Versão não definitiva de Luca Belli. (2024). Soberania em Inteligência Artificial: O que é e o quais facilitadores essenciais podem tornar o Brasil um país soberano em IA? in Ricardo Villas Bôas Cueva, Laura Schertel Mendes; Bruno Ricardo Bioni; Fabricio da Mota Alves. Inteligência Artificial e Regulação. Gen-Jurídico.

Soberania em Inteligência Artificial:

O que é e o quais facilitadores essenciais podem tornar o Brasil um país soberano em IA?

Luca Belli, Professor e Coordenador, Centro de Tecnologia e Sociedade da FGV Direito Rio.

Resumo

Um número crescente de países está desenvolvendo estratégias nacionais e propostas regulamentares destinadas a enquadrar a utilização da inteligência artificial (IA), principalmente através de uma abordagem baseada no risco. O principal objetivo do presente capítulo é sublinhar que a regulamentação dos riscos da IA é apenas um dos elementos essenciais que devem ser considerados para alcançar a uma situação de "soberania em IA". É importante ressaltar que este capítulo define a soberania da IA como a capacidade de compreender, desenvolver e regular sistemas de IA mantendo a capacidade de controle e agência e, em última análise, o direito fundamental à autodeterminação. Nesta perspectiva, este capítulo propõe um framework estratificado em camadas, denominado "Pilha de Soberania da IA", para analisar quais elementos são essenciais e qual tipo de pensamento estratégico é necessário para alcançar a soberania em IA. Estes elementos são definidos como "Facilitadores Essências de Soberania em IA" ou "FESIA" e devem ser considerados como interligados e interdependentes, opor meio de uma abordagem estratégica integrada. O capítulo aplica o framework baseado nos FESIA para analisar a maturidade do Brasil, investigando se as escolhas estratégicas e legislativas do País, bem como seus sistemas de governança, podem permitir-lhe de se afirmar como soberano em IA ou se, pelo contrário, conduzem a uma situação de dependência no que diz respeito em IA. A conclusão do capítulo salienta que a falta de soberania em IA é uma situação difundida na enorme maioria dos países e é particularmente evidente no Sul Global. Por último, defende que os governos nacionais devem esforçar-se por reverter a situação atual de dependência em IA e construir sua própria soberania em IA, porém procurando evitar impulsos protecionistas e continuando promover a cooperação. Tal esforço pode mitigar o atual cenário de colonialismo digital.[1]

Introdução

Enquanto tecnologia transformacional[2], a inteligência artificial (IA) é destinada a ter – e, de certa forma, já está produzindo – um impacto global e ramificações consideráveis nas economias, democracias e sociedades nacionais. Embora muitos países

[1] Este artigo baseia-se num estudo apresentado na Digital Democracy Network Conference 2023, organizada pelo Carnegie Endowment for International Peace, e publicado na coleção da conferência. Ver Belli, L. To Get Its AI Foothold, Brazil Needs to Apply the Key AI Sovereignty Enablers (KASE), em Feldstein S. (Ed.) (2023). Retorno aos Novos Dilemas Digitais: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms. Carnegie Endowment for International Peace. O autor gostaria de agradecer a Steven Feldstein, à equipe da Carnegie e aos participantes da Digital Democracy Network Conference 2023 pelos valiosos comentários à versão original deste capítulo apresentada na Conferência.

[2] Jarvenpaa, S. L., & Ives, B. (1996). Introducing transformational information technologies: the case of the World Wide Web technology. *International Journal of Electronic Commerce*, *1*(1), 95-126. https://www.jstor.org/stable/27750802

estejam desenvolvendo marcos de regulação de IA[3], o principal objetivo do presente documento é salientar que a regulação de IA é apenas um dos elementos essenciais que devem ser considerados para alcançar a soberania em IA.

A soberania em IA é um conceito novo, apresentado pelo autor, e ainda não é universalmente definido. O presente capítulo apresenta uma definição deste conceito, com base em pesquisas anteriores sobre soberania digital efetuadas pelo autor. Neste sentido, a Soberania em IA deve ser considerada como a **capacidade de um determinado país para compreender, desenvolver e regular os sistemas de IA**, e pode ser enxergada como uma espécie do mais amplo genus da soberania digital.[4]

Reconhecendo embora que o conceito de soberania digital ou cibernética pode ter e já foi utilizado com algumas conotações controversas, que flertam com o controle autoritário por meio de tecnologias digitais ou até o mero protecionismo, defendo que a Soberania da IA deve ser encarada na sua concepção positiva de facilitador essencial da agência, do controle individual e democrático, e de autodeterminação[5] sobre os sistemas de IA. Particularmente, esta concepção positiva baseia-se na abordagem voltada a

[3] Belli, L., Curzi, Y., & Gaspar, W. B. (2023). AI regulation in Brazil: Advancements, flows, and need to learn from the data protection experience. *Computer Law & Security Review*, *48*, 105767. https://www.sciencedirect.com/science/article/pii/S0267364922001108

[4] Para uma análise das diferentes dimensões da soberania digital, veja-se Belli L. et al. (2023). Cibersegurança: uma visão sistêmica rumo a uma proposta de Marco Regulatório para um Brasil digitalmente soberano. FGV Direito Rio; Belli, L. and Jiang, M. (Orgs.). (2024). Digital Sovereignty from the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance. Cambridge University Press.

[5] Em direito internacional, o direito à autodeterminação é designado como princípio primário ou princípio dos princípios, uma vez que desempenha um papel instrumental para permitir que os indivíduos usufruam dos seus direitos humanos, sendo assim um facilitador de outros direitos fundamentais. Por esta razão, está consagrado como primeiro artigo da Carta das Nações Unidas e do Pacto Internacional dos Direitos Humanos. De acordo com estes três instrumentos de direito internacional, os Estados acordaram que "todos os povos têm direito à autodeterminação" e que "em virtude desse direito, são livres de determinar o seu estatuto político e de prosseguir o seu desenvolvimento económico, social e cultural". É essencial sublinhar a relevância da dimensão interna da autodeterminação, ou seja, o direito dos povos a determinarem e prosseguirem livremente o seu desenvolvimento económico, social e cultural, incluindo através da escolha, desenvolvimento e adoção independentes de tecnologias digitais. Esta conceção é também corroborada pelo reconhecimento do direito fundamental à "autodeterminação informativa" como expressão do direito humano a ter e desenvolver uma personalidade, reconhecido pela primeira vez pelo Supremo Tribunal alemão, no processo Census de 1983. O direito fundamental ao livre desenvolvimento da personalidade é formalmente reconhecido a nível internacional. O artigo 22.º da Declaração Universal dos Direitos do Homem afirma que "toda a pessoa tem direito à efetivação dos direitos necessários à sua dignidade e ao livre desenvolvimento da sua personalidade", enquanto o Pacto Internacional sobre os Direitos Económicos, Sociais e Culturais consagra este princípio fundamental no que se refere ao direito de todos à educação e à participação na vida pública. Em particular, os signatários do Pacto acordaram que o direito à educação "deve ser orientado para o pleno desenvolvimento da personalidade humana e do sentido da sua dignidade [...] e permitir a todas as pessoas uma participação efetiva na sociedade" (artigo 13.1). Além disso, o livre desenvolvimento da personalidade é explicitamente considerado como um instrumento para o exercício do direito fundamental "de participar na vida cultural [e] de fruir os benefícios do progresso científico e das suas aplicações" (artigo 15.º). Ver Belli, Luca et al. Cibersegurança: uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. FGV Direito Rio. (2023: 69-94). https://bibliotecadigital.fgv.br/dspace/handle/10438/33784 Belli, Luca. Network Self-Determination and the Positive Externalities of Community Networks". Em L. Belli (Ed.) Community Networks: The Internet by the People for the People. Official Outcome of the UN IGF Coalition on Community Connectivity. FGV. (2017: 35-64) https://www.intgovforum.org/en/filedepot_download/4391/1132

maximizar a autodeterminação, que descrevi precedentemente como "Boa Soberania Digital"[6].

Nesta perspectiva, proponho um framework estratificado em camadas para analisar quais os elementos são essenciais para estabelecer a soberania da IA de um país, definindo-os como "Facilitadores Essências de Soberania em IA" ou "FESIA". Os elementos fundamentais que defino como FESIA incluem: dados (pessoais), algoritmos, capacidade computacional, conectividade, energia elétrica, promoção e retenção de talentos, cibersegurança e, por último, mas não menos importante, um quadro adequado que regule os riscos da IA. Cada um desses elementos deve ser considerado em termos de pesquisa, desenvolvimento, governança e regulação.

Assim, a segunda secção deste capítulo analisará o caso brasileiro, utilizando o framework FESIA, para compreender se as escolhas regulatórias e os sistemas de governança do Brasil podem permitir ao país afirmar-se como soberano em IA ou se são ineficazes para atenuar os riscos, ou mesmo contraproducentes, conduzindo a uma maior dependência tecnológica.

1. Como devem ser lidos os facilitadores essenciais de soberania em inteligência artificial (FESIA)

Este capítulo defende que a definição de uma solida governança e regulação[7], junto com pesquisa e desenvolvimento em todos os elementos da cadeia de valor da IA são essenciais para alcançar o crescimento econômico, a justiça social e a liderança industrial, que são pilares fundamentais da soberania (em IA). Neste sentido, ao evitar ou mitigar a dependência de sistemas de IA e infraestruturas exclusivamente importados do estrangeiro, os governos podem evitar a transformação dos seus países em colônias digitais, cuja amarração a tecnologias estrangeiras dificilmente poderá ser revertida.

É importante frisar que o objetivo do presente capítulo não é defender a uma abordagem autárquica à IA, nem negar a ampla gama de benefícios que o comércio e a cooperação internacional produzem. Pelo contrário, o objetivo do autor é discutir a forma como os países podem alcançar um nível suficiente de autonomia estratégica, diversificando as suas cadeias de valor de IA sendo capazes de compreender o funcionamento dos sistemas de IA e desenvolvendo esses sistemas. Assim o objetivo de tal abordagem é identificar os elementos estratégicos susceptíveis de permitir que os países que adotam sistemas de IA, inclusive o Brasil, não sejam meros consumidores de tais tecnologias, dependentes de pouquíssimos fornecedores estrangeiros capazes de exercer uma enorme influência sobre seus consumidores.

---

[6] Belli L. (June 2023). Building Good Digital Sovereignty through Digital Public Infrastructures and Digital Commons in India and Brazil. G20's Think20 (T20). https://t20ind.org/research/building-good-digital-sovereignty-through-digital-public-infrastructures/

[7] Para efeitos do presente documento, a governação é entendida como o conjunto de processos e mecanismos institucionais que estimulam, facilitam e organizam a coordenação das interações dos diferentes atores num espaço político, para confrontar diferentes opiniões e interesses relativamente a uma questão específica e, idealmente, chegar à proposta da melhor solução reguladora possível para enquadrar essas questões. A regulamentação pretende ser o produto da governação, consistindo numa ampla gama de instrumentos que podem promover a estabilidade e o bom funcionamento de sistemas complexos, onde a presença de múltiplos atores com interesses variados ou divergentes pode naturalmente conduzir à instabilidade e à disfunção. Belli, Luca. De la gouvernance à la régulation de l'Internet. Paris: Berger-Levrault. (2016 :17-132). https://hdl.handle.net/10438/33380

O objetivo do framework FESIA é permitir que a IA seja considerada de maneira sistêmica para que, idealmente, estratégias de IA consigam enxergar a complexidade e conectar os diferentes FESIA de forma a estimular a compreensão, a produção e regulação de sistemas de IA de forma justa e sustentável, evitando ou mitigando os efeitos da dependência tecnológica.

Este capítulo sublinha ainda que uma análise cuidadosa é necessária para enxergar não somente a importância de cada um dos FESIA, mas também entender a interligação entre tais elementos, que não devem ser considerados separadamente, mas através de uma **abordagem integrada**, por meio de uma "pilha de soberania da IA". Esta estrutura em camadas é proposta com a finalidade de informar a abordagem dos documentos que almejam definir as estratégias nacionais de IA tendo como objetivo reduzir a exposição do país às escolhas tecnológicas de atores estrangeiros (privados ou públicos) e, simultaneamente, aumentar a sua capacidade de ação, controle e autodeterminação sobre e através dos sistemas de IA.

A interconexão dos FESIA deve refletir-se na necessária coordenação entre as atividades de pesquisa e desenvolvimento, e os mecanismos de governança e regulação dos vários FESIA para poder formar uma pilha de soberania em matéria de IA que possa ser performante, eficiente e democrática. Idealmente, tal pilha deve constituir o esqueleto de um sistema de governança dedicado à soberania em IA, que permita aos representantes das autoridades responsáveis pela supervisão de cada FESIA cooperar com representantes das autoridades de setores conexos (incluindo reguladores de setores transversais como a concorrência, a proteção dos consumidores, a privacidade dos dados, os serviços financeiros, a energia e as infraestruturas de telecomunicações) para facilitar a organização, a cooperação e, em especial, a compartilhamento de informações.

É importante notar que este capítulo pretende adotar uma posição pragmática, sublinhando que alcançar a Soberania em IA estará longe de ser uma tarefa trivial, especialmente para os países do Sul Global, cuja maioria já sofre uma dependência tecnológica considerável. No entanto, na perspectiva do autor, a Soberania em IA deve ser considerada uma prioridade política urgente, para evitar que uma situação que beira o colonialismo digital possa se tornar irreversível.

O autor está ciente que o framework FESIA discutido na próxima seção requer um planeamento, recursos e capacidade de implementação consideráveis, mas deve ser visto como um objetivo altamente estratégico para o reforço da soberania nacional, da autonomia estratégica e da resiliência do país ao uso adversário de sistemas de IA, dominados por um número extremamente reduzido de atores dominantes estrangeiros.

2. Apresentação do framework FESIA e sua aplicação ao contexto brasileiro

A presente seção explora os supramencionados FESIA defendendo o papel fundamental de tais elementos para garantir que um país possa compreender, desenvolver e regular os sistemas de IA de acordo com os seus próprios interesses, valores e objetivos estratégicos nacionais, em vez de estar sujeito ao impacto inevitável do exercício da soberania em IA por outras entidades estrangeiras (sejam elas estatais ou empresariais[8]).

[8] Luca Belli. Structural Power as a Critical Element of Digital Platforms' Private Sovereignty. In Edoardo Celeste, Amélie Heldt and Clara Iglesias Keller (Eds). *Constitutionalising Social Media*. (Hart 2022) https://lucabelli.net/2021/08/10/structural-power-as-a-critical-element-of-social-media-platforms-private-sovereignty/

É importante notar que a soberania em IA é suscetível de se tornar um tópico cada vez mais relevante e estratégico à medida que o desenvolvimento e a evolução e adoção de sistemas de IA continuam a avançar, adquirindo um papel significativo em vários aspectos da sociedade, da administração pública e da governança democrática, não se limitando à economia. Os impactos e avanços da IA estão sendo objeto de considerável investigação, especialmente no âmbito da proteção de dados pessoais[9], e incluem uma vasta gama de setores críticos e serviços públicos essenciais, como a defesa, a segurança nacional, a gestão de infraestruturas, a saúde e a justiça.

Neste contexto, parece importante sublinhar que a capacidade de desenvolver e utilizar a tecnologia de IA, em vez de ser regulados através dela, não depende exclusivamente da elaboração e aplicação de marcos regulatórios baseados om risco e segurança de produtos. Pelo contrário, a concretização de uma Pilha de Soberania em IA implica a capacidade de exercer agência e autodeterminação em pelo menos oito dimensões diferentes que, em conjunto, permitem a construção de um ecossistema de IA sustentável e estrategicamente autônomo.

As próximas subseções apresentarão o framework FESIA que compõe o que defino como a Pilha de Soberania da IA analisando brevemente como o Brasil está aproveitando cada um dos FESIA.

2.1. Governança de dados

Os dados são o insumo vital dos sistemas de IA e ter acesso a dados diversificados e de alta qualidade é essencial para treinar e melhorar os modelos de IA. É importante notar que, dependendo do tipo de IA, os dados utilizados para alimentar sistemas podem ser categorizados como dados pessoais, governamentais (dados abertos), confidenciais, protegidos por direitos autorais, etc., incluindo assim uma certa complexidade e necessidade de conformidade regulamentar no contexto do seu tratamento. Por conseguinte, não só a disponibilidade de grandes volumes de dados heterogêneos é essencial para desenvolver IA, como também a capacidade de garantir que tais dados sejam coletados, armazenados, tratados ou transferidos para países terceiros em conformidade com a legislação em vigor. Um framework capaz de líder de maneira efetiva com tais aspectos é, portanto, um elemento crítico da soberania em IA.

Cabe ressaltar que países com bases de dados abrangentes sobre suas economias diversificadas, populações de grande tamanho e heterogeneidade (composição multiétnica etc.), juntamente com estratégias de dados, práticas consolidadas de abertura de dados, marcos regulatórios de proteção de dados pessoais e segurança da informação bem estruturados, podem ter uma vantagem competitiva. A correta combinação destes elementos e a correta implementação dos marcos normativos que os disciplinam permite a construção de soberania em matéria de dados e de IA.

No entanto, é importante sublinhar que poucos países gozam do privilégio de ter à sua disposição grandes conjuntos de dados heterogêneos e sistemas sólidos de governança de dados, capazes de facilitar inovação e evitar tratamentos abusivos. Neste contexto, parece importante considerar a necessidade de uma abordagem mais holísticas aos dados como ativo capaz de ser explorado no interesse nacional, porém precisando de solidas garantias contra tratamentos abusivos. Paralelamente, a fim de estimular uma soberania compatível com a cooperação e comercio internacional, parece essencial

[9] Ver por exemplo, os resultados da conferência CPDP LatAm, disponíveis em https://cpdp.lat/en/publications/

estabelecer novos marcos internacionais – regionais ou, idealmente, globais – de governança de dados e explorar os tratados intergovernamentais existentes, como a Convenção 108+, de modo que dados, sejam eles pessoais ou não, sejam utilizados de maneira lícita com base em normas harmonizadas.[10]

Particularmente, a governança dos dados necessários para alimentar sistemas de IA deve ter um caráter mais abrangente do que a mera proteção de dados pessoais, incluindo normas capazes de disciplinar a utilização e a reutilização de dados abertos e de informações protegidas por direitos autorais, bem como garantias contra a utilização indevida de informações sensíveis e confidenciais. Esta abordagem estratégica, mais complexa e mais abrangente, se for bem estruturada e implementada de maneira coordenada, pode atenuar os riscos e colher os benefícios de conjuntos de dados muito maiores e diversificados, proporcionando ao mesmo tempo segurança jurídica aos pesquisadores, desenvolvedores e usuários de IA.

Neste sentido, uma boa governança de dados almeja a proteção de dados pessoais, a proteção de diretos de propriedade intelectual, a garantia da segurança informacional e da segurança nacional, e o aproveitamento do valor dos dados para o desenvolvimento nacional. O Brasil fez progressos consideráveis em termos de governança de dados, estruturando uma das mais progressivas e refinadas políticas de dados abertos[11] e adotando um quadro de proteção de dados de última geração, a Lei Geral de Proteção de Dados ou LGPD. No entanto, a aplicação da LGPD permanece ainda muito tímida e incipiente, especialmente no que diz respeito aos sistemas de IA (generativa)[12]. Além disso, **o Brasil simplesmente não tem uma estratégia nacional de dados.** Portanto, parece altamente improvável que os assuntos destacados acima possam ser enfrentados de maneira orgânica e eficiente até a elaboração de tal documento estratégico e designação de um órgão voltado a sua implementação.

Por fim, cabe frisar que, no Brasil, a coleta de dados (pessoais) está consideravelmente concentrada nas mãos de gigantes tecnológicos estrangeiros, principalmente devido aos chamados planos de Internet móvel de zero rating[13] ou aplicativos patrocinados. Tais planos subsidiam o acesso móvel principalmente a pouquíssimas redes sociais dominantes, portanto concentrando a coleta e processamento

---

[10] Os melhores exemplos de cooperação internacional em matéria de política de dados são dados pelas iniciativas europeias. A Convenção 108 do Conselho da Europa é o exemplo mais conhecido - e até à recente entrada em vigor da Convenção de Malabo, o único - de tratado internacional relativo à proteção de dados pessoais. O exemplo mais refinado de abordagem coordenada da política de dados é oferecido pelo quadro da política de dados da União Europeia, que abrange o Regulamento Geral sobre a Proteção de Dados, a Diretiva "Dados Abertos" e a mais recente Lei dos Dados. É importante salientar que um quadro menos ambicioso, mas relevante, também poderia ser proposto a nível da América Latina, onde a maioria dos países já adotou leis de proteção de dados semelhantes. A este respeito, ver Luca Belli, Ana Brian Nougrères, Jonathan Mendoza Iserte, Pablo A. Palazzi e Nelson Remolina Angarita. Hacia un modelo latinoamericano de adecuación para la transferencia internacional de datos personales. Centro de Tecnologia y Sociedad de Universidad de San Andrés. (2023).

[11] De Magalhães Santos, L. G., & Dhaou, S. B. Open Data and Emerging Technologies: Connecting SDG Performance and Digital Transformation. https://cyberbrics.info/open-data-and-emerging-technologies-connecting-sdg-performance-and-digital-transformation/

[12] Belli, Luca. (23 maio 2023). Por que o ChatGPT descumpre a LGPD e por que peticionei à ANPD. Jota. https://www.jota.info/opiniao-e-analise/artigos/por-que-o-chatgpt-descumpre-a-lgpd-e-por-que-peticionei-a-anpd-23052023 ; Belli, L. Gaspar, W. Couto N. (25 agosto 2023). Por que o ChatGPT descumpre a LGPD – parte 2. Jota. https://www.jota.info/opiniao-e-analise/artigos/por-que-o-chatgpt-descumpre-a-lgpd-parte-2-25082023

[13] Veja Belli Luca. Neutralidade da rede, zero-rating e o Marco Civil da Internet, em Belli Luca e Cavalli Olga (2019). Governança e regulações da Internet na América Latina. FGV Direito Rio. (pp 175-204). Para maiores informações sobre as práticas de zero rating, ver http://www.zerorating.info/

de dados da maioria das comunicações individuais – e boa parte das comunicações comerciais – do País, como discutido na seção sobre conectividade abaixo, e frustrando assim a possibilidade de aproveitar os dados pessoais como um ativo nacional. Por último, a segurança dos dados continua também a ser muito desorganizada, devido à inexistência de uma lei geral sobre cibersegurança e de uma agencia reguladora, à falta de arcabouço regulatório abrangente sobre a segurança de informação, como destacaremos na subseção dedicada à cibersegurança.[14]

2.2. Governança algorítmica

Os algoritmos de software são a base dos sistemas de IA permitindo-lhes executar tarefas e tomar decisões. É importante notar que os algoritmos podem ser objeto de regulamentação, mas também podem desempenhar um papel instrumental na elaboração da regulamentação. Por um lado, o desenvolvimento e a implantação de algoritmos podem - pelo menos em parte - dar origem a riscos e problemas sociais que desencadeiam a necessidade de intervenção regulamentar.

Esses riscos devem ser cuidadosamente considerados, especialmente tendo em conta o fato de poderem variar enormemente em função dos sistemas de IA em questão. Por exemplo, os sistemas chamados “modelos fundamentais” apresentam riscos muito diferentes dos algoritmos treinados em bases de dados hiper personalizadas e localizadas. Neste sentido, a governança de algoritmos é intrinsicamente conectada com a regulação de riscos de IA, e se justapõe a várias áreas da regulação de plataformas e a regulação de tratamento automatizado de dados pessoais.

Por outro lado, os algoritmos podem apoiar a própria intervenção regulamentar, uma vez que são cada vez mais úteis e utilizados para implementar a própria regulamentação. Nesta perspectiva, o desenvolvimento de softwares, sejam proprietários ou open-source, proporciona uma vantagem competitiva considerável ao país, ou entidade desenvolvedora, e permitem a incorporação de valores normativos de acordo com as especificidades definidas pelos desenvolvedores. Investir na pesquisa e no desenvolvimento de ferramentas algorítmicas, abordando simultaneamente os riscos e as vantagens que estas representam, pode melhorar enormemente as capacidades tecnológicas e regulatórias de um país e reforçar a soberania da IA. Um exemplo neste sentido é o uso de infraestruturas publicas digitais para regular setores previamente dependente da atividade de reguladores públicos ou empresas privadas, como no caso dos pagamentos online.

Assim, a promoção da cooperação entre as várias partes interessadas para desenvolver algoritmos de software pode permitir reforçar a soberania da IA, seja quando os atores nacionais são estimulados a desenvolver software proprietário, seja quando o software for desenvolvido em código aberto através de um processo colaborativo adotado - ou mesmo liderado - pelas partes interessadas nacionais. Nesta última perspectiva, cabe frisar que o primeiro Governo Lula foi um verdadeiro pioneiro em termos de uma abordagem coletiva à soberania digital[15], promovendo a adoção de software livre e aberto (FOSS) como objetivo estratégico para o desenvolvimento nacional, já em 2003.

---

[14] Belli, Luca et al. Cibersegurança: uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. FGV Direito Rio.

[15] Belli, L. (2023, March 1). Brasil precisa reconstruir sua soberania digital. Estadão. https://www.estadao.com.br/politica/blog-do-fausto-macedo/brasil-precisa-reconstruir-sua-soberania-digital/ ; Belli, L. and Jiang, M. (Orgs.). (2024). Digital Sovereignty from the BRICS Countries: How the

Esta política permitiu não só ser estrategicamente autônomo em relação aos produtores de software estrangeiros, mas também aumentar a compreensão e o desenvolvimento nacionais de software. Infelizmente, esta política foi revertida pela administração Temer em 2016, desencadeando de fato o recente fenómeno de plataformização da administração pública, adotando principalmente software e infraestrutura em nuvem desenvolvidos por provedores estrangeiros.

É importante sublinhar que um renascimento do apoio nacional ao código aberto poderia ser uma forma significativa de reforçar o desenvolvimento nacional de IA, especialmente tendo em conta a existência de várias opções interessantes de modelos de código aberto, como o Llama, o Bloom ou o Falcon, baseados nos quais podem ser construídos novos sistemas abertos de IA.

Por fim, cabe ressaltar que, apesar da turbulência política, nas últimas duas décadas, o Brasil desenvolveu vários instrumentos de política industrial destinados a fomentar a indústria nacional de software e está atualmente planejando a adoção de uma nova política industrial que incluirá a transformação digital como um dos seus pilares fundamentais.[16] No entanto, o setor de desenvolvimento de software não se tornou tão próspero como poderia, principalmente devido à falta de consistência das políticas relacionadas com o software nas últimas décadas e à ausência de políticas centradas no estímulo ao desenvolvimento e implementação de software de forma orgânica, incluindo a facilitação do acesso ao capital para impulsionar a indústria nacional de algoritmos.

Em particular, as políticas brasileiras de software careceram de instrumentos complementares capazes de estimular a procura e a oferta, por exemplo, através de aquisições públicas de software desenvolvido a nível nacional, como acontece habitualmente na China, ou através da criação de infraestruturas públicas digitais, como fez a Índia com o India Stack[17] , ou através da organização de esforços de capacitação destinados a fomentar a procura, como fez a Coreia do Sul no final da década de 1990.

2.3. Capacidade computacional

É sabido que a IA pode exigir recursos computacionais substanciais para tarefas como o treino de modelos complexos e o processamento de grandes conjuntos de dados. Em particular, os sistemas de IA mais recentes, como a IA generativa, podem ser notavelmente intensivos em termos de capacidade informática, devido à sua maior complexidade. Garantir a existência ou o acesso contínuo a uma capacidade computacional suficiente deve ser visto como uma prioridade estratégica fundamental, sem a qual é impossível tornar escaláveis novos sistemas de IA. Evidências contundentes neste sentido são as parcerias nas quais as empresas OpenAI e Mistral, de fato, precisaram

Global South and Emerging Power Alliances Are Reshaping Digital Governance. Cambridge University Press.

[16] O Ministério do Desenvolvimento, Indústria, Comércio e Serviços do Brasil anunciou em janeiro de 2024 a sua nova política industrial, baseada em seis missões fundamentais. A missão número 4 visa "transformar digitalmente 90% de todas as empresas industriais brasileiras (hoje apenas 23,5% são digitalizadas) e triplicar a participação da produção nacional nos segmentos de novas tecnologias". Ver Ministério do Desenvolvimento, Indústria, Comércio e Serviços. (22 de janeiro de 2024). Brasil ganha nova política industrial com metas e ações para o desenvolvimento até 2033. https://www.gov.br/mdic/pt-br/assuntos/noticias/2024/janeiro/brasil-ganha-nova-politica-industrial-com-metas-e-acoes-para-o-desenvolvimento-ate-2033

[17] Veja https://indiastack.org/

entrar com a empresa Microsoft, sendo esta última um dos pouquíssimos atores capazes de fornecer a capacidade computacional necessária.

Neste sentido cabe enfatizar que o mercado global de computação em nuvem é dominado por um número extremamente reduzido de empresas, sendo que as "Três Grandes" - ou seja, Amazon Web Services, Microsoft Azure e Google Cloud - representam atualmente dois terços do crescente mercado, com uma notável taxa de crescimento anual de 20 % no final de 2023, em grande parte devido à explosão da "tecnologia e serviços de IA generativa que tiveram um grande impacto, ajudando a impulsionar ainda mais as despesas com computação em nuvem".[18].

A disponibilidade de infraestruturas de computação de alto desempenho depende de múltiplos fatores, desde a acessibilidade de semicondutores e chips especificamente concebidos para aplicações de IA e de unidades de processamento gráfico ou GPU de última geração, que estão se tornando particularmente relevantes para suportar o funcionamento da IA (generativa), até servidores especializados adaptados às especificidades de sistemas de IA. É importante frisar que o mercado de semicondutores especializados em IA é ainda mais concentrado, sendo neste momento dominado por uma única empresa, Nvidia.

A este respeito, é interessante notar que algumas das primeiras políticas adoptadas pela administração Lula 3 foram a reintrodução do programa nacional de apoio ao desenvolvimento de semicondutores (conhecido como "PADIS"), bem como a suspensão da decisão anterior da administração Bolsonaro de vender o Centro Nacional de Tecnologia Eletrônica Avançada (Ceitec), que é o único produtor de semicondutores da América Latina.[19] Mais recentemente, uma das principais prioridades identificadas pela nova política industrial brasileira é o apoio à indústria nacional de semicondutores.[20] Porém, apesar destes avanços positivos, a capacidade de produzir semicondutores e servidores de computação de última geração é ainda muito distante da realidade nacional.

Cabe frisar que estas medidas não são uma peculiaridade brasileira e que um número crescente de países está considerando-as. Um dos países com apolítica industrial digital mais estruturada é a China, que nos últimos anos investiu pesadamente na infraestrutura de IA, especialmente em seguida às restrições impostas pelos Estados Unidos e seus aliados. De acordo com dados da empresa chinesa de análise da indústria de semicondutores JW Consulting, o governo chinês atribuiu mais de 2,1 biliões de CNY (1,5 bilhões de Reais) a investimentos relacionados com semicondutores, entre 2021 e 2022, apoiando 742 projetos de investimento em 25 províncias e regiões chinesas.[21]

Além disso, é essencial sublinhar que a disponibilidade de recursos de computação em nuvem, por si só, não é suficiente para afirmar a soberania da IA, que exige que os

[18] Synergy Research Group. (February 2024). Cloud Market Gets its Mojo Back; AI Helps Push Q4 Increase in Cloud Spending to New Highs.https://www.srgresearch.com/articles/cloud-market-gets-its-mojo-back-q4-increase-in-cloud-spending-reaches-new-highs

[19] Decreto nº 11.456, de 28 de março de 2023. Altera o Decreto nº 10.615, de 29 de janeiro de 2021, que dispõe sobre o Programa de Apoio ao Desenvolvimento Tecnológico da Indústria de Semicondutores. https://www.in.gov.br/en/web/dou/-/decreto-n-11.456-de-28-de-marco-de-2023-473390191

[20] A visão geral das novas missões e prioridades da política industrial identificadas pelo Governo brasileiro em janeiro de 2024 está disponível em https://www.gov.br/mdic/pt-br/composicao/se/cndi/arquivos/missoes-politica-industrial.pdf. É importante sublinhar, no entanto, que, no momento da redação deste documento, o orçamento específico e a planificação detalhada da forma como esse orçamento será gasto ainda não tinham sido divulgados, não permitindo assim ao autor avaliar a solidez dos compromissos anunciados.

[21] Judy Lin. (27 June 2023). China invested US$290.8 billion in semiconductor projects between 2021-2022. DIGITIMES Asia. https://www.digitimes.com/news/a20230627VL205/china-ic-manufacturing-semiconductor-chips+components.html

recursos de nuvem estejam não só disponíveis, mas também em total conformidade com a legislação nacional. Um exemplo revelador de como isso está longe de ser a regra é oferecido pelos serviços de computação em nuvem que suportam as plataformas de educação online[22], principalmente fornecidos por duas grandes empresas estadunidenses no Brasil, que nem sequer mencionam políticas de conformidade com a LGPD.

Por fim, é importante ressaltar que a promoção de IA de código aberto pode ter um papel importante na mitigação da concentração computacional, pois permite o desenvolvimento de sistemas de IA mais econômicos e distribuídos, reduzindo a necessidade de responder a recursos computacionais altamente concentrados.

2.4. Conectividade significativa

Uma conectividade significativa, que permita aos usuários usufruir de uma infraestrutura de Internet confiável, com bom desempenho e universalmente acessível a um preço competitivo, desempenha um papel fundamental para que os sistemas de IA sejam utilizáveis pela maior parte possível da população. A conectividade significativa facilita o intercâmbio de dados, a colaboração e o acesso a serviços de IA baseados na nuvem. Ela permite aplicações em tempo real e apoia o desenvolvimento e a implantação de tecnologias de IA em vários setores, contribuindo para a construção da soberania de IA de um país.

Nos últimos dez anos, o Brasil fez enormes progressos em termos de penetração da Internet: o custo da conectividade diminuiu consideravelmente, enquanto a população conectada dobrou em uma década. [23] No entanto, este quadro otimista esconde digital divides menos visíveis, que não afetam a quantidade, mas sim a qualidade do acesso à Internet. A maior parte da população brasileira é considerada como "conectada", mas de fato está apenas parcialmente conectada.

De fato, mais de 70% da população brasileira conectada, e cerca de 85% da população com rendimentos mais baixos, têm acesso principalmente a um conjunto reduzido de aplicativos incluídos nos chamados planos de zero-rating.[24] Estes planos baseiam-se na definição de um volume de dados mensal limitado para os usuários e no patrocínio de alguns aplicativos selecionados pelas operadoras de Internet móvel, cuja consumo de dados não é contabilizado nas franquias de dados existentes. O objetivo de tais modelos é a concentração da atenção dos usuários, e a consequente coleta de dados pessoais deles, num número extremamente limitado de plataformas, percebidos como gratuitos pelos usuários, mas cujo acesso é de fato pago com dados pessoais ao invés que com dinheiro.

O fato de os aplicativos patrocinados no âmbito dos planos de zero rating serem normalmente plataformas de redes sociais dominantes torna particularmente difícil para qualquer outra empresa competir, sendo quase impossível desenvolver conjuntos de dados pessoais tão completos como os que pertencem à tais atores. Assim, além de concentrar artificialmente atenção de usuários, tais empresas consolidaram uma posição extremamente dominante devido a sua capacidade de treinar modelos de IA com suas

[22] Chacon, Guilherme; Bawden, Henrique; Xavier Morales, Luiza. Análise: Termos De Uso e Políticas De Privacidade do Google Workspace for Education e Microsoft 365 (Office 365 Educação). Laboratório de Políticas Públicas e Internet – LAPIN. (2022) https://zenodo.org/records/7718863

[23] TIC domicílios. (n.d.). Cetic.br - Centro Regional Para O Desenvolvimento Da Sociedade Da Informação. https://cetic.br/pt/pesquisa/domicilios/publicacoes/

[24] IDEC (2021). Barreiras e limitações no acesso à internet e hábitos de uso e navegação na rede nas classes C, D e E. https://idec.org.br/sites/default/files/pesquisa_locomotiva_relatorio.pdf

bases de dados, impossíveis para serem replicadas, e graças a um número de usuários extremamente elevado que somente tais empresas detém para testar e aperfeiçoar novos sistemas de IA.

2.5. Energia elétrica confiável

À medida que os sistemas de IA crescem em relevância e dimensão, necessitam de um fornecimento estável e cada vez mais relevante de energia eléctrica[25] para funcionarem eficazmente. Assim, garantir uma infraestrutura de energia confiável e o acesso a eletricidade a preços acessíveis é necessário para manter as operações de IA ininterruptas. A este respeito, pode dizer-se que o Brasil é provavelmente um dos países mais bem colocados para apoiar a expansão da infraestrutura da IA, uma vez que não só é independente em termos energéticos, como também entre 70% e 80% das suas necessidades energéticas anuais são satisfeitas através de energias renováveis, especialmente a energia hidroeléctrica[26].

No entanto, a rede elétrica nacional não está isenta de críticas. A curto prazo, o Brasil não corre o risco de falta de abastecimento de energia graças à complementaridade de várias fontes de energia com a hidrelétrica, mas a falta de planejamento estrutural e a possibilidade de hidrologia adversa - que se tem verificado nos últimos anos - podem alterar o custo da energia, tornando-o consideravelmente mais elevado. Assim, apesar de ter desenvolvido uma forte infraestrutura de energia, a capacidade brasileira de apoiar a implantação de tecnologias de energia irradiada requer um foco mais forte no planejamento para evitar a dependência potencial de fontes externas.

Cabe destacar, outrossim, que o elevado consumo de energia elétrica deve ser considerado como uma evidente externalidade negativa da infraestrutura de IA que pode ter um impacto considerável sobre a disponibilidade energética e a poluição ambiental. Portanto, tal tipo de consumo precisa ser monitorado e idealmente disponibilizado para autoridades reguladoras, considerando que é conhecido e monitorado detalhadamente pelas empresas fornecedoras de computação em nuvem.

O termo computação em nuvem é bastante equívoco ao não conseguir comunicar a dimensão essencialmente material das “nuvens” que, en realidade, sao compostas por servidores de computador, cabos coaxiais, tubos de fibra óptica, condicionadores de ar, unidades de distribuição de energia, transformadores, tubulações de água, e muito mais.[27] Para que a temperatura da “nuvem” seja mantida sob controle e os demais serviços computacionais sejam oferecidos sem interupçao 24 horas por dia, todos os dias, é necessario um abastimento constante de energia e, frequentemente, aqua.

Como analisa Monserrate, os condicionadores de ar para salas de computadores consomam uma quantidade extremamante elevada de energia, sendo equipamentos mais basicos, até mesmo nos data centers mais avançados.[28] Particularmente, em estados como

[25] Luccioni, S. (2023, April 12). The mounting human and environmental costs of generative AI. Ars Technica. https://arstechnica.com/gadgets/2023/04/generative-ai-is-cool-but-lets-not-forget-its-human-and-environmental-costs/

[26] Ministério de Minas e Energia. (31 March 2023). Brasil registra maior produção de energia limpa dos últimos 12 anos. https://www.gov.br/mme/pt-br/assuntos/noticias/brasil-registra-maior-producao-de-energia-limpa-dos-ultimos-12-anos

[27] Ver Amoore, L. “Cloud Geographies: Computing, Data, Sovereignty.” Progress in Human Geography 42, no. 1 (2018): 4–24. https://doi.org/10.1177/0309132516662147

[28] Monserrate, Steven Gonzalez. 2022. “The Cloud Is Material: On the Environmental Impacts of Computation and Data Storage.” *MIT Case Studies in Social and Ethical Responsibilities of Computing*, no. Winter 2022 (January). https://doi.org/10.21428/2c646de5.031d4553

a Virginia onde se concentra cerca de 70% do tráfego mundial da Internet e a maioria dos data centers dos EU, a energia utlizada para esfriar a nuvem é frequentemente produzida por centrais eléctricas a carvão.[29]

Por último, um elemento intimamente interligado é a necessidade de um grande abastecimento de água para arrefecer a infraestrutura de computação de IA. De fato, embora as empresas de IA sejam particularmente opacas em relação ao seu consumo de energia e água, estudos recentes ilustram que a pegada hídrica de alguns dos maiores modelos de IA é claramente insustentável.[30] Neste sentido, cabe destacar que apenas para "treinar o GPT-3 nos seus data centers, estima-se que a Microsoft tenha utilizado 700.000 litros de água doce. É água suficiente para encher a torre de arrefecimento de um reator nuclear."[31]

2.6. Promoção e retenção de talentos

Este ponto é crucial para o desenvolvimento sustentável do pais e pode ser dividido em duas áreas extremamente importantes: a educação digital, por meio da qual os talentos são promovidos, e os incentivos pelo meio dos quais os talentos são retidos ou até atirados de volta ao Pais, revertendo o fenômeno da chamada "fuga de cérebros".

Melhorar a educação digital da população, através do reforço das capacidades, da formação e da educação multigeracional, é essencial não só para conseguir uma mão de obra qualificada em IA, mas também para promover a cibersegurança e, em última análise, a soberania nacional[32]. Investir na educação, na pesquisa e no desenvolvimento no domínio da IA ajuda a criar um conjunto de profissionais de IA talentosos, ao mesmo tempo que difunde uma compreensão de como utilizar a tecnologia da melhor forma. Uma estratégia educativa sólida é, por conseguinte, vital para permitir que a população nacional evolua gradualmente de uma população constituída principalmente por consumidores de tecnologia digital para uma população composta por prossumidores, ou seja, indivíduos que podem desenvolver tecnologia e produzir inovação em vez de serem exclusivamente consumidores.

A criação de uma sólida reserva de talentos de pesquisadores de IA, engenheiros e cientistas de dados, permite a um país desenvolver e manter as suas capacidades de IA, aumentando a possibilidade de ser um exportador de tecnologia e reduzindo a probabilidade de se tornar uma colônia digital. É altamente promissor que o governo federal recentemente eleito já tenha adotado uma nova política nacional para a educação digital[33].

No entanto, continua a ser problemático constatar que o letramento digital continua a ser considerado uma prioridade apenas para as novas gerações de estudantes, esquecendo que literalmente ninguém no Brasil - como na maioria dos outros países - recebeu este tipo de educação, permanecendo assim analfabeto digital. Tal situação é particularmente arriscada num contexto de transformação digital acelerada e de

[29] *Idem.*

[30] Pengfei Li et al (2023). Making AI Less "Thirsty": Uncovering and Addressing the Secret Water Footprint of AI Models. https://arxiv.org/pdf/2304.03271.pdf

[31] Will Gendron. (14 April 2023). ChatGPT needs to 'drink' a water bottle's worth of fresh water for every 20 to 50 questions you ask, researchers say. Business Insider. https://www.businessinsider.com/chatgpt-generative-ai-water-use-environmental-impact-study-2023-4

[32] CyberBRICS. (2023, February 24). Cybersecurity and digital sovereignty: a new path for Brazil. CyberBRICS. https://cyberbrics.info/cybersecurity-and-digital-sovereignty-a-new-path-for-brazil/

[33] Lei nº 14.533 - Brasil, 11 de janeiro de 2023. https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/lei/L14533.htm

automatização, em que a compreensão do funcionamento da tecnologia se torna uma necessidade primária não só para a geração mais jovem, mas sobretudo para todos os indivíduos, cujas condições laborais, sociais e económicas são suscetíveis de serem afetadas pela implantação de sistemas de IA.

Por fim, é necessário considerar que a produção de talentos pode ser facilmente frustrada pelo fenômeno da fuga de cérebros, no âmbito do qual os talentos produzidos migram para outros países, atraídos para condições de trabalho mais palatáveis. Para reter talentos e reverter a fuga de cérebros, duas estratégias parecem promissoras: ambas incluem incentivos fiscais, capazes de tornar mais atrativas as condições salariais de quem trabalhar nas cadeias de valor de IA, bem como as condições fiscais de quem investir.

De um lado, a desoneração da folha de pagamentos pode reduzir sensivelmente os encargos trabalhistas relativos aos talentos que se deseja reter (cientistas de dados, analistas de IA, juristas especializados em regulação de IA etc.) e estimular a geração de emprego e renda adicional por tais talentos estratégicos. De outro lado, a redução da tributação da renda dos talentos que voltarem trabalhar no País pode ser uma medida extremamente interessante, produzindo um forte estímulo econômico para reverter a fuga dos cérebros.[34]

2.7. Cibersegurança

Os sistemas de IA podem ser alvo de vários tipos de ameaças à cibersegurança e podem ser utilizados para perpetrar ciberataques. Portanto, medidas robustas de cibersegurança bem como pesquisa e desenvolvimento nas diferentes áreas da cibersegurança são vitais para qualquer país, mas tornam-se ainda mais importantes no contexto da transformação digital cada vez mais acelerada e da implantação de sistemas de IA.

Em particular, é essencial proteger pessoas usuárias de sistemas de IA e infraestruturas críticas de IA contra ciberataques. O Brasil promulgou recentemente um número considerável de regulamentações setoriais de segurança cibernética, abrangendo o setor de telecomunicações, o setor bancário, o setor elétrico e a Lei Geral de Proteção de Dados.[35] Embora muitos progressos tenham permitido ao país subir no Índice de Cibersegurança da União Internacional das Telecomunicações[36], é de notar que este avanço positivo deve ser temperado com uma boa dose de pragmatismo.

Na verdade, o Brasil ainda não possui uma Lei Geral de Cibersegurança e uma Agência Nacional de Cibersegurança, embora tais elementos tenham sido propostos por um estudo produzido pelo Centro de Tecnologia e Sociedade da FGV[37] e por um Projeto

[34] Vários Países europeus estão experimentando tais incentivos. Por exemplo, recente reforma fiscal italiana sobre o regresso dos trabalhadores intelectuais introduz vantagens consideráveis em termos de pagamento de impostos. Os trabalhadores que regressem do estrangeiro beneficiam de uma redução de 50% no imposto sobre o rendimento durante quatro anos. O bónus aumenta para uma redução e 60% para quem tiver filhos e pode ser estender para sete anos, sendo a redução de imposição limitada de 50% nos últimos três anos. Para ter acesso a estes descontos fiscais, o trabalhador deve manter residência na Itália por pelo menos seis anos. Ver art. 5º do Decreto Legislativo nº. 209 de 27 de dezembro de 2023.

[35] Belli, L. *et al.* (2023). Cibersegurança: uma visão sistêmica rumo a uma Proposta de Marco Regulatório para um Brasil Digitalmente soberano. CyberBRICS. https://cyberbrics.info/ciberseguranca-uma-visao-sistemica-rumo-a-uma-proposta-de-marco-regulatorio-para-um-brasil-digitalmente-soberano/

[36] Brazil rises in international cybersecurity ranking. (2022, June 24). Serviços E Informações Do Brasil. https://www.gov.br/en/government-of-brazil/latest-news/2022/brazil-rises-in-international-cybersecurity-ranking

[37] Belli, L et al. (2023).

de Lei formulado pela Presidência[38]. Além disso, o Pais registrou um avanço muito positivo com a criação de um Conselho Nacional de Cibersegurança com caráter multissetorial, que pode ser enxergado como a primeira etapa rumo a construção de uma nova arquitetura de governança da cibersegurança.

Tal arquitetura devera reverter a abordagem altamente fragmentada da cibersegurança no país, impulsionada pelas iniciativas de agências setoriais sem competência geral em matéria de cibersegurança, e frustrada pela falta de estratégias nacionais coerentes. É possível argumentar que a falta de coordenação da abordagem brasileira à cibersegurança seja provavelmente uma das principais vulnerabilidades do país, que ainda não conseguiu criar um quadro de governança sólido para ligar, coordenar e alavancar a incrível quantidade de atores que já operam no ecossistema nacional de cibersegurança.

2.8. Regulação de riscos

Uma estrutura de governança de IA que englobe considerações éticas, leis de proteção de dados, um marco regulatório baseado em risco, junto com mecanismos de fiscalização, *enforcement* e padronização técnica[39] é crucial para a soberania da IA. Estabelecer diretrizes e padrões claros para o desenvolvimento, a implantação e o uso da IA é fundamental para garantir práticas de IA responsáveis. Nessa perspectiva, o Congresso brasileiro está elaborando um novo Marco Regulatório de IA[40] para ajudar a fortalecer os direitos dos cidadãos, promover segurança jurídica e prevenir riscos potenciais, visando assim orientar o desenvolvimento, a implantação e o uso de tecnologias de IA de forma sustentável.

É importante notar que, embora esta iniciativa seja certamente louvável e necessária, mesmo que ainda em curso, ainda não é claro até que ponto será capaz de orientar eficazmente a evolução da IA no país. Nos últimos cinco anos, pelo menos quinze projetos de lei extremamente heterogêneos foram apresentados no Congresso para criar um marco regulatório da IA no Brasil, nomeadamente os PLs 3.592/2023; 2.338/2023; 5.691/2019; 5.051/2019; 21/2020; 872/2021; 266/2024; 145/2024; 210/2024; 146/2024; 262/2024; 390/2024; 303/2024; 349/2024; 370/2024. É importante frisar que nenhum destes PLs define concretamente qual mecanismo de fiscalização, enforcement e padronização técnica deveria ser adotado para garantir a devida implementação do futuro marco regulatório e a consequente conformidade aos princípios e dispositivos normativos tão complexos para se regular.[41]

O PL 2338/2023 o único que chega a definir as atribuições de uma "autoridade competente" sem, porém, identificar qual órgão ou entidade da Administração Pública Federal poderia ser tal autoridade. Tal incerteza é susceptível de prejudicar enormemente a implementação de futura Lei, enquanto a ausência de uma autoridade, como proposto pela maioria dos PLs, pode ser ainda mais prejudicial.

---

[38] Projeto de Lei PNCiber https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf

[39] Belli L. (6 de março 2024). Regulação da inteligência artificial para inglês ver? A importância da fiscalização, padronização e enforcement. Jota https://www.jota.info/opiniao-e-analise/colunas/ia-regulacao-democracia/regulacao-da-inteligencia-artificial-para-ingles-ver-06032024

[40] PL 2338/2023 - Senado Federal. (s.d.). https://www25.senado.leg.br/web/atividade/materias/-/materia/157233

[41] Belli L. (6 de março 2024). Regulação da inteligência artificial para inglês ver? A importância da fiscalização, padronização e enforcement.

O PL 2.338/2023, apesar de não ser isento de críticas, é, sem dúvidas, o mais estruturado e completo entre os PLs apresentados até hoje no país. Porém, apesar de o artigo 19 do referido PL impor que os sistemas de IA incluam "o uso de interfaces ser humano-máquina adequadas" e "medidas de gestão de dados adequadas" e adotem "parâmetros adequados de separação e organização dos dados" e "medidas adequadas de segurança da informação" não indica como tais elementos essenciais poderiam ser determinados "adequados."

Definir um sistema que possa permitir não somente a adoção de um marco normativo moderno, ágil e capaz de maximizar direitos e reduzir riscos, mas também a implementação efetiva de tal marco, é essencial. A adoção de normas flexíveis é uma estratégia regulamentar bem-vinda para elaborar leis que se adaptem ao futuro e à evolução tecnológica. No entanto, para serem significativas, as cláusulas flexíveis devem também ser acompanhadas de um mecanismo de aplicação que permita a sua especificação através de regulamentação ou normalização.

Na ausência de tal mecanismo, a lei corre o risco de ser altamente ineficaz e vaga, em vez de flexível, e de se tornar simplesmente impossível de aplicar. A este respeito, é necessário considerar a recente experiência brasileira de regulamentação da proteção de dados para compreender que a adoção de uma lei moderna e a criação de uma nova autoridade reguladora é apenas o início do percurso regulamentar.

A elaboração de leis flexíveis de proteção de dados tem sido essencial para se chegar a um consenso quanto à aprovação do quadro brasileiro de proteção de dados. Mas a eficácia da estratégia regulamentar corre o risco de ser consideravelmente comprometida quando a tarefa premente de especificar a lei não é definida explicitamente pela lei ou é atribuída a uma entidade reguladora com tão poucos recursos que parece ter sido criada propositadamente para ser "ineficaz por padrão"[42].

3. Conclusões

É importante reiterar que os fatores de soberania de IA acima referidos estão interligados e reforçam-se mutuamente. Esta consideração é particularmente relevante num momento em que os legisladores e os governos de todo o mundo estão estudando a regulamentação da IA concentrando-se frequentemente apenas na regulamentação dos riscos e ignorando a extrema importância de todos os outros elementos fundamentais que compõem o framework FESIA. Considerar a interligação dos facilitadores expostos através de uma abordagem integrada é essencial para alcançar a soberania da IA.

No entanto, essa abordagem integrada parece estar ausente da Estratégia Brasileira de Inteligência Artificial (EBIA)[43] de 2021. Felizmente, o Ministério da Ciência e Tecnologia do Brasil decidiu reformular a EBIA, sinalizando ter percebido a falta de visão, de objetivos e, em última análise, de visão da estratégia adotada em 2021.[44] Este último documento tem sido objeto de críticas unânimes por parte dos observadores, uma vez que se limita a incluir considerações gerais sobre como a IA poderia ser implementada

[42] New Data Architectures in Brazil, China, and India: From Copycats to Innovators, towards a post-Western Model of Data Governance Luca Belli. (n.d.). IJLT. https://www.ijlt.in/journal/new-data-architectures-in-brazil%2C-china%2C-and-india%3A-from-copycats-to-innovators%2C-towards-a-post-western-model-of-data-governance

[43] Gaspar, W. (2022, March 28). Artificial Intelligence in Brazil still needs a strategy. CyberBRICS. https://cyberbrics.info/artificial-intelligence-in-brazil-still-needs-a-strategy/

[44] Ministério da Ciência, Tecnologia e Inovação (MCTI). (11 December 2023). MCTI anuncia revisão da Estratégia Brasileira de Inteligência Artificial. https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/noticias/2023/12/mcti-anuncia-revisao-da-estrategia-brasileira-de-inteligencia-artificial

em vários setores, sem definir nem os elementos que permitam coordenar a implementação da estratégia, nem os que permitam avaliar essa implementação, nem quem seria responsável por essa implementação.

Ao fornecer um entendimento preliminar sobre quais são os elementos essenciais que os países precisam considerar na sua abordagem estratégica à IA, este documento também pretende oferecer uma contribuição como matéria de reflexão que possa inspirar a revisão da abordagem estratégica brasileira à IA pela atual administração. Conforme observado, uma abordagem integrada que considere os FESIA é fundamental para alcançar a Soberania da IA desenvolvendo capacidades nativas de IA fortalecendo e diversificando as cadeias de suprimentos, aumentando a alfabetização digital da população, promovendo investimentos e parcerias estratégicas e salvaguardando a segurança da infraestrutura crítica de IA, além de regular os riscos de IA.

Por fim, é importante ser realista e reconhecer que nem todos os países poderão ser capazes de elaborar e implementar as mudanças estratégicas, políticas e institucionais necessárias, que permitam construir o que este artigo define como Pilha de Soberania de IA. Esse esforço pode ser especialmente hercúleo para os países do Sul Global, que normalmente dependem de tecnologias estrangeiras. No entanto, uma combinação cuidadosa de pensamento criativo e visão política relativamente ao desenvolvimento tecnológico pode permitir ultrapassar alguns dos obstáculos mais pesados para os países com baixos rendimentos, por exemplo, promovendo a utilização de software livre e de modelos abertos de IA, para ultrapassar os custos financeiros consideráveis determinados pela dependência de software estrangeiro.

Em última análise, a soberania de IA deve ser vista como um objetivo ideal que todos os países devem procurar alcançar, mas que pode não ser viável para todos os países. Aqueles países que possuem fortes capacidades nas áreas FESIA não só estão mais bem posicionados para manter o controle sobre as suas tecnologias, políticas e dados de IA, como provavelmente aumentarão a sua relevância tecnológica, reduzindo a dependência de fontes externas e preservando os seus interesses nacionais e autonomia no panorama da IA. Os países que não têm essa capacidade precisam de reconsiderar minuciosamente as suas abordagens estratégicas à IA, para minimizar os riscos consideráveis provocados pela dependência da IA que o fenômeno, já em curso, do colonialismo digital[45] que a dependência em IA é suscetível de exacerbar.

[45] Avila Pinto, R. (2018). Digital sovereignty or digital colonialism? New tensions of privacy, security and national policies. SUR: International Journal on Human Rights, 15(27), 15-27; Couldry, N. & Mejias, U. (2019). The costs of connection: How data Is colonizing human life and appropriating it for capitalism. Stanford, CA: Stanford University Press.