Nesta edição - Renata Ávila . E. Woodhouse e D. Thakur . Marina Pita . Farzaneh Badii . Diego R. Canabarro

POLITICS

Uma publicação do Instituto Nupef | Ano X | nº29 | jun-set 2019

Brinquedos conectados
e os riscos à infância

Distribuição gratuita

A Democracia digital e o futuro dos cidadãos
Sobre as estratégias de marketing político digital adotadas nos últimos anos em campanhas de presidentes eleitos como as de Donald Trump e Jair Bolsonaro.
Página 3

Banda larga para todos
Apesar de crescente, o acesso à internet segue sendo um desafio em países de baixa e média renda, onde muitas vezes o preço cobrado por ele é inacessível a boa parte da população.
Página 11

ICANN e Amazon.com
A controvérsia envolvendo a delegação do domínio de topo **.amazon**, pela Corporação da Internet para Atribuição de Nomes e Números (ICANN) para a empresa de comércio eletrônico Amazon.
Página 30

Editorial

Nesta edição da POLI**TICS** são apresentados temas atuais de absoluta importância para a democracia com a densidade que eles merecem ser tratados.

O artigo de Renata Ávila, advogada internacional de direitos humanos e diretora executiva da Fundação Cidadão Inteligente, no Chile, discute as estratégias de marketing político digital adotadas nos últimos anos em campanhas de presidentes eleitos como a de Donald Trump e de Jair Bolsonaro, e sugere o que precisa ser feito nessa conjuntura para evitar que a democracia seja ameaçada.

Apesar de crescente, o acesso à internet segue sendo um desafio em países de baixa e média renda, onde muitas vezes o preço cobrado por ele é inacessível a boa parte da população. É isso que nos mostram Woodhouse e Thakur, pesquisadores da Alliance for Affordable Internet (A4AI), em texto especial para a POLI**TICS**, por meio de pesquisa realizada com base nos preços dos serviços da banda larga móvel em 99 países, com especial atenção para a América Latina e o Caribe.

Marina Pita, jornalista, pesquisadora de mídias digitais e direitos das crianças do programa Prioridade Absoluta e assessora para advocacy do Instituto Alana, apresenta os desafios impostos pelos brinquedos inteligentes para a proteção de crianças e adolescentes. Tendências no mercado mundial, os brinquedos conectados representam ao mesmo tempo oportunidades de inovação criativa para o desenvolvimento das crianças e grandes riscos para sua privacidade e segurança.

Por fim, a presente edição da POLI**TICS** traz dois textos sobre a controvérsia envolvendo a delegação do domínio de topo .amazon, pela Corporação da Internet para Atribuição de Nomes e Números (ICANN), para a empresa de comércio eletrônico Amazon.

Farzaneh Badii, diretora executiva do Internet Governance Project (IGP) e pesquisadora associada da Escola de Política Pública do Instituto de Tecnologia da Georgia, nos Estados Unidos, defende a delegação do domínio e a não interferência de governos nas decisões da ICANN, remetendo a uma campanha liderada pelo Grupo de Interesse de Usuários Não Comerciais (NCUC) da entidade, iniciada há 12 anos ("Keep the Core Neutral"), motivada originalmente pelas resistências à aprovação do domínio .xxx.

Já Diego Canabarro, consultor do Comitê Gestor da Internet no Brasil (CGI.br) até maio de 2019, em texto especial para a POLI**TICS**, relata o processo em detalhes e discute as possíveis consequências e riscos da delegação do domínio para a empresa – tanto para a ICANN como para a prática pluralista na governança da Internet.

Boa leitura!

29

POLI**TICS** 29 | Ano X | junho-setembro de 2019

Todas as edições da POLITICS estão disponíveis em **https://politics.org.br**

Se você quiser receber gratuitamente a edição impressa da revista, envie um e-mail para **politics@nupef.org.br** com seu nome, endereço completo - incluindo o CEP - e a sua área de atuação.

Uma publicação do Instituto Nupef
https://nupef.org.br

ISSN 1984-8803

INSTITUTO NUPEF

Renata Ávila, advogada internacional de direitos humanos, diretora executiva da Fundação Cidadão Inteligente, Chile

A DEMOCRACIA DIGITAL e o FUTURO DOS CIDADÃOS[1]

Será que temos informação suficiente para poder regular a atividade dos provedores de dados que desempenham hoje um papel chave no desenvolvimento das campanhas eleitorais e de nossas democracias?

A vitória de Jair Bolsonaro no Brasil em 2018 colocou em evidência o papel das empresas de marketing nas redes sociais nas eleições e a sua poderosa influência na polarização dos processos políticos. Houve sem dúvida um impacto na deflagração da vitória de partidos políticos e de líderes outrora estranhos ao mundo da política.

Esta tendência é agora a regra e não a exceção nas sociedades democráticas. O que os meios de comunicação em todo o mundo qualificaram como excepcional, como a suposta intervenção estrangeira que levou à derrota de Hillary Clinton nas eleições presidenciais de 2016 nos Estados Unidos, ou a vitória do Brexit em um referendo no mesmo ano no Reino Unido, se converteu em um evidente padrão em todos os processos eleitorais desde então.

Com a crescente popularidade das redes sociais e da Internet, as técnicas de propaganda política e as campanhas *online* foram se adaptando para tirar proveito da enorme

1. O texto foi publicado originalmente em espanhol e em inglês em 18 de Janeiro de 2019, no sítio https://www.opendemocracy.net

quantidade de dados pessoais disponíveis. As novas técnicas de publicidade utilizam dados (que se encontram disponíveis *online*), programas de aprendizado automático e pesquisa psicológica para gerar mensagens destinadas a públicos-alvos específicos.

Essas mensagens baseiam-se não apenas em dados demográficos refinados, como também em informações relativas ao nosso comportamento *online*. Os pontos que faltam para concluir um esboço de determinado perfil quase sempre são completados com base em semelhanças com outros usuários ou clientes que disponibilizam um conjunto de dados mais amplo. O interesse dos responsáveis nas campanhas eleitorais pelo uso de técnicas de publicidade o mais eficazes possível os tem levado a adotar essas abordagens de marketing baseada em dados.

Mas como uma campanha baseada em dados se dá por dentro? E quais as normas existentes para preservar a liberdade dos eleitores e garantir a imparcialidade durante a campanha e as eleições? São levados em conta os direitos digitais dos eleitores?

Anatomia das campanhas eleitorais baseadas em dados: o papel dos provedores privados

Nos últimos meses, o projeto Data Politics, coordenado pelo Transparency Toolkit,[2] desenvolveu uma wiki para compilar informação sobre os provedores que oferecem serviços digitais para campanhas *online*. O objetivo desse repositório não é somente mostrar o alcance e a variedade dos atores envolvidos no marketing político, mas também proporcionar uma ferramenta colaborativa que ajude a aprofundar as pesquisas sobre a indústria do marketing político.

Até agora, o Data Politics identificou centenas de empresas que prestam serviços para diferentes fases das campanhas eleitorais baseadas em dados e que utilizam táticas de marketing. O acervo contém informações e referências de até 300 provedores envolvidos em campanhas eleitorais, ilustrando assim um fenômeno que vai muito além do célebre e triste escândalo da Cambridge Analytica.[3] Ainda que a pesquisa inicial tenha enfocado provedores mexicanos, o objetivo do "Data Politics" é ampliar suas fontes.

Para uma melhor compreensão, vamos guiar o leitor através de cada fase do processo:

1. Coleta de dados dos eleitores

Para poder influenciar os eleitores, a primeira coisa a se fazer é estabelecer quem eles são e o que pensam. Isso se consegue através da coleta de listas de eleitores, dados demográficos e opiniões, crenças, comportamento ou preocupações. E isso se obtém por meio do acesso a dados oficiais, como listas de pessoas com direito a voto, facilitadas pelas autoridades eleitorais, dados públicos disponíveis, como o censo, além de informações comerciais e outras coletadas com objetivos políticos.

O problema nessa fase é a tênue linha que separa a coleta de dados com fins políticos e aqueles com fins comerciais, que permitem uma elaboração de perfis cada vez mais refinados em relação aos hábitos preferenciais dos consumidores. Esta informação está sendo vendida hoje aos responsáveis pelas campanhas eleitorais. Os "proprietários" desses dados são geralmente intermediários, de modo que o negócio emergente de intermediação de dados está começando a ter um papel relevante.

Um exemplo interessante é o caso de Pig.gi,[4] uma empresa de pesquisas em Xochimilco, no México, e a iniciativa sem precedentes – vinculada à Cambridge Analytica –, levada a cabo por esta empresa, de proporcionar Internet gratuita a comunidades previamente desconectadas.

Tudo começou em Tizilingo, uma localidade tão pequena que não aparece no Google Maps. Ainda que nenhum dos residentes dispusesse de computador pessoal, uns 60 tinham telefones móveis, muitos dos quais podiam conectar-se à rede gratuita. Para muitos deles, então, o acesso gratuito à Internet chegou antes que a água encanada.

Mas o que fez Pig.gi nessa pequena comunidade de 100 pessoas ao sul da Cidade do México, em aparente coordenação com a Cambridge Analytica, apaga a linha que separa o altruísmo da exploração e camufla o custo oculto do acesso gratuito à Internet – algo que as comunidades pobres do México e outras muitas partes do mundo não

2. https://transparencytoolkit.org
3. https://pt.wikipedia.org/wiki/Cambridge_Analytica
4. https://pig.gi

conseguem compreender totalmente.

O que estamos presenciando, cada vez mais, é a realização de provas de práticas de coleta de dados em populações desfavorecidas para sua posterior exploração e reutilização. À primeira vista, um projeto como o de Pig.gi parece de caridade, mas na realidade a contrapartida é a obtenção de dados da comunidade. E a supervisão que exercem as autoridades eleitorais e as autoridades de proteção de dados na atualidade resulta inadequada em circunstâncias em que se utiliza esse tipo de ferramentas para monitorar e influenciar as opiniões dos eleitores pobres, que são geralmente votantes indecisos.

Também se tornaram atores fundamentais de todo o processo de coleta de dados os gigantes tecnológicos. As redes sociais são fantásticas fontes de informação sobre os eleitores. Seus sites servem para compilar dados demográficos, monitorar opiniões e conversas e coletar outras informações que os usuários expressam explicitamente.

Além disso, sobre essa base podem ser elaborados novos dados através de processos de inferência: existem estudos que mostram como se podem deduzir traços de personalidade, pontos de vista políticos e outras características através de dados como "curtir" do Facebook. Ademais, há empresas de escuta social ("*social listening*") especializadas em monitorar, agregar e analisar discussões nas redes sociais sobre determinados temas, candidatos, partidos ou marcas.

Tais empresas coletam dados das plataformas das redes sociais mediante o uso de APIs públicas, rastreadores da rede (rastreador web) ou simplesmente os comprando. Portanto, utilizam suas próprias ferramentas ou *software* disponível no mercado para analisar tendências e identificar usuários influentes.

Outro tipo de empresa são as intermediárias de dados que coletam informações sobre pessoas a partir de fontes diversas: redes sociais, registros públicos e empresas privadas. Estas empresas partem, geralmente, de informações limitadas, como uma lista de e-mails de clientes ou contas de redes sociais, e as combinam com informações de contato mais detalhadas – comportamento de compra, detalhes demográficos e dados de pesquisa e navegação na Internet – de pessoas que aparecem na lista inicial.

A quantidade de dados disponíveis para esses intermediários depende das regulações dos países onde operam. Os atores mais recentes neste campo de coleta de dados são as empresas de psicologia política. Seus consultores realizam pesquisas para obter dados sobre os eleitores e desenvolver perfis psicológicos. Seus serviços incluem desde a coleta de dados a partir de simples levantamentos sobre as intenções de votos até a realização de pesquisas sobre opiniões e crenças.

> "As redes sociais são fantásticas fontes de informação sobre os eleitores. Seus sites servem para compilar dados demográficos, monitorar opiniões e conversas e coletar outras informações que os usuários expressam explicitamente."

As próprias campanhas eleitorais e as empresas de marketing baseado em dados que oferecem um serviço completo normalmente contratam empresas de psicologia política para realizar pesquisas de apoio ("*background research*") que ajudam a criar perfis para o direcionamento de mensagens aos eleitores. Essas empresas são, até o momento, as de que menos se exige prestar contas.

2. Segmentação e identificação dos eleitores

Os dados demográficos, os perfis psicológicos e outras informações obtidas durante a fase de coleta de dados são combinados e utilizados para segmentar públicos – ou seja, para agrupar os eleitores em conjuntos menores. A informação acumulada durante a fase de coleta se guarda na mesma base de dados usada para administrar as listas de eleitores adquiridas na primeira fase do processo, ou em um *software* distinto.

Sempre que possível, os pacotes de dados são consolidados para gerar perfis pessoais mais completos. Alguns programas incluem visualizações de mapas, gráficos ou ferramentas de campanha para aproveitar os dados dos eleitores, como se pôde ver na ocasião da exitosa campanha eleitoral de Emmanuel Macron, que utilizou os serviços da empresa francesa Liegey Muller Pons.[5]

Devido à complexidade do marketing político baseado em dados, existe uma necessidade cada vez maior de que as empresas integrem todas as etapas do processo em uma solução completa para oferecer às campanhas, aos partidos ou aos candidatos. Esse é o papel de empresas como Cambridge Analytica.

O valor principal de sua oferta é a combinação de vários pacotes de dados da primeira fase do processo com as técnicas de difusão da última etapa. E isso se consegue por meio de um conjunto de elementos: pessoal próprio, ferramentas internas, *software* criado por outras empresas, dados adquiridos e a associação com outras organizações. As empresas de marketing político que oferecem o serviço completo vão desde pequenas companhias que prestam seus serviços a campanhas locais até grandes empresas internacionais que trabalham em várias campanhas de alto nível a cada ano.

As empresas internacionais geralmente trabalham associando-se a empreendimentos nacionais para conseguir proximidade com o contexto local, ou como forma de ocultar sua participação na campanha eleitoral. As companhias de marketing político que oferecem um "pacote completo" de soluções apresentam uma ampla gama de combinações de serviços.

Algumas dessas empresas seguem com rigor todas as regulações eleitorais e de uso de dados vigentes, criam anúncios identificados como tais, utilizam-se de técnicas de propaganda positiva e operam de maneira transparente sob seu próprio nome. Outras fazem um mau uso dos dados, de técnicas dissimuladas para manipular opiniões, criam anúncios que exploram os medos das pessoas, se envolvem em práticas duvidosas como chantagem e recorrem a empresas de fachada para ocultar sua participação nas campanhas eleitorais.

As fontes de dados e as técnicas de publicidade que utilizam umas e outras são determinadas pelo contexto local, a experiência, as associações e os distintos padrões éticos em relação à proteção de dados. As empresas de serviços não completos também podem se situar em qualquer ponto do espectro ético.

A criação de perfis completos dos eleitores permite aos responsáveis das campanhas dividi-los em segmentos de público mais concretos e detalhados de modo que possam ser objeto de mensagens específicas. Depois de identificar esses segmentos de público, criam conteúdos que se ajustam às opiniões e preocupações de cada subgrupo. Uma das técnicas em que se destacam as empresas de serviços completos é a de *microtargeting*, que requer combinar dados de muitas fontes com uma variedade de mecanismos de difusão das mensagens.

Na etapa de evolução das técnicas de marketing político em que nos encontramos, as autoridades eleitorais e de proteção de dados em grande medida se destacam por sua ausência. Não dispõem ainda de recursos e capacidades necessários para fiscalizar e avaliar os conteúdos e as práticas dos provedores de dados nas campanhas eleitorais.

Nenhum país desenvolveu ainda a legislação nem tampouco programas de formação necessários para poder implementar este nível de avaliação e garantir o cumprimento das normas.

Isso quer dizer que as eleições ficam expostas a perigosas manipulações de opiniões, distorcendo sua imparcialidade. Não parece haver vontade política para abordar as implicações que as campanhas eleitorais baseadas em dados e o modelo de negócios que as impulsiona têm para os direitos humanos.

Etapa final: difusão de mensagens e tentativas de influenciar os eleitores

Depois de identificar os eleitores (os públicos) e segmentá-los, as mensagens e outras formas de persuasão podem difundir-se através de distintos canais para incidir sobre seu voto. Além disso, meios oficiais de propaganda política, as redes sociais comerciais oferecem oportunidades adicionais para enviar mensagens tanto diretamente a partir das contas oficiais das campanhas ou indiretamente por meio de robôs (*bots*) e *trolls*.

5. A empresa agora tem o nome de Explain – https://explain.fr

Embora os anúncios possam ser exibidos em diferentes sites, utilizando por exemplo o Google Ads, os responsáveis pelas campanhas optam geralmente pelas plataformas de redes sociais. As pessoas passam, nelas, enorme quantidade de tempo ao longo do dia, o que faz delas um caminho fácil para se chegar aos eleitores. E ainda que as propagandas nas redes sociais sejam geralmente acompanhadas da sinalização de "conteúdo patrocinado", um estudo revela que 32% dos usuários não percebem isso e aceitam a publicidade de maneira parecida com a que recebem conteúdos publicados por seus amigos.

As empresas que oferecem assessoria em temas de gestão de conteúdo nas redes sociais proliferam. Elas podem criar conteúdos para diferentes plataformas de redes sociais que se difundem diretamente a partir das contas da campanha do candidato. Em alguns casos, as campanhas podem assumir essa gestão, mas também existem empresas especializadas que oferecem como serviço campanhas tradicionais nas plataformas. Essas empresas podem utilizar também outras técnicas, como anúncios, robôs (*bots*) e *trolls*, no âmbito de uma estratégia abrangente de redes sociais.

Há também os anúncios, pagos através de canais oficiais, que se dirigem especificamente a pessoas em função de seu perfil – personalidade, histórico de compras ou de navegação, dados demográficos ou outros atributos. O nível de sofisticação varia: desde anúncios genéricos exibidos a muitas pessoas até mensagens muito específicas exibidas diversas vezes a pessoas que fazem parte de pequenos segmentos de público. Os destinatários também podem ser selecionados em função de sua interação com mensagens anteriores. Esta última fase é a mais preocupante do ponto de vista dos direitos digitais, já que é a que se encontra hoje menos regulada e menos transparente.

No entanto, é também a fase que oferece mais oportunidades para que as autoridades eleitorais realizem reformas que garantam que este tipo de avanço tecnológico não seja utilizado de maneira prejudicial à liberdade de pensamento dos eleitores, ou que se torne uma forma de realizar campanhas que minem o conceito de eleições livres e justas.

É precisamente neste ponto que as autoridades de proteção de dados e as organizações de consumidores poderiam desempenhar um importante papel de monitoramento – por exemplo, garantindo que todos os partidos gozem de igual acesso aos mesmos dados. E garantindo que os dados pessoais coletados para publicidade e marketing não sejam reutilizados com fins políticos.

Esta separação entre usos comerciais e eleitorais de nossos dados é muito importante. É a única forma de se exigir responsabilidades dos partidos políticos por seu investimento em infraestrutura de coleta de dados, obrigando-os a manter-se dentro dos limites legítimos de despesas com campanha política, bem como a demonstrar que seus métodos de compilação de dados foram éticos segundo a legislação de direitos humanos.

Busca-se: uma revisão urgente dos sistemas eleitorais *online*

A qualidade das eleições nos sistemas democráticos é medida pela imparcialidade e a atenção ao devido processo que garanta a liberdade do pleito eleitoral. Os desenvolvimentos tecnológicos nos contextos *online* nos obrigam a reexaminar se as salvaguardas atuais são suficientes para garantir o jogo limpo entre aquelas forças políticas que têm acesso às últimas tecnologias e a conjuntos de dados sofisticados para dirigir suas mensagens à população e as que não o têm.

Os níveis atuais de despesas com eleições dos partidos políticos foram fixados sobre a base do tipo de informação e divulgação analógica de tempos anteriores à Internet: *outdoors*, cartazes e tempo na TV e no rádio. Mas as campanhas eleitorais transformaram-se. Agora os partidos políticos estão investindo em ferramentas de campanha que escapam muito mais às prestações de contas, como a infraestrutura de dados e os algoritmos que os permitem direcionar suas mensagens aos eleitores.

As campanhas baseadas em grandes coletas de dados, em *softwares* sofisticados e em uma combinação de técnicas de publicidade *online* que utilizam algoritmos estão definindo nos dias de hoje os investimentos feitos pelos partidos políticos em futuras campanhas eleitorais. O que acontecerá com aqueles que não podem realizar tais investimentos? Como as campanhas futuras poderão ser iguais e justas existindo essas desigualdades entre os candidatos quanto ao acesso às bases de dados e aos sistemas de suporte? É alarmante o quão distante estamos de cumprir esses requisitos, considerando o número de países que carecem de leis básicas de privacidade e de proteção de dados.

Os reguladores e os encarregados de garantir que as eleições sigam sendo livres

> “Ver o potencial que essas tecnologias têm para interferir na democracia e testemunhar a forma como alguns dos Estados mais poderosos do mundo as têm utilizado já deveria, então, ter-nos chamado a atenção para o que estava por vir.”

e justas não deram atenção às advertências feitas por Edward Snowden em 2013, quanto ao perigo que representa o uso indevido de dados pessoais para os direitos e liberdades fundamentais das pessoas e para os processos democráticos. Na época, já era preocupante saber como as tecnologias comerciais e os dispositivos utilizados diariamente por um cidadão médio estavam se convertendo em armas de vigilância e de manipulação e em ferramentas, por parte das autoridades e de empresas, para a utilização do que se sabe sobre os usuários de Internet em uma variedade de situações – por exemplo, para espionar missões humanitárias, conseguir uma injusta vantagem estratégica e comercial, infiltrando-se em sistemas informáticos dos concorrentes e de partes contrárias em negociações diplomáticas ou comerciais.

Ver o potencial que essas tecnologias têm para interferir na democracia e testemunhar a forma como alguns dos Estados mais poderosos do mundo as têm utilizado já deveria, então, ter-nos chamado a atenção para o que estava por vir. Mas, além da revisão da Lei Geral de Proteção de Dados (LGPD ou GDPR) europeia,[6] o que tais revelações fizeram foi acelerar a regularização de muitas atividades ilegais das agências de espionagem. O escândalo da Cambridge Analytica só serviu para destacar a existência dessa nova realidade difícil de enfrentar: o uso estratégico das tecnologias digitais e em rede para enfraquecer os processos democráticos baseados na devida consulta, deliberação e avaliação.

Nem a Cambridge Analytica é um ator isolado nem as eleições nos Estados Unidos foram uma exceção, mas o caso ajudou a colocar luz sobre a existência de uma próspera indústria muito pouco regulada que, em diferentes etapas das campanhas eleitorais, com ou sem autorização, e geralmente sem fiscalização, utiliza dados públicos para tentar alterar o voto dos eleitores da mesma forma que se utilizam de nossos dados pessoais para vender produtos. A falta de ação já não é uma opção.

Adaptando-nos aos novos desafios: a atualização dos controles democráticos *online*

Esses acontecimentos trouxeram à tona o evidente conflito de interesses das plataformas comerciais considerando os diferentes papeis que desempenham durante as campanhas eleitorais.

As plataformas de redes sociais e os navegadores se tornaram atores chaves como provedores de dados neste contexto. No entanto, eles ainda precisam desenvolver políticas de transparência adequadas e melhores práticas responsáveis para demonstrar sua imparcialidade nas disputas eleitorais. Atualmente é impossível fazer auditorias nelas com base nos marcos regulatórios globais vigentes. E essas plataformas, além disso, mantêm o segredo como vantagem comercial.

Mas considerando-se o papel que desempenham hoje nas campanhas eleitorais, devem-se estabelecer exceções a suas práticas comerciais – por exemplo, regras para impedir que as plataformas “atraiam os votantes” de

6. https://eugdpr.org

forma ativa, ou que ofereçam informação sobre em quem devem votar:

• *Sua função como provedores de dados entra em conflito não somente com a participação "cívica", mas também com seu crescente papel na organização de debates online ou como "pontos de informação" para os eleitores. Dito de outro modo, as plataformas comerciais não devem extrapolar seu papel de provedores de propaganda política regulados.*

• *Por essa razão, a transparência do algoritmo é também um elemento chave para garantir que não se dê, em um dado momento, uma vantagem injusta a algum candidato durante uma campanha eleitoral em função da quantidade de dados personalizados e específicos que o candidato em questão pode comprar.*

• *Deve-se também obrigar as equipes de campanha a divulgar os tipos de dados que utilizam, a origem de tais dados e o seu projeto de utilização deles. Uma parceria entre associações de consumidores, autoridades de proteção de dados e eleitorais poderia supervisionar também o uso de dados pessoais compilados com fins comerciais para manter as bases de dados separadas e aferidas.*

O problema hoje em dia é que, no lugar de se estabelecer limites, tanto as autoridades eleitorais como o público em geral estão pedindo que as empresas de redes sociais façam mais coisas – por exemplo, adotar medidas para abordar o tema da violência política, o assédio virtual (*cyberbullying*) ou para impedir a interferência de atores estrangeiros nas campanhas eleitorais. No contexto atual, essas demandas contraditórias conduzem a conflitos de interesse cada vez mais complexos.

Isso coloca a questão de se é possível que as plataformas comerciais se associem a organizações de direitos humanos e organismos de controle eleitoral, assim como a autoridades policiais, para responder rapidamente a possíveis sequestros de espaços eleitorais durante as campanhas com o objetivo de intimidar ou manipular os eleitores. E se isso for possível, como poderia funcionar essa parceria considerando que as plataformas comerciais não querem divulgar suas técnicas?

• *As mudanças nas legislações, entre elas o requisito para que os operadores comerciais abram sua "caixa-preta", levarão tempo e precisarão de vontade política para avançar. Mas uma resposta imediata poderia ser as plataformas abrirem voluntariamente suas bases de dados a pesquisadores independentes interessados em estudar os processos eleitorais. Atualmente, o preço e a disponibilidade de dados estão fora do alcance de pesquisadores e auditores independentes.*

• *Os governos devem ter também capacidade de adaptação e agilidade para enfrentar os desafios colocados pelas inovações tecnológicas aplicadas às campanhas eleitorais. Existem novas ameaças e novos repertórios de técnicas, inclusive de "truques", que podem ser acessados pelos responsáveis das campanhas. Isso requer um monitoramento amplo, do qual poderiam participar ativistas digitais. A sociedade civil, os organismos de controle eleitoral e as missões de observação podem sem dúvida desempenhar um papel crucial em preservar a democracia na era digital mediante a atualização e adaptação de seus mecanismos e sistemas de supervisão. O que implica a necessidade de se contar com voluntários e funcionários formados em direitos humanos, além de especialistas em tecnologia.*

• *A melhoria da transparência e da prestação de contas das campanhas em ambientes digitais e em rede poderia incluir a solicitação de uma lista de todos os provedores, produtos e serviços utilizados nas campanhas baseadas em dados (não somente de nível superior contratados pela campanha, como também a lista dos sistemas de onde os dados foram retirados e quem contratou tais provedores).*

• *Também deveriam ser a norma a realização de auditorias completas e a divulgação dos detalhes das infraestruturas de dados usadas pelos partidos. Isso implica melhorar a forma de levar a contabilidade das despesas políticas com a gestão de dados, bases de dados e a gama de técnicas de segmentação à disposição das equipes de campanha.*

• *Os requisitos de privacidade digital e online e o papel que podem desempenhar as autoridades de proteção de dados são também chave para preservar a liberdade dos eleitores na hora de decidir seu voto, sem manipulações indesejadas através das redes sociais de que são usuários, de seus aparelhos de telefonia móvel ou de seus*

amigos e familiares. O monitoramento do uso das bases de dados utilizadas pelos partidos nas campanhas é crucial para se conseguir zelar por essa liberdade.

As organizações da sociedade civil estão começando a realizar campanhas de *crowdsourcing* (colaboração aberta e distribuída) para implementar tarefas de monitoramento da propaganda política e poder, assim, identificar ao menos os que violam as regulações eleitorais vigentes. Mas poderiam ir mais longe:

- *Criando consciência entre os eleitores acerca da necessidade de monitorar a forma como se enquadram as mensagens para dirigi-las a diferentes grupos demográficos durante as campanhas eleitorais.*

- *Desenvolvendo um plano ético: apesar dos aspectos preocupantes das campanhas baseadas em dados até hoje, as técnicas utilizadas poderiam se transformar, com políticas públicas adequadas e a coordenação entre diferentes autoridades, em oportunidades para o uso mais eficaz dos recursos – por exemplo, para potencializar a participação política através do tipo de divulgação facilitadas por elas. Por outro lado, as campanhas baseadas em meios digitais podem terminar sendo mais baratas que as convencionais para partidos políticos pequenos e candidatos independentes, desde que tenham habilidades e capacitação adequadas. E os robôs podem ser planejados não para tirar do prumo os processos eleitorais democráticos, mas para fazer chegar informação a populações absenteístas e animá-las a conhecer seus direitos e a votar. As autoridades eleitorais poderiam promover projetos deste tipo com fins cívicos em vez de comerciais.*

- *Criando outro tipo de medida, que poderia ser a proibição, por parte das autoridades eleitorais, do intercâmbio de inteligência de* marketing *e de perfis de consumidores com os partidos políticos, para evitar formas ocultas de manipulação do comportamento eleitoral através da exploração das pegadas digitais dos eleitores.*

A chave em todos os âmbitos é a adoção de medidas eficazes e eficientes com suficiente antecipação, sem dar por consolidada a democracia, e reconhecendo-a como um sistema em evolução que deve assegurar constantemente a sua resistência e atualização. ■

BANDA LARGA PARA TODOS

Competição no mercado móvel, planos de dados e custo da Internet na América Latina e Caribe

E. Woodhouse e D. Thakur, pesquisadores da Alliance for Affordable Internet (A4AI)

Introdução

O acesso à Internet continua muito caro para bilhões de pessoas em todo o mundo, a maioria vivendo em países de baixa e média renda. Com base nos dados de preços mais recentes da Alliance for Affordable Internet (A4AI) sobre o custo da banda larga móvel em 99 desses países, um gigabyte (1 GB) de dados custa uma média de 5,76% da renda mensal de um indivíduo (renda nacional mensal bruta per capita). As opções que os consumidores têm em termos de compra de um ou mais planos de dados pré-pagos para chegar a 1 GB ao longo do mês variam muito.

No nível regional, os usuários da América Latina e do Caribe que usam 1 GB por mês precisam comprar planos mais caros com licenças de dados maiores em comparação com usuários com franquia similar na África ou na Ásia. Convertendo os planos de referência da A4AI para uma taxa por GB, a acessibilidade diminui de forma consistente em todo o mundo; e a diferença de acessibilidade entre os planos teoricamente calculados e o que os usuários podem realmente adquirir é maior na América Latina e no Caribe. O que incentiva essa disparidade regional?

Este artigo explora e adiciona novo entendimento às condições de mercado que influenciam o preço da banda larga móvel. Argumentamos que, à medida que as operadoras de redes móveis montam os planos de dados e, a partir disso, criam níveis de preços escalonados, a renda média mensal e a concorrência no mercado parecem desempenhar fatores determinantes. Este último é um fator mais estreito e tem um papel estatisticamente mais significativo no preço final que um indivíduo deve pagar. Isso deve encorajar os formuladores de políticas a dar atenção especial à concorrência no mercado, se tiverem a intenção de expandir o acesso à Internet e estimular preços de banda larga mais acessíveis para todos.

Este artigo resume em primeiro lugar o estado da acessibilidade da Internet em países de baixa e média renda, usando os últimos dados divulgados recentemente pela A4AI. Em seguida, considera as diferenças regionais e econômicas que contextualizam os custos da conectividade. Em terceiro lugar, comparamos os planos de dados reais que os consumidores devem comprar para alcançar o mínimo de 1GB de banda larga móvel com referência comparada e comparamos com uma versão pro-rata com base nas franquias de dados que os usuários devem adquirir para alcançar esse mínimo. Quarto, propomos um modelo preliminar de regressão linear que identifica potenciais influências no preço da banda larga móvel. Com base nessas descobertas, concluímos com um apelo por pesquisas adicionais e defesa de políticas incidentes na concorrência de mercado no setor.

Situação do custo da Internet

Nos últimos quatro anos, a A4AI monitorou os preços de banda larga móvel em países de baixa e média renda para medir a acessibilidade econômica e incentivar a mudança de política para reduzir os custos da indústria de banda larga. Seus dados mais recentes baseiam-se nos preços de mercado de dezembro de 2018 e cobrem 99 países.[1] Os dados incluem pontos de preço para pacotes de 100 MB, 500 MB, 2 GB, 5 GB e 10 GB, além de 1 GB, e são baseados na mesma metodologia usada pela União Internacional da Telecomunicação (UIT) para os seus indicadores de preços.

Esta última atualização avalia os 1 GB como 5,76% da renda mensal, em média, nos países cobertos, bem acima do limite de acessibilidade estabelecido pela Comissão de Banda Larga da ONU e a A4AI, onde 1 GB de dados móveis tem preço de não mais que 2% da renda média.[2] De fato, apenas 31 dos países pesquisados têm banda larga móvel acessível. Isso significa que, entre os abrangidos, quase 1,3 bilhão de pessoas vivem em um país onde um plano básico de 1 GB de dados móveis não é acessível. Outros bilhões vivem em países que atendem ao limite "1 para 2", mas, por terem uma renda menor que a média, ainda assim lutam para pagar por pacotes básicos de dados móveis.

A utilização desses dados de preços nos permite compreender melhor a relação entre a acessibilidade da Internet, a estrutura dos mercados de telecomunicações e os impactos socioeconômicos do acesso à Internet. Com uma visão ampliada de 99 países este ano, somos capazes de construir modelos mais fortes e realizar análises com maior confiança. A A4AI também permite o acesso gratuito a seus dados de preços, que podem ser baixados em seu portal Web. Os dados coletados refletem a realidade do mercado de um usuário: o plano mais barato disponível para que alguém possa obter 1 GB de dados por mês.

Detalhando mais: análise de acessibilidade ao nível do plano de dados

No nível global, existe uma ampla relação entre os preços da internet móvel e a renda média em um país. Olhando para os 99 países, a renda média de um país se correlaciona positivamente com o preço que um consumidor paga por 1 GB de dados móveis **(r = 0,356, p ←0,001)**. Isso faz sentido no mercado: os operadores podem cobrar um preço mais alto em países de renda mais alta, onde os usuários têm mais renda disponível, e um preço mais baixo é necessário em países de baixa renda para assegurar que ainda haja uma economia de escala para apoiar o desenvolvimento da rede. Esse entendimento também se conecta

1. https://a4ai.org/new-mobile-broadband-pricing-data-reveals-stalling-progress-on-affordability/
2. https://a4ai.org/what-is-affordable-internet-access-anyway/

com as práticas do Banco Mundial,[3] ITU[4] e Comissão de Banda Larga da ONU,[5] que avaliam a acessibilidade como uma porcentagem da renda em vez do preço de mercado simples isoladamente. No entanto, as condições e tendências geográficas também devem ser levadas em conta.

Em uma comparação regional, os dados são menos acessíveis em toda a América Latina e Caribe do que uma tendência de renda apenas sugeriria. Entre os países estudados, os da América Latina e do Caribe representam metade dos países de renda média-alta **(n = 16 na ALC, 32 no total)** e apenas um dos 40 países de baixa renda. Ao mesmo tempo, o custo de dados móveis de 1 GB é de 3% da renda média em toda a região, comparado a 2% nos países asiáticos, onde a renda média é menor. Quando dividimos essas informações por grupo de renda, a tendência de menor acessibilidade para os usuários da América Latina e do Caribe é consistente em todas as três regiões entre os países de renda média. Dada essa divergência regional, analisamos os planos de dados comparativos para entender melhor esse fenômeno (Fig.1).

A variedade de diferentes planos de dados oferece oportunidades para as operadoras estruturarem o mercado de banda larga móvel. Além do preço, os planos de dados frequentemente diferenciam-se no período de validade e no volume de dados. Com o controle

(Fig. 1). Acessibilidade (preço do plano em relação à renda mensal média) - comparações entre países de baixa e média renda.

Região	N	Acessibilidade de 1 GB	Grupo de renda	N	Acessibilidade de 1 GB
África	48	9,0%	Baixa	26	14,5%
			Baixa-média	14	3,2%
			Alta-média	8	1,8%
América Latina e Caribe	21	3,0%	Baixa	1	3,9%
			Baixa-média	4	5,6%
			Alta-média	16	2,3%
Ásia	26	2,0%	Baixa	3	5,3%
			Baixa-média	15	1,6%
			Alta-média	8	1,3%
Fonte: Cálculos dos autores com base em dados da Alliance for Affordable Internet (2019)					

3. https://openknowledge.worldbank.org/handle/10986/30437
4. https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2017.pdf
5. https://broadbandcommission.org/Documents/publications/wef2018.pdf

> “Os tipos de planos de dados disponíveis para um usuário têm consequências sobre a acessibilidade dos dados para bilhões. À medida que monitoramos isso, as investigações sobre as condições de mercado que determinam os termos sob os quais o acesso é concedido é um tópico maduro para futuras pesquisas.”

dessas variáveis, as operadoras de redes móveis detêm um poder fundamental na definição dos termos sob os quais milhões acessam a Internet: a que custo, por quanto tempo, quanto, a que velocidade e, em certos casos, até mesmo a que hora do dia ou da noite.[6]

Usando os dados de preços mais recentes, juntamente com outros indicadores, pretendemos entender mais sobre as dinâmicas que afetam a acessibilidade da Internet, concentrando-nos nas tendências de quais tipos de planos de dados são as rotas mais acessíveis para a referência de 1 GB. Dada a divergência regional já mencionada na América Latina e no Caribe, essa região é o foco de nosso estudo aqui. Uma visão básica permite uma certa comparação de diferentes custos em distintas regiões do mundo, mas investigar mais profundamente permite resultados mais precisos sobre as dinâmicas influentes que afetam a acessibilidade geral. Com essa abordagem, a pesquisa pode levar a casos mais claros e mais convincentes de intervenção política ou de mercado para estimular maior acessibilidade e acesso.

Comparação de planos de dados

Em média, a rota mais barata para 1 GB de dados móveis por mês na América Latina exige que o usuário compre mais 1,6 GB além desse mínimo. A metodologia da UIT usada para avaliar a acessibilidade de preços requer apenas um mínimo de 1 GB de dados móveis com validade de pelo menos um mês: não é necessário que um usuário alcance essa referência com precisão. Por isso, em 29 dos 99 países estudados - dos quais 12 estão na região da América Latina e Caribe -, a rota mais barata para 1 GB de banda larga móvel exige que o usuário compre pelo menos 2 GB de dados. Isso constitui mais da metade dos países da ALC no estudo da A4AI, onde a estrutura de mercado incentiva os usuários a comprar acima, a preços mais altos, mesmo quando o uso de seus dados pode não exigir tal despesa. O plano de referência médio na região para o 1 GB mais barato de dados móveis na verdade inclui 2,6 GB: isso se compara a 1,8 GB na Ásia e 1,4 GB na África. Embora a as categorias de preços tenham um impactos específicos em cada região, a prática parece ser particularmente prolífica e influente na América Latina e no Caribe. A contabilização dessa diferença de volume pode alterar as percepções de acessibilidade.

Ao calcular os preços dos dados em uma base proporcional, a diferença de acessibilidade entre os países de renda média diminui. Calculamos uma taxa teórica "por GB" para medir onde a variação de preço pode confundir a acessibilidade como um complemento metodológico aos dados de preços da A4AI. Ao fazer isso, a acessibilidade média de 1 GB entre os países de renda média cai de 2,4% da renda média mensal para 1,6%.

6. https://eugdpr.org

(Fig. 2). Comparação da variância de preços em países de renda média entre o custo para o consumidor de 1 GB de banda larga móvel e uma acessibilidade proporcional.

	Acessibilidade média do consumidor 1 GB	Acessibilidade proporcional média 1 GB	Variância média
África	2,75%	2,04%	26,4%
América Latina e Caribe	2,96%	1,75%	42,8%
Ásia	1,51%	1,01%	29,7%
Países de renda média (média)	*2,36%*	*1,58%*	*32,6%*
Fonte: cálculos dos autores com base em dados da Aliança para Internet Acessível (2019)			

Com uma comparação regional, os custos caem mais na América Latina e no Caribe: 43% de sua realidade de mercado. Isso sugere uma equivalência de custo estrutural entre os países de renda média que não é convertida em termos reais de acessibilidade para os consumidores no mercado (Fig.2).

Como consequência dessa estrutura, uma espécie de inflação de preços esconde um potencial de menor acessibilidade para a banda larga móvel na região da América Latina e Caribe. Dados precisos sobre acessibilidade devem refletir a realidade do mercado para os consumidores. O preço proporcional teórico de 1 GB baseado no plano de referência não é, em si, uma ferramenta útil. No entanto, com ela e na comparação da variância de preços entre planos de dados reais e planos teóricos, a lógica para o estudo da manipulação de mercado torna-se mais forte.

Os tipos de planos de dados disponíveis para um usuário têm consequências sobre a acessibilidade dos dados para bilhões. À medida que monitoramos isso, as investigações sobre as condições de mercado que determinam os termos sob os quais o acesso é concedido é um tópico maduro para futuras pesquisas. Tentamos iniciar este estudo com um modelo preliminar de regressão linear para entender a dinâmica que afeta a precificação de banda larga móvel.

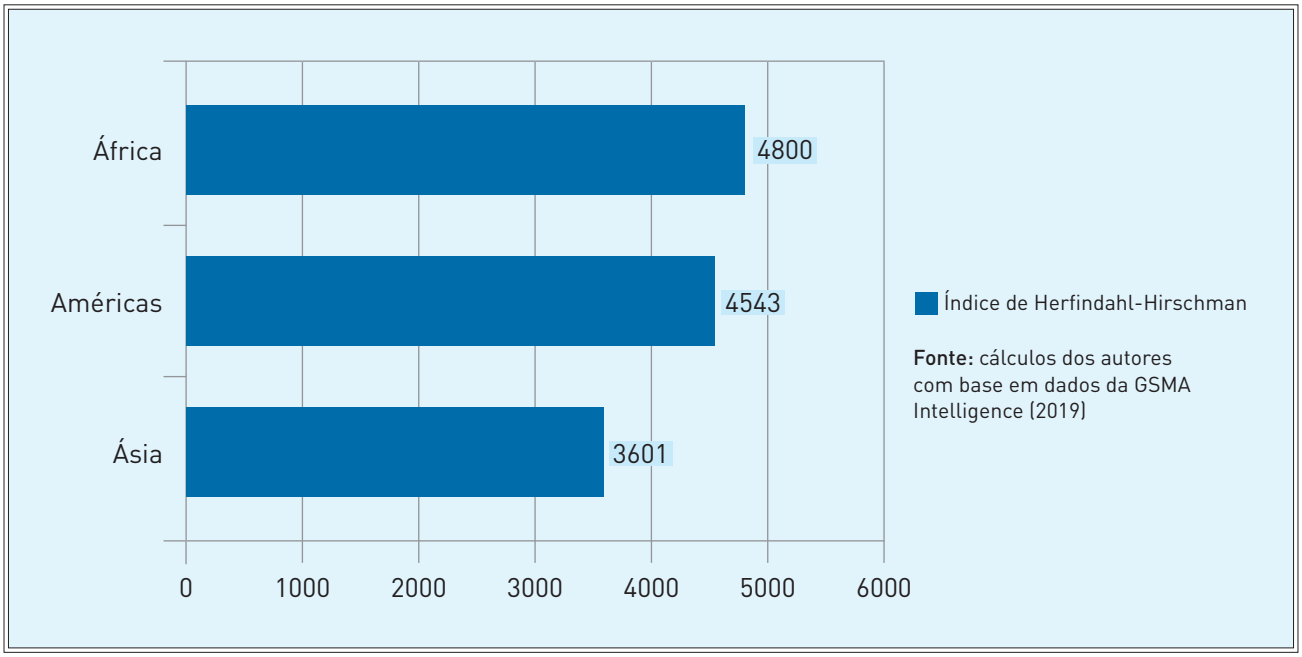
Competição de mercado e preços de dados

Como os preços e concessões do plano de dados permanecem em grande parte como uma prerrogativa das operadoras de redes móveis que os oferecem, este estudo enfoca os fatores que poderiam influenciar sua tomada de decisão e considera a concorrência de mercado particularmente importante. Nossa análise inicial baseou-se na comparação da concorrência de mercado entre os 99 países no estudo de preços da A4AI. Isso é medido pelo Índice Herfindahl-Hirschman (IHH),[7] que é baseado na adição do valor ao quadrado da participação no mercado de banda larga móvel de todos os operadores (Fig.3).

Nesta comparação, os países asiáticos apresentam consistentemente os menores escores do IHH (indicando mercados mais competitivos) entre todos os três grupos de renda medidos (renda baixa, média baixa e média alta). A força da disparidade regional estimulou sua inclusão em um modelo mais avançado.

7. O índice Herfindahl (também conhecido como Índice Herfindahl–Hirschman, ou IHH) é uma medida da dimensão das empresas relativamente à sua indústria e um indicador do grau de concorrência entre elas. Assim chamado a partir do nome dos economistas Orris C. Herfindahl e Albert O. Hirschman, é um conceito econômico amplamente utilizado na aplicação das regras da defesa da concorrência, da regulação antitruste e também da gestão da tecnologia. Ver https://pt.wikipedia.org/wiki/%C3%8Dndice_Herfindahl (n.ed.)

(Fig. 3). Comparação entre regiões da concorrência no mercado de banda larga móvel.



(Fig. 4). Indicadores no modelo de regressão linear.

Indicador	Definição	Fonte
Preço de 1 GB de dados móveis (variável dependente)	O preço que um indivíduo deve pagar para aceder a pelo menos 1 GB de dados móveis com pelo menos 30 dias de validade.	Alliance for Affordable Internet, 2019
Renda média mensal	Renda Nacional Bruta per capita por mês.	World Development Indicators, 2019[8]
Competição de mercado	Índice Herfindahl-Hirschman Index,baseado na participação no mercado de banda larga móvel.	Cálculos dos autores, baseados em dados da GSMA Intelligence, 2009
Franquia do plano de dados	A franquia de dados que um indivíduo adquire quando compra o(s) plano(s) necessário s) para atender à variável dependente.	Alliance for Affordable Internet, 2019
População	População nacional total.	União Internacional da Telecomunicação, 2019
Custo do terminal (aparelho móvel com acesso à Internet ou smartphone)	Um valor normalizado para o custo do smartphone ou aparelho móvel com acesso à Internet mais barato (originalmente expresso como uma proporção do PIB per capita).	GSMA Mobile Connectivity Index, 2017[9]
Assinantes únicos de internet móvel	O número de assinantes únicos de internet móvel como porcentagem da população nacional.	GSMA Intelligence, 2019
Taxa de alfabetização	A porcentagem de indivíduos que relatam possuir a capacidade de ler ou escrever em um idioma, com base em censos e estimativas nacionais.	Our World in Data, 2019[10]

8. http://datatopics.worldbank.org/world-development-indicators/
9. https://www.mobileconnectivityindex.com
10. https://ourworldindata.org/literacy

Montamos um modelo de regressão linear para explorar quais fatores podem influenciar os preços dos dados. Nosso modelo testa o preço que um consumidor teria que pagar em dezembro de 2018 (convertido em USD) contra a renda média mensal (também em USD), a concorrência de mercado, o subsídio de dados que o usuário realmente paga, a população do país, um valor normalizado para o custo médio de um aparelho móvel no país, a porcentagem de assinantes únicos de internet móvel no país e a taxa de alfabetização mais recente do país para considerar outros fatores, particularmente aqueles que poderiam afetar a escala econômica (Fig.4).

Descobrimos que esse modelo representa um primeiro esforço promissor ao relacionar esses fatores ao preço dos dados móveis. Um modelo de regressão linear limitado reafirma a concorrência no mercado como um fator influente na determinação dos preços dos dados. Ao incluir todas as variáveis, apenas a renda média mensal e a competição de mercado tiveram significância estatística. Esse modelo sugere que, à medida que os mercados de banda larga móvel se tornarem menos competitivos e mais concentrados, o preço que um consumidor terá que pagar para obter pelo menos 1 GB de banda larga móvel também aumentará.

Embora esse modelo seja limitado e seu resultado, preliminar, a importância estatística do resultado afirma que a concorrência de mercado deve ser uma área de atenção política. Olhando para uma posição sumária a partir de uma perspectiva global, a concorrência e a renda média aparecem como os fatores mais influentes para a precificação de mercado da banda larga móvel. Uma ampla agenda social e econômica é necessária para abordar a renda média em um país; no entanto, a

(Fig. 5). Resumo de resultados do modelo de regressão linear

Info do modelo
Observações: 91 (8 observações ausentes excluídas) Variável dependente: preço de referência para 1 GB (USD) Tipo: regressão linear OLS

Ajuste do modelo
F(7,83) = 5,49, p = 0,00 R^2 = 0,32 Aj. R^2 = 0,26

Erros padrão: OSL	Est.	S.E.	t val.	p
(Interceptação)	-0,587	3,47	-0,17	0,866
Renda média mensal	8,804e-03	0,00	3,19	0,002 **
Competição de mercado	1,451e-03	0,00	3,96	0,000 ***
Franquia do plano de dados	2,044e-04	0,00	0,50	0,615
População	-2,622e-09	0,00	-1,04	0,303
Custo do aparelho	-1,531e-02	0,08	-019	0,852
Assinantes únicos de internet móvel	-4,776	5,07	-0,94	0,349
Taxa de alfabetização	0,028	0,04	0,67	0,507

*** significativo ao nível 0,01*

**** significativo ao nível 0,001*

concorrência no mercado oferece um ponto mais estreito e discreto para a intervenção política.

VI. Conclusão

A Internet acessível continua sendo uma prioridade fundamental para a pesquisa e a defesa de políticas no futuro próximo. No final de 2018, marcamos a data em que mais da metade da população mundial passou a estar conectada à internet.[11] No entanto, as condições sob e o ritmo de entrada da metade restante da população mundial ainda estão por ser determinados. Em todos os países de renda baixa e média, 1 GB de banda larga móvel custa em média 5,76% da renda mensal de um indivíduo. Essa barreira de custos mantém bilhões *offline* e, para enfrentá-la, é necessário entender a dinâmica do mercado que a determina.

Os planos de dados estruturam o mercado de banda larga móvel, e a disponibilidade de certos planos para os usuários traz consequências nas medidas de acessibilidade e acesso à internet. Os planos de dados contêm uma variedade de iterações em torno de seu preço, franquia de dados e período de validade. As opções ofertadas no mercado pelas operadoras de rede móvel são um fator determinante sobre como os consumidores usam a Internet. Na América Latina e no Caribe, essa estrutura de mercado significa que os usuários que buscam 1 GB para durar um mês normalmente precisam comprar mais do que necessitam utilizar. Este artigo inicia uma pesquisa sobre o motivo e quais fatores podem influenciar.

A concorrência no mercado parece oferecer um ponto de intervenção precoce e significativo para os formuladores de políticas e de mais estudos para pesquisadores. Com base em um modelo de regressão linear considerando uma variedade de fatores socioeconômicos relevantes para as telecomunicações móveis, a renda média mensal e a concorrência de mercado emergem como as influências estatisticamente significativas no preço que um consumidor paga por 1GB. Isso apresenta evidências iniciais de que mercados mais competitivos tendem a oferecer rotas mais acessíveis para os planos básicos de dados móveis para os usuários.

Este artigo contribui para a crescente literatura sobre os aspectos socioeconômicos do acesso à Internet e sua acessibilidade. Analisa especificamente o tipo de planos de dados oferecidos aos usuários e como essas ofertas influenciam o mercado de banda larga móvel. No nível das comparações regionais, a classificação de preços criada por vários planos de dados afeta as medidas de acessibilidade. Analisando fatores potencialmente influentes na precificação de dados, a competição de mercado na banda larga móvel apresenta o fator mais promissor para uma análise mais aprofundada. A partir dessa primeira abordagem, continuaremos nosso estudo por meio de publicações como o *A4AI Affordability Report* (que será lançado em 2019)[12] e convidaremos outras pessoas a enriquecer ainda mais essa discussão com seus próprios desafios e contribuições. ■

11. https://www.itu.int/en/mediacentre/pages/2018-pr40.aspx (acesso em abril de 2019).
12. Edições anteriores disponíveis online em https://a4ai.org/affordability-report

Marina Pita, formada em comunicação social pela Pontifícia Universidade Católica de São Paulo, pesquisadora de mídias digitais e direitos das crianças do programa Prioridade Absoluta do Instituto Alana, do qual é também assessora para *advocacy*

Brinquedos conectados e os riscos à infância

Considerando a necessidade de acompanhar o desenvolvimento tecnológico com vistas a maximizar oportunidades e reduzir riscos no uso de Tecnologias da Informação e Comunicações (TICs) por crianças e adolescentes, é fundamental que nos debrucemos o quanto antes sobre a tendência de conexão de objetos, um processo que vem sendo chamado de Internet das Coisas (IoT, na sigla em inglês).

Na esteira da ampliação da oferta de novos dispositivos domésticos conectados, cabe atenção especial para o mercado de brinquedos conectados e inteligentes. De acordo com pesquisa da Juniper Research, em 2017, a receita com brinquedos inteligentes nas Américas estava estimada em 2,14 bilhões de dólares e a remessa, nas Américas, em 118,2 milhões de unidades.

Em junho de 2017, a consultoria avaliou que o baixo custo de componentes digitais, o avanço de tecnologias de conexão-sem-fio de baixo consumo energético e as melhorias em capacidade de processamento criaram um ambiente tecnológico em que a barreira de preço já não seria mais um fator restritivo à expansão do mercado de brinquedos inteligentes e conectados.

O mercado de brinquedos conectados pode ser suportado por *smartphones* e *tablets*, cuja penetração na população já alcança patamares altos, inclusive no Brasil. Ainda, o desenvolvimento e a popularização da computação em nuvem são

fatores auxiliares ao desenvolvimento desse tipo de produtos, já que, segundo a Juniper Research:

"O brinquedo pode apenas funcionar como um dispositivo de gravação, cuja função é a retransmissão de informações à nuvem, onde podem ser processadas. Este fator permite que dispositivos locais excedam suas limitações em termos de capacidade de processamento".

Outro importante motor para a ampliação das vendas de brinquedos conectados é a preocupação crescente de mães, pais, educadores e responsáveis com o uso crescente de telas por crianças e os efeitos deste hábito – ao qual o uso de brinquedos inteligentes poderia, teoricamente, se contrapor. A mesma pesquisa avalia que "os brinquedos conectados educacionais são uma reação a isso [crítica ao uso exagerado de telas por crianças], já que são percebidos como uma atividade mais produtiva".

Por essa lista de fatores, a consultoria enquadrou a indústria de brinquedos conectados como uma das principais tendências tecnológicas. Em apresentação sobre suas apostas para o mercado de tecnologia, escreveu:

"acreditamos que este será o ano para os brinquedos focados em educação, com ênfase em ensino de programação, se tornarem uma tendência dominante".

Os brinquedos conectados permitem que a indústria estabeleça um contato – e também contrato – prolongado com as crianças e utilize o modelo de "desbloqueio" de funcionalidades (pagas) ao longo do tempo, a cada atualização com novos desenvolvimentos. Assim, o retorno financeiro com o brinquedo conectado não é apenas o preço pago pelo dispositivo em sua aquisição. Este modelo provê à indústria de brinquedos uma forma de se reinventar, compensando a queda nas vendas de fornecedores tradicionais.[1]

Os elementos apresentados demonstram a necessidade de atenção dos agentes públicos e da sociedade como um todo para o mercado de brinquedos conectados, em franca expansão, para assim garantir que a inovação tecnológica esteja calcada no melhor interesse das crianças, na responsabilidade empresarial e não unicamente na rentabilidade das empresas.

Os itens a seguir procuram sistematizar alguns dos riscos aos direitos de crianças relacionados aos brinquedos conectados, a partir de uma análise das implicações pós-digitalização da Convenção dos Direitos das Crianças, das Nações Unidas, observando, prioritariamente, o direito da criança à participação e à proteção, conforme abordagem proposta por Livingstone e O'Neill.[2]

Acesso não autorizado

Entre 2016 e 2017, a organização britânica de defesa do consumidor Which? realizou, em parceria com diversas entidades de defesa dos consumidores e especialistas em segurança, uma série de testes com brinquedos inteligentes.[3] Os resultados apontam a facilidade para qualquer pessoa se conectar aos brinquedos a partir de um *smartphone*, inclusive sem a necessidade de violar o funcionamento normal dos dispositivos, tão pouco seguros eram seus sistemas. Sobre tais descobertas, a Which? escreveu:

"Algumas das funcionalidades dos brinquedos tornam possível que qualquer um possa enviar seu próprio áudio para ser reproduzido para quem estiver ao alcance do alto-falante do brinquedo. Ou, qualquer um poderia capturar um áudio, remotamente, através do brinquedo, e ouvi-lo por um telefone ou laptop. Vulnerabilidades significativas tornam esses brinquedos alvos de hackeamento ou algo mais sinistro. Alguém com intenções maliciosas poderia usar esses brinquedos para falar com seus filhos diretamente, de fora de sua casa."

O brinquedo falante e conectável *Furby*, fabricado pela empresa Hasbro e vendido no Brasil por cerca de 260 reais,[4] foi um dos testados. A empresa de segurança da informação parceira da Which?, a Context IS – a partir de uma sugestão de hacking disponível na Web –, conseguiu fazer o objeto tocar uma música e foi capaz de manipular os gráficos que aparecem em seu olho/tela.

O fato de a forma de acesso não autorizado ao brinquedo ter sido encontrada na Web é relevante. A cultura *hacker* considera a invasão de dispositivos como um desafio[5] que, após superado, deve ser

1. https://oglobo.globo.com/economia/negocios/receita-da-mattel-cai-com-barbie-fora-de-moda-21240940
2. Livingstone, S., & O'Neill, B. (2014). "Children's rights online: Challenges, dilemmas and emerging directions". In S. van der Hof, B. van den Berg, & B. Schermer (Eds.), Minding minors wandering the web: Regulating online child safety (pp. 19– 38). Berlin: Springer.
3. https://www.which.co.uk/reviews/smart-toys/article/smart-toys-should-you-buy-them
4. https://www.americanas.com.br/busca/furby
5. https://makezine.com/2017/02/06/toy-hacking-simone-giertz

divulgado, como troféu, à comunidade e, claro, para possibilitar a correção dos erros pelos responsáveis. Ou seja, é comum que as formas encontradas para acessar dispositivos sejam divulgadas em comunidades *online*. Sendo este fato notório e diante da inércia da fabricante, que pode ser entendida como negligência, é possível concluir que a preocupação com as vulnerabilidades dos dispositivos lançados está longe de ser uma prioridade da companhia.

Ainda, de acordo com o levantamento, não foi possível acessar os áudios coletados pelo *Furby*, no tempo em que a pesquisa foi realizada, mas a Context IS afirmou que provavelmente este objetivo seria alcançado com um pouco mais de dedicação, por meio da modificação do firmware (*software* que controla *hardware*) do brinquedo.

Assim como o *Furby*, a quase totalidade dos brinquedos testados não dispunha de qualquer processo de autenticação, o que significa que estranhos poderiam, por exemplo, enviar mensagens pelos brinquedos e, inclusive, como no cachorro-robô *Toy-Fi Teddy*, da fabricante Spiral Toys, receber a resposta da criança.[6]

No caso do *i-Que Intelligent Robot*, fabricado pela Genesis Toys, a investigação descobriu que qualquer pessoa poderia baixar o aplicativo, encontrar um *i-Que* por meio da busca do *bluetooth* e passar a usar a voz do robô, simplesmente digitando em uma caixa de texto no aplicativo. A mesma empresa manufatura a boneca *My Friend Cayla*, cuja conexão por *bluetooth* não pode ser desligada ou protegida por senhas, motivo que levou à proibição de sua comercialização na Alemanha.[7]

Após analisar os brinquedos conectados, a pesquisadora independente de segurança cibernética, Sarah Jamie Lewis, afirmou que muitos dos produtos não adotaram medidas básicas para garantir que suas comunicações sejam seguras e que as informações de uma criança sejam protegidas. Segundo ela, os brinquedos agiam como "dispositivos espiões descontrolados"[8] porque os fabricantes não incluíam um processo que permitisse que os gadgets se conectassem apenas por certos dispositivos selecionados.

Até mesmo o mais icônico dos brinquedos americanos, a *Barbie*, teve sua versão conectada e inteligente *hackeada*. O pesquisador americano em segurança digital, Matt Jakubowski,[9] descobriu que, quando conectada ao *Wi-Fi*, a boneca se tornava vulnerável. Ele conseguiu acessar o sistema de informação, os dados da conta, os áudios gravados e o microfone, inclusive burlando o sistema de criptografia para o envio de dados.[10]

A ausência de sistemas seguros em brinquedos conectados também deixa vulneráveis dados extremamente sensíveis como de localização das crianças usuárias. A análise do Q50[11], um relógio inteligente para crianças, comercializado como uma forma de ajudar os pais a se comunicarem facilmente com seus filhos e acompanharem sua localização em tempo real, mostrou que as falhas no dispositivo permitiriam que *hackers* interceptassem todas as comunicações, ouvissem remotamente a vizinhança e falsificassem a localização da criança.

A pesquisa do órgão governamental Conselho de Consumidores da Noruega (NCC, na sigla em inglês) acerca dos relógios conectados[12] demonstra que este não é um caso isolado. A pesquisa identificou outros dois modelos dos chamados *smartwatches* em que um estranho poderia assumir o controle do relógio, seguindo alguns passos simples. E poderia também realizar escutas não autorizadas das conversas da criança, rastrear sua localização e até contatá-la e conversar com ela. Em outros modelos, os dados, inclusive de localização, são transmitidos e armazenados sem criptografia, vulneráveis à interceptação.

O amplo e preocupante espectro de vulnerabilidades no acesso aos dados apresentado em brinquedos conectados já disponíveis no mercado é tamanho que o Federal Bureau de Investigation (FBI) americano decidiu manifestar-se. O órgão do sistema de segurança daquele país publicou um alerta intitulado *"Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children"*.[13] Na abertura do documento, o FBI é bastante explícito:

"O FBI incentiva os consumidores a considerarem a segurança cibernética antes de introduzir brinquedos inteligentes, interativos e

6. Conforme pesquisa realizada pela organização de defesa do consumidor alemã Stiftung Warentest em parceria com a Which?
7. https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2017/17022017_cayla.html?nn=404422
8. https://www.nytimes.com/2017/12/21/technology/connected-toys-hacking.html
9. https://about.me/jaku
10. https://www.theguardian.com/technology/2015/nov/26/hackers-can-hijack-wi-fi-hello-barbie-to-spy-on-your-children
11. https://www.top10vpn.com/privacy-central/privacy/smart-toys-safety-review
12. https://snl.no/smartklokke
13. Consumer Notice: Internet-Connected Toys Could Present Privacy and Contact Concerns for Children. Disponível em https://www.ic3.gov/media/2017/170717.aspx

conectados à Internet em suas casas ou ambientes confiáveis. Brinquedos inteligentes e dispositivos de entretenimento para crianças estão incorporando cada vez mais tecnologias que aprendem e adaptam seus comportamentos com base nas interações com o usuário. Esses brinquedos normalmente contêm sensores, microfones, câmeras, componentes de armazenamento de dados e outros recursos multimídia – incluindo reconhecimento de fala e opções de georreferenciamento. Esses recursos podem colocar em risco a privacidade e a segurança das crianças devido à grande quantidade de informações pessoais que podem serreveladas involuntariamente".

Informações pessoais (como nome, data de nascimento, fotos, endereço) geralmente são fornecidas ao criar contas de usuário nesses sistemas. Além disso, as empresas coletam grandes quantidades de dados adicionais, como mensagens de voz, conversas, geolocalização, histórico de uso da Internet e endereços IPs. A exposição dessas informações a pessoas mal-intencionadas cria condições favoráveis a fraudes de identidade infantil. Além disso, o potencial uso indevido de dados confidenciais, como informações de localização, identificadores visuais como fotos ou vídeos, combinados com listagem de interesses, podem ser determinantes para angariar a confiança de uma criança, aumentando os riscos de exploração por criminosos.

A vulnerabilidade por padrão dos dispositivos produzidos para crianças fere o princípio de que, para garantir o direito da criança à privacidade e a proteção de seus dados, as empresas devem tomar medidas que impeçam o acesso e intrusão não autorizada, conforme indicado em documento orientador de melhores práticas para a indústria, formulado pelo Fundo da Nações Unidas para a Infância (UNICEF).[14] Demonstra ainda o quão longe a indústria de brinquedos conectados está de considerar a privacidade ao longo no processo de desenvolvimento do produto, contrariando outra orientação do órgão.

Vulnerabilidades no armazenamento de dados

O total descaso com a segurança das crianças demonstrado pela indústria dos brinquedos conectados vai além dos dispositivos em si. Também nos centros de armazenamento e processamento de dados das empresas constata-se a ausência de rígido controle e de padrão elevado de qualidade na operação, esperado de entidades que gerenciam dados pessoais, especialmente de hipervulneráveis como são as de 12 anos.

A VTech, fabricante de relógios inteligentes e outros dispositivos conectados voltados para o público infantojuvenil, teve seus sistemas hackeados em 2015, o que resultou na exposição de dados de aproximadamente 6,4 milhões de pessoas – o maior vazamento de dados envolvendo crianças até hoje.

Em janeiro de 2018, a VTech chegou a um acordo com a Federal Trade Comission (FTC), dos Estados Unidos, para encerrar o processo de investigação contra ela, iniciado a pedido do Departamento de Justiça do país,[15] pelo qual pagará 650 mil dólares ao órgão norte-americano.

A empresa violou a lei de privacidade de crianças dos EUA ao coletar informações pessoais de crianças sem fornecer notificação direta nem obter o consentimento de seus pais. Adicionalmente, infringiu a legislação local ao deixar de tomar medidas razoáveis para proteger os dados coletados, tais como salvaguardas e medidas de segurança adequadas para proteger informações transmitidas e armazenadas, e implementar um sistema de prevenção ou detecção de intrusões que pudessem alertar a empresa de invasão não autorizada a sua rede.

Ainda, de acordo com a FTC, a VTech mentia em sua política de privacidade ao declarar que boa parte dos dados dos usuários, fornecidos por meio de sua plataforma, seriam criptografados. Além da multa, a empresa deverá implementar um amplo programa de proteção de dados, sujeito a auditorias independentes, por 20 anos.

Mais recentemente, a empresa CloudPets foi acusada de expor as informações pessoais de meio milhão de pessoas, incluindo endereços de e-mail, senhas, fotos de perfil e mais de dois milhões de gravações de voz de crianças e adultos, que usaram os brinquedos de pelúcia da marca,[16] segundo o reconhecido serviço de informação de vazamentos de dados, *"have I been pwned?"*.[17]

Os dados pessoais de crianças expostos ou vazados a partir dos centros de processamento de dados das empresas podem ser usados, da mesma

14. UNICEF (2018). Industry Toolkit: Children's online and freedom of expression. Disponível em: https://issuu.com/unicefusa/docs/unicef_toolkit_privacy_expression?e=29613278/60947364
15. https://www.ftc.gov/system/files/documents/cases/vtech_file_stamped_complaint_w_exs_1-8-18.pdf
16. https://www.theguardian.com/technology/2017/feb/28/cloudpets-data-breach-leaks-details-of-500000-children-and-adults
17. Disponível em https://haveibeenpwned.com

forma que aqueles obtidos diretamente por intrusão nos brinquedos, para fraudes e por criminosos.

Vale lembrar que, uma vez expostos, estes dados jamais poderão ser completamente eliminados. A Internet tem um caráter distribuído e aberto, em que todos os pontos conectados estão habilitados a salvar conteúdo e a redisponibilizá-los a qualquer momento. Isso significa que o impacto na vida das crianças e a violação de seus direitos pode perdurar indefinidamente, exigindo esforço constante de proteção dos dados pessoais.

Ainda, ausência de padrões rígidos de segurança no armazenamento de dados fere os princípios da responsabilidade e da prevenção, além dos já apontados princípios do desenvolvimento de produtos observando as garantias da segurança e da privacidade. Também é notório que as empresas não tenham mecanismos para identificar intrusões e procedimentos para alertar os usuários em caso de exposição ou vazamento de dados, ou que não estejam obrigadas a fazê-lo, o que pode significar a manutenção da condição de risco e violação de direitos.

O estabelecimento de práticas de apagamento para que os dados pessoais sejam conservados apenas durante o período considerado necessário para a prestação do serviço é fundamental para reduzir o risco de vazamentos no médio e longo prazos.

A redução do volume de dados coletados também é uma medida adequada, especialmente em se tratando de informações de crianças. Os dados pessoais deverão ser adequados, pertinentes e limitados ao necessário e apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios. O UNICEF recomenda, inclusive, que empresas considerem a possibilidade de oferta de uma versão de seus produtos que não coletem dados de crianças.[18]

Exploração comercial de dados

Em uma economia cada vez mais orientada por dados,[19] seja pela venda simples ou pela análise de grandes e complexas bases de dados, é fundamental compreender como os dados de crianças estão sendo usados. Ou, uma vez armazenados, como podem ser utilizados no futuro.

O modelo mais reconhecido de uso de dados é para direcionamento de conteúdo e publicidade, para grupos ou indivíduos específicos.[20] Este processo ocorre por minucioso processo de micro-segmentação dos consumidores.[21] As grandes empresas utilizam o conhecimento acerca das preferências de cada pessoa para personalizar ofertas comerciais e influenciar comportamento e opinião.

Por meio de tecnologias sofisticadas e aplicação de métodos psicológicos e comportamentais,[22] os dados pessoais são, muitas vezes, utilizados para seduzir consumidores-alvos, tornando-os ainda mais fragilizados nesta relação já tão desigual, marcada pela assimetria informacional.

Se o alvo do anúncio é uma criança, a desigualdade informacional é ainda maior. Não à toa, a doutrina consumerista já considera crianças hipervulneráveis e hipossuficientes.[23] Em um contexto de massiva coleta e tratamento de dados pessoais e de avanço nas tecnologias de análise e direcionamento de publicidade, este grupo está ainda mais suscetível às pressões advindas desta complexa relação entre empresas e consumidores, já que crianças não detêm as ferramentas biopsíquicas adequadas para responder com igualdade a essas pressões.

Quando uma boneca ou outro brinquedo conectado pergunta a brincadeira, cor, animal, vídeo ou música preferida de uma criança, está construindo um banco de dados sobre suas preferências. Este conhecimento sobre o imaginário infantil pode facilmente ser traduzido em ofertas comerciais, que podem se dar por meio do próprio brinquedo, mediante a citação do produto, por exemplo.

O uso de dados também pode ocorrer em contextos diferentes daquele em que houve a coleta. Isso pode ocorrer pelo uso de telas em que o cruzamento de endereços IPs e perfil identifique o

18. UNICEF (2018). Industry Toolkit: Children's online and freedom of expression. Disponível em https://issuu.com/unicefusa/docs/unicef_toolkit_privacy_expression?e=29613278/60947364

19. The Economist. "Data is giving rise to a new economy" (Maio 2017). Disponível em https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy. Acesso em: 14 de maio de 2018.

20. Pesquisa da americana Data & Marketing Association aponta que anunciantes gastaram US$15,5 bilhões em dados e serviços atrelados a dados em 2018, para personalizar publicidade. Disponível em: https://thedma.org/news/seeking-customer-personalization-marketers-spend-15-6-billion-data-data-services. Acesso em 14 de maio de 2018.

21. Pesquisa da empresa SalesForce com anunciantes indica que 90% usam ou planejam usar dados coletados online, em 2018. Cinquenta por cento usam ou pretendem usar dados adquiridos de terceiros, intenção que cresce em 30% quando questionados sobre o uso de dados adquiridos de terceiros, em dois anos. Os terceiros são agregadores de dados cujo negócio é comercialização. Disponível em https://c1.sfdcstatic.com/content/dam/web/en_us/www/assets/pdf/datasheets/digital-advertising-2020.pdf. Acesso em: 14 de maio de 2018.

22. Recentemente, um modelo de análise de dados pessoais para inferir personalidade e comportamento e influenciá-los, desenvolvido por pesquisadores da Stanford University e do Psychometrics Center da University of Cambridge, ficou mundialmente conhecido. Disponível em https://www.nytimes.com/2018/03/20/technology/facebook-cambridge-behavior-model.html. Acesso em: 14 de maio de 2018.

23. Código Brasileiro de Defesa do Consumidor comentado pelos Autores do Anteprojeto. São Paulo: Editora Forense. p. 299-300.

usuário, ou a partir da identificação da criança por mecanismos de reconhecimento facial.

À medida que as lojas, centros comerciais e mesmo sistemas de transporte de massa[24] adotam ferramentas de coleta de dados,[25] utilizando identificação de dispositivos móveis ou por reconhecimento facial, o direcionamento de ofertas nestes ambientes se tornará mais comum. E a tecnologia não é nova. Em janeiro de 2016, artigo[26] no blog do Information Commissioner's Office (ICO), regulador do uso de dados do Reino Unido, já apontava que lojas poderiam modificar preços ou oferecer determinados produtos por perfil do transeunte, a partir da identificação por sistema de conexão *wi-fi*, *bluetooth* e reconhecimento facial.

O uso de informações coletadas em um dispositivo para oferta comercial em outros contextos e ambientes é dificilmente rastreável, até mesmo para especialistas, de forma que a capacidade de resposta a usos indevidos, por meio de atuação *ex-post*, é prejudicada. Considerando o modelo de análise de risco versus oportunidade, comum na definição das práticas comerciais das empresas, agentes privados poderiam estar inclinados a ver aqui uma oportunidade de rentabilização dos dados sem que possam ser responsabilizados pela abusividade.

Mas os dados de crianças não necessariamente precisam ser usados imediatamente para que tenham valor comercial e possam ser vendidos. Há toda uma indústria de compra e venda de dados no atacado, que opera sem conhecimento do público e cujas práticas são desconhecidas.[27] A necessidade de regulação da operação destas empresas, chamadas de Data Brokers, vem sendo uma tônica em diversas partes do mundo. A Federal Trade Comission fez um alerta ao Congresso norte-americano neste sentido[28] e a lei europeia de proteção de dados[29], vigente desde maio de 2018, tratou desta preocupação.

Termos de uso genéricos

As empresas fabricantes de brinquedos conectados não estão assumindo a devida responsabilidade por garantir a privacidade de crianças e ainda estão usando os termos de uso para se blindarem. A VTech, por exemplo, alterou os termos e condições de uso para incluir que não é responsável por nenhum vazamento de dados.[30]

> "As empresas fabricantes de brinquedos conectados não estão assumindo a devida responsabilidade por garantir a privacidade de crianças e ainda estão usando os termos de uso para se blindarem."

O modelo binário de aceitar ou negar os termos dos brinquedos conectados, em desrespeito ao princípio da necessidade, pelo qual a coleta de dados deve ser justificada para determinada finalidade, tem limitado a escolha dos pais e impõe que tenham de aceitar a totalidade do contrato para que seus filhos possam usar plenamente os jogos e aplicativos.

"Isso posiciona pais e cuidadores como os únicos responsáveis pela privacidade de dados e segurança das crianças, transferindo a

24. https://veja.abril.com.br/tecnologia/portas-da-linha-4-do-metro-vao-fazer-reconhecimento-facial-de-usuarios
25. https://www.theguardian.com/technology/2016/jan/21/shops-track-smartphone-uk-privacy-watchdog-warns
26. https://iconewsblog.org.uk/2016/01/21/how-shops-can-use-your-phone-to-track-your-every-move
27. Yael Grauer. "What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?". Disponível em https://motherboard.vice.com/en_us/article/bjpx3w/what-are-data-brokers-and-how-to-stop-my-private-data-collection. Acesso em 12 de junho de 2018.
28. Federal Trade Comission. FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information. Disponível em https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more. Acesso em 12 de junho de 2018.
29. Regulamento (ue) 2016/679 do Parlamento Europeu e do Conselho relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a diretiva 95/46/ce (Regulamento Geral sobre a Proteção de Dados). Disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em 12 de junho de 2018.
30. Global News. "Hacked toy maker VTech changes terms to say it's not liable for data breaches". Ver http://globalnews.ca/news/2508781/hacked-toy-maker-vtech-changes-terms-to-say-its-not-liable-for-data-breaches

responsabilidade legal pela coleta, armazenamento, análise e compartilhamento de dados das empresas para eles. Essas estratégias dão às entidades sinal verde para que continuem, e até expandam as práticas de coleta de dados, mesmo de crianças com menos de 13 anos".[31]

Os termos e condições dos brinquedos conectados, em muitos casos, não exige o consentimento livre, expresso e informado de mães, pais ou responsáveis, mesmo quando a oferta desses produtos se dá em países cuja legislação exige consentimento parental, como no Brasil, Estados Unidos[32] e União Europeia.[33] Ao assumir que o uso dos dispositivos significa o consentimento e aceite dos termos de uso e de privacidade, empresas violam o direito à privacidade das crianças, bem como ignoram sua condição de hipervulnerável e, portanto, incapaz de celebrar contrato.

Mesmo os brinquedos que exigem que o responsável autorize a coleta de dados da criança, por registro de e-mail, por exemplo, apresentam termos de uso e política de privacidade em longos textos,[34] escritos em letra diminuta, que exigem longo tempo para leitura e, frequentemente, encontram-se escondidos em página alternativa. Este modelo de termos de uso e política de privacidade é uma forma de perpetuação dos modelos de negócios das empresas, sem controle social ou governamental.

Vale destacar que quarenta por cento dos brasileiros não se atentam ao contrato de licença durante a instalação de um aplicativo no celular, e outros 15% não leem as mensagens de instalação dos programas, apenas clicam em 'avançar' e 'aceito', sem saber o que estão autorizando.[35] Este dado, bem como a análise do modelo de oferta de informação por empresas, demonstra o potencial risco de uso inescrupuloso dos dados de crianças , sem conhecimento real dos responsáveis.

Mesmo quando os pais leem os termos de uso e privacidade para consentir, o fato de estes serem continuamente alterados, sem obrigação de notificação e novo consentimento, torna o modelo uma carta branca às empresas, especialmente porque o adulto responsável pode não manter vigília constante quando se trata de um dispositivo ou sistema usado pela criança.

Ou seja, o atual modelo de oferta de informações a pais e responsáveis e mesmo a exigência de consentimento parental, sem o estabelecimento de padrões éticos de coleta e tratamento de dados de crianças, é insuficiente diante da opção social pela proteção integral das crianças. O atual modelo de funcionamento da indústria coloca sobre a família todo o peso da responsabilidade pela garantia da segurança, bem-estar e melhor interesse da criança, sem oferecer-lhe os instrumentos adequados.

O consentimento para o tratamento dos dados de crianças deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca do responsável legal. Nos casos em que o tratamento sirva a fins múltiplos, deverá ser dado um consentimento para todos esses fins.

O princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples, inclusive para crianças, em respeito a seu estágio de desenvolvimento constante e o direito a acessar informações que tenham impacto em seus direitos.

Violação da privacidade e datatificação da infância

A medida em que brinquedos conectados, assistentes digitais e outros dispositivos habilitados com sensores e conectados à Internet passam a fazer parte do cotidiano das crianças, um grande volume de dados detalhados sobre elas passa a ser

31. Donell Holloway & Lelia Green (2016). 'The Internet of toys", Communication Research and Practice, DOI: 10.1080/22041451.2016.1266124. Ver http://dx.doi.org/10.1080/22041451.2016.1266124

32. Nos Estados Unidos, a Lei de Proteção da Privacidade de Crianças (COPPA, na sigla em inglês) institui regras para responsáveis por websites e serviços online visando a promoção da privacidade de crianças e adolescentes de até 13 anos na internet. Entre as obrigações estabelecidas pela norma está a de disponibilizar de forma clara sua política de privacidade para este público. A coleta de informações de meninos e meninas, salvo exceções, fica condicionada à obtenção de consentimento dos pais que também podem corrigir ou solicitar a exclusão dos registros. Pela regra, websites e serviços online ficam proibidos de repassar informações coletadas de crianças a terceiros, devendo mantê-las somente enquanto forem necessárias no processo de tratamento.

33. O Regulamento Geral de Proteção de Dados na União Europeia (GDPR) estabelece proteção específica aos dados pessoais de crianças e adolescentes, que se aplica para efeitos de comercialização, de criação de perfis e na coleta de dados pessoais em serviços disponibilizados diretamente a eles. Para serviços da sociedade da informação, há a obrigação de consentimento parental ou de responsável legal para coleta e tratamento de dados de pessoas com até 16 anos de idade, ainda que os Estados-membros possam definir a idade de maioridade para consentimento, desde que não inferior a 13 anos.

34. Leitura de 'termos e condições' de serviços na internet exige 4,5 horas. Ver http://www1.folha.uol.com.br/tec/2017/12/1945132-leitura-de-termos-e-condicoes-de-servicos-na-internet-exige-45-horas.shtml. Acesso em 8 de maio de 2018.

35. 40% dos usuários brasileiros não leem termos de uso ao instalar aplicativos. Ver http://tecnologia.ig.com.br/2016-03-29/40-dos-usuarios-brasileiros-nao-leem-termos-de-uso-ao-instalar-aplicativos.html. Acesso em 8 de maio de 2018.

gerado, armazenado, analisado e distribuído.

O primeiro risco atrelado a este crescente tratamento de dados de crianças diz respeito a seu direito à privacidade. Isso é um fator fundamental para o desenvolvimento natural de crianças. A privacidade está diretamente atrelada à formação da identidade, desenvolvimento da personalidade e à habilidade de construir relacionamentos sadios com outros.[36]

No momento do brincar, a criança exterioriza certos aspectos de si mesma em um movimento de elaboração de suas primeiras experiências. Para elas, não é simples a compreensão de que estes objetos, de uso íntimo, podem ser portas de acesso ao momento de intimidade, especialmente porque os sensores – microfones e câmeras, por exemplo – não chegam a ser visíveis. Violar o momento do brincar significa interferir em um processo necessário de desenvolvimento e cujos impactos ainda são desconhecidos. Sabe-se, no entanto, que tal prática pode reduzir a confiança na capacidade de discernimento acerca do ambiente e em seus pais e responsáveis.

Adicionalmente, os brinquedos e demais dispositivos conectados estimulam a vigilância parental invasiva, sem necessariamente o conhecimento do sujeito vigiado, com implicações na privacidade da criança, em sua liberdade e desenvolvimento. A Hello *Barbie*, da Mattel, por exemplo, envia trechos das conversas da criança com a boneca aos pais por e-mail e disponibiliza botões para compartilhamento nas redes sociais em evidente estímulo à exposição da intimidade deste grupo.

De acordo com o relatório *Guidelines for Industry on Child Online Protection*, produzido pela UNICEF em parceria com a UIT, quando algum programa permite que pais e responsáveis monitorem a comunicação da criança no universo *online*, é importante que isso seja discutido abertamente com ela. "Do contrário, tal conduta pode ser percebida como vigilância e pode minar a confiança entre os membros da família".[37]

Mas as práticas de vigilância e controle parental podem ter outros efeitos nefastos. Segundo Charlotte Faircloth, professora sênior do Departamento de Ciências Sociais da Universidade de Roehampton e membra fundadora do Centro para Estudos da Parentalidade,[38] "até o momento, pesquisas sociológicas acerca da crescente tecnologização da vida familiar apontam para o aumento da ansiedade dos pais, mais do que sua diminuição".

Adicionalmente, a inserção da IoT nos lares pode amplificar a tendência em direção ao que chama de "parentalidade performativa", em que os pais, em vez de apenas brincarem com as crianças porque é divertido ou desejado, se engajarão em fazê-lo como uma forma de "otimizar o desenvolvimento cerebral" ou de "modelar o bom comportamento", na avaliação de Charlotte Faircloth.

Ainda, à medida que a privacidade é substituída pela vigilância e que a criança toma consciência de que está acompanhada a todo momento, é provável que passe a agir de forma diferente,[39] com impacto em sua liberdade e no desenvolvimento de sua identidade e personalidade. Considerando que as oportunidades de uma pessoa são, de forma crescente,[40] definidas pelos tipos de ordenação social proporcionados pela análise de dados, a criança exposta a sistemas de coletas de dados está suscetível a formas de perfilamento que podem afetar seu futuro, sem que ela tenha consciência ou conhecimento.

Julgamentos ou inferências com base em dados abrem a possibilidade de que o resultado dessas práticas seja a circunscrição das complexidades e potencialidades da criança. Por ser a criança uma pessoa em desenvolvimento, o perfilamento tem potencial de dano e violação de direitos maior do que o uso desta tecnologia em adultos.

A estas questões se somam a expansão e complexificação dos sistemas de classificação e perfilamento, já em andamento, que tende a reduzir cada vez mais as oportunidades para as pessoas desafiarem as inferências e previsões feitas por algoritmos. Nesse sentido:

> *"As pessoas geralmente têm pouco conhecimento sobre como as corporações estão explorando os dados pessoais e os utilizando para construir perfis detalhados usados para decisões sobre acesso a empregos, impostos, benefícios sociais, ofertas especiais e crédito".*[41]

36. http://www.cyanb.ca/images/ChildrensOnlinePrivacy-e.pdf
37. UNICEF e UIT. Guidelines for Industry on Child Online Protection. Ver https://www.unicef.org/csr/files/COP_Guidelines_English.pdf
38. https://www.designcouncil.org.uk/news-opinion/will-internet-things-set-family-life-back-100-years
39. Elmer, 2003.
40. Lyon e Bauman, 2013; Robinson et al.,2014; Rosenblat et al., 2014. The datafied child: The dataveillance of children and implications for their rights". Ver http://journals.sagepub.com/doi/pdf/10.1177/1461444816686328. Acesso em 8 de maio de 2018.
41. Crawford e Schultz, 2014. "The datafied child: The dataveillance of children and implications for their rights". Disponível em http://journals.sagepub.com/doi/pdf/10.1177/1461444816686328

A "perfilização" acaba por gerar novas identidades virtuais sobre os indivíduos, baseadas em estereótipos e que podem ser determinantes para acesso a serviços, produtos e oportunidades de educação e trabalho[42] no presente e no futuro.

O impacto da perfilização por sistemas baseados em dados e inteligência artificial para o acesso a oportunidades vem sendo estudado simultaneamente à aplicação dessas técnicas, com grande risco de discriminação. O fato de anúncio de emprego com salário alto ser direcionado, por mecanismos automáticos de seleção de perfis com base em dados, mais frequentemente a homens, conforme indica pesquisa da Carnegie Mellon University,[43] poderia afetar o acesso de mulheres a cargos executivos e de liderança. A busca de nomes em mecanismos de pesquisa apresentar, com mais frequência, referências relacionadas a registros criminais quando tais nomes são mais usados pela comunidade negra, como aponta levantamento da Harvard University,[44] pode afetar o sucesso pessoal e profissional de negros e negras. A perfilização utilizada por agentes de segurança pública tem levado à discriminação racial contra grupos historicamente oprimidos, [45] uma vez que as bases de dados já estavam contaminadas por preconceitos.

Atenta a estas questões, a Casa Branca norte-americana encomendou em 2015 um levantamento sobre os riscos de discriminação a partir de processos automatizados de análise de grande volume de dados,[46] que concluiu:

"ao lado de seu potencial benéfico, de ser usado para ampliar o acesso a crédito ou melhorar os resultados da educação, reside o potencial de as tecnologias de big data serem usadas para a discriminação contra indivíduos, tanto intencionalmente quanto inadvertidamente, permitindo resultados discriminatórios, com redução de oportunidade e das opções disponíveis a estes".

O relatório tem como principais recomendações a limitação do uso de dados educacionais de crianças, para protegê-las deste potencial discriminatório e o fortalecimento das agências de defesa do consumidor e de direitos civis, com vistas a expandir o conhecimento técnico, de forma a capacitá-las a identificar práticas discriminatórias resultantes do uso de ferramentas de análise de dados, bem como desenvolvimento de planos de investigação e solução para potenciais violações.

Reconhecer o potencial de exploração comercial e de resultados discriminatórios pelo uso de dados é um primeiro passo, mas o tempo de ajuste das políticas públicas e da legislação para resolver tais questões pode não dar conta de proteger as crianças, de forma que medidas rápidas devem ser tomadas para disciplinar a coleta e tratamento de dados de crianças, bem como sua perfilização.

Os riscos de discriminação e de violação ao desenvolvimento livre da criança a partir de tratamento de dados ainda são desconhecidos por boa parte da população e as reflexões acerca do tema seguem limitadas a rodas de especialistas. Certamente os perigos mais facilmente compreendidos são aqueles que têm a ver com a segurança física e psicológica imediata da criança, os riscos de que pessoas não autorizadas tenham acesso à criança, ganhem a confiança da mesma por meio das informações obtidas na web e por acesso não autorizado a dados.

Mas, à medida que os sistemas de análise de dados avançam, outros riscos surgem e não são tão conhecidos das famílias, dos reguladores e muito menos das crianças. O potencial para que o perfil de dados de uma pessoa afete sua experiência cotidiana no presente ou no futuro aumenta, conforme aponta relatório da Children's Commission inglesa, publicado em novembro de 2018.[47]

E, ainda que pesquisas apontem que as crianças têm mostrado conhecimento e preocupação acerca dos dados que compartilham nas relações interpessoais, resultados preliminares de levantamento realizado pela professora Sonia Livingstone, da London School of Economics and Political Science, mostra que as crianças têm pouca ciência das dimensões institucionais da privacidade, como as que envolvem os dados que as escolas têm, por exemplo, e como podem ser usados, assim como os dados que empresas comerciais coletam.

42. https://www.wired.com/2012/04/ff_klout/all/1
43. Amit Datta, Michael Carl Tschantz, and Anupam Datta. "Automated Experiments on Ad Privacy Settings". Ver http://www.andrew.cmu.edu/user/danupam/dtd-pets15.pdf
44. Latanya Sweeney. "Discrimination in Online Ad Delivery". Ver https://dataprivacylab.org/projects/onlineads/1071-1.pdf
45. https://www.hrw.org/news/2012/04/17/us-end-discriminatory-profiling-police
46. White House. About Big Data: Seizing Opportunities, Preserving Values.Ver https://obamawhitehouse.archives.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf. Acesso em 11 de junho de 2018.
47. Children's Comission. "Who Knows What About Me? A Children's Comissioner Report into the collection and sharing of children's data". Ver https://www.childrenscommissioner.gov.uk/wp-content/uploads/2018/11/who-knows-what-about-me.pdf. Acesso em 17 dez. 2018.

> "O algoritmo responsável pelas escolhas de repertório dos brinquedos, bem como os seus princípios, parâmetros e fundamentos, são inacessíveis. Existe uma agenda algorítmica que, cada vez mais, toma decisões que afetam a vida das crianças, sem que pais, mães, sociedade e Estado possam acessá-la."

Alexas Fotos por Pixabay

Agenda camuflada

Os brinquedos conectados interagem com as crianças e propõem ações. Mas o algoritmo responsável pelas escolhas de repertório dos brinquedos, bem como os seus princípios, parâmetros e fundamentos, são inacessíveis. Ou seja, existe uma agenda algorítmica que, cada vez mais, passa a tomar decisões que afetam a vida das crianças, sem que pais, mães, sociedade e Estado possam acessá-la. São uma caixa-preta.

Considerando que estes brinquedos estão associados a modelos de negócio complexos, suas interações com a criança podem partir de acordos preestabelecidos, não necessariamente informados aos pais e responsáveis. A empresa Genesis Toy, por exemplo, foi acusada de imiscuir comunicação mercadológica no repertório da boneca conectada *My Friend Cayla*. O brinquedo, conforme pesquisa, foi pré-programado a fazer referência à *Disneyworld* e aos filmes da Disney. "A Cayla diz às crianças que seu filme favorito é Pequena Sereia e sua música preferida é *Let It Go*, trilha da animação *Frozen*, ambos da Disney. A boneca também afirma que adora ir à Disneylândia e ao parque Epcot, na Disneyworld".[48] A Genesis Toy, por sua vez, veiculou publicidade no Disney Channel, em que informava ser "uma orgulhosa patrocinadora" do canal.

A agenda algorítmica destes dispositivos pode facilmente incluir referências a partir de acordos comerciais com terceiros, induzir ao consumo constante de jogos e adereços relacionados ao próprio brinquedo e/ou incentivar padrões de comportamento como competição, consumismo e vaidade excessivos. Ademais, se já há consenso sobre a dificuldade de a criança reconhecer e compreender a comunicação mercadológica,[49] este formato de disseminação de conteúdo torna esta tarefa praticamente impossível, inclusive muito difícil até para adultos.

Porém, essa estratégia comercial, baseada em uma relação personalizada de confiança e identificação da criança com os brinquedos, pode ser extremamente eficiente. Ao fazer com que as crianças se identifiquem com um produto, a empresa é mais capaz de envolver a criança e prepará-la para ser uma consumidora fiel desde a mais tenra idade.

A preocupação acerca dos princípios e fundamentos da mediação algorítmica deve ser maior à medida que assistentes digitais – como o Echo, da Amazon – passam a organizar a vida das crianças e a selecionar produtos e conteúdos a serem consumidos por elas, não apenas no mundo virtual, mas possivelmente no mundo concreto, já que a expectativa para este segmento é que automatize as tarefas domésticas como, por exemplo, compras. Há que se questionar desde já se a escolha de itens que estarão à disposição das crianças vai ser baseada no melhor interesse da criança ou em acordos comerciais. ■

48. https://epic.org/privacy/kids/EPIC-IPR-FTC-Genesis-Complaint.pdf
49. Angela J. Campbell, Georgetown University Law Center. "Rethinking Children's Advertising Policies for the Digital Age". Disponível em: https://scholarship.law.georgetown.edu/facpub/1945. Acesso em 12 de junho de 2018.

A ICANN precisa delegar o **.amazon**[1]

Dra. Farzaneh Badii, diretora executiva do Internet Governance Project (IGP), pesquisadora associada da Escola de Política Pública do Instituto deTecnologia da Georgia, Estados Unidos

A Corporação da Internet para Atribuição de Nomes e Números (ICANN)[2] está mostrando que pode ser intimidada pelos governos. Essa captura só pode levar a mais politização do sistema de nomes de domínio e encorajar mais tensão geopolítica sobre a governança da Internet. Nunca é o processo multissetorial que cria tais problemas, é o próprio Conselho Diretor da ICANN. No caso recente sobre a delegação do gTLD[3] .amazon à empresa Amazon, o Conselho Diretor da ICANN demonstra sua falta de vontade de respeitar seus próprios estatutos e princípios e lidar com a questão. Neste texto trato dos recentes desenvolvimentos sobre a designação do .amazon e os conflitos que foram criados em torno dele. Também destacarei como o Conselho Diretor da ICANN não está disposto a seguir seu próprio estatuto e tomar uma decisão sobre o aplicativo .amazon.

Por que houve um conflito?

Em 2012, a Amazon Corporation solicitou o .amazon de acordo com a Diretriz Para Candidatos a novos gTLDs (um documento normativo aprovado em processo multissetorial). Em uma primeira avaliação, a diretriz recebeu a maior pontuação possível. Mas a ICANN não aprovou o .amazon devido a objeções recebidas de alguns governos da região amazônica. Os argumentos desses governos não apresentaram qualquer razão de política pública, nem se basearam em nenhuma lei internacional incidente. Eles simplesmente não queriam que a empresa Amazon tivesse um gTLD refletindo o nome de um rio em sua região. Curvando-se ao Comitê Assessor de Governos (GAC) em 2014, o Conselho Diretor da ICANN rejeitou o pedido. A Amazon apresentou uma reclamação usando o Processo de Revisão Independente (IRP) da ICANN. Em última análise, o processo de revisão independente deu ganho de causa à empresa. O painel revisor concluiu que o Conselho Diretor "não pode aceitar os pareceres consensuais do GAC como conclusivos" e que, ao negar a solicitação, a ICANN não forneceu razões suficientes para fazê-lo. O painel também concluiu que o GAC falhou ao não tratar a empresa de forma justa.

No entanto, em vez de corrigir seu erro, a ICANN tentou fazer com que a Amazon e seus oponentes chegassem a um acordo negociado. Depois de dois anos, esse esforço falhou.

O processo de negociação falido

A empresa Amazon ofereceu um Compromisso de Interesse Público (PIC) extremamente generoso e compensações em dinheiro aos países envolvidos, incluindo a criação de TLDs alternativos, como o .amazonas, sob o controle desses países. No

1. Publicado originalmente no portal Web do Internet Governance Project, em 2 de maio de 2019: https://www.internetgovernance.org/2019/05/02/icann-needs-to-delegate-amazonPublica
2. https://icann.org
3. gTLD: sigla em inglês de nome de domínio de topo genérico da Internet. Além dos tradicionais como .net, .com, .org, há centenas de novos domínios de topo ativos na Internet aprovados pela ICANN (n.ed.).

entanto, não foi suficiente. Os países, através da Organização do Tratado de Cooperação Amazônica (OTCA),[4] tentaram reivindicar direitos de propriedade sobre alguns dos nomes de domínio de segundo nível que poderiam terminar em .amazon, declararam direitos de soberania sobre um nome que já é de uso comum como marca registrada, e requereu participação na governança do .amazon.[5] Em última análise, a empresa Amazon aceitou a proposta. Enviou um compromisso e está solicitando ao Conselho Diretor da ICANN que tome uma decisão sobre a delegação de .amazon.

Ainda assim, parece que o Conselho Diretor da ICANN está permitindo que o conflito se prolongue, na esperança de que as partes cheguem a um acordo sem que a ICANN tenha que tomar uma decisão. Para agradar alguns governos e sinalizar ao GAC que pode reivindicar poder de veto arbitrário, o Conselho Diretor da ICANN propôs a continuidade dessas negociações intermináveis. Desta vez, deu à OTCA e à empresa Amazon até 7 de junho de 2019 para negociar.[6] Assim, a batalha de sete anos ainda está acontecendo.

Por que a ICANN não pode seguir suas próprias regras?

Na maioria das controvérsias sobre solicitações de gTLDs, quando os governos estão envolvidos, a ICANN toma decisões que não são independentes, objetivas e neutras, ao contrário do exigido pelos estatutos da entidade. Ou prolonga o processo de tomada de decisão. Essa não é apenas a nossa observação: o painel do Processo de Revisão Independente, um órgão neutro de resolução de disputas, também emitiu declarações a favor de requerentes de TLDs que alegam que a ICANN não agiu de forma objetiva e atrasou o processo. Isso aconteceu em casos como .halal, .islam e .africa. Em .halal e .islam, o painel do IRP declarou que a ICANN violou seus próprios valores, conforme o estatuto, ao suspender as solicitações.[7] Apesar de saber de casos anteriores em que isso viola seu estatuto, o Conselho Diretor da ICANN voltou a adiar a decisão sobre o aplicativo .amazon, dando à OTCA mais tempo para negociar com a empresa Amazon.

Está claro por que a ICANN retarda a decisão. Não há base legítima sobre a qual a ICANN possa negar a aprovação do .amazon. No entanto, ela não tem coragem de dizer aos governos nacionais da região que seus argumentos não têm mérito. O Conselho Diretor deve estabelecer se uma questão de política pública está em jogo para aceitar ou rejeitar o aplicativo .amazon. Ele não pode confiar nos pareceres consensuais do GAC, que neste caso e em outros semelhantes, não apresentam nenhum argumento racional, sendo baseados principalmente na política. O Conselho Diretor não pode criar políticas públicas a partir do nada, tampouco uma lei internacional aplicável a este caso. Se o Conselho Diretor negar a aplicação .amazon, fará isso por razões puramente políticas para satisfazer os governos.

“Não há base legítima sobre a qual a ICANN possa negar a aprovação do .amazon. No entanto, ela não tem coragem de dizer aos governos nacionais da região que seus argumentos não têm mérito.”

Hora de decidir

A ICANN precisa ser firme e tomar a decisão certa. A OTCA e o GAC não têm respaldo no direito internacional para sua posição. A ICANN tem a autoridade legal e moral para ignorar suas objeções. Não há nada que eles possam fazer se a ICANN recusar-se a ceder às suas exigências arbitrárias. Já passou da hora dela fazer isso.

E isso não é, principalmente, sobre a Amazon, que ficará bem com ou sem o domínio. Trata-se da imparcialidade, objetividade e independência da governança da Internet. Todos e quaisquer direitos da sociedade civil no espaço do nome de domínio correm risco se um grupo de governos puder usar o regime da ICANN para assegurar o controle sobre recursos globais sobre os quais não têm direito legal ou moral. ■

4. http://www.otca-oficial.info
5. https://www.icann.org/en/system/files/correspondence/zaluar-to-chalaby-23apr19-en.pdf
6. https://www.icann.org/en/system/files/correspondence/chalaby-to-moreira-15apr19-en.pdf
7. https://www.icann.org/en/system/files/files/irp-agit-final-declaration-30nov17-en.pdf

Diego R. Canabarro, Doutor em Ciência Política, mestre em Relações Internacionais e Bacharel em Direito pela Universidade Federal do Rio Grande do Sul (UFRGS). Assessor do CGI.br de maio de 2014 a maio de 2019

O **.amazon** é bem mais que um mero nome de domínio

A batalha final entre a empresa Amazon e os países da região amazônica (Bolívia, Brasil, Colômbia, Equador, Guiana, Peru, Suriname e Venezuela) em torno do domínio de topo .amazon chegou ao fim em 15/05/2019 (e com um desfecho preocupante para a proteção do patrimônio histórico, sociocultural e biológico da Amazônia). De 2013 até aqui, os dois lados da disputa viveram vitórias e derrotas alternadas no âmbito da ICANN – a entidade que, ao mesmo tempo, é encarregada de coordenar centralmente os recursos de endereçamento da Internet e o funcionamento das diversas porções distribuídas que integram o sistema de nomes de domínio da rede (DNS), bem como servir de arena política para a articulação das diversas partes interessadas e a definição de políticas e regras que determinam o funcionamento harmônico do sistema.

O caso transformou-se, numa lógica de teoria dos jogos, em uma situação do tipo perde-perde para a ICANN: a não delegação do .amazon a colocaria em maus lençóis perante sua comunidade marcadamente centrada na economia política estadunidense (e principalmente perante o governo dos Estados Unidos); a delegação definitiva (que foi o que efetivamente aconteceu) coloca agora a organização em rota de colisão com os países amazônicos (algo que pode reanimar a discussão a respeito da legitimidade da ICANN como estrutura de coordenação central do endereçamento da Internet global).

Detalhes do caso

O pleito da Amazon iniciou-se em 2012, quando a comunidade que gira em torno da ICANN decidiu que faria uma ampliação na quantidade de "nomes de domínios genéricos" existentes na raiz do DNS.

O "programa de novos gTLDs"[1] recebeu quase duas mil candidaturas de entidades interessadas em controlar de forma direta e independente sua própria zona no ponto mais alto da hierarquia do sistema nomes da Internet sem depender de domínios tradicionais como o .com ou um código de país como o .br.[2] Com uma taxa de inscrição de quase US$200 mil, o resultado da rodada de 2012 do programa de novos domínios genéricos foi absurdamente assimétrico e desigual: a esmagadora maioria das candidaturas veio de entidades empresariais do norte desenvolvido.[3]

A Amazon foi a única candidata ao domínio .amazon (e suas variações em japonês e chinês). Essa candidatura seguiu, formal e regularmente, todas as etapas e os procedimentos previstos no edital do programa. Mas, assim que começaram esses procedimentos, os países amazônicos conseguiram arregimentar o consenso de todos os demais países integrantes do "Conselho Consultivo Governamental" (GAC)[4] em torno da ideia segundo a qual o .amazon não deveria prosperar, por conta das diversas implicações e contradições entre os interesses comerciais da empresa e os imperativos de proteção e promoção da cultura e das tradições, da história, da biodiversidade, da pluralidade de línguas etc., relacionados à região amazônica.

O GAC – nos termos do estatuto da ICANN – é uma espécie de assembleia que congrega mais de 130 autoridades governamentais e várias organizações intergovernamentais, e é encarregado de emitir pareceres a respeito das implicações que o funcionamento do DNS pode ter para o campo das políticas públicas em geral. Nesse sentido, em 2013, o Comitê emitiu por consenso um parecer indicando de forma genérica ao Conselho Diretor da ICANN (a instância de cúpula da organização e encarregada de decidir, segundo as regras do programa, a procedência ou não de determinada candidatura) que o pleito da empresa não deveria prosperar. O Conselho Diretor corroborou o consenso governamental e, em 2014, decidiu pela improcedência do pedido do .amazon.

Em consequência, e seguindo as próprias regras da ICANN, a empresa constituiu um painel arbitral (formado por três árbitros estadunidenses) contra essa decisão, alegando (em uma grosseira síntese) que o Conselho Diretor – ao acatar integralmente e sem ressalvas o parecer dos governos – violou as regras criadas pela "comunidade" para nortear o programa de novos gTLDs. O painel arbitral (considerado "neutro" por determinados grupos de interesse na ICANN), em meados 2017 deu ganho de causa à empresa, apontando que o Conselho Diretor da ICANN não explicitou as "razões de política pública" que fundamentaram a aceitação irrestrita

1. Sigla de "generic top-level domain". A política de expansão englobou genéricos (.jobs, .guru), geográficos (.rio, .osaka) e de marcas (.aramco, .ibm). Para uma lista bem detalhada, ver https://newgtlds.icann.org/en/program-status/delegated-strings
2. Alguns casos célebres – incluindo alguns controversos – são .music, .blog, .gay, .xyz, .web, .bradesco, .natura, .globo etc.
3. Nesse sentido, ver: http://reseaux.blog.lemonde.fr/2013/04/23/icann-alchimie-noms-domaines
4. "Government Advisory Committee", um dos comitês consultivos setoriais da ICANN, constituído por representantes de governos.

do parecer dos governos e, em última análise, a improcedência da candidatura ao .amazon.

Entre 2018 e maio de 2019, a questão seguiu indefinida e houve diversas tentativas de composição da celeuma. Sem nenhum sucesso, a ICANN tentou mediar um resultado mutuamente satisfatório para a questão. Entretanto, em março de 2019, a entidade retirou-se da mediação e deu prazo para que as partes encontrassem uma saída mutuamente satisfatória.

Em 2015, a empresa havia apresentado uma proposta de cogestão do nome, que foi integralmente rechaçada pelos governos amazônicos. Em 2018, os países tentaram resgatar a proposta de 2015 como alternativa ao plano de utilização do .amazon apresentado pela empresa após a vitória no painel arbitral de 2017. Essa proposta envolvia, basicamente, a concessão de um nome embaixo do .amazon para uso coletivo dos oito países, a definição de uma lista de nomes reservados e a concessão de uma contraprestação pecuniária total de US$ 5 milhões (em produtos e serviços comercializados pela empresa) em favor dos países amazônicos.

Em negociações mais recentes, a empresa concordou em consignar um nome a cada país da região e ampliar o alcance da lista de nomes protegidos. A empresa também divulgou um "compromisso de interesse público": uma carta de intenções onde explica de que forma utilizará o .amazon respeitando determinadas promessas feitas aos países da região. A observância dessa carta pode ser cobrada da empresa mediante uma modalidade de arbitragem especial que pode ser realizada no âmbito do arcabouço institucional da ICANN. Para alguns, essas concessões da empresa representam uma "generosa oferta" aos países da região. Apenas a título de argumentação, US$ 5 milhões é um valor ínfimo quando comparado ao somatório dos PIB dos países amazônicos (mais de US$ 3 trilhões).

O que se pode dizer é que, com base no resultado do painel arbitral e com a invocação da observância estrita do edital do programa de novos gTLDs, a empresa passou a exercer pressão para que continuasse o processamento de sua candidatura e resultasse na inserção definitiva do .amazon na raiz do DNS (algo que foi definitivamente decidido pelo Conselho Diretor da ICANN em 15/05/2019).

Os países amazônicos tentaram resistir na virada de 2018 a 2019, apegando-se ao fato de que uma questão tão complexa como o caso do .amazon não deveria ser resolvida sem que fossem consideradas outras questões que vão muito além da mera gestão técnica do sistema de nomes de domínio da Internet. Entretanto, sua própria desorganização após o colapso da diplomacia na região a partir da crise da Venezuela (com especial destaque para a postura unilateral assumida pelos governos do Brasil e da Colômbia desde então) enfraqueceu a ação coletiva coordenada do bloco e pode ser uma das principais causas do êxito da pressão exercida pela Amazon sobre o Conselho Diretor da ICANN para o encerramento da questão.

A comunidade, o Conselho e a organização

A ICANN é multidimensional. Ela congrega três partes bastante distintas: a "comunidade" de pessoas envolvidas com o DNS; a organização ICANN (entendida aqui como o corpo de profissionais que trabalha na execução das atividades rotineiras da entidade); e o Conselho Diretor (o órgão de cúpula na complexa estrutura da ICANN).

A comunidade envolve atores provenientes do setor empresarial, dos governos, da sociedade civil organizada, das comunidades técnicas e acadêmicas, bem como usuários individuais. Essa comunidade multissetorial está agrupada em torno de pautas comuns (por exemplo, a entidade que gira em torno dos domínios genéricos; o coletivo de administradores de códigos de país; o comitê governamental; os administradores de servidores-raiz, etc.).

O grupo mais heterogêneo em termos de composição é aquele que perambula em torno dos domínios genéricos: há aqueles grupos que mantêm contratos com a ICANN (concessionários de domínios, os "registries", e revendedores de nomes no varejo, ou "registrars") e há aquele conjunto de usuários (individuais ou corporativos) do DNS e que participam da definição de políticas nessa mesma condição (ativistas e entidades da sociedade civil preocupadas com a defesa de direitos fundamentais como a liberdade de expressão; empresas e entidades interessadas na preservação de direitos autorais; provedores de conectividade; usuários comerciais em geral). É dentro desse caldeirão que foram formuladas as regras do programa de novos gTLDs de 2012. Além daqueles, os grupos que congregam administradores de códigos de país, governos, usuários individuais e comunidades técnicas, seguem, cada um, uma lógica distinta de organização interna. E o estatuto de constituição e organização da ICANN (seguindo a legislação

da Califórnia) orquestra a forma de interação de todos esses grupos. Após a chamada "transição IANA" (que não há espaço para tratar em detalhes aqui)[5], pode-se dizer que o arcabouço de articulação e coordenação de todos esses grupos transformou a ICANN em uma verdadeira "organização internacional não governamental".

O Conselho Diretor, por sua vez, envolve um grupo de 19 pessoas (mais o CEO da organização, num total de 20): algumas delas são eleitas pelos diferentes grupos de interesse da ICANN e outras são especialistas selecionadas por um "Comitê de Seleção". O Conselho representa uma instância plural, composto a partir de imperativos de diversidade geográfica, linguística, de gênero, de competências profissionais e de aptidão temática.

A organização ICANN, por sua vez, congrega o conjunto de departamentos encarregados de desempenhar tanto as funções técnicas relacionadas à coordenação do DNS, quanto o trabalho de apoio ao funcionamento da arena política que ICANN encerra – na qual a comunidade dialoga e delibera permanentemente e o Conselho Diretor, após apreciar as questões estratégicas envolvidas nos direcionamentos dado pela comunidade, toma as decisões que definem os rumos do DNS.

O mito de que o DNS pode/deve estar imune à "politização"

Historicamente, de Clinton a Obama, o desenvolvimento institucional da ICANN foi sempre pautado pelo "ideal" de "privatização da governança da Internet", o que ajuda a explicar uma certa ojeriza a tudo aquilo que venha dos governos (e, por consequência, do GAC).

Algo que geralmente acompanha a ideia de uma "governança liderada pelo setor privado" é o cultivo do mito segundo o qual a Internet só alcançou o sucesso que tem hoje porque sua governança sempre foi técnica e não política. Ainda hoje, mesmo depois do que foi escancarado com a Cúpula Mundial Sobre a Sociedade da Informação entre 2003 e 2005;[6] da publicação de trabalhos de fôlego e muito rigor que escancaram "a política dos protocolos",[7] "quem governa a raiz"[8] e "quem governa a Internet";[9] do teor da Declaração NETmundial sobre o futuro da governança global da Internet;[10] e da indissociável vinculação da Internet ao alcance das metas de desenvolvimento sustentável constantes da Agenda 2030,[11] há quem faça de conta que, em um passado perdido, a governança da Internet foi meramente técnica e apolítica, e defenda que esse ideal normativo seja perseguido como condição existencial para que a Internet siga sendo uma rede aberta e de caráter global.

Disso decorre um estado de permanente objeção e crítica à participação dos governos em processos decisórios no âmbito da ICANN. O GAC tem apenas a prerrogativa de aconselhar a ICANN a respeito das implicações que políticas para o DNS podem ter para as políticas públicas em uma perspectiva mais ampla. É verdade que o Comitê pode opinar sobre todo e qualquer assunto que lhe der na telha, desde que demonstre sua relação com o tema das políticas públicas. Ainda assim, a opinião dos governos não é vinculante nem mesmo para esses temas. Até 2016, todo e qualquer parecer do Comitê deveria ser seguido pelo Conselho Diretor em suas decisões (que deveria prestar esclarecimentos sempre que deixasse de segui-lo). A partir de 2016, a comunidade (que um respeitado centro de pesquisas da Índia classificou como "nem global, nem multissetorial")[12] decidiu que somente pareceres adotados consensualmente pelos governos teriam o status especial que tinham outrora. Essa guinada (que diminui ainda mais a prerrogativa dos governos incidirem no resultado dos processos de desenvolvimento de políticas na ICANN), inclusive, teve grande oposição de um grupo considerável de países sob a liderança do Brasil.

Por temas que vão desde a morosidade de processos governamentais e intergovernamentais vis-à-vis processos decisórios no setor privado e em ambientes técnicos, passam pelo questionamento da legitimidade dos governos para falar em nome de suas populações e chegam até a alegações de que governos são essencialmente auto-interessados e corruptos, pode-se dizer que a discussão a respeito do papel dos governos na governança da Internet, no contexto da ICANN, não é séria (e merece cuidados em virtude do potencial

5. Mais detalhes em "A transição IANA chegou à outra margem do Rubicão" na 23ª edição da poliTICs. Disponível em: https://www.politics.org.br/categoria/politics-23.
6. https://cgi.br/publicacao/cadernos-cgi-br-documentos-cmsi
7. DENARDIS, L. Protocol Politics - The Globalization of Internet Governance. Cambridge, MA: The MIT Press, 2009.
8. MUELLER, M. L. Ruling the root: internet governance and the taming of cyberspace. 1. paperback ed ed. Cambridge, MA: MIT Press, 2004.
9. GOLDSMITH, J.; WU, T. Who controls the Internet? Illusions of a borderless world. New York: Oxford University Press, 2006.
10. http://netmundial.br/pt
11. http://www.agenda2030.org.br
12. https://cis-india.org/internet-governance/blog/global-multistakeholder-community-neither-global-nor-multistakeholder

destrutivo que tem para a própria organização).

Não se pode afirmar categoricamente, sob pena de incorrer no ridículo, que governos, de forma indistinta, são essencialmente maus; que agem sempre de forma desvinculada dos mandatos recebidos pelo eleitorado e de forma inteiramente desvinculada dos interesses de suas populações, como é comum de se ouvir no ambiente ICANN. Por mais que a democracia representativa esteja sendo crescentemente posta à prova (o que é bom e, inclusive, é em parte viabilizado pela própria popularização da Internet), não se pode desconsiderar que os governos (e também seus poderes legislativos) constituem a institucionalidade por meio da qual, direta e indiretamente, as populações de cada país perseguem suas pautas prioritárias e o alcance dos interesses nacionais. Nem todos os governos são tiranos. E nem todas as populações dos 193 países que atualmente compõem a Organização das Nações Unidas estão completamente alijadas dos rumos adotados pelos governos que escolhem para lhes representar. Pelo contrário: a evolução da prática democrática contemporânea no mundo inteiro seguiu – durante a maior parte do Século XX e do início deste século – um caminho de constante fortalecimento e qualificação.

Essa espécie de demonização da política (e, em grande medida, da institucionalidade por meio da qual a política se manifesta) mistura a aspiração idealista de matriz libertária e os objetivos concretos de determinados atores (inclusive de atores estatais) com o intuito de esvaziar a participação do setor público na economia política contemporânea.[13] É com esse pano de fundo que proliferaram narrativas segundo as quais o caso .amazon deveria ser decidido única e exclusivamente nos termos das regras procedimentais adotadas pela comunidade da ICANN em 2012, desvinculando a questão de outros aspectos que transcendem a governança do DNS em uma perspectiva mais estrita.

Quem ganha o quê, como e quando?

Alega-se que a contaminação da "política do DNS" por questões que transcendem a técnica podem comprometer a credibilidade e a neutralidade da ICANN para ocupar o papel que ocupa hoje, de coordenação dos identificadores da Internet em benefício do interesse público. Essa pretensão de neutralidade, pela própria complexidade da estrutura apresentada acima, não merece prosperar. Além disso, a enorme diversidade sociopolítica, econômica e cultural das partes do planeta integradas hoje na rede mundial de computadores faz com que seja difícil conceber que uma organização como a ICANN (subordinada à legislação da Califórnia e pautada principalmente pelos atores envolvidos com a economia dos nomes de domínio -- algo enormemente vinculado à economia dos Estados Unidos) consiga dar conta da pluralidade de assuntos envolvidos na relação circular entre Internet e sociedade. Mesmo que fosse possível extirpar integralmente a participação dos governos desse complexo mosaico que conforma a governança da Internet hoje, ainda assim a pergunta crucial de qualquer análise política ("quem ganha o quê, como e quando?") segue inteiramente válida e é bastante instrutiva para que se possa entender o que está efetivamente em jogo no caso do .amazon.

Cumpra-se o edital, ainda que pereça o mundo

As regras do edital do programa de novos gTLDs previam algumas reservas a nomes de cunho geográfico – nomes de capitais de países; nomes de cidades em geral quando seu uso fosse associado à cidade e não a outro objeto homônimo; nomes de lugares e regiões subnacionais constantes da lista ISO 3166-2;[14] nomes de regiões nos termos definidos em lista mantida pela UNESCO; nomes de regiões constantes da lista de regiões continentais e regiões subcontinentais, de grupos econômicos e outros mantida pela ONU.

O nome do estado brasileiro do Amazonas faz parte da lista ISO 3166-2. Nenhuma das outras categorias previstas no edital, entretanto, confere qualquer proteção à região amazônica propriamente dita e, principalmente, ao termo específico "amazon". De forma reiterada, tanto a Amazon, quanto outros países (como é o caso dos Estados Unidos) e até mesmo funcionários da própria ICANN, apontaram publicamente que não há, no direito internacional e até mesmo na ordem jurídica interna de qualquer país, qualquer empecilho ou proteção ao mero uso do nome "amazon" (inclusive no DNS global).

O edital, entretanto, previa algumas janelas

13. WINNER, L. "Cyberlibertarian Myths and the Prospects for Community". SIGCAS Comput. Soc., v. 27, n. 3, p. 14–19, 1997.
14. https://www.iso.org/iso-3166-country-codes.html

de objeção que poderiam ser utilizadas pelos governos para expressar sua preocupação e eventual contestação à delegação de nomes de cunho comunitário, geográfico e religioso. Os governos poderiam enviar mensagens preliminares aos proponentes explicando sua preocupação com o uso de determinado nome. O GAC poderia emitir pareceres com oposição a determinada candidatura. E, ainda, havia a possibilidade (para grupos de interesse em geral, não apenas os governos) de desencadear a ação de um "contestante independente" (um perito contratado pelo programa de novos gTLDs para fazer o papel de uma espécie de "advogado do diabo" no caso). Em suma, o .amazon contou com todos esses expedientes: as mensagens preliminares não fizeram a empresa desistir de sua candidatura; o parecer do contestante independente não foi considerado procedente pelo Comitê do Programa de Novos gTLDs; e o parecer do GAC foi revertido posteriormente pelo painel arbitral movido pela empresa contra o Conselho Diretor da ICANN. Em caso similar, diante de contestações semelhantes, a empresa Patagonia (do ramo de vestimentos e acessórios para turismo de aventura), com menor poder econômico e respaldo político que a Amazon, acabou desistindo de sua candidatura ao .patagonia.[15]

O curioso da reversão é que o painel arbitral não determinou à ICANN que procedesse imediatamente com a liberação do .amazon. Ele apenas indicou que o Conselho Diretor falhou em apontar as razões de políticas públicas que o fizeram acatar sem ressalvas um parecer consensual do GAC que expressava, de forma genérica, oposição à candidatura. Eis aí algo bastante relevante para a compreensão dos acontecimentos recentes (e talvez até mesmo a respeito do que está por vir não apenas dentro do escopo dos novos nomes de domínios genéricos, mas, também, em relação ao futuro da própria ICANN).

O governo dos EUA como o (verdadeiro) fiel da balança

A compreensão do caso do .amazon passa, ainda, pela oscilação de posicionamento do governo dos Estados Unidos em relação ao tema. O panorama favorável aos governos amazônicos, entre 2013 e 2015, está intimamente ligado ao enfraquecimento da voz do governo Obama nas questões de governança da Internet no contexto do escândalo Snowden e das reações do Brasil e aliados em diversas esferas da política internacional.

A não objeção dos EUA (e países que tradicionalmente o acompanham) ao parecer do GAC em 2014 pode ser entendida como uma concessão feita pelo país para evitar que o caso .amazon e a própria arquitetura institucional da governança global do DNS virassem objeto de contestação fora da estrutura da ICANN. É verdade que o Encontro NETmundial, liderado pelo Brasil, serviu como espaço para a discussão do futuro da governança da Internet. Entretanto, imediatamente antes do evento, o governo dos EUA habilmente anunciou sua intenção de abandonar seu papel de supervisor-garante unilateral das atividades da ICANN, e concentrou a atenção da comunidade da ICANN em torno do longo processo, que durou de 2014 a 2016, de reformulação da estrutura da entidade de modo a torná-la independente e autônoma em relação à supervisão governamental.

Ao sinalizar positivamente ao pleito de outros governos em uma questão pontual como o caso .amazon, os Estados Unidos angariaram o apoio necessário para conferir legitimidade ao processo de reforma do multissetorialismo da ICANN (contendo a tradicional e sempre frequente demanda de realocação das funções dessa última a arenas intergovernamentais já existentes ou a serem eventualmente criadas).

Encerrado o período de transição, a partir de 2017, a retórica do governo estadunidense e de seus países aliados no GAC passou a ser mais perceptível e mais claramente favorável ao pleito da Amazon, na cobrança da estrita observação das regras definidas pela comunidade multissetorial da ICANN.

A reificação do multissetorialismo da ICANN e a pretensão de que ele é imune a críticas

O grande ponto a considerar no caso do .amazon é a forma autorreferenciada como a comunidade da ICANN trata de temas complexos e com diversas interfaces com aspectos políticos e estratégicos mais amplos, que transcendem a mera coordenação técnica do funcionamento da Internet pelo planeta.

Em primeiro lugar, diversos grupos de interesse

15. https://icannwiki.org/.patagonia

"Por mais internacionalizada e obcecada pelo seguimento de regras de governança corporativa que seja, as ações da ICANN enquanto organização são muito influenciadas pelo ethos e pelos direcionamentos de uma comunidade que reflete consideravelmente os interesses do setor empresarial dos EUA."

ainda fazem de conta que essa coordenação pode ser feita de forma inteiramente neutra, sem implicações culturais, sociais, econômicas e políticas mais amplas. A Internet cresceu demais e essa noção idílica é atualmente insustentável.

Em segundo lugar, a invocação do mito da eficiência técnica vem sempre acompanhada da necessidade de estrita observância das regras e procedimentos internos, como requisito de legitimidade do papel da ICANN na coordenação dos recursos críticos ao funcionamento da Internet no mundo. Mesmo que isso deixe margem para que a ICANN coloque-se frontalmente em contradição e conflito com outras esferas da governança global (seja processos inteiramente intergovernamentais, seja trilhas onde diversas modalidades de práticas multissetoriais são desenvolvidas para dar conta dos dilemas da ação coletiva e dos problemas comuns a mais de um ator no plano internacional). O mais chocante, nesse caso, é que a própria sociedade civil organizada (tradicionalmente envolvida, alhures, com discussões substantivas em prol da justiça social e do combate a desigualdades e assimetrias em geral), na ICANN, tende a pautar-se por um formalismo estrito bastante similar aos ideais de uma governança inteiramente "privatizada" patrocinados maciçamente por setores empresariais e alguns países de viés mais liberalizante.

Por fim, há que se retomar a distinção crucial entre a comunidade, a organização e o Conselho Diretor. A comunidade da ICANN é bastante dominada por representantes de empresas envolvidas com o mercado de nomes de domínio, bem como usuários corporativos da Internet. Há uma expressiva participação da sociedade civil organizada nas atividades da ICANN (sobretudo por parte de ativistas e entidades do norte desenvolvido, focadas na proteção e promoção da liberdade de expressão e outros direitos fundamentais *online*), mas em menor intensidade e com muito menos recursos disponíveis que o setor empresarial em geral. Por vezes, os interesses de uns e de outros conflitam. Por vezes, esses setores atuam em sintonia (e até mesmo como proxies uns dos outros).

Os governos, nesse meio, têm a prerrogativa de falar sobre tudo aquilo que os demais grupos fazem e decidem, desde que (a) articulem aspectos de políticas públicas e, para serem decisivos e capazes de influenciar os processos, (b) alcancem o consenso entre si. Esse condicionamento reduz a capacidade de influência coletiva dos governos na ICANN, sobretudo diante da impossibilidade de se desvincular os interesses individuais de cidadãos e de corporações privadas (com ou sem fins lucrativos) dos interesses nacionais perseguidos pela diplomacia onde quer que seja (inclusive em uma arena como a ICANN).

A organização ICANN, por sua vez, apesar de servir para viabilizar as atividades da comunidade e do Conselho Diretor, segue sendo uma entidade privada sem fins lucrativos sediada nos Estados Unidos. Por mais internacionalizada e obcecada pelo seguimento de regras de governança corporativa que seja, as ações da ICANN enquanto organização são muito influenciadas pelo ethos e pelos direcionamentos de uma comunidade que reflete consideravelmente os interesses do setor empresarial dos EUA. Isso ocorre, inclusive, em virtude da grande proximidade que os funcionários

da organização têm com os diversos grupos de interesse no cotidiano do funcionamento da mesma.

O Conselho Diretor segue essa toada, mas em menor medida; algo que deriva não apenas de sua pluralidade de composição, mas, também, de um olhar estratégico a respeito de tudo que está em jogo na interface da coordenação do DNS com o restante da governança global. Prova disso é que o Conselho foi bastante reticente e cauteloso com o processamento do caso .amazon ao longo dos anos. Mas foi impossível ao Conselho resistir à pressão crescente da Amazon e da própria comunidade da ICANN (incluídos aí o governo dos Estados Unidos e seus aliados) e barrar a criação do gTLD .amazon. Isso claramente acabou sendo facilitado pelos limites da organização e da coordenação da resistência dos países sul-americanos na virada de 2018 para 2019 (e por uma série de erros estratégicos que ocorreram ao longo dos sete anos de tramitação do pedido – algo que não vem ao caso neste momento).

Acontece, porém, que o fim do caso .amazon parece ser apenas o início de um novo período de contestação à ICANN (a exemplo do que tem ocorrido sucessivamente desde a Cúpula Mundial Sobre a Sociedade da Informação[16] até os dias atuais). Deve-se lembrar, novamente, que o painel arbitral não determinou à ICANN a delegação tout court do .amazon. Apenas apontou que o Conselho Diretor falhou em apontar as razões de políticas públicas que fundamentariam o óbice à candidatura. Assim, o Conselho Diretor decidiu delegar o .amazon sem enfrentar o cerne da questão: quais razões de políticas públicas fundamentaram a aceitação irrestrita do parecer consensual dos governos? Ou por que o consenso de todos os países do GAC (algo raro de se alcançar) não é uma razão de política pública suficientemente forte para fundamentar a improcedência do .amazon? Pode ser que um novo painel arbitral surja, movido pelos governos, justamente para questionar a falta de explicação do Conselho para desconsiderar o consenso de todos os governos. Em última análise, a questão pode até mesmo ser judicializada perante um tribunal da Califórnia (ainda que essa seja uma hipótese bastante remota).

Mas o mais importante: dependendo de como o caso for conduzido fora dos limites da ICANN enquanto arena política e chegar a outros espaços onde a interface entre TICs e governança global é objeto de discussão e deliberação, pode ser que a ICANN saia enfraquecida. Sobretudo, porque a estrutura da ICANN como um todo, marcada pelas distorções de um multissetorialismo enviesado, ainda tem muito a provar para que possa ser considerada uma arena política pluralista e democrática capaz de ser percebida sem ressalvas como o locus plenamente legítimo para a consecução de atividades tão (e cada vez mais) relevantes para a governança global. ■

16. https://www.itu.int/net/wsis

POLITICS

Uma publicação do Instituto Nupef | junho-setembro de 2019 | https://nupef.org.br

29

A tiragem das edições da POLI**TICS** é pequena. Se você quiser receber gratuitamente a edição impressa, envie um e-mail para **politics@nupef.org.br** com seu nome, endereço completo - incluindo o CEP - e a sua área de atuação.

Todas as edições estão disponíveis em **https://politics.org.br**
Nosso contato: **politics@nupef.org.br**

ISSN: 1984-8803

apoio FORDFOUNDATION nic.br

*A POLI**TICS** procura aderir à terminologia e abreviaturas do Sistema Internacional de Unidades (SI), adotado pelo Instituto Nacional de Metrologia do Brasil (Inmetro). Assim, todos os textos são revisados para assegurar, na medida do possível e sem prejuizo ao conteúdo, aderência ao SI. Para mais informação: http://www.inmetro.gov.br/consumidor/unidLegaisMed.asp*

Originais compostos em LibreOffice e Linux.