SOBERANIA DIGITAL OU COLONIALISMO DIGITAL?

Renata Ávila Pinto

- *Novas tensões relativas à privacidade, segurança e políticas nacionais*

RESUMO

Além das tensões referentes à privacidade e segurança, estamos testemunhando na atualidade um confronto real entre controle e liberdade, não apenas do indivíduo, mas de populações e regiões inteiras, aumentado pelas tecnologias e pela coleta e análise massiva de dados – desde prever e influenciar comportamentos, até a automação dos serviços públicos e a capacidade de controlar e interromper totalmente esses serviços, mesmo que remotamente; desde obter acesso a uma plataforma de comunicação global, até perder a capacidade de proteger os direitos daqueles que estão interconectados por meio dessas plataformas. Estamos testemunhando uma nova forma de colonialismo digital?

Este artigo se concentra em soluções regionais, nacionais e comunitárias para restaurar o controle e a propriedade sobre as principais infraestruturas de informações e comunicações, o único primeiro passo possível para corrigir a atual violação massiva de direitos à privacidade. Em seguida, o artigo sugere algumas medidas locais para experimentar e promover alternativas em diferentes níveis de intervenção e ação, incluindo política proativa, capacitação e novos projetos inspirados em um conjunto de valores e princípios diferentes daqueles dos atores dominantes no mercado.

PALAVRAS-CHAVE

Vigilância | Soberania tecnológica | Colonialismo digital | *Software* livre | Privacidade | Controle de dados | Espionagem econômica | Povos indígenas

"Todos os aplicativos digitais que podem ser usados para vigilância e controle serão usados para vigilância e controle."
Professora Shoshana Zuboff [1]

1 • Definindo o problema: Colonialismo digital e feudos tecnológicos

Uma análise simplista da atual situação das tensões entre privacidade e segurança (a narrativa predominante na mídia) provavelmente declarará o seguinte: os Estados estão espionando cidadãos nacionais e estrangeiros e essa tendência só aumentará, conforme adquirirem tecnologias mais baratas, proporcionais a seus poderes militares e tecnológicos. O setor privado também faz isso, mas não com intenções inerentemente más ou propósitos políticos. O que interessa ao setor privado é a "experiência" do usuário, a captura máxima de seus dados e como oferecer os melhores produtos e serviços. Danos colaterais, como a violação de dados no Facebook, por empresas como a Cambridge Analytica, são a exceção à regra.[2] Quanto à população, ela não está realmente preocupada se seu governo a espiona. A população está um pouco preocupada com a vigilância do setor privado, mas está disposta a concordar com isso, especialmente se permitir a utilização de serviços "gratuitos" ou melhorar sua experiência em geral. Isso ocorre apesar do fato de que a preocupação com a privacidade esteja aumentando gradualmente e as regras, ligeiramente melhorando em algumas regiões, especialmente na Europa, por exemplo, após a entrada em vigor do Regulamento Geral sobre a Proteção de Dados (RGPD), corrigindo um sistema falido de erosão sistêmica da privacidade e extração de dados.

Contudo, para além dessa análise simplista, a situação é mais complexa e envolve um elemento adicional que é frequentemente negligenciado. O poder da vigilância e a concentração dos dados coletados tanto pelos mecanismos públicos quanto privados centram-se em um pequeno número de atores, públicos e privados, sediados sobretudo em uma única jurisdição, e levam a uma rápida erosão da soberania do Estado e da democracia.

Nunca um setor pequeno teve tanto poder sobre o mundo inteiro, para monitorar o presente e prever comportamentos futuros não apenas de indivíduos, mas de populações inteiras. O problema é mais alarmante quando consideramos como os setores público e privado estão se fundindo em corporações em busca da dominação global, penetrando em todos os governos, movimentos populares, mediando toda ação na vida de cada pessoa conectada por meio de dispositivos digitais e coleta de dados.

As Tecnologias da Informação e Comunicação (TIC), a inovação da inteligência artificial e a capacidade de rapidamente implantar sistemas e infraestrutura nos mercados emergentes estão concentradas em apenas alguns países, que agora estão engajados em uma corrida para atingirem a liderança.

Além disso, esses países e empresas têm três elementos que a maioria dos países em desenvolvimento e até países de renda média não possuem atualmente. O primeiro elemento são recursos, tanto de capital (propriedade e controle de cabos, servidores e dados) quanto intelectuais (técnicos e instituições de pesquisa de ponta). O segundo elemento é a atual arquitetura jurídica nacional e internacional, que impede que os pequenos países adotem políticas que favoreçam a produção e compra de bens e serviços produzidos domesticamente, com a ameaça de processos judiciais nos tribunais internacionais pela adoção de medidas anticoncorrenciais. Isso limita a capacidade de pesquisa e inovação dos países em desenvolvimento e de renda média; o atual sistema de patentes e direitos autorais restringe artificialmente o compartilhamento de conhecimento e a capacidade de inovar em ritmo acelerado. Tais restrições só aumentarão, com pouca possibilidade de reversão, devido ao novo grupo de acordos de livre comércio, a Parceria Transpacífica (Trans Pacific Partnership - TPP, na denominação em inglês), a Parceria Transatlântica de Comércio e Investimentos¬ (Transatlantic Trade and Investment Partnership – TTIP, na denominação em inglês) e o Acordo para o Comércio de Serviços (Trade in Services Agreement – TISA, na denominação em inglês). Algumas das disposições da nova geração de acordos comerciais consideram até as leis e políticas de privacidade mais rígidas em um país como uma barreira para o comércio, desconsiderando a primazia das normas de direitos humanos sobre qualquer outra lei.[3]

O terceiro elemento, acessível de imediato a somente um pequeno grupo de países, é a disponibilidade de capital financeiro para testar e projetar novos modelos, por meio de fundos públicos, capital de risco ou parcerias público-privadas. Esses países estão investindo massivamente em pesquisa e desenvolvimento, não apenas para manter sua posição dominante no setor e expandir agressivamente para o maior número possível de mercados, mas também para explorar maneiras inovadoras de integrar a tecnologia da informação em todos os aspectos da administração pública, setor privado, sua defesa e segurança e o cumprimento dos direitos dos cidadãos.

O cenário é radicalmente diferente para países em desenvolvimento, nos quais a austeridade é a norma e a desigualdade digital logo será um problema bastante visível, inclusive em lacunas em educação e pesquisa, levando à absoluta dependência tecnológica. Esses países representam um terreno relativamente fácil de dominar e há uma corrida para isso por grandes empresas de tecnologia, particularmente entre os Estados Unidos da América e a China, à medida que a Europa fica para trás e suas empresas lutam para competir com seus homólogos nos EUA e na Ásia.

Portanto, as populações off-line do mundo são o território disputado dos impérios tecnológicos, porque quem as aprisionar em seu feudalismo digital deterá a chave para o futuro. Os gigantes da tecnologia estão, sem dúvida, influenciando fortemente a maneira como campanhas eleitorais, governos e política operam.

Eles também influenciam a política e as políticas para delinear padrões internacionais que sirvam seus modelos de negócios,[4] cada vez mais baseados em coleta de dados,

monitoramento e identificação de padrões, corroendo inevitavelmente a privacidade de muitas pessoas. Além de Bruxelas[5] e Washington, os gigantes da tecnologia estão atualmente engajados em esforços agressivos para investir em áreas que tradicionalmente pertenciam ao Estado ou a outras agências e provedores especializados. Atualmente, duas empresas de tecnologia sediadas na Califórnia (Facebook e Google), uma gigante do espaço na Califórnia (SpaceX) e uma empresa de satélites em New Jersey (OneWeb) estão envolvidas em corridas aceleradas para conectar os desconectados.[6] Essas empresas estão fornecendo infraestrutura vital para os cidadãos em troca de seus dados pessoais, que assim se tornam potenciais destinatários de publicidade. Na maioria dos países, nem o governo nem os investidores privados podem competir com a velocidade e os recursos que essas grandes empresas têm para fornecer conectividade a áreas não atendidas.

Essas corporações, considerando-se que geralmente uma delas representará a primeira experiência digital do usuário, normalmente combinam seus programas com o fornecimento de *hardware, software* e conteúdo limitado, não dando aos cidadãos nem ao Estado muita escolha. Normalmente, os novos usuários são submetidos a contratos confidenciais de longo prazo que permitem que as companhias tenham acesso total a quaisquer de seus dados. Isso é agravado pelo fato de que estamos geralmente falando de territórios com privacidade e proteção de dados inexistentes ou limitadas. Os contratos também costumam conter cláusulas com penalidades rigorosas em caso de descumprimento. Esta situação permite formas novas e disfarçadas de exploração e subordinação.

Os programas de rápida digitalização dependem muito de tecnologias móveis para conectar novos usuários à internet cada vez mais comercializada. Essa abordagem difere dos programas iniciais, como o *One Laptop Per Child*, que defendia o desenvolvimento de capacidades criativas e alfabetização para os pobres, a fim de desenvolver plenamente a capacidade de programar, criar *hardwares* e até mesmo desenvolver habilidades em robótica.[7] Esses primeiros programas contrastam com os programas atuais, que permitem que os usuários acessem apenas um conjunto de sites previamente instalados e bloqueiam qualquer capacidade de criação, já que é muito difícil fazer tudo isso com um telefone celular. Além disso, esses programas aumentam o risco de vigilância e perfilamento de populações desfavorecidas, porque os telefones celulares em vários países estão vinculados a um cartão SIM registrado.[8] O monitoramento e a comercialização de todas as atividades on-line dos usuários são a principal motivação para os esforços quase filantrópicos de conectar o próximo bilhão de pessoas e, dessa forma, obter seus dados. Os dados dos usuários são a matéria-prima básica ao aprendizado das máquinas e à inteligência artificial, quando combinados com algoritmos sofisticados e o poder computacional dos conglomerados tecnológicos concentrados.

Na maioria dos casos, as atuais políticas de conectividade estabelecidas por atores corporativos externos – bem como algumas instituições de caridade internacionais associadas ou próximas a empresas de telecomunicações ou de tecnologia – não levam em consideração o poder criativo e a autonomia das pessoas ou da comunidade local. Os dispositivos, *softwares* e *hardwares* costumam ser projetados para consumo pessoal,

em vez de criação ou usos coletivos. Todos os programas operam com prontidão para conectar o maior número possível de pessoas, o mais rápido possível, negligenciando considerações como conteúdo, sustentabilidade em longo prazo ou educação básica em questões importantes como privacidade e segurança on-line. Quando a infraestrutura básica é fornecida por outra pessoa, é difícil melhorar ou impor configurações aprimoradas de privacidade, já que a infraestrutura e o equipamento são geralmente projetados para atender aos propósitos de países onde a vigilância massiva é a regra.[9] Em seu artigo "Dark Google",[10] a professora Shoshana Zuboff explica as razões por trás da corrida para conectar os pobres de todo o mundo de uma maneira específica. Ela também adverte sobre os perigos dos intercâmbios entre as maiores empresas e seus governos, que poderiam ser tentados a usar a tecnologia para sua vantagem geopolítica:

> *Google, Facebook e outras plataformas mudaram para um modelo de publicidade que exigia a captura secreta de dados de usuários como moeda para vendas de anúncios. Os lucros rapidamente se materializaram e motivaram uma coleta de dados cada vez mais implacável e determinada. A nova ciência da mineração de dados explodiu, impulsionada em parte pelo sucesso espetacular do Google.*[11]

E há experimentos que já estão ocorrendo nesse sentido. Por exemplo, durante o último governo de esquerda na Argentina, o YCombinator,[12] um fundo de investimento de risco, apoiou e financiou um partido político emergente da oposição, uma situação que em 2018 poderia causar um escândalo sem precedentes agora que finalmente se tornou visível que a tecnologia tem o potencial de impactar a política. O experimento não foi bem-sucedido – o partido em questão não continua mais como um partido político registrado –, mas demonstra as possibilidades de intervenção do Vale do Silício na política de outros países. O caso Zunzuneo, em Cuba, mostrou como os governos estão cada vez mais contando com a indústria de tecnologia para pressionar por uma nova forma de intervenção.[13] E, por fim, o escândalo da Cambridge Analytica, que vem abalando as democracias ocidentais desde o início de 2018, somente confirmou que nem os países mais poderosos do mundo estão livres de tais intervenções.[14]

Na verdade, não se trata apenas de um problema dos países menos desenvolvidos e mais desconectados. Os governos de países de renda média estão, cada vez mais, ativamente envolvendo empresas para ajudá-los a reprimir algumas formas de discurso que consideram uma ameaça à segurança de seus países. Manifestações legítimas estão sendo monitoradas e inibidas, caso a plataforma na qual o material é publicado concorde com o governo que tais conteúdos são prejudiciais, mesmo que o material seja produzido no exterior e destinado a diferentes públicos.[15] (Por exemplo, veja o Online Censorship Project – Projeto de Censura On-line, na tradução livre em português: https://onlinecensorship.org). Além disso, os governos estão, cada vez mais, sendo vítimas de ataques a sistemas, ativos e pessoas importantes, como o recente ataque ao *software* da companhia elétrica da Ucrânia[16] ou a invasão seletiva de contas de altas autoridades em diversos países da América Latina.[17]

Países inteiros e suas indústrias são totalmente dependentes de infraestrutura, *softwares* e *hardwares* essenciais fornecidos por poucas empresas sediadas em um pequeno grupo de países. Quase toda atividade é mediada por nossa interação com tecnologias e serviços oferecidos por um conglomerado cada vez mais concentrado. Analisar os casos dos *softwares* e *hardwares* é cada vez mais alarmante e é uma das questões mais urgentes a serem abordadas quando se discute a segurança de nossa infraestrutura de informação e comunicação.

Apesar das recentes revelações sobre as capacidades e práticas das agências de inteligência, poucos líderes internacionais (todos bem cientes do problema) estão dando passos reais rumo a soluções concebidas para respeitar os direitos humanos universais de forma eficaz e que também sejam compatíveis com um mundo global e interconectado, além de acessíveis, confiáveis e cuja expansão seja possível. Além disso, quaisquer esforços nesse sentido são precipitadamente rotulados como fragmentação da internet ou esfacelamento da rede.

A maioria dos elementos-chave que permitem que qualquer pessoa, corporação ou governo se conecte à internet estão concentrados na jurisdição da Califórnia. A maior parte das empresas é dos EUA, com o grosso do capital vindo de lá. Em um ambiente geopolítico conturbado, essa concentração de empresas de tecnologia poderia resultar em uma suspensão legal, mas ilegítima, de produtos e serviços para um governo estrangeiro ou indústrias fundamentais em outro país.[18]

As companhias comerciais são suscetíveis à pressão política – conforme comprovado pelo caso WikiLeaks, em que Visa, MasterCard, American Express, Western Union e PayPal bloquearam pagamentos à organização.[19] As defesas do consumidor são frágeis e custosas de serem implementadas, e mesmo para os cidadãos da União Europeia muitas vezes não há reparações em tais circunstâncias, como foi o caso do Wikileaks,[20] assim como durante a crise catalã de 2017.[21] No caso dos governos, as sanções podem afetar seriamente as atividades do dia a dia. A dependência de certas tecnologias para gerir a administração pública é difundida porque poucas empresas no mundo, localizadas em um número ainda menor de países, cumprem os requisitos para fornecer aos governos os *softwares* e *hardwares* necessários para conduzir os negócios públicos a um preço acessível que se adapte às regras de licitação pública cada vez mais uniformes, que geralmente favorecem a opção com menor preço. O resultado é um cenário em que os governos são altamente dependentes da infraestrutura básica advinda de um pequeno conjunto de provedores, que geralmente são suscetíveis a ordens secretas, pressão política e suspensão de atividades devido às sanções. E ao considerar a substituição de um provedor a favor de um provedor nacional que poderia oferecer preços mais baixos, o governo enfrenta severas penalidades.

Conforme a tecnologia continua a penetrar nas principais atividades de todo e qualquer ramo do governo, o próprio governo se torna mais vulnerável do que nunca, contando com infraestruturas essenciais que não controla. Qualquer governo local ou nacional é, sem dúvida, menos livre quando o mercado é "livre", embora, na realidade, dominado por uma situação de quase monopólio.[22] Quando discutimos tecnologias digitais em

grande escala, encontramos um conjunto de empresas que se desenvolveram a partir de subsídios e pesado financiamento de um governo que, ao mesmo tempo, dominava e continua dominando as regras do comércio internacional.[23] Essas regras corroem severamente a liberdade dos departamentos públicos de contratações de escolher alternativas locais mais caras ou subsidiar suas indústrias locais.

A dependência da tecnologia estrangeira só aumenta quando se lida com infraestruturas fundamentais. Em 14 de abril de 2008, a Microsoft anunciou[24] que a empresa não forneceria mais atualizações de segurança para o sistema operacional Windows XP. O anúncio deixou milhares de sistemas estatais completamente vulneráveis, já que dependiam desse sistema operacional para operar infraestruturas fundamentais, como o sistema alfandegário de uma nação latino-americana. Embora uma situação semelhante no ambiente físico – uma fronteira cheia de lacunas de segurança e controles fracos – provavelmente resultaria em uma investigação do congresso, o nível de conscientização sobre infraestruturas tecnológicas cruciais deixou essa questão permanecer sem resolução durante meses.

Diversos governos dependem de infraestruturas de comunicação que estão localizadas nas nuvens (ou seja, em centros de dados estrangeiros sob uma legislação estrangeira aplicável) em sua totalidade. Além disso, esses serviços são fornecidos sob condições de uso em constante mudança e suspensão arbitrária de serviços. O problema não é somente a dependência de um provedor estrangeiro ou as leis aplicáveis a dados digitais; o problema também trata da ausência de políticas públicas para abordar a questão em todos os níveis. A situação da dominação digital, próxima ao colonialismo, ainda não constitui a principal prioridade da agenda política global. Quase quarenta anos após a invenção da internet, a capacidade de políticos e líderes sociais de entender as dimensões do problema ainda é escassa.

2 • Explorando espaços de resistência e soberania tecnológica

A América Latina liderou os primeiros passos rumo à soberania digital no início dos anos 2000. Alguns países tomaram medidas adequadas para estar prontos para substituir os fornecedores estrangeiros pelos locais. Embora na Índia o uso de *software* de código aberto pelo Estado seja obrigatório desde 2005,[25] países da América Latina como o Brasil[26] e a Venezuela[27] (Decreto nº 3.390 2004) promulgaram leis, ainda antes, em 2004, estabelecendo a migração de dados governamentais para *softwares* livres. Iniciativas semelhantes ocorreram posteriormente no Equador (Decreto nº 1014 2008),[28] no Uruguai[29] (Lei nº 19.179 2013) e na Bolívia[30] (Decreto Presidencial nº 1793 de 2013). Em todos esses países, a mudança foi combinada com estratégias para aumentar a alfabetização em *softwares* livres para as crianças de escolas primárias, desenvolvendo projetos como o Plan Ceibal no Uruguai e Canaima na Venezuela. Os países latino-americanos tinham capacidade humana suficiente para produzir internamente pelo menos parte dos softwares de que necessitavam, inclusive exportando alguma produção, ao mesmo tempo em que investiam no processo de capacitação. Como forma de contornar o embargo dos EUA, Cuba desenvolveu seu próprio

sistema operacional, chamado "Nova". O país fez isso não apenas por causa do embargo, mas também como forma de controlar seus próprios sistemas. Essa adoção foi vital, pois Cuba tem restrições para acessar licenças de *softwares* e atualizações de segurança fornecidas pelos maiores provedores. A migração completa para *softwares* livres foi anunciada recentemente pela Rússia, como forma de antecipar o impacto das atuais e futuras sanções.[31]

Mas simplesmente adotar *softwares* livres não é suficiente para um Estado construir uma política abrangente que garanta a soberania tecnológica de suas comunicações. Na tentativa de substituir as escolhas dominantes ou dos proprietários, os governos e as iniciativas comunitárias estão encontrando desafios crescentes para atender às expectativas dos usuários, em termos de velocidade de entrega e qualidade da experiência dos usuários. A sustentabilidade também está entre os desafios, assim como a adoção em massa, a menos que ditada pela lei e a implementação de políticas públicas com recursos, como no Plan Ceibal, no qual todo o sistema educacional foi migrado para um *software* (e *hardware*) de código aberto. Em relação a *hardwares* e equipamentos, um grupo de médicos está usando máquinas de impressão 3D para fornecer estetoscópios aos hospitais de Gaza, afetados pelos bloqueios israelenses.[32] Modelos similares poderiam ser explorados por outros países que permanecem dependentes de outros Estados para equipamentos importantes. O desenvolvimento de novos modelos que permitam a produção nacional é particularmente importante após inúmeras revelações de implantes e falhas de segurança possibilitadas por fornecedores estrangeiros para permitir a espionagem estrangeira, comprometendo a segurança dos usuários.[33]

O acadêmico indiano Sunil Abraham também aponta nessa direção, destacando a importância de desenvolver tecnologias que levem em consideração os direitos humanos em sua concepção, incluindo programações que não podem ser restringidas pela lei de direitos autorais ou que poderiam ser usadas como uma ferramenta de resistência contra certas leis, o que aumentaria tensões. Abraham descreve como "a programação poderia ser usada para impedir a regulamentação por meio da lei, convertendo, assim, as camadas de dispositivos e redes de *software* e *hardware* em um campo de batalha pela soberania entre o *hacker* de *software* livre e o Estado".[34]

À medida que as pessoas em todo o mundo obtêm acesso à tecnologia mais sofisticada em âmbito pessoal a que tiveram acesso desde a televisão, uma nova geração de desenvolvedores e criadores de conteúdo está surgindo. A próxima geração de tecnologias, produzidas fora dos gigantes da tecnologia, pode trazer as soluções que estamos buscando, desde que sejam projetadas, desenvolvidas e distribuídas levando em consideração um conjunto diferente de valores, comportamentos sociais e dinâmicas. Mas tal poder criativo pode ser bloqueado se não detivermos o atual rumo da arquitetura tecnológica que restringe a criatividade em vez de possibilitá-la e que incentiva o consumo e centraliza o poder.

Quando a autonomia tecnológica for alcançada, pessoas e comunidades poderão implementar os princípios delas na maneira como escolherem se comunicar. Conforme

declarado pelo povo nativo maori, ao considerar a necessidade urgente dos povos indígenas de desenvolverem sua própria política de TIC: "...a substituição deliberada de tecnologias locais por tecnologias carregadas de lucros e valores eurocêntricos tem sido parte da agenda colonizadora por muitos séculos".[35]

A inovação constante também desempenha um papel fundamental na resistência e derrota do domínio tecnológico. Pensar além do mercado é algo que as nações desenvolvidas já estão fazendo. Como a Dra. Francesca Bria afirma:

> *Formas alternativas de propriedade pública e compartilhada para plataformas ajudarão a criar uma economia mais democrática, transcendendo a lógica dos sistemas de redes orientados pelo mercado, por rentistas e privatizados. Diversas vezes, isso leva a decisões baseadas em visões de curto prazo, na extração de lucro e na apropriação de recursos comuns para ganhos privados. É necessária uma abordagem de longo prazo para tecnologia, economia e política, na qual recursos e bens públicos são de propriedade, gerenciados e distribuídos para o bem coletivo. Essa tarefa diz respeito à construção da democracia do século XXI.*[36]

Para países de média e baixa renda que ainda estão lutando para correr atrás do atraso e compreender o potencial das novas tecnologias – e, ao mesmo tempo, evitar violações dos direitos de seus cidadãos – há várias opções que precisam começar a ser implementadas com urgência. A maioria delas existe em compromissos nacionais e regionais de médio a longo prazos em múltiplas camadas e envolve uma colaboração fluida entre governos, cidadãos e empresas nacionais. No nível constitucional, os países devem garantir a manutenção da capacidade de legislar e regular as tecnologias emergentes e seu impacto nos direitos fundamentais de seus cidadãos. As constituições devem ser modificadas de modo a não permitirem o envolvimento do Poder Executivo em compromissos internacionais que possam privar o governo de sua competência de fazer valer os direitos internamente. As constituições também devem garantir que o Estado possa possuir autonomia e controle sobre infraestruturas fundamentais de tecnologia[37] e posições-chave[38] em ativos e indústrias importantes.

Paralelamente, também é necessário desenvolver uma estratégia financiada pelo Estado para a soberania digital. Ela deve abarcar todos os aspectos, incluindo a modificação dos currículos escolares para desenvolver os recursos humanos necessários para os próximos cinquenta anos; investimentos pesados em fundos como as Plataformas de Sensibilização Coletiva para a Sustentabilidade e a Inovação Social (Collective Awareness Platforms for Sustainability and Social Innovation – CAPS, na denominação em inglês) e outras iniciativas de pesquisa e desenvolvimento para que experimentos locais possam ser conduzidos; levar em consideração necessidades específicas, habilidades e visão de cada país; e investir recursos de maneira proativa em aplicativos sociais de tecnologia. O intercâmbio de habilidades, informações e pesquisas no Sul Global poderia ser incentivado e financiado.

Enquanto isso, a simples regulamentação de padrões de código aberto, *softwares* livres, *hardwares* disponíveis abertamente e transparência de algoritmos poderia ser desenvolvida, pelo menos para as compras e práticas estatais. A Bolívia fez isso recentemente,[39] sob a liderança do vice-presidente indígena do Parlamento boliviano, Nelida Sifuentes, e sob a orientação de Richard Stallman.[40] Alcançar direitos iguais para todos e saídas eficazes contra a vigilância em massa para os cidadãos no Sul Global só será possível com mudanças financiadas, de longo prazo e abrangentes nas políticas públicas, na tecnologia e na política rumo à autonomia e soberania. Isso pouco a pouco permitirá uma cultura de dignidade digital com padrões de direitos humanos incorporados em protocolos em âmbito regional e internacional.

3 • Conclusão

É necessário, portanto, que os líderes globais – especialmente aqueles que defendem a igualdade e a justiça social – tomem consciência dos perigos que a rápida mercantilização digital representa para as pessoas vulneráveis em todo o mundo e seu impacto sobre a democracia e a dignidade.

Como o acadêmico Dan Schiller adverte:

> *Para a maioria dos povos do mundo, se o crescimento lucrativo do capital pode ser renovado, e por quem, é muito menos importante do que as consequências da mercantilização digital para o emprego, a exploração e a desigualdade; pela perspectiva do autogoverno democrático; para o ambiente devastado; e para o caráter e a qualidade dos serviços culturais necessários para sustentar vidas significativas. Os choques da mercantilização digital estão escrevendo um novo capítulo na longa história do violento deslocamento do capitalismo. Isso faz com que a discussão de estratégias para alternativas sociais seja essencial, de fato, urgente.*[41]

Para começar a abordar as desigualdades digitais globais e abraçar um futuro que coloca a autonomia digital e a dignidade humana em seu núcleo, a inovação social deve ser incentivada e institucionalizada no âmbito da comunidade e do cidadão para garantir sua adaptabilidade e permanência. As comunidades autônomas e linguísticas devem ser encorajadas a desenvolver a sua própria tecnologia e seu conteúdo digital e a preservar e exportar as suas culturas para o ambiente digital. As políticas públicas devem ser promulgadas para garantir que a adoção de novas tecnologias em larga escala não crie mais desigualdade, exclusão ou imposição de valores e práticas que sejam alheias às comunidades destinatárias. Em vez disso, as políticas públicas podem ser uma oportunidade para resgatar e desenvolver mais conhecimento local. Enraizadas na cultura local, descentralizadas e com a lógica da produção digital aberta: essas são as características das políticas que vencem o colonialismo digital.

NOTAS

1 • Shoshanna Zuboff, "Dark Google." Frankfurter Allgemeine Zeitung, 30 de abril de 2014, acesso em 18 de janeiro de 2016, http://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshanna-zuboff-dark-google-12916679.html.

2 • Carole Cadwalladr e Emma Graham-Harrison, "Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach." The Guardian, 17 de março de 2018, acesso em 20 de junho de 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

3 • Michael Geist, "How the TPP Puts Canadian Privacy at Risk." Michael Geist website, 14 de outubro de 2015, acesso em 18 de janeiro de 2016, http://www.michaelgeist.ca/2015/10/how-the-tpp-puts-canadian-privacy-at-risk/; veja também Tyler Orton, "From IP to Privacy – Why TPP is 'Potentially Dangerous' for B.C. Tech Sector." Business Vancouver, 17 de novembro de 2015, acesso em 18 de janeiro de 2016, https://www.biv.com/article/2015/11/trade-deal-potentially-dangerous-bc-tech-sector.

4 • James Fontanella-Khan, "Brussels: Astroturfing Takes Root." Financial Times, 26 de junho de 2013, acesso em 20 de junho de 2018, https://www.ft.com/content/74271926-dd9f-11e2-a756-00144feab7de; Nancy Marshall-Genzer, "Why US Tech Lobbyists Have Descended on Brussels." Marketplace, 11 de agosto de 2014, acesso em 20 de junho de 2018, https://www.marketplace.org/2014/08/11/world/why-us-tech-lobbyists-have-descended-brussels.

5 • Tony Romm, "Tech Giants Get Deeper Into D.C. Influence Game." Politico, 1° de janeiro de 2015, acesso em 20 de junho de 2018, http://www.politico.com/story/2015/01/tech-lobby-apple-amazon-facebook-google-114468#ixzz3wV2vx4H0.

6 • Tim Cross, "Connecting the World: Four Firms Hope to Bring Internet Access to Everybody." The World in 2016, 6 de novembro de 2015, acesso em 18 de janeiro de 2016, http://www.theworldin.com/article/10646; as companhias são Google, Facebook, SpaceX e OneWeb.

7 • Anna Heim, "Uruguay's One Laptop Per Child Program: Impact and Numbers." TNW News, 17 de abril de 2013, acesso em 18 de janeiro de 2016, http://thenextweb.com/la/2013/04/07/uruguays-one-laptop-per-child-program-impact-and-numbers.

8 • Mohammed Lubowa, "Invasion Of Privacy: The Legal Implications of Mandatory SIM Card Registration on Mobile Users in Uganda." Master Thesis, 2013, acesso em 20 de junho de 2018, https://www.duo.uio.no/handle/10852/38120.

9 • "The Problem with Cell Phones," Electronic Frontier Foundation, 15 de fevereiro de 2015, acesso em 18 de janeiro de 2016, https://ssd.eff.org/en/module/problem-mobile-phones.

10 • Zuboff, "Dark Google." 2014.

11 • *Ibid.*

12 • Max Chafkin, "Why YCombinator Funded a Radical Political Party in Argentina." Fast Company, 12 de março de 2015, acesso em 18 de janeiro de 2015, http://www.fastcompany.com/3043388/the-y-combinator-chronicles/why-y-combinator-funded-a-radical-political-party-in-argentina.

13 • Associated Press, "US Secretly Created 'Cuban Twitter' to Stir Unrest and Undermine Government." The Guardian, 3 de abril de 2014, acesso em 20 de junho de 2018, http://www.theguardian.com/world/2014/apr/03/us-cuban-twitter-zunzuneo-stir-unrest.

14 • Cadwalladr e Graham-Harrison, "Revealed..." 2018.

15 • Para exemplos diferentes, veja o Online Censorship Project, Homepage, 2018, acesso em 20 de junho de 2018, https://onlinecensorship.org/.

16 • Nick Buckley e Hanna Kuchler, "Hackers Shut Down Power Grid in Ukraine." Financial Times, 5 de janeiro de 2016, acesso em 20 de junho de 2018,

http://www.ft.com/cms/s/0/0cfffe1e-b3cd-11e5-8358-9a82b43f6b2f.html.

17 • Claudio Guarnieri, John Scott-Railton, Morgan Marquis-Boire, e Marion Marschalek, "Packrat: Seven Years of a South American Threat Actor." Citizen Lab, 8 de dezembro de 2015, acesso em 20 de junho de 2018, https://citizenlab.org/2015/12/packrat-report/.

18 • Veja Yochai Benkler, "WikiLeaks and the PROTECT-IP Act: A New Public-Private Threat to the Internet Commons," *Dædalus* 140, no. 4 (2011): 154-64, acesso em 18 de janeiro de 2016, http://benkler.org/WikiLeaks_PROTECT-IP_Benkler.pdf.

19 • Parmy Olson, "Has Western Union Snubbed WikiLeaks?" Forbes, 10 de dezembro de 2010, acesso em 20 de junho de 2018, http://www.forbes.com/sites/parmyolson/2010/12/29/has-western-union-snubbed-wikileaks.

20 • Don Reisinger, "Credit Card Companies' WikiLeaks Block Just Fine, EU Says." CNET.com, 27 de novembro de 2012, acesso em 18 de janeiro de 2016, http://www.cnet.com/uk/news/credit-card-companies-wikileaks-block-just-fine-eu-says.

21 • Sam Jones, "Catalan Leaders Compare Spain to North Korea After Referendum Sites Blocked". The Guardian, 27 de setembro de 2017, acesso em 20 de junho de 2018, https://www.theguardian.com/world/2017/sep/27/catalans-compare-spain-to-north-korea-after-referendum-sites-blocked.

22 • Christopher Williams, "Google Charged with Monopoly Abuse." The Telegraph, 15 de abril de 2015, acesso em 20 de junho de 2018, http://www.telegraph.co.uk/finance/newsbysector/mediatechnologyandtelecoms/digital-media/11537546/Google-charged-with-monopoly-abuse.html.

23 • Bruce Upbin, "Debunking the Narrative of Silicon Valley's Innovation Might." Forbes, 13 de junho de 2013, acesso em 18 de janeiro de 2016, http://www.forbes.com/sites/bruceupbin/2013/06/13/debunking-the-narrative-of-silicon-valleys-innovation-might.

24 • "Your Windows XP Computer Isn't as Secure as it Used to Be," Microsoft, [n.d.], acesso em 18 de janeiro de 2016, http://www.microsoft.com/windows/en-us/xp/default.aspx.

25 • Eileen Yu, "Indian Government Mandates Use of Open Source Software." ZDNet, 31 de março de 2015, acesso em 18 de janeiro de 2016, http://www.zdnet.com/article/indian-government-mandates-use-of-open-source-software.

26 • Todd Benson, "Brazil: Free Software's Biggest and Best Friend." The New York Times, 29 de março de 2005, acesso em 20 de junho de 2018, http://www.nytimes.com/2005/03/29/technology/brazil-free-softwares-biggest-and-best-friend.html.

27 • Na Venezuela, um decreto foi aprovado em 2004 declarando *software* livre e padrões abertos o padrão para a administração pública. "Decreto 3390," Software Libre, 2004, acesso em 20 de junho de 2018, http://www.softwarelibre.gob.ve/images/stories/leyes/decreto3390softwarelibre.pdf.

28 • "Decreto 1014," Esteban Mendieta, 2008, acesso em 20 de junho de 2018, http://www.estebanmendieta.com/blog/wp-content/uploads/Decreto_1014_software_libre_Ecuador.pdf.

29 • "Ley 19179," Parlamento Del Uruguay, 2014, acesso em 20 de junho de 2018, www.parlamento.gub.uy/leyes/ley19179.htm.

30 • Plano de Implementação de Software Livre e Padrões Abertos: "Plan de Implementación de Software Libre y Estándares Abiertos 2015-2022," Comité Plurinacional de Tecnologías de la Información y Comunicación – COPLUTIC, agosto de 2015, acesso em 20 de junho de 2018, http://coplutic.gob.bo/IMG/pdf/propuesta_plan_de_implementacion_de_software_libre_y_estandares_abiertos.pdf.

31 • Adrian Offerman, "Russia to Replace Proprietary Software with Free Software." Joinup, 23 de junho de 2015, acesso em 20 de junho de 2018, https://joinup.ec.europa.eu/community/osor/news/russia-replace-proprietary-software-open-source.

32 • Kashmira Gander, "Gaza Doctor Tarek Loubani Creates 3D Printed Stethoscopes to Alleviate Medical Supply Shortages Caused by Blockade." The Independent, 10 de setembro de 2015, acesso

em 20 de junho de 2018, http://www.independent.co.uk/news/world/middle-east/gaza-doctor-tarek-loubani-creates-3d-printed-stethoscopes-to-alleviate-medical-supply-shortages-10495512.html.

33 • Glenn Greenwald, "How the NSA Tampers with US-made Internet Routers." The Guardian, 12 de maio de 2014, acesso em 20 de junho de 2018, http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden.

34 • Sunil Abraham, "The Fight for Digital Sovereignty," *Economic & Political Weekly* XLVIII, no. 42 (October 19, 2013), acesso em 18 de janeiro de 2016, http://cis-india.org/a2k/blogs/epw-vol-xlviii-42-october-19-2013-sunil-abraham-the-fight-for-digital-sovereignty.

35 • Tania Wolfgramm, "Re-Claiming our Technological Sovereignty." Planet Maori, 2015, acesso em 20 de junho de 2018, http://planetmaori.com/Files/Content/2015/Re-Claiming_our_Technological_Sovereignty_-_Paper_-_Tania_Wolfgramm_2014.pdf.

36 • Francesca Bria, *Public Policies for Digital Sovereignty* (New York: OR Books, 2015).

37 • Jonathan Watts, "NSA Accused of Spying on Brazilian Oil Company Petrobras." The Guardian, 9 de setembro de 2013, acesso em 18 de janeiro de 2016, http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras.

38 • AFP, "NSA Spied on French Economy Ministers, Top Companies: Reports." Yahoo! News, 30 de junho de 2015, acesso em 18 de janeiro de 2016, http://news.yahoo.com/nsa-spied-french-economy-ministers-top-companies-reports-061342870.html; veja também Spiegel Staff, "Embassy Espionage: The NSA's Secret Spy Hub in Berlin." Spiegel Online, 27 de outubro de 2015, acesso em 18 de janeiro de 2016, http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.

39 • "Plan de Implementación de Software Libre y Estándares Abiertos," Comité Plurinacional de Tecnologías de la Información y Comunicación – COPLUTIC, julho de 2016, acesso em 20 de junho de 2018, http://coplutic.gob.bo/rubrique3.html.

40 • "Free Software Designer in Bolivia," Prensa Latina, 1º de abril de 2013, acesso em 18 de janeiro de 2016, http://www.ssig.gov.my/blog/2013/04/01/free-software-designer-in-bolivia.

41 • Dan Schiller, "Geopolitics and Economic Power in Today's Digital Capitalism." Apresentação para o Hans Crescent Symposium, 13 de dezembro de 2015, acesso em 20 de junho de 2018, http://informationobservatory.info/2015/12/14/geopolitics-and-economic-power-in-todays-digital-capitalism.

RENATA ÁVILA PINTO – *Guatemala*

Renata Ávila, nascida na Guatemala, é advogada internacional e defensora de direitos digitais. Renata se especializou em propriedade intelectual e tecnologia e seu trabalho aborda a importante interseção entre direitos humanos, comércio digital, informação, mudanças tecnológicas e as disparidades de poder entre o Norte e o Sul Global. Como advogada na Guatemala, Ávila representou indígenas vítimas de genocídio e outras violações de direitos humanos, incluindo Rigoberta Menchu Tum, importante líder indígena e Prêmio Nobel da Paz.

Como parte de seu longo trabalho de advocacy no campo da internet e dos direitos humanos, Renata coordena juntamente com o inventor da *World Wide Web*, Sir Tim Berners-Lee, uma campanha global para defender os direitos humanos na era digital em mais de setenta e cinco países. Ela é membro do conselho da Creative Commons, integra o conselho gestor da *Courage Foundation* – uma organização criada para auxiliar delatores em risco – e é membro do conselho consultivo da Diem25, que explora o potencial das tecnologias descentralizadas na Europa. Atualmente, Renata reside em Belgrado e na Guatemala, está escrevendo um livro sobre o colonialismo digital e é conselheira da Web Foundation sobre suas novas estratégias de igualdade digital. Ela também representa a sociedade civil no Comitê sobre a Política de Economia Digital da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE).

contato: *renata.avila@webfoundation.org*

Recebido em maio de 2018.
Original em inglês. Traduzido por Fernando Sciré.