

A Influência Europeia na Agenda Digital Brasileira

Agostinho Linhares
IPE Digital

agostinho.linhares@ipedigital.tech

Leonardo Euler de Moraes
IPE Digital

leonardoeuler@hotmail.com

Humberto Pontes
Anatel

humbertobruno@anatel.gov.br

Raphael Marcelino
Marcelino de Almeida Adv
raphael@marcelinodealmeida.adv.br

Luciano Freitas
World Bank
lucianofreitas@live.com

BIOGRAFIAS

Agostinho Linhares é Doutor e Mestre em Telecomunicações, possuindo especializações em Administração Pública e em Regulação de Serviço de Telecomunicações, além de MBA Executivo em Gestão Empresarial (em execução). É Diretor-Executivo do Instituto de Pesquisa para Economia Digital (IPE Digital).

Leonardo Euler de Moraes é Doutorando e Mestre em Economia pela Universidade de Brasília (UNB). Foi presidente da Agência Nacional de Telecomunicações (Anatel) e membro titular no Comitê Gestor da Internet (CGI). Atualmente, é VP da Vestas para Assuntos Institucionais e Governamentais na América Latina. É Diretor Institucional do Instituto de Pesquisa para Economia Digital (IPE Digital).

Humberto Pontes é um especialista em regulação da Anatel com 17 anos de experiência. Com formação em Ciências Sociais, Engenharia de Redes e atualmente cursando Direito (UnB). Possui mestrado em Computação Aplicada ênfase em Gestão de Risco (MSc UnB), MBA em Gestão de Projetos (FGV) e Especialização em Gestão de Segurança da Informação e Comunicações (UnB).

Raphael Marcelino é pós-doutorando em Direito pela UERJ. Doutor em Direito pela USP. Mestre e graduado pela UNB. Autor de livros e artigos jurídicos. Palestrante em eventos nacionais e internacionais. Professor de cursos de graduação e pós-graduação em diversas instituições de ensino. Advogado e árbitro.

Luciano Charlita de Freitas é PhD em Políticas de Desenvolvimento. Especialista em Regulação. Consultor em Desenvolvimento Digital do Banco Mundial. Research Fellow no Centro de Direito e Regulação.

RESUMO

O objetivo deste trabalho é apresentar iniciativas dos três Poderes que abordam temas da Agenda Digital, com foco em serviços e mercados digitais, incluindo segurança cibernética e inteligência artificial. A abordagem destaca a desarticulação das discussões, quando todos esses temas estão interligados, especialmente no contexto da possível criação de novas Agências Reguladoras. Adicionalmente, analisa-se a regulamentação europeia e americana em comparação com os instrumentos brasileiros. Considerando a *expertise* e o poder de *enforcement* já estabelecidos pelas Autarquias Especiais atuais, sugere-se que pode ser mais vantajoso expandir as competências dessas entidades existentes, em vez de criar novas agências. Ainda, no tocante ao debate legislativo verifica-se que muitos dos projetos de lei em discussão no Brasil foram inspirados em propostas europeias; entretanto, recomenda-se que se utilize a experiência internacional de forma criteriosa, pois nem tudo pode ser adequado ao Brasil. Por fim, reconhece-se a importância da convergência regulatória com outros países e recomenda-se medidas de incentivo à geração de oportunidades de novos negócios na economia digital.

Palavras-Chave

Agenda Digital. *Big Techs*. Economia Digital. Inteligência Artificial. Segurança Cibernética.

1 - INTRODUÇÃO

Recentemente, tem ganhado holofote a regulação de serviços e mercados digitais no Brasil, com a possibilidade de criação de novas agências reguladoras. Essa Agenda Digital abrange um amplo debate legislativo, com vários Projetos de Lei (PL's) tramitando no Congresso Nacional, incluindo até Proposta de Emenda Constitucional (PEC). Dentro desse conjunto destacam-se temas sobre: (i) **regulação de Big Techs (PL 2630/2020 e PL 2.768/2022)**; (ii) **Inteligência Artificial (PL 2338/2023)**; e, (iii) **Segurança Cibernética (PEC 3/2020 e um anteprojeto do Gabinete de Segurança Institucional (GSI))**. Adicionalmente, há diversos outros temas correlatos em discussão, como a monetização de dados (PLP 234/2023) e bloqueio ao *fair share*¹ (PL 469/2024). Este último, e diversos outros PL's, propõem alterações no Marco Civil da Internet (MCI). Este trabalho irá se aprofundar nos tópicos destacados.

Uma preocupação transversal ao debate é que não se percebe nessa discussão política uma avaliação da correlação dos temas, nem uma busca consistente para aproveitar a *expertise* de agências reguladoras ou autoridade nacional já estabelecidas, o que poderia gerar ganhos de escala e de escopo, além de redução de custos. Ao contrário, verifica-se um debate fragmentado com diversas propostas de criação de Agências e órgãos de regulação.

Nesse contexto de possível ampliação no número de Autarquias Especiais, a Tabela I apresenta a Lista de Agências Reguladoras (federais), com as respectivas Leis de criação. Ressalta-se que a Autoridade Nacional de Proteção de Dados, ANPD, não é Agência Reguladora, como eventualmente alguns a classificam equivocadamente. No caso da ANPD, esta foi criada como órgão vinculado à Presidência da República, que com a conversão da Medida Provisória nº 1.124, de 2022, na Lei nº 14.460, de 25 de outubro de 2022, a referida Autoridade Nacional foi transformada em autarquia de natureza especial, modificando a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), porém sem o *status* de Agência Reguladora (AR) e sem possuir autonomia administrativa e financeira².

Quanto ao debate do texto legislativo, destacam-se o PL 2630/2020 (PL das *Fake News*), do Senador Alessandro Vieira (CIDADANIA/SE), já aprovado no Senado Federal e remetido à Câmara dos Deputados. Sua ementa é: “Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet.”. Por outro lado, PL 2.768/2022, de autoria do Deputado João Maia (PL/RN), ainda está em discussão em Comissões da Câmara, e dispõe sobre a organização, o funcionamento e a operação das plataformas digitais que oferecem serviços ao público brasileiro.

O PL 2338/2023, do Senador Rodrigo Pacheco (PSD/MG), que dispõe sobre o uso da Inteligência Artificial, ainda está no Senado Federal, sob avaliação da CTIA - Comissão Temporária Interna sobre Inteligência Artificial no Brasil. O PL brasileiro tem forte influência do modelo europeu, assim como ocorreu com a LGPD (Lei Geral de Proteção de Dados, Lei nº 13.709/2018), em relação ao GDPR (*General Data Protection Regulation* – Lei Europeia).

A PEC 3/2020, que atribui à União a tarefa de legislar sobre defesa cibernética e segurança cibernética, já foi aprovada pela Comissão de Constituição e Justiça (CCJ) do Senado Federal, e está pronta para deliberação do Plenário do Senado (desde o dia 13/3/2024).

Evidentemente, dentro da Agenda Digital brasileira, “Conectividade” é um dos tópicos prioritários, evidenciando o entendimento do legislador quanto à importância da infraestrutura digital como habilitadora de serviços e mercados, possuindo PL's para aperfeiçoar a Legislação nacional, onde se destaca o PLP nº 77/2002, de autoria da Senadora Daniella Ribeiro (PSD/PB), que visa impedir o contingenciamento do FUST (Fundo de Universalização dos Serviços de Telecomunicações).

Tabela 1 – Lista de Agências Reguladoras com leis de criação

Nome da Agência Reguladora	Lei de Criação
Agência Nacional de Energia Elétrica (Aneel)	Lei nº 9.427, de 26 de dezembro de 1996

¹ Ministério das Comunicações pretendia propor Projeto de Lei sobre *fair share* até junho/2024.

<https://teletime.com.br/28/02/2024/mcom-promete-projeto-de-lei-para-big-techs-investirem-em-inclusao-digital/>

²

“É o que se verifica, por exemplo, no que concerne à gestão administrativa e financeira da autarquia, atualmente dependente de delegações e aprovações do Ministério Supervisor, para atos ordinários como contratações e assinatura de contratos administrativos” (estrato da Justificativa do PL 615/2024).

Agência Nacional do Petróleo, Gás Natural e Biocombustíveis (ANP)	Lei nº 9.478, de 6 de agosto de 1997
Agência Nacional de Telecomunicações (Anatel)	Lei nº 9.472, de 16 de julho de 1997
Agência Nacional de Vigilância Sanitária (Anvisa)	Lei nº 9.782, de 26 de janeiro de 1999
Agência Nacional de Saúde Suplementar (ANS)	Lei nº 9.961, de 28 de janeiro de 2000
Agência Nacional de Águas (ANA)	Lei nº 9.984, de 17 de julho de 2000
Agência Nacional de Transportes Aquaviários (Antaq)	Lei nº 10.233, de 5 de junho de 2001
Agência Nacional de Transportes Terrestres (ANTT)	Lei nº 10.233, de 5 de junho de 2001
Agência Nacional do Cinema (Ancine)	Medida Provisória Nº 2.228-1, de 6 de setembro de 2001
Agência Nacional de Aviação Civil (Anac)	Lei nº 11.182, de 27 de setembro de 2005
Agência Nacional de Mineração (ANM)	Lei nº 13.575, de 26 de dezembro de 2017

2 – Agenda Digital no Brasil: Contextualização e Cenário Internacional

Este capítulo discorre sobre o *status* das discussões relacionadas à regulação de grandes empresas de tecnologias e Internet ou, simplesmente, “*Big Techs*” inteligência artificial (IA) e segurança cibernética. Destaca-se que não é exclusividade brasileira as tratativas desses temas, pois ocorre em outros países e regiões, sendo que decisões da União Europeia (UE) têm influenciado o arcabouço legal e regulatório brasileiro.

Atualmente, no Brasil, regulação das *Big Techs* e inteligência artificial já possuem projetos de lei em trâmite no Congresso Nacional. Enquanto Segurança Cibernética possui além de uma PEC, um anteprojeto de Lei elaborada pelo Gabinete de Segurança Institucional (GSI), que foi disponibilizado para consulta pública, e que com a publicação do Decreto nº 11.856, de 26 de dezembro de 2023, que instituiu a “Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança”, espera-se que seja encaminhado na forma de um PL pelo Governo ao Congresso Nacional³.

Adicionalmente, o Judiciário também tem atuado em temas abordados acima, principalmente em relação ao combate à desinformação, definindo obrigações às *Big Techs*, e ao uso ilícito da IA. Por exemplo, decisões judiciais recentes, conforme as recém aprovadas Resoluções do Tribunal Superior Eleitoral (TSE) que regerão as Eleições Municipais de 2024, geram jurisprudência que incluem instrumentos para que a Justiça Eleitoral combata as *fake News* e as *deepfakes*⁴. Para acelerar a operacionalização de decisões judiciais, o TSE e a Anatel assinaram um Acordo Técnico⁵ que institui um fluxo de comunicação direto entre os órgãos visando acelerar o cumprimento de determinações judiciais para a retirada de sítios do ar. Há discussões sobre se o conteúdo de algumas das instruções emitidas pelo TSE estaria extrapolando o poder regulamentar do Tribunal. Coêlho (2017) e Angelo (2022) apresentam visões sobre a extensão do poder de polícia do TSE.

Tema 1: Regulação das “Big Techs”

O período de pré-eleição presidencial de 2022 no Brasil foi marcado por várias acusações de disseminação de notícias fraudulentas, mais conhecidas por “*fake news*”. Nesse ambiente virtual hostil, com implicações diretas na interação social, discute-se questões relacionadas a responsabilização civil por ação ou omissão relacionados a disseminação de *fake news* e sua regulação.

³ <https://www.cnnbrasil.com.br/politica/governo-deve-apresentar-pl-para-criar-agencia-reguladora-de-ciberseguranca/>

⁴ <https://www.tse.jus.br/comunicacao/noticias/2024/Fevereiro/tse-proibe-uso-de-inteligencia-artificial-para-criar-e-propagar-conteudos-falsos-nas-eleicoes>

⁵ <https://www.tse.jus.br/comunicacao/noticias/2023/Dezembro/tse-e-anatel-assinam-acordo-para-reforçar-o-combate-a-desinformação-com-uso-de-inteligência-artificial>

Nesse contexto de polarização política, ataques à democracia e combate à desinformação, ganhou força o Projeto de Lei (PL) nº 2630/2020 (Senado Federal), que pretende instituir a “Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet”, sendo mais conhecido como PL das *Fake News*. A explicação de sua ementa disponível no sítio do Senado é a seguinte:

Estabelece normas relativas à transparência de redes sociais e de serviços de mensagens privadas, sobretudo no tocante à responsabilidade dos provedores pelo combate à desinformação e pelo aumento da transparência na internet, à transparência em relação a conteúdos patrocinados e à atuação do poder público, bem como estabelece sanções para o descumprimento da lei.

Amato (2021) apresenta uma análise mais pormenorizada do tema combate às *Fake News*, partindo da doutrina até a proposição do PL nº 2630/2020, destacando as potencialidades do instituto da “autorregulação regulada”.

O ministro do Supremo Tribunal Federal (STF) Gilmar Mendes já defendeu a regulamentação das redes sociais, destacando a necessidade de se definir um órgão competente para a fiscalização das plataformas⁶: “Esse é um debate que está posto, e não sei se será posto à Anatel ou outra agência que poderá ser criada...”

O presidente da Anatel, Carlos Baigorri, também já se manifestou⁷ sobre o PL das *Fakes News* defendendo o regulador de telecomunicações como entidade autônoma de supervisão nesse PL. Adicionalmente, observou que a Agência já teria experiência no combate a *Fake News* e que não seria necessário ampliação do quadro de servidores do órgão regulador, somente sua recomposição.

Adicionalmente, o PL nº 2.768/2022, propõe uma regulação para o funcionamento e a operação de plataformas digitais que atuam no Brasil. Este PL define a Anatel como órgão responsável por fiscalizar, regulamentar e aplicar sanções a Serviço de Valor Adicionado (SVA). Assim, a competência da Anatel seria ampliada para atuar em temas como ferramentas de busca *online*; redes sociais *online*; plataformas de compartilhamento de vídeo; serviços de comunicações interpessoais (mensageria) e serviços de publicidade *online* ofertados por operador das plataformas digitais, entre outras aplicações digitais.

A UE tratou do tema “Serviços Digitais” no “*Digital Services Act (DSA)*”. Essa Lei aprovada em 2022, e vinculante para os países da UE, regula as obrigações dos serviços digitais que atuam como intermediários no seu papel de conectar os consumidores de bens, serviços e conteúdo, incluindo mercados *online*, entre outros. O contexto⁸ da DSA é mais amplo do que está sendo tratado no Brasil (PL nº 2630/2020), mas inclui questões de (co)regulação de *Big Techs* e combate à *Fake News*, além de diversos outros temas, como conteúdo ilegal, venda de produto pirata, entre outros. Não existe um regulador específico, mas cada Estado membro terá que definir um Coordenador de Serviços Digitais (*Digital Services Coordinator*), que será uma entidade independente responsável por supervisionar as *Big Techs*, em coordenação com especialistas setoriais. Resumidamente, seu objetivo é estabelecer regras claras e responsabilidades para as empresas de serviços digitais em relação ao conteúdo que é publicado e compartilhado em suas plataformas.

Ademais, a UE também aprovou o “*Digital Market Act (DMA)*”, ou Lei de Mercados Digitais, em português. O DMA é voltado para as plataformas digitais que são classificadas como “*gatekeepers*”, ou seja, aquelas que têm um poder de mercado significativo no ambiente digital, exercendo posições dominantes. Na própria Justificação do PL nº 2.768/2022, o autor cita o DMA, e facilmente percebe-se a influência do DMA no PL em discussão no Brasil.

Nos Estados Unidos não existe regulação similar ao DSA ou DMA europeus, porém há Leis e regulamentação dispersas que tratam de serviços/plataformas digitais. Alguns desses instrumentos são:

Seção 230 do Communications Decency Act (CDA): Esta lei garante a não-responsabilização civil às plataformas *online* por conteúdos postados por terceiros (princípio da inimputabilidade da rede), ao mesmo tempo em que as permite moderar conteúdos, incluindo sua remoção em certas circunstâncias.

Lei Federal do FTC (*Federal Trade Commission Act*): O *FTC Act* proíbe práticas injustas ou enganosas no comércio, incluindo também aquelas relacionadas aos serviços digitais e plataformas *online*.

Lei de Proteção da Privacidade Online de Crianças - *Children's Online Privacy Protection Act (COPPA)*: regulamenta a coleta e uso de informações pessoais de crianças abaixo de 13 anos por serviços *online*.

⁶ <https://www.poder360.com.br/iii-simposio-telcomp/gilmar-mendes-fala-em-orgao-para-regulamentar-big-techs/>

⁷ <https://www.gov.br/anatel/pt-br/assuntos/noticias/presidente-da-anatel-se-manifesta-sobre-pl-das-fake-news>

⁸ https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348

Tema 2: Inteligência Artificial

Inteligência artificial (IA) é um dos temas que mais ganhou destaque no mundo, a partir da grande repercussão de IA generativa. Entende-se por IA generativa sistemas que a partir de requisições que utilizam linguagem comum, são capazes de gerar respostas em diferentes formatos, como texto ou imagem. Essa evolução na IA tem desencadeado diversos debates que envolvem, por exemplo, proteção de direitos fundamentais, inclusive preocupação com algoritmos potencialmente discriminatórios, direitos autorais, responsabilidade civil, questões éticas, e, no limite, até a proteção do futuro da raça humana.

Um ponto relevante é que muitos algoritmos de inteligência artificial utilizam “*machine learning*”, isto é, um sistema treinado a partir de determinados padrões e informações para executar operações. Porém, em um ambiente repleto de informações fraudulentas, a máquina poderia ser treinada a partir de dados viesados, ou até intencionalmente errados, gerando a produção de mais conteúdo com vícios. Este é um exemplo, de como “*Fake News*” pode se relacionar com inteligência artificial, com potencial de gerar um ciclo vicioso.

Apesar de não ser o único sobre o tema, o PL 2338/2023⁹, que dispõe “sobre o uso de inteligência artificial” ganhou um maior destaque, dado a popularidade do *ChatGPT* e outros sistemas similares. Tal PL, entre diversas providências, propõe que o Poder Executivo designe uma “autoridade competente” para zelar pela implementação e fiscalização da lei. Na esteira desse debate, a ANPD publicou análise preliminar do PL 2338/2023¹⁰, na qual defende que “tendo em vista a forte sinergia da proposta apresentada no PL 2338/2023 com os temas tratados na LGPD, esta Autoridade entende que possui papel-chave na governança da IA e proteção de dados pessoais”, demonstrando o interesse em ser a “agência reguladora¹¹ da inteligência artificial”.

Em 2022, durante reunião¹² de Comissão do Senado Federal, especialistas já defendiam a criação de uma agência reguladora de inteligência artificial no Brasil. Em 2021, a União Europeia¹³ começou o trabalho para aprovar lei que regulamentasse o uso de inteligência artificial na Europa. O *Artificial Intelligence Act*¹⁴ foi aprovado pelo Parlamento Europeu em março de 2024 e determina a avaliação de sistemas de IA, os categorizando em diferentes classes, a saber: **risco inaceitável**, **risco alto**, **risco moderado** e **risco mínimo**, assim como apresentado na Fig. 1. O regulamento também prevê regras específicas para modelos de IA de Uso Geral (GPAI), como as IA Generativas, e estabelece requisitos mais rigorosos para modelos GPAI com “capacidades de elevado impacto” que possam representar um risco sistêmico. Por outro lado, o PL 2338/2023 categoriza os riscos em somente duas categorias: (i) **Risco Excessivo**; e (ii) **Alto Risco**.

Alguns dos tópicos que são cobertos, tanto no documento europeu quanto no referido PL, incluem a categorização de riscos, a designação de “autoridades nacionais de supervisão”, o impacto algorítmico, os incidentes graves, a governança, entre outros temas. Essa estrutura em comum indica a influência do trabalho realizado na Europa sobre a principal proposta em discussão no Brasil, mesmo que em alguns pontos existem diferenças relevantes. Milena (2023) faz uma análise comparativa do PL 2338/2023 e do “*EU AI Act*”, em que aborda semelhanças e diferenças desses instrumentos, principalmente relacionados a categorização de riscos e a responsabilidade civil, sendo que em relação a este último, aponta uma lacuna no documento europeu, pois diferente da proposta brasileira que estabelece quando a responsabilidade será objetiva e subjetiva, a norma europeia limita-se a definir requisitos e obrigações, que após análise, determinarão a responsabilidade do fornecedor.

Destaca-se outro tema coberto no PL, que é tratado de forma mais superficial no “*EU AI Act*”, que é o processo de mineração de dados e texto em sistemas de inteligência artificial e a possível ofensa a direitos autorais. O PL propõe um conjunto de regras aplicáveis para preservação do direito autoral, esclarecendo os casos que não constituiriam ofensas a esse princípio. Porém, a leitura de outra norma europeia, a “*Directive (EU) on copyright and related rights in the Digital Single Market*” indica sua influência no PL sobre IA no Brasil.

Nos Estados Unidos, existem discussões no Congresso americano e algumas cidades e estados já aprovaram leis que limitam o uso de IA em áreas como investigações policiais e contratações¹⁵. Além disso, o presidente Joe Biden instruiu agências governamentais a avaliar futuros produtos de IA quanto a possíveis riscos à segurança nacional ou econômica, por

⁹ <https://www25.senado.leg.br/web/atividade/materias/-/materia/157233>

¹⁰ https://www.gov.br/anpd/pt-br/assuntos/noticias/analise-preliminar-do-pl-2338_2023-formatado-ascom.pdf

¹¹ <https://www.convergenciadigital.com.br/Governo/ANPD-quer-ser-agencia-reguladora-da-inteligencia-artificial-63676.html>

¹² <https://teletime.com.br/28/04/2022/especialistas-defendem-criar-agencia-independente-para-regular-inteligencia-artificial/>

¹³ <https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>

¹⁴ https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_EN.html

¹⁵ <https://www.bloomberg.com/news/articles/2024-03-13/regulate-ai-how-us-eu-and-china-are-going-about-it>

meio do “*Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*”¹⁶, de 30 de outubro de 2023.

EU AI act risk-based approach

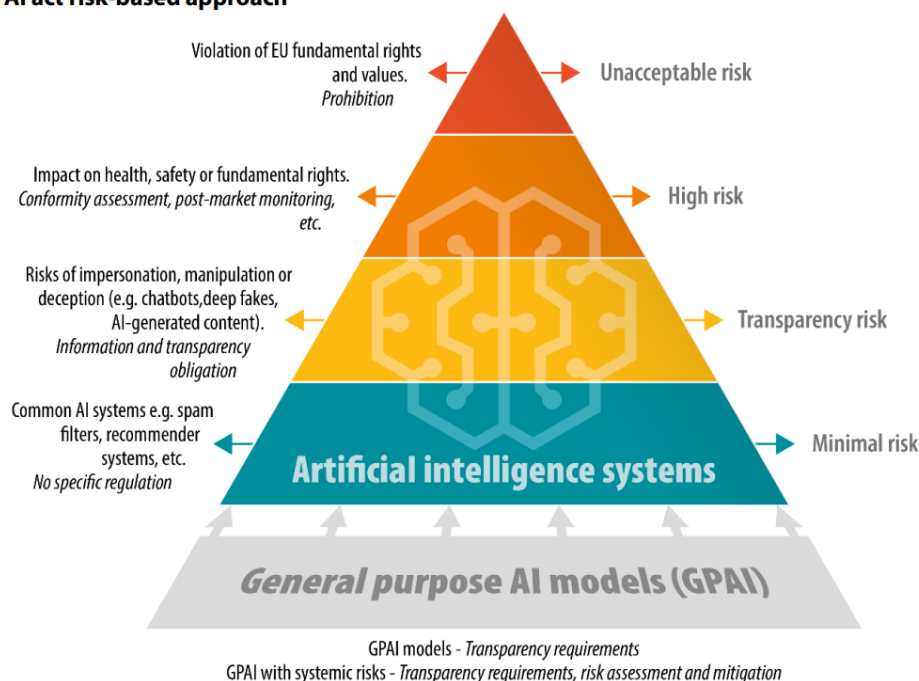


Fig.1 – Abordagem Baseada em Risco da Regulamentação Europeia de IA.

Fonte: “[https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI\(2021\)698792_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf)”

Tema 3: Segurança Cibernética

Em 26 de dezembro de 2023, foi aprovado o Decreto nº 11.856, que instituiu a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança. Anteriormente, já existiam outras políticas públicas tratando especificamente de cibersegurança e que tratavam segurança cibernética como espécie do gênero segurança da informação, conforme apresentado na Estratégia Nacional de Segurança Cibernética (E-Ciber), aprovada pelo Decreto nº 10.222, de 5 de fevereiro de 2020, que explica:

“Em nível superior aos debates sobre a segurança no espaço cibernético está a Segurança da Informação, área sistêmica, e diretamente relacionada à proteção de um conjunto de informações e ao valor que estas possuem para um indivíduo ou para uma organização. Desse modo, segundo o art. 2º do Decreto nº 9.637, de 2018, a Segurança da Informação abrange a segurança cibernética, a defesa cibernética, a segurança física e a proteção de dados organizacionais, e tem como princípios fundamentais a confidencialidade, a integridade, a disponibilidade e a autenticidade.” (Estratégia Nacional de Segurança Cibernética –E-Ciber, pg.4)

No âmbito da administração pública federal, a “Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal 2015-2018” ilustra essa visão de segurança da informação e comunicação; segurança cibernética e defesa cibernética, conforme apresentado na Fig.2.

Todavia, dada a relevância do tema Segurança Cibernética, o Decreto que aprovou a nova Política Nacional de Cibersegurança revogou dispositivo do Decreto nº 9.637, de 26 de dezembro de 2018, que elencava a Segurança Cibernética

¹⁶

<https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/>

como estando dentro da Segurança da Informação e Comunicações, de tal forma que agora Segurança Cibernética está ao lado da Segurança da Informação, isto é, possuem formalmente o mesmo *status*, porém o primeiro está em foco, inclusive com uma PEC¹⁷ para acrescentar que a União possuiu competência privativa para legislar sobre Defesa Cibernética e sobre normas de Segurança Cibernética aplicáveis à prestação de serviço público (art.22 da Constituição Federal), e acrescentar, também, como competência comum da União, Estados, do Distrito Federal e dos Municípios “zelar pela segurança cibernética dos serviços públicos” (art.23 da CF-88).

Destaca-se que Segurança Cibernética e Defesa Cibernética não representam exatamente o mesmo conceito. O primeiro concentra-se na salvaguarda de sistemas, redes e informações contra-ataques ou acessos não autorizados, ao passo que o segundo está ligado à proteção da soberania nacional contra ameaças originadas no ambiente cibernético. Assim, corroborando com a Fig.2, Defesa Cibernética está dentro de um conceito mais amplo, que é Segurança Cibernética.

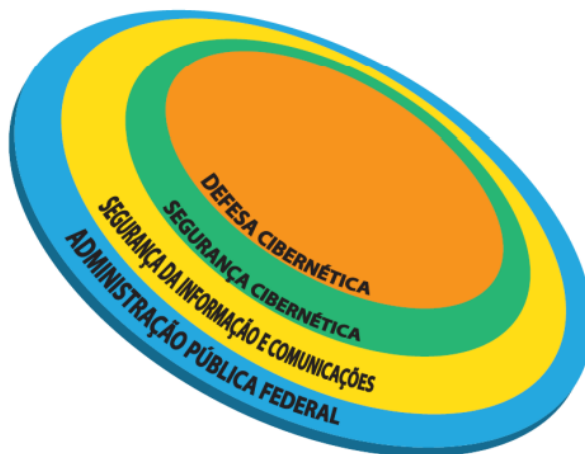


Fig.2 – Visão em camadas da Segurança da Informação e Comunicações, Segurança Cibernética e Defesa Cibernética no âmbito da administração pública.

Fonte: Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da APF 2015-2018

Quase concomitantemente, o GSI, órgão da administração pública direta, com status de ministério, elaborou proposta¹⁸ de PL (anteprojeto), que institui a Política Nacional de Cibersegurança, cria o Sistema Nacional de Cibersegurança e a Agência Nacional de Cibersegurança. Nesse documento, o GSI reconhece:

De forma similar ao ocorrido na Lei Geral de Proteção de Dados (LGPD), amplamente influenciada pela GDPR europeia, nosso modelo central foi aquele proposto pelo Parlamento Europeu, a diretiva NIS2, de dezembro de 2022. Esse modelo pressupõe a existência de um órgão central nacional, no nosso caso a Agência Nacional de Cibersegurança (ANCiber), de um “ente” fiscalizador, na nossa proposta o Comitê Nacional de Cibersegurança (CNCiber) e de um Gabinete de Gerenciamento de (Ciber)Crises, que nossa proposta denominou GGCiber.

Adicionalmente, o GSI propõe ser o ministério supervisor dessa possível nova agência, com a seguinte argumentação:

A ANCiber, então, tem que ser vinculada a um Ministério. Como se trata de uma questão afeta à segurança nacional, a opção mais adequada é pelo Ministério responsável pelo tema, o GSI. Ainda, desde 2010 o GSI está a cargo da cibersegurança da Administração Pública Federal, o que foi reiterado pela atual administração. Outrossim, acumula tradição e experiência na temática. Por conseguinte, o GSI é o órgão natural de vinculação da ANCiber

Destaca-se que a primeira parte desse trabalho do GSI foi absorvido, parcialmente, pela própria aprovação do Decreto nº 11.856/2023, pois atualizou a “Política Nacional de Cibersegurança”, além da criação do “Comitê Nacional de Cibersegurança (CNCiber)”, porém persistem as discussões sobre uma possível nova Agência, além da atualização de políticas

¹⁷ https://legis.senado.leg.br/sdleg-getter/documento?dm=9565530&ts=1710468158289&rendition_principal=S&disposition=inline

¹⁸ <https://www.gov.br/gsi/pt-br/composicao/SSIC/dsic/audiencia-publica/PNCiberAudienciaPublicaProjetoBase.pdf>

públicas correlatas e elaboração de um novo Projeto de Lei. O referido Decreto criou o CNCiber no âmbito da Câmara de Relações Exteriores e Defesa Nacional do Conselho de Governo, e possui a finalidade de orientar a atividade de cibersegurança no país. Em março/2024¹⁹ foi realizada a primeira reunião desse Comitê e foram estabelecidos os seguintes Grupo de Trabalho Temático (GTT): (i) GTT para atualização da Estratégia Nacional de Cibersegurança - e-Ciber; (ii) GTT para Elaboração de Proposta de Projeto de Lei para criação de Órgão para a Governança da Cibersegurança Nacional; (iii) GTT para Definição de Parâmetros de Atuação Internacional do Brasil em Cibersegurança.

Retornando ao estudo original do GSI, também foi avaliado o quantitativo de pessoal e o custo para criar a autarquia especial, responsável por cibersegurança. Resumidamente²⁰, seriam 800 (oitocentos) novos servidores públicos e custo anual de 600 (seiscentos) milhões de reais.

Indo para o cenário internacional, a própria Organização das Nações Unidas (ONU) possuiu uma série de Resoluções²¹ que tratam de Segurança Cibernética e Novas Tecnologias, com algumas datando do início dos anos 2000, como a Resolução 57/239²², que trata da “criação de uma cultura global de segurança cibernética”, adotada pela Assembleia Geral da ONU (UNGA – *United Nations General Assembly*) em 2003.

A Organização para a Cooperação e Desenvolvimento Econômico - OCDE também possui uma série de recomendações sobre o que chamam de Segurança Digital²³. Este termo é conceituado pela OCDE como: “A segurança digital refere-se aos aspectos econômicos e sociais da cibersegurança, em contraste com aspectos puramente técnicos e aqueles relacionados à aplicação da lei criminal ou à segurança nacional e internacional. O termo “digital” está em consonância com expressões como economia digital, transformação digital e tecnologias digitais. Ele forma a base para um diálogo internacional construtivo entre partes interessadas que buscam promover confiança e maximizar oportunidades provenientes das TICs.”.

No âmbito da OCDE, destaca-se também o documento “Arcabouço de políticas da OCDE sobre segurança digital - Cibersegurança para a prosperidade²⁴” (*OECD policy framework on digital security - Cybersecurity for prosperity*), que mapeia a dimensão econômica e social da cibersegurança, destaca a abordagem da OCDE em relação às políticas de segurança digital e capacita os formuladores de políticas a utilizar as Recomendações de segurança digital da OCDE para desenvolver políticas melhores. O arcabouço também identifica as ligações com outras áreas políticas abordadas por meio dos padrões e ferramentas existentes da OCDE.

A União Internacional de Telecomunicações (UIT) também tem atuado na discussão de Segurança Cibernética²⁵, pois baseado na orientação da Cúpula Mundial sobre a Sociedade da Informação (WSIS – *World Summit on the Information Society*) e na Conferência Plenipotenciária da UIT, construir confiança e segurança no uso de Tecnologias da Informação e Comunicação (TICs) é um papel fundamental dessa Agência Especializada da ONU. A WSIS atribuiu à UIT o papel de facilitadora da Ação C5, “Construir confiança e segurança no uso de TICs”. Derivado desse comando, a UIT lançou, a Agenda Global de Cibersegurança²⁶, como uma estrutura para a cooperação internacional nessa área.

Já em relação à Europa, a Diretiva NIS²⁷ (*Network and Information System Directive 2*) estabelece a base para as medidas de gestão dos riscos de cibersegurança e as obrigações de comunicação de informações em todos os setores abrangidos pela diretiva, como energia, transportes, saúde e infraestruturas digitais, eliminando divergências nos requisitos de segurança cibernética e na implementação de medidas de segurança cibernética nos diferentes Estados-Membros. Adicionalmente, estabelece requisitos mínimos de arcabouço regulatório e estabelece mecanismos para uma cooperação eficaz entre as autoridades relevantes em cada Estado-Membro. Por fim, define a lista de setores e atividades sujeitos a obrigações de cibersegurança e prevê soluções e sanções para garantir a aplicação.

Ademais, a Europa também aprovou a “Lei de Cibersegurança” (*Cybersecurity Act*²⁸), que por sua vez criou a Agência Europeia de Cibersegurança (*ENISA – European Union Agency for Cybersecurity*). Se por um lado a Diretiva NIS2 foca nos requisitos de segurança cibernética para operadores de infraestrutura crítica e provedores de serviços digitais, por outro a Lei de

¹⁹ <https://www.gov.br/gsi/pt-br/centrais-de-contendo/noticias/2024/comite-nacional-de-ciberseguranca-promove-sua-primeira-reuniao>

²⁰ <https://teletime.com.br/15/06/2023/agencia-reguladora-de-ciberseguranca-pretende-ter-800-servidores-e-gasto-anual-de-r-600-milhoes/>

²¹ <https://www.un.org/counterterrorism/cybersecurity>

²² https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf

²³ <https://www.oecd.org/digital/digital-security/>

²⁴ https://read.oecd-ilibrary.org/science-and-technology/oecd-policy-framework-on-digital-security_a69df866-en#page9

²⁵ <https://www.itu.int/en/action/cybersecurity/Pages/default.aspx>

²⁶ <https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx>

²⁷ <https://www.nis-2-directive.com/>

²⁸ <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>

Segurança Cibernética visa fortalecer a estrutura de cibersegurança na UE, aprimorando as capacidades, cooperação e mecanismos de certificação.

No caso americano, o “*Cybersecurity Information Sharing Act (CISA)*” é uma lei federal projetada para melhorar a cibersegurança nos Estados Unidos por meio do aprimoramento do compartilhamento de informações sobre ameaças cibernéticas e para outros fins. As principais disposições do projeto de lei tornam mais fácil para as empresas compartilharem informações pessoais com o governo, especialmente em casos de ameaças de segurança cibernética. Sem exigir o compartilhamento dessas informações, a lei cria um sistema para que agências federais recebam informações sobre ameaças de empresas privadas²⁹.

Embora tanto a Diretiva Europeia NIS2, quanto a Lei Americana *CISA* visem reforçar a segurança cibernética, elas abordam aspectos diferentes do tema, adaptadas às necessidades e desafios específicos das respectivas jurisdições, refletindo o momento em que foram aprovadas, esta em 2014 e aquela em 2022. Conforme explicitamente indicado pelo GSI e apresentado anteriormente, a proposta desse Gabinete segue o modelo europeu.

Ainda se tem que aguardar pelo PL que sairá do CNCiber, mas assim como ocorreu com o PL do GSI, tanto a Diretiva NIS2, quanto o “*Cybersecurity Act*” são influências para o trabalho que está sendo desenvolvido no Brasil. Um ponto que será crucial dessa proposta é o modelo de governança, que poderá ensejar a criação de uma Autoridade Nacional de Segurança Cibernética, que inclusive poderá ser enquadrada como Agência Reguladora. Cravo (2023) discorre sobre a necessidade de estabelecimento de estrutura de governança adequada para segurança cibernética no Brasil.

3. Efeito Bruxelas e a Influência de Regulamentações e Normas no Brasil

O conceito de "Efeito Bruxelas" refere-se à capacidade da União Europeia de influenciar regulamentações globais devido ao seu mercado significativo e normas rigorosas. No contexto da regulação digital, esse efeito é evidente à medida que muitas legislações brasileiras se inspiram em marcos regulatórios europeus. A Lei Geral de Proteção de Dados (LGPD), por exemplo, foi amplamente baseada no GDPR europeu. Essa influência continua a moldar as discussões sobre a regulação de Big Techs, Inteligência Artificial e Segurança Cibernética no Brasil, com propostas que frequentemente refletem as normas estabelecidas pela UE.

A tendência de alinhar-se às normas europeias pode trazer diversos benefícios, como a facilitação de negócios internacionais e a adoção de padrões elevados de proteção ao consumidor. No entanto, é crucial que o Brasil avalie cuidadosamente essas normas para garantir que sejam adequadas ao contexto nacional. As especificidades do mercado brasileiro e as necessidades locais devem ser consideradas para evitar a implementação de regulamentações que possam ser excessivamente restritivas ou inadequadas para a realidade brasileira.

Por outro lado, alguns países têm adotado abordagens distintas, visando promover um ambiente mais favorável à inovação. O Reino Unido, por exemplo, após o Brexit, tem buscado uma abordagem "pró-inovação" para a regulação de IA (UK Government, 2021). A Argentina também anunciou uma "abordagem menos restritiva" para atrair empresas de tecnologia que buscam escapar do escrutínio regulatório europeu (Argentina, 2022). Da mesma forma, Emirados Árabes Unidos (UAE, 2021) e Singapura (Singapore, 2020) têm criado *sandboxes* regulatórios que incentivam a inovação dentro de um ambiente de negócios amigável.

Dada a importância estratégica e econômica da Inteligência Artificial como a próxima tecnologia de propósito geral, a regulação desse campo está naturalmente sujeita às condições de mercado locais. Isso resulta em divergências significativas nas abordagens regulatórias. Enquanto a UE adota uma postura mais rigorosa com sua Lei de IA, que categoriza sistemas de acordo com níveis de risco, outras jurisdições podem optar por regulamentos mais flexíveis, focando em incentivar o desenvolvimento tecnológico. É essencial que o Brasil encontre um equilíbrio entre essas duas abordagens, aproveitando o melhor das normas internacionais enquanto promove um ambiente propício à inovação e desenvolvimento tecnológico local.

3 – Considerações Finais

²⁹ <https://harvardnsj.org/2014/02/06/the-current-landscape-of-cybersecurity-policy-legislative-issues-in-the-113th-congress/>

A Agenda Digital no Brasil está ativa nos três Poderes Federais. Há diversas propostas de atualização legal e procedimental, algumas incluindo a criação de novas Agências Reguladoras. Porém, não se percebe no debate em curso uma avaliação da correlação dos novos temas, no caso aqui tratados, regulação das *Big Techs*, inteligência artificial e segurança cibernética; nem uma busca consistente para aproveitar a *expertise* de agências já estabelecidas, o que poderia gerar ganhos de escala e de escopo.

Ademais, visando soluções mais econômicas e efetivas para sociedade e facultar uma ação imediata sobre os temas, parece fazer sentido buscar alternativas a criação de novas entidades, como ampliar a competência de agências já estabelecidas, a habilitação de sistemas de autorregulação, ou definição de comitês gestores, a depender do caso.

Adicionalmente, convém que o arcabouço legal no Brasil busque um equilíbrio entre a proteção da sociedade, a manutenção do potencial de inovação que as novas tecnologias podem oferecer e obrigações razoáveis para os envolvidos, conforme o caso (ex. plataformas digitais ou detentores de infraestrutura de telecomunicações).

Conforme indicado no estudo do GSI que sugeriu a criação de uma Agência Nacional de Segurança Cibernética, seriam necessários 600 milhões de reais para manter essa infraestrutura, com 800 servidores envolvidos. Frente a este quantitativo de servidores e custos anuais estimados, faz sentido melhor avaliar a conveniência e oportunidade de ampliar competências de Autarquias Especiais já estabelecidas, a fim de buscar o uso mais racional de recursos públicos.

Nesse debate sobre a Agenda Digital no Brasil, resta clara a importância da infraestrutura de telecomunicações, *data centers* e aplicações (ex. como aquelas oferecidas pelas *Big Techs*) quando se discute Segurança Cibernética, Regulação de *Big Techs* e Inteligência Artificial, incluindo o poder de *enforcement* das entidades já existentes. A partir da constatação desses elementos básicos, percebe-se o papel crucial que a Anatel tem nesses temas, de tal forma que é uma forte candidata para ter o escopo de atuação ampliado.

O Brasil tem se inspirado nas decisões da União Europeia (UE) para definir sua legislação específica no ambiente digital, reflexo do “efeito Bruxelas”. Exemplos disso incluem a Lei Geral de Proteção de Dados Pessoais (LGPD) e as discussões sobre regulação de mercados e serviços digitais, inteligência artificial e segurança cibernética. O desafio é aplicar as melhores práticas internacionais de maneira que sejam adequadas ao Brasil, mantendo uma convergência regulatória que não apenas proteja, mas também incentive a geração de novas oportunidades de negócios na economia digital.

Em meio às transformações digitais globais, é crucial que o Brasil continue a se inspirar nas melhores práticas internacionais, mas também reconheça e valorize sua capacidade de inovação regulatória. Exemplos recentes, como o leilão do 5G e a implementação do PIX, demonstram que o Brasil pode não apenas adotar normas de outros países, mas também exportar suas próprias regulamentações e inovações. Essas iniciativas não só fortaleceram a infraestrutura tecnológica nacional, como também serviram de modelo para outros países, criando um “Efeito Brasília” no cenário global.

Esse caminho de mão dupla, onde o Brasil se inspira e, ao mesmo tempo, inspira o mundo, é fundamental para o desenvolvimento sustentável e a competitividade do país na economia digital. Continuar promovendo soluções inovadoras, eficientes e adaptadas à realidade local, enquanto se busca uma harmonização com as normas internacionais, pode posicionar o Brasil como um líder global em regulação digital. Assim, o país não apenas protege seus cidadãos e empresas, mas também contribui significativamente para o avanço tecnológico e regulatório em escala mundial.

BIBLIOGRAFIA

AMATO, Lucas Fucci. Fake news: regulação ou metarregulação? Revista de Informação Legislativa: RIL, Brasília, DF, v. 58, n. 230, p. 29-53, abr./jun. 2021. Disponível em: https://www12.senado.leg.br/ril/edicoes/58/230/ril_v58_n230_p29. Acesso em 14 de março de 2024.

ÂNGELO, Tiago e MENDES, Lucas. Especialistas divergem sobre resolução que amplia poderes do TSE. Sítio PODER360, publicado em 20 de outubro de 2022. Disponível em: <https://www.poder360.com.br/justica/especialistas-divergem-sobre-resolucao-que-amplia-poderes-do-tse/>. Acesso em 18 de março de 2024.

Argentina (2022). Ministerio de Ciencia, Tecnología e Innovación. Plan Nacional de Ciencia, Tecnología e Innovación 2030. Buenos Aires. Disponível em <https://www.argentina.gob.ar/ciencia/plan-nacional-cti/plan-cti>. Acesso em 25 de junho de 2024.

COELHO, Marcus Vinicius Furtado. A NOVA CONSTITUIÇÃO: O poder regulamentar do TSE na jurisprudência do Supremo. Sítio Consultor Jurídico, publicado em 29 de outubro de 2017. Disponível em

<https://www.conjur.com.br/2017-out-29/constituicao-poder-regulamentar-tse-jurisprudencia-supremo/> . Acesso em 18 de março de 2024.

CRAVO, Vanessa Copetti. Em busca de uma estratégia nacional de segurança cibernética: marco legal e autoridade nacional de segurança cibernética – Porto Alegre-RS: Editora Fundação Fênix, 2023.

Monetary Authority of Singapore (2020). FinTech Regulatory Sandbox Guidelines. Singapura. Disponível em <https://www.mas.gov.sg/development/fintech/regulatory-sandbox>. Acesso em 25 de junho de 2024.

Office of Artificial Intelligence, United Arab Emirates - UAE (2021). UAE Artificial Intelligence Strategy 2031. Abu Dhabi. Disponível em <https://ai.gov.ae/wp-content/uploads/2021/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf>. Acesso em 25 de junho de 2024.

SANTOS, Millena de Almeida. Responsabilidade Civil e Inteligência Artificial no Brasil: análise comparativa do PL 2338/2023 e *AI Act Europeu*. Faculdade Milton Campos, dezembro de 2023. Disponível em <https://repositorio.animaeducacao.com.br/items/b3b80d2e-dee3-4624-a72e-d06ff1406e3d/full>. Acesso em 18 de junho de 2024.

UK Government (2021). The National AI Strategy. Londres: Department for Digital, Culture, Media & Sport. Disponível em <https://www.gov.uk/government/publications/national-ai-strategy>. Acesso em 25 de junho de 2024.