

ARTIGOS ACEITOS PARA PUBLICAÇÃO
DIREITO DIGITAL E SETOR PÚBLICO - 2020.2

ITS RIO

Pós-Graduação em Direito Digital

CEPED



ITS

REGULAÇÃO E PLANEJAMENTO ESTRATÉGICO DA TRANSFORMAÇÃO DIGITAL NO BRASIL: ONDE ESTAMOS, PARA ONDE VAMOS

Anderson Röhe Fontão Batista

REGULAÇÃO E PLANEJAMENTO ESTRATÉGICO DA TRANSFORMAÇÃO DIGITAL NO BRASIL: ONDE ESTAMOS, PARA ONDE VAMOS

Anderson Rôhe Fontão Batista

Pós-graduando em Direito Digital e Inovação no Setor Público pela UERJ e ITS Rio

Resumo

Hoje a transformação digital tem o potencial de aprimorar não só a economia e a vida em sociedade, como garantir soberania e melhor posição estratégica no sistema internacional. Ainda mais em contextos emergenciais de crise, em que não se questiona o se, e sim como será feita. Não por acaso, Inteligência Artificial (IA) e 5G estão no centro das disputas hegemônicas entre EUA e China. No Brasil, contudo, ainda não há uma estratégia nacional que planeje e coordene a implementação dessas tecnologias emergentes, o que faz com que o país esteja atrás não só das grandes potências, como de seu entorno regional. Os objetivos do trabalho são, então, verificar o atual estágio do Brasil, traçar seu perfil e apresentar recomendações. É, portanto, propositivo - no sentido de atentar para a melhora dos indicadores brasileiros em termos de planejamento, inovação, segurança, infraestrutura e capacidade digital – quanto proativo, a fim de garantir que direitos e salvaguardas mitiguem eventuais impactos negativos para a vida, saúde e segurança dos cidadãos, os mais vulneráveis nesse processo de adaptação. Logo, a ênfase da pesquisa está em compreender a problemática além de sua dimensão tecnológica, envolvendo também questões morais/éticas, políticas e sociológicas. Sobretudo em saber como harmonizá-las no caso concreto, já que as tecnologias emergentes não são neutras, inclusivas nem proporcionalmente benéficas e acessíveis a todos os envolvidos.

Palavras-chave: 5G; Brasil; Inteligência Artificial; tecnologias emergentes; transformação digital

Introdução

Entre tantas reconfigurações do sistema internacional (CEBRI, 2020) ainda persiste no imaginário coletivo a ideia de que quem detiver o manejo tecnológico “dominará” o mundo (HILLS, 2002). Hoje, essa mentalidade puramente tecnicista vem sendo questionada não só por um certo fetichismo quanto às novas tecnologias digitais de informação e comunicação (TICs), mas por abusos, distorções éticas e vieses políticos-ideológicos. Não por acaso, redes móveis de 5ª geração (5G) e Inteligência Artificial (IA) estão no centro das disputas geopolíticas entre EUA e China. Ainda mais em contextos emergenciais de crise, como o da pandemia do novo coronavírus, em que não se questiona o “se”, e sim “como” será feito esse processo de adaptação; e, sobretudo, qual será seu impacto para os cidadãos e segmentos mais vulneráveis. Desafio que, pela perspectiva de direitos e liberdades, envolve não apenas a dimensão material das TICs (MURDOCK apud DIGILABOUR, 2020), como também modelo de negócios hoje inerente às plataformas digitais e à indústria 4.0 (HAN, 2018).

O Brasil, por sua vez, não está totalmente preparado para essa transformação digital via inovação, integração em rede e mega processamento de dados, já que não existe um plano nacional que articule e coordene sua implementação e/ou atualize suas estratégias para o paradigma do século XXI, sobretudo em se tratando de soberania digital e segurança cibernética (ALMEIDA, 2018; CONVERGÊNCIA DIGITAL, 2019; MCTIC, 2020).

Toma-se como exemplo a desconexão das iniciativas do Brasil em proteção de dados, IoT (BELLI, 2019), mas principalmente em 5G e IA (INTERNETLAB; ITS RIO, 2020) em razão do atraso não só em relação às grandes potências como comparativamente às nações vizinhas (LE MOS; OXFORD INSIGHTS, 2020). Defasagem que pode levar a uma situação de retrocesso e assimetria tanto das relações de controle e poder, quanto de submissão e dependência tecnológica do Brasil frente ao monopólio das grandes plataformas chinesas e estadunidenses, em um processo de indesejada reedição do colonialismo (WENTZEL, 2019).

O objetivo do trabalho é, portanto, primeiro verificar o atual estágio da transformação digital no Brasil (subitem 1) e, assim, traçar seu perfil, segundo critérios técnicos e científicos relacionados ao planejamento, à inovação, defesa, segurança, infraestrutura e capacidade digital. Em seguida, apontar quais falhas e deficiências (subitem 2) podem trazer riscos, sobretudo socioeconômicos. Depois, o que pode ser feito para a potencialização desses indicadores, em termos de diretrizes e boas práticas (subitem 3) para aumento de produtividade e competitividade do modelo de negócios, bem como recomendações (subitem 4) para a melhora qualitativa e de eficácia das políticas públicas. O desenvolvimento do trabalho se divide, então, em quatro partes, tomando os modelos chinês, estadunidense e europeu como *benchmarking*.

Quanto à relevância da pesquisa, atentar para a necessidade de um plano nacional estratégico para escolher qual caminho ou modelo a seguir, como eleger áreas prioritárias onde haja potenciais benefícios. Planejamento em termos: a) proativos, na tentativa de se antecipar e estar melhor preparado para eventuais falhas sistêmicas e de mercado; b) responsivos, mediante reparação e/ou prestação de contas pelos danos eventualmente causados, já que a tecnologia não é neutra nem inclusiva e/ou proporcionalmente benéfica e acessível a todos os envolvidos.

A ênfase da pesquisa está, então, nas questões políticas e sociológicas que extrapolam a área técnica, mas que também influenciam as escolhas e o resultado dos processos decisórios. A metodologia utilizada é transdisciplinar e multidimensional, pela análise comparativa de indicadores quantitativos e qualitativos de fontes primárias e secundárias relacionadas às Ciências Comportamental, do Direito, da Sociologia, Comunicação e Computação.

Desenvolvimento

1. Atual estágio da transformação digital no Brasil

Hoje, acerca da definição de estratégias pelo Brasil, foram apontados cinco passos para sua transformação digital (GOVERNO DIGITAL, 2020). Para tanto, antes é preciso ter uma dimensão: a) dos serviços públicos ofertados; b) de seu ferramental (o que inclui petição e acompanhamento eletrônico, login único e autenticação, avaliação pelo usuário, interoperabilidade e análise de dados); c) da escala, no sentido de aceleração da digitalização e melhor forma de procedê-la; d) de planejamento (via monitoramento, diagnóstico do grau de digitalização, acompanhamento das metas e promoção de eventuais correções); assim como de e) mobilização e engajamento das plataformas e grandes empresas de tecnologia (Big Techs). Ou seja, tecnologia e inovação são indutores que darão agilidade e otimização a esse processo de transformação que visa oferecer serviços mais eficientes, baratos e de maior qualidade.

Só que nesse contexto de digitalização e datificação, a rede móvel de 5ª geração (5G) é vista como infraestrutura não só necessária, mas primeiro passo para a sua integração por IA e Big Data, mas principalmente via internet das coisas (IoT) e computação em nuvem (cloud computing). Assim, a nação que estiver desprovida e/ou desaparelhada dessa infraestrutura tecnológica terá menos condições de atração para investimentos em setores estratégicos para a economia e a vida em sociedade, como trabalho, finanças, educação, saúde pública, transportes, *e-commerce* e telecom (CONVERGÊNCIA DIGITAL, 2019; OXFORD INSIGHTS, 2020).

No entanto, a questão da transformação digital não é só tecnológica, mas também uma decisão política, sobretudo no Brasil, que está no centro das disputas entre China e EUA, particularmente por pressão estadunidense. O debate sobre leilão e definição de frequências do 5G ganha, portanto, conotação ideológica, já que agora uma política de alinhamento – sobretudo de lealdade ao Trumpismo, que saiu derrotado nas eleições – não traria contrapartidas objetivas para o Brasil. Ainda mais porque a liderança do 5G se dá por empresas privadas chinesas, sueca e finlandesa, ficando assim, em aberto, questões como defesa, segurança, interoperabilidade e cobrança de oferta pelo governo estadunidense (JORNAL DA USP; STUENKEL, 2020).

Esse imbróglio geopolítico também traz atrasos para o Brasil. A defasagem já é visível em Inteligência Artificial, uma vez que o Brasil ocupa apenas o 63º lugar em um ranking de 172 nações, segundo o *Government AI Readiness Index* (OXFORD INSIGHTS, 2020), atrás não só de grandes potências como EUA e China, mas de outras nações latino-americanas, como México, Colômbia, Chile, Argentina e Uruguai, especialmente em capacidade de IA (LEMOS,

2020). Não por acaso, estas duas estão à frente do Brasil por uma questão temporal, de maior amadurecimento institucional e adequação de sua legislação à transferência internacional de dados, sobretudo às diretrizes da União Europeia, referência em IA, portabilidade e proteção de dados (EUROPEAN COMMISSION; VIOLA, 2019; SILVA e EHRHARDT JÚNIOR, 2020).

Dentre os fatores promissores, há o subaproveitamento do potencial brasileiro. Afinal, há mais celulares do que brasileiros, fazendo do Brasil uma das nações mais conectadas do mundo (JORNAL DA USP, 2020). Hoje, o brasileiro passa nove horas diárias na *web*, e isso não é uma exclusividade dos mais ricos, já que 78% dos internautas são das classes C, D e (AGÊNCIA BRASIL, 2020). O Brasil também ocupa o primeiro lugar na América Latina em serviços online, o que revela o grau de adaptabilidade do brasileiro e o tamanho de seu setor tecnológico. Há, portanto, oportunidades no tempo presente, como capacidade futura, que fariam jus ao Brasil o título de 5ª maior infraestrutura mundial em telecomunicações, considerando o número de celulares e usuários da internet (OXFORD INSIGHTS, 2020).

Porém, na prática, ainda é preciso levar em conta uma considerável lacuna entre o campo e a cidade, em termos de uso e conectividade da internet. Assim como atenção para a capacitação e qualificação da mão de obra, e a crescente preocupação com ética e privacidade (OXFORD INSIGHTS, 2020). Não só porque aparelhos e plataformas digitais dão acesso a um grande volume de dados (matéria-prima indispensável para muitas das aplicações de IA), mas porque se planeja criar uma base de dados única, cujos cadastros dos brasileiros, contendo informações pessoais, sensíveis e sigilosas, seriam amplamente compartilhados entre agências e departamentos governamentais. Sem esclarecer, contudo, sob quais parâmetros os dados serão coletados, armazenados e finalmente tratados para tal (FRAZÃO, 2019).

O fator transparência é, portanto, um problema a ser enfrentado. Segundo o governo, cerca de 60% dos 3,8 mil serviços públicos federais já são acessíveis por meios digitais, em contraste ao um terço de outrora (GOVERNO DIGITAL, 2020). E a expectativa é de 100% até 2022, aproveitando o *boom* da digitalização pela pandemia (CONVERGÊNCIA DIGITAL, 2020). No entanto, além da questão de atingir metas ambiciosas no curto prazo, a digitalização estaria hoje comprometida pela escalada da desinformação, mormente de notícias imprecisas, desencontradas e exageradas que superestimam os gastos e as ações do governo, a ponto de não se saber ao certo se a Estratégia de Governo Digital 2020-2022 é realmente eficiente, integrada e inteligente; sobretudo confiável e centrada no cidadão (RIBEIRO e CUNHA; ZANATTA *et al*, 2020).

2. Quais deficiências sistêmicas e falhas de mercado

Hoje tem-se alertado para um crescente fetichismo tecnológico dos setores militar e de inteligência, sobretudo do Departamento de Estado estadunidense, ao securitizarem a agenda das telecomunicações, superestimando, assim, o alcance e até a eficácia das TICs (COMOR *In*: HOPE e THOMPSON, 2017). O mesmo pode ser dito da indústria de processamento de dados, que teria que inspirar maior confiança e segurança quanto à coleta e compartilhamento de dados pessoais, como nome, endereço e geolocalização, já que o fluxo global de dados constitui não só a base, mas o pressuposto para seu modelo de negócios. Contudo, não é essa a percepção de 42% de mil entrevistados nos EUA que se recusam a fornecê-los por qualquer motivo, e 51% que se sentem desconfortáveis em repartir informações pessoais. O que denota o alto nível de desconfiança e preocupação com privacidade e proteção de dados, mormente sobre o que está sendo coletado e como está sendo usado (PRIVITAR, 2020).

Há descompasso entre governo, mercado e cidadão porque ainda não há consenso em como haverá transformação digital: se pela lógica mais flexível e descentralizada do *nudging*, ou mais restritiva e punitiva (MOROZOV, 2020), mormente em tempos de crise. No entanto, digitalização e datificação não deveriam servir de “solucionismo tecnológico” para problemas existenciais (IRIS, 2020). Pois heurísticas e generalizações são uma contradição ao ideário de liberdade e neutralidade, como também um reducionismo à própria complexidade da rede. Principalmente após o 11 de setembro, por legitimar um estado permanente de vigilância e monitoramento dos meios de comunicação, sob o pretexto de combater o terrorismo e extremismo transnacional. Mas que igualmente serve para organizar e produzir conhecimento em larga escala, sobretudo de dissidentes e “inimigos” internos, por meio de sistemas de reconhecimento facial e de algoritmos de perfilamento e psicométrica comportamental, o que dá um salto exponencial às TICs. Salto que gera benefícios e oportunidades, mas também cria novos déficits, ameaças, assim como reforça vulnerabilidades e assimetrias históricas e estruturais (EUBANKS, 2018; BATISTA; TACTICAL TECH, 2019).

Essa concepção epistemológica da rede, que de modo indiscriminado, trata todos os usuários como suspeitos em potencial e invariavelmente os criminaliza, viola tanto a presunção de inocência, o contraditório e o devido processo legal, quanto compromete o próprio estado democrático de direito. Pois o tecnicismo, a longo prazo, acaba normalizando regimes de exceção que justificam uma escala autoritária (HARARI, 2018). O mesmo pode ser dito para a aceleração desse processo de transformação digital, já que a urgência e/ou pressa de não ficar

para trás, sem maior cuidado e planejamento, suprimem ou abreviam etapas cruciais para sua consolidação de forma ética, sustentável e responsável. Afinal, o capital humano também requer atenção (AGÊNCIA BRASIL; PEIXOTO e STEINBERG, 2020).

Por conseguinte, há autores, como Morozov (2015), que são mais céticos quanto à retórica estadunidense de “mundo e internet livre” que, hoje, soa deficitária quanto à moral e legitimidade de quem fala, inclusive de seus aliados. Sobretudo após o escândalo de espionagem da NSA e as revelações de Edward Snowden que, por sinal, impulsionaram a aprovação do Marco Civil da Internet no Brasil (IDEC). Assim, potências como Rússia e China, quando buscam soberania digital e menor dependência dessa arquitetura, seriam responsivas àqueles paradoxos e inconsistências discursivas. Pois, sem uma postura mais assertiva, ainda estariam encapsuladas por esse arranjo engendrado por seu rival geopolítico. Logo, é preciso desmistificar essa narrativa de concorrência desleal e “vigilância total” que só a elas é creditada (OXFORD, 2018; ARTIGO 19; DoS; SIMON, 2020).

As evidências estão nas prioridades dos modelos de governança e transformação digital. De um lado, o “Made in China 2025” é emblemático no sentido de revelar como os chineses pretendem superar a desvantagem de seu soft power (ZHANG, 2019) através do investimento maciço em ciência, tecnologia e inovação (CT&I). Do outro, uma escalada na política externa estadunidense que reforça essa retórica higienista de eliminação de todo “concorrente” que ameace sua hegemonia, liderança global e/ou contrapõe suas crenças, valores e visão particular de mundo (DoS, 2020). No entanto, o mundo não precisa necessariamente de uma rede “limpa”, e sim de uma rede “confiável” (KNAKE, 2020), em que haja livre fluxo informacional de dados e proteção da privacidade. Bem como de conjugação de esforços para um ambiente de maior sinergia, diálogo, comprometimento e fortalecimento de mecanismos multilaterais de adequação e cooperação internacional (VIOLA, 2019).

Já a China, ao menos no discurso, pretende melhorar o ambiente cibernético pela via da inclusão, e não da exclusão; seja atentando para questões éticas, legais e sociais relacionadas à IA, seja criando leis e melhores estruturas regulatórias; o que inclui uma coalizão multissetorial para garantir seu desenvolvimento sustentável e a criação de sistemas de explicabilidade e responsabilização para o uso de IA. Portanto, essa narrativa de coexistência se compatibiliza com o “sonho chinês” de abertura, cooperação e futuro compartilhado (CEBC, 2020). Sobretudo para acelerar a capacitação e atrair novos talentos do exterior (ITS Rio, 2020).

3. Diretrizes e Boas práticas

Na União Europeia (UE) já há iniciativas que prezam por esse ideal de governança compartilhada, seja pela implementação de um Plano Coordenado de Inteligência Artificial "Made in Europe"; pelo projeto piloto do Conselho Europeu de Inovação; pelo desenvolvimento de uma plataforma "AI-on-demand" que proporcionará acesso a todos usuários da comunidade; ou através do programa Marie Skłodowska-Curie Actions, que apoia e fornece subsídios a centros de pesquisa e pesquisadores (ITS Rio, 2020). A UE intenta, assim, criar sinergias e um ambiente colaborativo para reunir dados e maximizar investimentos, de modo a alcançar soberania digital e reduzir sua dependência exterior. Sobretudo no contexto em que 92% dos dados do Ocidente estão armazenados nos EUA (AMIOT *et all*, 2020).

O Regulamento Geral de Proteção de Dados (GDPR) europeu, que inspirou a Lei Geral de Proteção de Dados (LGPD) no Brasil, também é um passo importante para criar confiança, garantir clareza, transparência e segurança jurídica no uso da IA (ITS Rio, 2020). Sobretudo quando a IA passa a ser peça-chave na "guerra" por informação online (NAKAGAWA, 2020).

Para tanto, a Comissão Europeia reforça que o uso e desenvolvimento da IA deve ser centrado nas pessoas, por meio de participação e controle supervisionado dos sistemas inteligentes (COLLINGRIDGE, 1980); respeitando, assim, a diversidade e pluralidades de gênero, raça e orientação sexual, entre outras. Enfatiza também a garantia de rastreabilidade e explicabilidade, assegurando o direito à privacidade e autodeterminação informativa, pelo controle do indivíduo sobre seus dados (NAKAGAWA, 2020). Para tanto, em 2019, divulgou suas Diretrizes Éticas para Inteligência Artificial Confiável e o Relatório sobre Responsabilidade pela Inteligência Artificial e Outras Tecnologias Emergentes (EUROPEAN COMMISSION; ITS Rio, 2020).

Percebe-se, então, que as ênfases e os estágios das pesquisas são distintos, conforme as prioridades dadas às tecnologias emergentes. Assim, enquanto os EUA ainda não possuem um plano estratégico efetivo para coordenar suas atividades, a China traz o Plano Nacional de Pesquisa e Desenvolvimento com metas claras e detalhadas, inclusive com marcos temporais definidos, já que almeja a liderança mundial em IA até 2030 (ITS Rio, 2020). Assim, não é à toa que os chineses desenvolveram o "Internet +" e o Programa de Implementação e Atividades de Três Anos da IA para fomentar a pesquisa e o desenvolvimento em ciência, tecnologia e inovação.

Já no caso dos EUA os estudos em IA datam de 2016, a partir do governo Obama, quando foram entregues três relatórios. Contudo há uma outra abordagem no governo Trump, mais aut centrada, preferindo focar em segurança, geração de empregos e remoção de barreiras regulatórias, visto que orientada para o livre mercado de IA. Para tanto, foi lançado o site AI.gov para facilitar o acesso e a compreensão das várias iniciativas governamentais (ITS Rio, 2020).

E como o Brasil se insere nessa dinâmica? Uma ala mais ideológica do governo federal vem seguindo uma política de alinhamento aos EUA, sobretudo nas agendas de cultura, educação, meio ambiente e direitos humanos. Mas sem se preocupar com contrapartidas objetivas para o Brasil, como transferência de tecnologia e investimentos nos setores mais deficitários, como CT&I, infraestrutura, energia e telecom. Vazio que tem sido ocupado pela China, seu maior parceiro comercial e investidor (CEBC, 2020; SHI-KUPFER, 2019). Há, portanto, muita politização e ideologização em toda a tomada de decisão. Subjetividade que, em última instância, tumultua, retarda ou traz entraves para o processo de transformação digital brasileiro (DENARDIS, 2009; VADELL, RAMOS e NEVES, 2016).

Brasil e EUA também se alinham quando se mede o fator liberdade. Mas em razão do retrocesso e piora das métricas que o avaliam, relacionadas ao declínio do espaço cívico e digital para se expressar e engajar-se em debates públicos. Também há deterioração da liberdade de imprensa; proteção e segurança de defensores de direitos humanos; e transparência e acesso à informação, a fim de auditar, fiscalizar e prestação de contas públicas. Segundo o ARTIGO 19 (2020), uma organização internacional de direitos humanos que mede a liberdade de expressão e informação no mundo, o Brasil é o que mais se destaca negativamente pela piora em todas as comparações realizadas. Com 46 pontos em um total de 100, o Brasil ocupa a 94ª posição em um ranking de 161 nações, ficando atrás de todos os representantes da América do Sul, exceto apenas da Venezuela. Declínio este que foi acentuado e acelerado com a chegada do atual governo, com queda de 28% em apenas um ano. E que é atribuído não só à desigualdade, violência, corrupção e crise de confiança nas autoridades e de credibilidade dos meios de comunicação, mas também ao aumento da censura e vigilância no Brasil.

4. Recomendações

Em uma abordagem estreita, conceitos de jurisdição e governança da internet antes se referiam à gestão centralizada de protocolos, nomes de domínio e números IP por uma única entidade como a ICANN - *Internet Corporation for Assigned Names and Numbers* (KURBALIJA, 2014; BELLI e CAVALLI, 2018). Já em uma abordagem mais ampla e atual,

a governança na internet vai além da mera gestão de nomes e domínios, englobando diferentes *stakeholders*; desde agentes do governo ao setor privado e à representantes da sociedade civil que, de forma colaborativa, multissetorial e em regime de correção, trabalham juntos para desenvolver princípios e normas, bem como estabelecer limites morais, éticos e padrões procedimentais para o ambiente digital. Afinal, os protocolos não são neutros, mas também políticos (DENARDIS, 2009), não se distinguindo bem o interesse público do privado. Então, é preciso compartilhar responsabilidades, seja no âmbito civil, penal e administrativo, quando houver incidentes de segurança (OECD, 2020). Responsabilidade que, na era informacional, assume um caráter proativo, ora objetiva, ora subjetiva, conforme o papel que cada um desempenha dentro do ecossistema das TICs (DE MORAES e DE QUEIROZ, 2019).

Por isso, o campo da regulação necessita de uma melhor adequação à era digital, funcionando como uma espécie de balizador (BINENBOJM, 2019) a fim de não inviabilizar nem a livre iniciativa e o modelo de negócios das Big Techs (assim como o progresso, avanço tecnológico e a própria capacidade de inovação e desenvolvimento do país), nem as salvaguardas de direitos, garantias e liberdades civis. Um desafio, portanto, do ponto de vista informacional das TICs como das relações de controle e poder (BAPTISTA e KELLER, 2016).

Ainda mais no Brasil, onde o campo da regulação ainda é disfuncional, já que, visto em retrospecto, tende a ser mais punitivo do que propositivo (CONVERGÊNCIA DIGITAL, 2019); isto é, espera a lesão ou o dano acontecer para só então tomar uma providência, ou, quando atua preventivamente, vem a abusar desse poder, afastando-se de seu propósito original. Sobretudo pela opacidade e falta de acurácia dos sistemas de IA, que ainda precisam de ajustes.

Por tais razões, o modelo europeu de transformação digital deveria ser o caminho a ser seguido pelo Brasil. Não só por manter uma equidistância pragmática das grandes potências, mas por força das salvaguardas e da matriz principiológica da LGPD que são assemelhadas ao GDPR. Dessa forma, a decisão do Brasil seria mais técnica do que política e, assim, mais centrada no elemento humano. E, a exemplo da Argentina e Uruguai, nem mesmo a falta de independência formal da Autoridade Nacional de Proteção de Dados seria um obstáculo se o Brasil acordasse com a UE e assumisse o compromisso de vir a atingir um nível mais adequado e compatível de proteção, firmando, p.ex., um sistema de certificação e reconhecimento de adequação recíproca. Sobretudo quando postula seu ingresso na OECD (VIOLA, 2019).

Conclusão

A transformação digital exige uma nova abordagem quanto à regulação tecnológica, a fim de conferir maior transparência, eficiência, produtividade e competitividade a diferentes segmentos da economia, mas também garantias mais amplas à área social. Daí a urgência em articular e coordenar políticas públicas no campo tanto de defesa e soberania digital, quanto de proteção de dados e segurança cibernética, seja nas fases de elaboração como de implementação e acompanhamento de um plano nacional estratégico.

Hoje há quase uníssono de que o uso e o desenvolvimento das tecnologias emergentes têm que ser centrados no elemento humano. Ainda mais em contextos emergenciais de crise, como a do novo coronavírus, em que aceleração da digitalização vem como “solucionismo tecnológico”, nem que isso signifique relativização de direitos e liberdades civis. Por isso é fundamental ditar o ritmo de como se dará esse processo da transformação, precisando o como, para que, até quando, e a cargo de quem devem ser reguladas as novas tecnologias digitais. Um desafio, portanto, quanto ao tempo, modo e sua finalidade regulatória, já que, se por um lado, uma regulação tecnológica precoce pode vir a inviabilizar o progresso e o fator inovação, por outro, permitir experimentações automatizadas com base na “tentativa e erro” pode levar a danos irreparáveis e retrocessos de garantias processuais já consolidadas.

No caso do Brasil há o agravante de haver a difusão de discursos análogos à Guerra Fria que, por sua vez, acarretam polarização e politização dos processos decisórios. Conjectura que o prejudica, sobretudo em um contexto global caracterizado pela interdependência econômica e hiper conectividade informacional/computacional. Bem como potencializa os riscos de se investir no país, reduz seu poder de manobra/barganha e atenta contra a imagem e o interesse nacional. Portanto, antes de replicar um modelo desenvolvimentista/civilizatório, seja europeu, chinês ou estadunidense, e na falta de uma inserção internacional autônoma, o Brasil deve ponderar os riscos e avaliar os impactos à luz do custo-benefício da adoção de um sistema em detrimento do outro. Um jogo soma zero é perigoso e traz revezes, ainda que intangíveis e imperceptíveis à primeira vista, já que passam a impactar negativamente tanto a credibilidade e legitimidade das autoridades e instituições, quanto a própria efetividade das políticas públicas. Processo acumulativo que, com o tempo, mina a própria capacidade de governar.

Então, é preciso quebrar esse ciclo vicioso. De que maneira? Primeiro, não adiando o leilão do 5G, o que exigirá pragmatismo do Brasil, através da análise objetiva das vantagens comparativas e valorização de políticas de Estado, e não de governos. Isso virá pela combinação

de parcerias e esforços multissetoriais que tenham continuidade a longo prazo, e não sejam abandonados a cada nova gestão.

Segundo, reconhecendo a necessidade premente de planejar e se precaver, antecipando-se ao dano, seja atualizando o marco regulatório das telecoms, seja acelerando a transformação digital no Brasil. Então, é preciso ser proativo e desenvolver o quanto antes um projeto nacional que seja integrado, mais bem estruturado e elaborado com métricas claras e pré-definidas; seja por meio auditoria, boas práticas e código de conduta, seja investindo em políticas regulatórias sustentáveis, centradas no elemento humano e ambiental, e não apenas em criminalizar o comportamento dos usuários e/ou punir por eventuais falhas de mercado e deficiências técnicas das plataformas digitais. Dessa forma, haverá mais respeito ao estado democrático de direito, à justiça, autonomia e dignidade humana, e aos princípios e garantias processuais.

Então, embora haja iniciativas em andamento, conclui-se que o Brasil ainda não está preparado. Há um longo caminho até atingir um nível aplicável, adequado e interoperável de proteção. Hoje seu perfil é autocentrado, e mais reativo do que preventivo; postura que o vulnerabiliza e pouco leva em conta as extraterritorialidades com o intenso fluxo informacional, volume de dados, transmissão e alocação em nuvem. Uma nova realidade que lhe traz custos, salvaguardas adicionais e demanda visão holística acerca de cibersegurança e soberania digital. Sobretudo ao voltar seus olhos para o passado, quando deveria direcioná-los para o futuro.

Referências Bibliográficas

AGÊNCIA BRASIL. **Brasil discute estratégia para inteligência artificial**. Época Negócios. Disponível em: <<https://epocanegocios.globo.com/Tecnologia/noticia/2020/09/brasil-discute-estrategia-para-inteligencia-artificial.html>>. Acesso em: 22 out. 2020.

ALMEIDA, V. **Brasil precisa de estratégia para inteligência artificial**. Disponível em: <www.abc.org.br/2018/08/08/brasil-precisa-de-estrategia-para-inteligencia-artificial>. Acesso em: 30 set. 2020.

AMIOT, E. *et al.* **European Digital Sovereignty**. In: Oliver Wyman. Publicado em: <<https://www.oliverwyman.com/our-expertise/insights/2020/sep/european-digital-sovereignty.html>>. Acesso em: 30 nov. 2020.

ARTIGO 19. **Relatório Global de Expressão 2019/2020**: o estágio da liberdade de expressão ao redor do mundo. Sumário Executivo em português. Disponível em: <http://artigo19.org/wp-content/blogs.dir/24/files/2020/10/SumarioExecutivoGxR_PT.pdf>. Acesso em: 20 out. 2020.

BAPTISTA, P.; KELLER, C. I. Por que, quando e como regular as novas tecnologias? **Os desafios trazidos pelas inovações disruptivas**. In: Revista de Direito Administrativo, Rio de Janeiro, set./dez. 2016, v. 273, p. 123-163.

BATISTA, A. R. F. **O sistema chinês de vigilância pública e reconhecimento facial: solução ou ameaça para o mundo?** Dissertação de Mestrado – IRI, PUC Rio, Rio de Janeiro, 2019. Disponível em: <<https://www.maxwell.vrac.puc-rio.br/46806/46806.PDF>>. Acesso em: 10 nov. 2020.

BELLI, L. **5G e IoT: BRICS precisam de cooperação em cibersegurança** (2019). Disponível em: <<https://cyberbrics.info/5g-e-iot-brics-precisam-de-cooperacao-em-ciberseguranca/>>. Acesso em: 2 nov. 2020.

_____. CAVALLI, O. (org.). **Gobernanza y regulaciones de Internet en América Latina**. Disponível em: <<http://governanzainternet.org/libro>>. Acesso em: 22 nov. 2019.

BINENBOJM, G. **Inovações disruptivas e a dinâmica das mudanças regulatórias** (2019). Disponível em: <<https://www.jota.info/opiniao-e-analise/artigos/inovacoes-disruptivas-e-a-dinamica-das-mudancas-regulatorias-10042019>>. Acesso em: 2 set. 2020.

CEBRI. **Artificial intelligence, technological warfare and changes in the world order: China, USA and Brazil**. XIX Reunião do Grupo de Análise sobre China. Disponível em: <<https://www.cebri.org/portal/publicacoes/cebri-artigos/xix-reuniao-do-grupo-de-analise-sobre-china:-artificial-intelligence,-technological-warfare-and-changes-in-the-world-order:-china,-usa-and-brazil>>. Acesso em: 3 nov. 2020.

COLLINGRIDGE, D. **The social control of technology**. London: Frances Pinter, 1980.

COMOR, E. Technological Fetishism and US Foreign Policy: the mediating role of digital ICTs. *In*: HOPE, Wayne; THOMPSON, Peter. **The Political Economy of Communication**. V. 5, N. 2, 2017, p. 3 - 21. Disponível em: <<http://www.polecom.org/index.php/polecom/issue/view/13>>. Acesso em: 20 out. 2020.

CONSELHO EMPRESARIAL BRASIL CHINA – CEBC. **Bases para uma Estratégia de Longo Prazo do Brasil para a China**. Disponível em: <<http://cebc.org.br/download/5614/>>. Acesso em: 26 nov. 2020.

_____. **Who is winning the AI race: China, the EU or the United States?** Disponível em: <cebc.org.br/2019/09/26/who-is-winning-the-ai-race-china-the-eu-or-the-united-states/>. Acesso em: 26 nov. 2020.

CONVERGÊNCIA DIGITAL. **63º Painel Telebrasil 2019**. *In*: Revista Transformação Digital, ed. 63, 2019. Disponível em: <<https://issuu.com/convergenciadigital/docs/63paineltelebrasil2019>>. Acesso em: 9 out. 2020.

_____. **Governo chega à marca de 1 mil serviços públicos digitalizados**. Disponível em: <<https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infolid=55179&sid=16&utm%25252525255Fmedium=>>. Acesso em: 24 nov. 2020.

DE MORAES, M. C. B.; DE QUEIROZ, J. Q. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGDP. *In*: **Proteção de dados pessoais: privacidade versus avanço tecnológico**. Cadernos Adenauer xx (2019), nº 3. Fundação Konrad Adenauer, Rio de Janeiro, out. 2019.

DENARDIS, L. **Protocol Politics**. The globalization of internet governance. MIT Press, 2009.

DIGILABOUR. **Materialidades da comunicação e crítica da economia política**: entrevista com Graham Murdock. Disponível em: <<https://digilabour.com.br/2020/09/20/materialidades->

da-comunicacao-e-critica-da-economia-politica-entrevista-com-graham-murdock>. Acesso em: 21 set. 2020.

EUBANKS, V. **Automating Inequality**. How high-tech tools profile, police, and punish the poor. St. Martin's Press. New York, 2018.

EUROPEAN COMMISSION. **Ethics Guidelines for Trustworthy AI**. Disponível em: <<https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai>>. Acesso em: 23 out. 2020.

_____. **Liability for Artificial Intelligence: and other emerging digital technologies** (2019). Disponível em:

<<https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608>>. Acesso em: 23 out. 2020.

FRAZÃO, A. **Quais devem ser os parâmetros éticos e jurídicos para a utilização da IA?** Disponível em: <https://www.jota.info/paywall?redirect_to=//www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/quais-devem-ser-os-parametros-eticos-e-juridicos-para-a-utilizacao-da-ia-24042019>. Acesso em: 22 out. 2020.

GOVERNO DIGITAL. **Estratégia de Governo Digital 2020-2022 já tem 86% de suas iniciativas em execução ou concluídas**. Disponível em: <<https://www.gov.br/governodigital/pt-br/noticias/estrategia-de-governo-digital-2020-2022-ja-tem-86-de-suas-iniciativas-em-execucao-ou-concluidas>>. Acesso em: 6 nov. 2020.

_____. **Transformação Digital. 5 passos para a transformação digital**. Disponível em: <<https://www.gov.br/governodigital/pt-br/transformacao-digital/5-passos-para-a-transformacao-digital>>. Acesso em: 6 nov. 2020.

INTERNETLAB. **As contribuições do InternetLab para a Estratégia Nacional de Inteligência Artificial**. Disponível em: <<https://www.internetlab.org.br/pt/privacidade-e-vigilancia/as-contribuicoes-do-internetlab-para-a-estrategia-nacional-de-inteligencia-artificial>>. Acesso em: 16 out. 2020.

INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE – IRIS. **Digitalização do serviço público: uma solução para quais problemas?** Disponível em: <<https://irisbh.com.br/digitalizacao-do-servico-publico/>>. Acesso em: 4 nov. 2020.

INSTITUTO DE TECNOLOGIA E SOCIEDADE - ITS RIO. **Estratégias Nacionais sobre Inteligência Artificial: a experiência internacional**. Disponível em: <<https://itsrio.org/pt/publicacoes/estrategias-nacionais-sobre-inteligencia-artificial>>. Acesso em: 15 out. 2020.

HAN, B. C. **Psicopolítica**. O neoliberalismo e as novas técnicas de poder. Editora Àyné, 1ª edição, set. 2018.

HARARI, Y. N. **Why Technology Favors Tyranny**. The Atlantic. Disponível em: <<https://www.theatlantic.com/magazine/archive/2018/10/youval-noah-harari-technology-tyranny/568330>>. Acesso em: 13 jul. 2020.

HILLS, J. **The Struggle for Control of Global Communication: The Formative Century**. Urbana and Chicago: University of Illinois Press, 2002.

IDEC. **Linha do tempo dos dados pessoais no Brasil**. Disponível em: <<https://idec.org.br/dadospessoais/linha-do-tempo>>. Acesso em: 4 nov. 2020.

JORNAL DA USP. Podcast Live Ciência USP #02 – **Rede 5G: Tecnologia e Geopolítica**. Disponível em: <<https://jornal.usp.br/podcast/live-ciencia-usp-02-rede-5g-tecnologia-e-geopolitica/>>. Acesso em: 27 nov. 2020.

KNAKE, R. K. **What’s wrong with the Clean Network Initiative? China can’t join it**. Council on Foreign Relations. Disponível em: <<https://www.cfr.org/blog/whats-wrong-clean-network-initiative-china-cant-join-it>>. Acesso em: 18 out. 2020.

KURBALIJA, J. **Uma introdução à governança da internet**. In: CGI.br. Disponível em: <https://cgi.br/media/docs/publicacoes/1/CadernoCGIbr_Uma_Introducao_a_Governanca_da_Internet.pdf>. Acesso em: 17 out. 2020.

LEMOS, R. **Brasil derrapa em Inteligência Artificial**. In: ITS Rio. Disponível em: <<https://itsrio.org/pt/artigos/brasil-derrapa-em-inteligencia-artificial>>. Acesso em: 11 out. 2020.

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA, INOVAÇÕES E COMUNICAÇÕES - MCTIC. **Consulta Pública - Estratégia Brasileira de Inteligência Artificial**. Disponível em: <<https://issuu.com/mctic/docs/estrategia-inteligencia-artificial>>. Acesso em: 15 out. 2020.

MOROZOV, E. **The tech ‘solutions’ for coronavirus take the surveillance state to the next level**. Disponível em: <<https://www.theguardian.com/commentisfree/2020/apr/15/tech-coronavirus-surveillance-state-digital-disrupt>>. Acesso em: 3 nov. 2020.

_____. **Who’s the true enemy of internet freedom - China, Russia, or the US?** Disponível em: <<https://www.theguardian.com/commentisfree/2015/jan/04/internet-freedom-china-russia-us-google-microsoft-digital-sovereignty>>. Acesso em: 9 set. 2020.

NAKAGAWA, L. **Inteligência artificial: quais os riscos que a tecnologia pode gerar?** In: Olhar Digital. Disponível em: <<https://olhardigital.com.br/noticia/inteligencia-artificial-quais-os-riscos-que-a-tecnologia-pode-gerar/106725>>. Acesso em: 11 out. 2020.

OXFORD INSIGHTS. **Government AI Readiness Index 2020**. Disponível em: <<https://www.oxfordinsights.com/government-ai-readiness-index-2020>>. Acesso em: 4 out. 2020.

PEIXOTO, T.; STEINBERG, T. **Citizen Engagement**. Emerging digital technologies create new risks and value. Disponível em: <<https://openknowledge.worldbank.org/bitstream/handle/10986/32495/Citizen-Engagement-Emerging-Digital-Technologies-Create-New-Risks-and-Value.pdf>>. Acesso em: 30 nov. 2020

PRIVITAR. **New Privitar survey reveals business opportunity to build consumer loyalty through data privacy**. Disponível em: <<https://www.privitar.com/press-releases/new-privitar-survey-reveals-business-opportunity-to-build-consumer-loyalty-through-data-privacy/>>. Acesso em: 25 nov. 2020.

RIBEIRO, A.; CUNHA, A. R. **Bolsonaro deu 653 declarações falsas ou distorcidas sobre Covid-19 em seis meses de pandemia**. In: Aos Fatos. Disponível em: <<https://www.aosfatos.org/noticias/bolsonaro-deu-656-declaracoes-falsas-ou-distorcidas-sobre-covid-19-em-seis-meses-de-pandemia/>>. Acesso em: 12 set. 2020.

SHI-KUPFER, K. **China: a devoção à tecnologia e a crença no progresso preenchem o vácuo ideal deixado pela revolução cultural de Mao**. Tradução do Autor. Disponível em: <<https://www.nzz.ch/meinung/das-moralische-vakuum-fuellen-chinas-technologieglaeubigkeit-ld.1485165?reduced=true>>. Acesso em: 4 nov. 2020.

SILVA, G. B. P.; EHRHARDT JÚNIOR, M. Diretrizes éticas para a Inteligência Artificial confiável na União Europeia e a regulação jurídica no Brasil. *Revista IBERC*, v. 3, n. 3, p. 1-28, 4 nov. 2020.

SIMON, R. **Mito da nova Guerra Fria é nocivo ao Brasil**. Disponível em: <<https://www1.folha.uol.com.br/colunas/roberto-simon/2020/08/mito-da-nova-guerra-fria-e-nocivo-ao-brasil.shtml>>. Acesso em: 20 ago. 2020.

STUENKEL, O. **Huawei or not? Brazil faces a key geopolitical choice**. Disponível em: <<https://americasquarterly.org/article/huawei-or-not-brazil-faces-a-key-geopolitical-choice/>>. Acesso em: 27 nov. 2020.

TACTICAL TECH. **Personal Data: Political Persuasion**. Inside the Influence Industry. How it works. Disponível em: <https://cdn.ttc.io/s/ourdataourselves.tacticaltech.org/Personal-Data-Political-Persuasion-How-it-works_print-friendly.pdf>. Acesso em: 23 out. 2020.

THE ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT - OECD. **Recommendation of the Council on Artificial Intelligence**, OECD LEGAL 0449. Disponível em: <<https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449>>. Acesso em: 28 out. 2020.

US DEPARTMENT OF STATE - DoS. **Announcing the Expansion of the Clean Network to Safeguard America's Assets**. Disponível em: <<https://www.state.gov/announcing-the-expansion-of-the-clean-network-to-safeguard-americas-assets>>. Acesso em: 18 out. 2020
_____. **United States Releases National Strategy for Critical and Emerging Technologies**. Disponível em: <<https://www.state.gov/united-states-releases-national-strategy-for-critical-and-emerging-technologies>>. Acesso em: 16 out. 2020.
_____. **The Clean Network**. Disponível em: <<https://www.state.gov/the-clean-network>>. Acesso em: 18 out. 2020.

VADELL, J.; RAMOS, L.; NEVES, P. **As implicações internacionais do modelo chinês de desenvolvimento do Sul Global: Consenso Asiático como network power**. In: LIMA, Marcos Costa (org.). *Perspectivas asiáticas*. Centro Internacional Celso Furtado de Políticas para o Desenvolvimento: Folio Digital, Rio de Janeiro, 2016, p. 67-90.

VIOLA, M. **Transferência de dados entre Europa e Brasil: análise da adequação da legislação brasileira**. ITS Rio. Disponível em: <<https://somos.itsrio.org/transferencia-dados-europa-brasil>>. Acesso em: 4 nov. 2020.

WENTZEL, M. **Como a corrida mundial pelo processamento de dados pode 'colonizar' o Brasil e outros países?** BBC News Brasil. Disponível em: <<https://www.bbc.com/portuguese/internacional-49981458>>. Acesso em: 13 out. 2019.

ZANATTA, R. A. F. *et al.* **Relatório Privacidade e Pandemia: recomendações para o uso legítimo de dados no combate à Covid-19**. In: *Data Privacy Brasil*. Disponível em: <https://www.dataprivacybr.org/wp-content/uploads/2020/04/relatorio_privacidade_e_pandemia_final.pdf>. Acesso em: 4 nov. 2020.

ZHANG, J. **A China está buscando um plano para compensar a fraqueza do soft power com a força da tecnologia - os EUA estão se opondo a isso**. Tradução do Autor. Disponível em: <<https://www.nzz.ch/meinung/china-verfolgt-den-plan-die-schwaecher-der-soft-power-durch-die-staerke-der-technologie-zu-kompensieren-die-usa-stellen-sich-dem-entschieden-entgegen-ld.1485393?reduced=true>>. Acesso em: 4 nov. 2020.