (ético ou jurídico), seja do ponto de vista da eficácia.

Um dos exemplos típicos é a censura[31]. Restrições à atividade jornalística e à circulação de informações que não sejam estritamente fraudulentas, caluniosas ou semelhantes contrariam frontalmente valores e necessidades fundamentais para uma sociedade democrática, como a livre circulação de ideias, que é a principal proteção do público contra a manipulação deliberada e contra a perpetuação de preconceitos, atitudes dogmáticas, reificações de atitudes e comportamentos etc. (Shaffer, 2023). Mesmo diante da proliferação de informações deliberada e manifestamente falsas divulgadas por adversários, a ocorrência de censura põe em xeque o caráter democrático de uma sociedade e/ou e um regime (Pryhara, 2018).

Além disso, do ponto de vista de seu objetivo principal, há fortes indícios de que a censura seja ineficaz, principalmente no ambiente informacional contemporâneo, em que os indivíduos não dependem de grandes organizações centralizadas de difusão de notícias para terem acesso a informações providas por outrem. Embora esteja claro que restrições e dificuldades técnicas reduzem o acesso e desincentivam a busca por informações censuradas até mesmo por parte de indivíduos com algum grau de sofisticação digital, o fato é que estes podem facilmente contornar essas restrições com baixo risco para si próprios e difundi-las para seus contatos (Golovchenko, 2022).

Uma pesquisa na China (Chen; Yang, 2018) mostrou que simplesmente dispor de capacidade de contornar bloqueios não teve impacto significativo na demanda espontânea pelo acesso a páginas censuradas por parte dos estudantes – incluindo sítios de notícias de outros países; entretanto, para uma parte do grupo, que foi incentivada a acessar sítios de veículos de imprensa de outros países fez aumentar sua confiança nesses veículos, e tornou-os mais dispostos a realizar os esforços e pagar os custos para acessá-los, resultando num aumento duradouro na busca e obtenção de informação censurada por parte daqueles estudantes[32] – o que mostra que não são nem os custos nem os riscos da censura que restringem a busca da informação censurada, mas, simplesmente, o desconhecimento de seu valor. Além disso, a obtenção de informação sensível torna os estudantes mais bem informados sobre eventos atuais e do passado; mais pessimistas com relação ao crescimento econômico chinês; mais céticos com relação ao governo, menos satisfeitos com relação a seu desempenho e mais propensos a demandar reformas institucionais; e mais interessados a deixar o país por meio de algum programa de pós-graduação (Chen; Yang, 2018, p. 2296).

O estudo acima sugere, inclusive, que a censura pode ser contraproducente. Também o chamado "efeito Streisand" descreve a situação em que a censura chama e atrai a atenção do público para a informação censurada, deixando-o mais curioso sobre esta, e gerando indignação pela própria ocorrência da censura, o que então faz aumentar a busca e o acesso à informação censurada (Jansen;

[31] É importante deixar claro que não se está tratando, aqui, da proteção do sigilo legítimo relacionado, por exemplo, a informações de cunho propriamente militar, mas sim de restringir o acesso da população própria a informações veiculadas por adversários, ou por seus aliados, ou informações inconvenientes provenientes de quaisquer fontes.

[32] "*By the end of the experiment, about 23% of the newly exposed students pay to continue their uncensored Internet access*". (Chen; Yang, 2018, p. 2296).

Martin, 2015). Os autores deixam claro que isso não ocorre sempre, mas o fato é que pode ocorrer.

Por sua vez, uma outra pesquisa realizada na China, mostrou que a censura torna o público mais propenso a acreditar em rumores políticos que percebem que têm maior probabilidade de serem censurados – rumores que tendem a ser politicamente sensíveis e contrários ao governo (Wu, 2020). Assim, um efeito curioso da censura é que ela pode gerar maior credibilidade para rumores e boatos desfavoráveis ao governo – o que, evidentemente, prejudica a credibilidade até mesmo das informações verdadeiras divulgadas por este, ou de seu interesse. Principalmente no ambiente informacional contemporâneo, esse pode ser um efeito especialmente contraproducente da censura oficial.

Assim, como lidar com a propaganda e a desinformação deliberada adversas? A experiência ucraniana revela duas estratégias importantes, uma reativa e outra proativa.

A estratégia reativa é o esforço sistemático de desmascarar (*debunking*) a propaganda e, principalmente, a desinformação adversa. Um exemplo que parece ter sido particularmente bem-sucedido é a experiência do grupo voluntário de jornalistas *StopFake*[33]. De acordo com Haig; Haig; Matychak (2019):

> "Seus verificadores de fatos [fact-checkers], tradutores e editores colaboravam on-line para selecionar notícias de aparência duvidosa, refutá-las usando análise forense de mídia e publicar as análises resultantes em vários idiomas (principalmente inglês e russo). Uma análise do trabalho inicial do grupo mostrou que as técnicas usadas contra notícias falsas eram mais diretas e menos dependentes de especialistas neutros do que as usadas no trabalho tradicional de verificação de fatos – por exemplo, mostrando que uma imagem em uma reportagem havia sido manipulada em relação à sua aparência original ou legendada de forma enganosa (por exemplo, mostrando a devastação na Ucrânia, em vez da Síria) (...). O StopFake foi amplamente lido na Rússia e na Ucrânia, e seu trabalho apareceu com destaque em reportagens sobre o conflito escritos por jornalistas ocidentais." (Haig; Haig; Matychak, 2019, p. 158)

Os autores chamam a atenção para as limitações desse esforço. O problema mais óbvio é que o esforço toma muito tempo, o que significa que o desmascaramento só ocorrerá depois que a notícia já tiver produzido impactos, inclusive emocionais – sendo que alguns desses impactos tendem a ser duradouros, mesmo após a informação ser aceita como falsa pelos seus destinatários (Chan *et al.*, 2017). Além disso, é frequente que a informação falsa original e o seu desmascaramento sejam recebidos por audiências distintas entre si – sendo que o público mais propenso a acessar o desmascaramento já tenderia a ser um público mais crítico, de qualquer forma. Um outro elemento é que o retorno dos desmascaramento, para uma dada fonte, tende a ser decrescente (mas por bons motivos): uma vez que uma fonte seja desmascarada como veiculadora de informação falsa, os poucos remanescentes que ainda recebem a informação ali veiculada e creem nela dificilmente deixarão de fazê-lo por causa de algum novo desmascaramento (Haig; Haig; Matychak, 2019). Ainda assim, isso mostra que tais esforços podem ser muito bem-sucedidos em desmascarar não apenas informações falsas individualmente, mas inclusive em desacreditar as fontes que as divulgam.

O outro tipo de estratégia, que pode ser considerado mais proativo, refere-se ao conjunto de iniciativas chamadas de "alfabetização midiática" (*media literacy*) ou "alfabetização informacional" (*information literacy*). Em linhas gerais, esses esforços estão voltados para qualificar o público na análise de notícias, checagem de fontes, identificação de técnicas de propaganda, detecção de manipulação emocional e ambiguidade e outros recursos para detecção de informações falsas. Para

[33] A StopFake não foi a única iniciativa o tipo, mas foi a mais conhecida. A página do grupo está disponível em https://www.stopfake.org/en/main/, acesso em 2 de outubro de 2023.

atingir públicos mais amplos de maneira mais acelerada, esses esforços geralmente envolvem uma etapa de qualificação de instrutores, que, posteriormente, qualificarão outros segmentos do público. Haig; Haig; Matychak (2019) descrevem com mais detalhe um desses programas, chamado "Aprender a Discernir" (originalmente chamado "Alfabetização Midiática Cidadã")[34]. Esse projeto foi desenvolvido junto a bibliotecas, com o apoio de organizações como a *International Research and Exchange* (IREX)[35]. O esforço foi amplamente considerado bem-sucedido, e expandiu-se até mesmo junto a escolas, e é bastante recomendado.

Uma das vantagens de programas de alfabetização midiática é que eles podem ser conduzidos e realizados com calma e eficácia sem que, ou muito antes que, situações mais críticas os tornem urgentes e mais dificilmente realizáveis. Além disso, os benefícios que trazem para os destinatários, e para suas sociedades, vai muito além das demandas urgentes de situações altamente conflitivas: as pessoas que são treinadas estão em melhores condições de serem melhores consumidoras em geral, mais críticas em relação a notícias e, tudo somado, cidadãos mais conscientes.

Toda essa discussão traz luz também para a comunicação com o público próprio. *Principalmente se esforços consistentes em alfabetização midiática tiverem sido realizados para combater propaganda e desinformação adversa*, a comunicação feita por lideranças junto a seus públicos próprios tem como principal ativo a preservar a sua própria credibilidade. Como já foi visto, uma das características do ambiente informacional contemporâneo é a independência do público com relação a grandes veículos de informação centralizados; informações relevantes podem ser produzidas por indivíduos e seus celulares, comentários pertinentes podem ser feitos por cidadãos em blogues e plataformas de mídias sociais, e há vários canais por meio dos quais essas informações podem ser circuladas. Para além do seu dever de informar adequada e corretamente o público, a própria capacidade de transmitir mensagens e informações, *inclusive verdadeiras*, para produzir efeitos desejados ficará comprometida caso as lideranças percam credibilidade.

Sob esse prisma, um aspecto relevante do ambiente informacional vigente hoje no Brasil, como já salientado, é a comparativamente alta credibilidade de fontes jornalísticas estabelecidas, e a tendência que os próprios usuários têm de divulgá-las para suas redes de contatos. Isso sugere que a sociedade brasileira tenderia a beneficiar-se muito significativamente, se situações críticas chegarem a ocorrer, de amplos e sistemáticos esforços de qualificação na interpretação de notícias, imagens, propagandas e outras técnicas de persuasão.

3 CONSIDERAÇÕES FINAIS

Sob vários aspectos, o ambiente informacional brasileiro contemporâneo pode ser considerado robusto. TV e Internet têm grande penetração no país, apesar de variações regionais e por tipo de ambiente (urbano *versus* rural), e por mais de uma forma de acesso, incluindo satélite. Apesar de um decréscimo em relação a anos anteriores, veículos jornalísticos, particularmente da imprensa televisiva e seus portais na Internet, gozam de grande credibilidade. Entretanto, alguns aspectos da infraestrutura física exigem um pouco mais de atenção: é necessário um diagnóstico mais preciso das vulnerabilidades físicas das instalações de IXPs, dos pontos de chegada dos cabos submarinos de transmissão de dados;

[34] Entretanto, as referências mais frequentemente citadas para as atividades de alfabetização midiática são os trabalhos de W. J. Potter – p. ex., Potter (2014).

[35] A página da IREX é https://www.irex.org, acesso em 5 de outubro de 2010.

e talvez seja preciso ampliar a redundância da capacidade de transmissão de informações por satélite.

No que concerne à dimensão informacional, a forte dependência da população, para o acesso a notícias e informações, para com plataformas de mídias sociais e aplicativos de mensagem cujas sedes estão no exterior – a imensa maioria das quais pode vir a ceder a pressões advindas de seus países de origem, com raras exceções –, sem nenhum substituto óbvio amplamente disponível, pode ser considerada uma séria vulnerabilidade do ambiente informacional brasileiro contemporâneo.

Outra vulnerabilidade significativa é a potencial dificuldade do público em identificar informações falsas, ou indícios de que o sejam. Para essa vulnerabilidade, a única forma de ação com efeito em curto prazo – a censura – não é eticamente aceitável, principalmente em democracias, e tende a ser contraproducente ao longo do tempo. Apesar de importantes, esforços de desmascarar informações falsas tomam muito tempo e muitos recursos, e eventualmente só alcançarão o público após uma série de consequências produzidas pela informação falsa originalmente difundida. Desse modo, ganha destaque como uma alternativa importante, e que parece promissora, são os programas de "alfabetização midiática" ou "alfabetização informacional", que qualificam o público para identificar informações falsas. Essa qualificação leva tempo, mas, por outro lado, seus benefícios não só tendem a ser duradouros, como são também úteis até mesmo no dia a dia; portanto, parece valer a pena começar uma discussão a respeito disso.

A partir dessa análise, pensada como um diagnóstico preliminar, pode-se começar um esforço de conceber alternativas de enfrentamento daquelas vulnerabilidades.

REFERÊNCIAS

Adamy, David L. 2021. *EW 105: Space Electronic Warfare*. Boston (Mass.), Artech House.

Antonik, Luís Roberto. 2013. *Tudo o que você precisa saber sobre rádio e televisão: licenças, outorgas, taxa de penetração, receitas, audiências e receptores*. Brasília, Associação Brasileira de Emissoras de Rádio e Televisão (ABERT), 2013 (abril). Disponível em https://www.acaert.com.br/storage/files/ckeditor/files/Tudo_o_que_voc%C3%AA_precisa_saber_sobre_r%C3%A1dio_e_televis%C3%A3o_v%20ers%C3%A3o_maio_2013.pdf, acesso em 3 de outubro de 2023.

BNamericas. 2021. *Spotlight: Who leads Brazil's cloud market and in which verticals?* November 26, 2021. Disponível em https://www.bnamericas.com/en/features/spotlight-who-leads-brazils-cloud-market-and-in-which-verticals, acesso em 3 de outubro de 2023.

Bonaventura, Adalto. 2023. "Samsung lidera o mercado de celulares no Brasil; veja o ranking". Disponível em https://www.oficinadanet.com.br/smartphones/44420-market-celulares-janeiro-2023-brasil, acesso em 2 de outubro de 2023.

Chan, Man-pui Sally; Jones, Christopher R.; Jamieson, Kathleen Hall; Albarracín, Dolores. 2017. "Debunking: A Meta-Analysis of the Psychological Efficacy of Messages Countering Misinformation". Psychological Science, 28 (11), pp. 1531-1546.

Chen, Yuyu; Yang, David Y. "The Impact of Media Censorship: 1984 or Brave New World?" *American Economic Review*, Vol. 109, No. 6, June 2019, pp. 2294-2332.

Dave, Paresh. 2022. "YouTube blocks Russian state-funded media channels globally". *Reuters*, March 11, 2022. Disponível em https://www.reuters.com/business/media-telecom/youtube-blocks-russian-state-funded-media-channels-globally-2022-03-11/, acesso em 3 de outubro de 2023.

Diniz, 2023a. “Mapeamento Preliminar da Trajetória das Discussões sobre ‘Ambiente Informacional’ e ‘Guerrear Informacional’”. *Análise Estratégica* 30 (3), pp. 69-97.

Diniz, 2023b. ““Guerrear Informacional” e Atividades de Influência no Ambiente Informacional Contemporâneo: Uma avaliação preliminar”. *Análise Estratégica* (no prelo).

Fung, Brian. 2021. “Parler has now been booted by Amazon, Apple and Google”. *CNN*, January 11, 2021.

Golovchenko, Yevgeniy. 2022. “Fighting Propaganda with Censorship: A study of the Ukrainian ban on Russian Social Media”. *The Journal of Politics*, 84 (2), April 2022.

Haigh, Maria; Haigh, Thomas; Matychak, Tetiana. 2019. “Information Literacy vs. Fake News: The Case of Ukraine”. *Open Information Science* 2019; 3, pp. 154–165

Henry, Caleb. 2019. “Brazil to order second dual civil-military communications satellite”. *Space News*, April 10, 2019. Disponível em https://spacenews.com/brazil-to-order-second-dual-civil-military-communications-satellite/, acesso em 2 de outubro de 2023.

International Telecommunications Union. 2023. *Brazil country review: regulation in the digital transformation*. Disponível em https://www.itu.int/hub/publication/d-pref-them-31-2023/, acesso em 4 de outubro de 2023.

Jansen, Sue Curry; Martin, Brian. 2015. “The Streisand Effect and Censorship Backfire”. *International Jornal of Communication*, 9(1), pp. 656-671.

Paczkowski, John; Mac, Ryan. 2021. “Amazon Will Suspend Hosting for Pro-Trump Social Network Parler”. *BuzzFeedNews*, January 9 (updated January 10), 2021. Disponível em https://www.buzzfeednews.com/article/johnpaczkowski/amazon-parler-aws, acesso em 3 de outubro de 2023.

Pennington, Josh; Lyngaas, Sean. 2023. “Starlink in use on ‘all front lines,’ Ukraine spy chief says, but wasn’t active ‘for time’ over Crimea”. *CNN*, September 10, 2023. Disponível em https://edition.cnn.com/2023/09/10/europe/ukraine-starlink-not-active-crimea-intl-hnk/index.html, acesso em 4 de outubro de 2023.

Potter, W. J. 2014. “Guidelines for media literacy interventions in the digital age”. *Medijska istraživanja: znanstveno-stručni časopis za novinarstvo i medije*, 20 (2), pp. 5-29.

Pryhara, Iryna. 2018. *Understanding and Countering Russia’s Information Warfare*. Disponível em https://ruor.uottawa.ca/bitstream/10393/37999/1/PRYHARA%2c%20Iryna%2020185.pdf, acesso em 15 de julho de 2023.

Reuters Institute for the Study of Journalism. 2021. *Reuters Institute Digital News Report 2021*. Disponível em https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2021-06/Digital_News_Report_2021_FINAL.pdf, acesso em 3 de outubro de 2023.

Reuters Institute for the Study of Journalism. 2022. *Reuters Institute Digital News Report 2022*. Disponível em https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2022-06/Digital_News-Report_2022.pdf, acesso em 3 de outubro de 2023.

Shaffer, Christian. 2023. “Deplatforming Censorship: How Texas constitutionally barred social media

platform censorship". *SSRN Paper*, disponível em https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4332206, acesso em 19 de julho de 2023.

The International Institute for Strategic Studies (IISS). 2023. "Brazil". In: _____. *Cyber Capabilities and National Power Volume 2*. London, he International Institute for Strategic Studies, pp. 11-28.

Vaiano, Bruno. 2023. "Starlink, o verdadeiro X de Elon Musk". *Superinteressante*, setembro de 2023, pp. 32-39.

Welti, Robert. 2012. *Satellite Basics for Everyone: An illustrated guide to satellites for non-technical and technical people.* Bloomington (IN), Iuniverse.

Western Australian Auditor General. 2023. *Better Practice Guide: Security Basics for Protecting Critical Infrastructure from Cyber Threats*. Disponível em https://audit.wa.gov.au/wp-content/uploads/2023/06/Report-24_-Security-Basics-for-Protecting-Critical-Infrastructure-from-Cyber-Threats.pdf, acesso em 2 de outubro de 2023.

Wu, Ziyi. 2020. "Censorship Can Be Counterproductive: Why are certain kinds of political rumors more credible than others? A mixed-method study on Chinese social media". *American Political Science Association Annual Conference 2020*. Disponível em https://preprints.apsanet.org/engage/api-gateway/apsa/assets/orp/resource/item/5f46a0111073290013cc710f/original/censorship-can-be-counterproductive-sensitivity-and-media-credibility.pdf, acesso em 19 de julho de 2023.