Relatório do artigo 74 da Lei nº 20.212

Recomendações para uma regulação da Inteligência Artificial (IA) voltada ao desenvolvimento ético, à proteção dos direitos humanos e à promoção da inovação tecnológica

Autores: Áreas de Secretaria Jurídica e Sociedade da Informação

Versão 1
Ano: 2024

Conteúdo

Apresentação 7
Antecedentes 9
Objetivos 9
Estrutura do relatório 10
Orientações para a elaboração deste relatório 11
O desenvolvimento ético da IA, a proteção dos direitos humanos e o sistema democrático 11
O desenvolvimento ético da IA 11
A proteção dos direitos humanos e da democracia no contexto do desenvolvimento da IA 15
A promoção da inovação tecnológica e a busca da soberania em IA 18
Pressupostos deste relatório 22
Instrumentos internacionais em IA e lições aprendidas 23
Definições básicas para o relatório 27
Entidades que contribuíram para a elaboração do relatório 34
Eixos temáticos considerados 35
Aspectos gerais 35
Eixo de institucionalidade e governança 35
Considerações preliminares 35
Seleção de antecedentes internacionais 37
Diagnóstico sobre institucionalidade e governança da IA 40
Eixo de direitos humanos 43
Considerações preliminares 43
Seleção de antecedentes internacionais 44
Diagnóstico sobre IA e direitos humanos 50
Eixo de propriedade intelectual 56
Considerações preliminares 56
Seleção de antecedentes internacionais 58
Diagnóstico sobre IA e propriedade intelectual 59
Eixo de infraestrutura e cibersegurança 63
Considerações preliminares 63
Seleção de antecedentes internacionais 64
Diagnóstico sobre infraestrutura e cibersegurança para IA 65
Eixo de trabalho e capacitação em IA 68
Considerações preliminares 68

Seleção de antecedentes internacionais 69
Diagnóstico sobre trabalho e capacitação para IA 69
Eixo de responsabilidade civil e direitos do consumidor 71
Considerações preliminares 71
Seleção de antecedentes internacionais 73
Diagnóstico sobre responsabilidade civil e direitos do consumidor 74
Eixo de medidas de promoção da IA 76
Considerações preliminares 76
Seleção de antecedentes internacionais 77
Diagnóstico preliminar sobre medidas de promoção da IA 78
Outros eixos temáticos identificados a partir das contribuições recebidas 79
O uso de sistemas de IA para vigilância 79
Inserção e cooperação internacional 80
Eixo de institucionalidade e governança 82
Eixo de direitos humanos 82
Eixo de trabalho e capacitação para IA 83
Eixo de propriedade intelectual 83
Eixo de responsabilidade civil e direitos do consumidor 84
Eixo de infraestrutura e cibersegurança 84
Eixo de medidas de promoção 85
Recomendações 87
Conceitos preliminares 87
Recomendações gerais 88
Recomendações específicas 93
Institucionalidade e governança da IA 93
O papel da Agesic na institucionalidade da IA 93
A institucionalidade da IA no âmbito interno das organizações 95
Perspectiva multissetorial e multidisciplinar 96
Governança de dados 97
Ética, direitos humanos e democracia 100
O ponto de partida para a proteção dos direitos humanos 100
Medidas especiais voltadas à proteção dos direitos humanos 101
Implementação de direitos 104
Igualdade e não discriminação 104
Enfrentar os desafios para as democracias 105

Mecanismos e recursos acessíveis, adequados e efetivos 106
Regulação do desenvolvimento, uso e aquisição de IA no setor público 107
Capacitação e educação para IA 108
Inovação responsável 111
Segurança jurídica nos aspectos de responsabilidade civil e propriedade intelectual 111
Infraestrutura e cibersegurança 113
Uma perspectiva integral da infraestrutura e dos processos para a transformação digital 115
Impactos ambientais da infraestrutura 116
Medidas de promoção 117
Anexo 1: Antecedentes nacionais 121
Mapeamento da legislação nacional 121
Institucionalidade da IA 121
Governança de dados 122
Aplicação de princípios em IA 124
Propriedade intelectual 124
Infraestrutura e cibersegurança 127
Trabalho e capacitação para IA 130
Responsabilidade civil e direitos do consumidor 131
Medidas de promoção 132
Anexo 2: Antecedentes internacionais 135
Princípios e recomendações internacionais 135
Nações Unidas 136
Recomendação da UNESCO sobre a ética da IA (2021) 136
Princípios e recomendações preliminares do Órgão Consultivo de Alto Nível sobre Inteligência Artificial (2023). 142
Resolução A/RES/78/265 da Assembleia Geral da ONU (2024) 145
Outros processos intergovernamentais 148
Recomendação da OCDE sobre Inteligência Artificial (2019) 148
Princípios de Inteligência Artificial do G20 (2019) 151
Princípios orientadores internacionais para organizações que desenvolvem sistemas avançados de IA, Princípios de Hiroshima (2023) 151
Convenção-Quadro do Conselho da Europa (2024) 154
Processos na América Latina e no Caribe 159
Agenda digital para a América Latina e o Caribe, e-LAC (2022) 159

Declaração de Santiago (2023) 160
As recentes regulações nos Estados Unidos e na União Europeia 161
Ordem Executiva de 2023 dos Estados Unidos 161
Lei de Inteligência Artificial da União Europeia 165
Anexo 3: Contribuições recebidas no processo de consulta 169

Apresentação

A expansão acelerada da Inteligência Artificial (IA) e seus potenciais usos e impactos gerou um amplo debate sobre suas implicações éticas, sociais, econômicas e políticas, entre outras. O tema tem feito parte das discussões nas agendas de organismos internacionais e regionais e dos governos nacionais.

No caso do nosso país, em 2023 o Parlamento estabeleceu as primeiras diretrizes para uma política de IA, baseada em padrões internacionais e voltada ao desenvolvimento ético, à proteção dos direitos humanos e à promoção da inovação.

O artigo 74 da Lei nº 20.212, de 6 de novembro de 2023, estabelece também um prazo para que esta Agência apresente recomendações com essas orientações, o que motivou um processo de elaboração no qual se procurou contemplar diferentes perspectivas e opiniões de diversos setores da sociedade.

Este relatório e as recomendações associadas são o resultado desse processo. Nesta Agência, esperamos que permitam iniciar um debate público e uma construção coletiva sobre um tema que, sem dúvida, tem e terá impactos significativos e duradouros em nossa sociedade.

Hebert Paguas

Diretor Executivo

Antecedentes

Objetivos

A Lei nº 20.212, de 6 de novembro de 2023, estabeleceu, em seu artigo 74, duas grandes inovações no que se refere à regulação da Inteligência Artificial (IA) em nosso país:

Em relação à Estratégia Nacional de IA, destacou a liderança da Agência para o Desenvolvimento do Governo de Gestão Eletrônica e da Sociedade da Informação e do Conhecimento (Agesic) em seu desenvolvimento e implementação; determinou a atuação obrigatória da Unidade Reguladora e de Controle de Dados Pessoais (Urcdp) quando estivessem envolvidos dados pessoais; vinculou a estratégia à Estratégia Nacional de Dados; definiu seus princípios orientadores; atribuiu papel fundamental à participação de múltiplas partes interessadas por meio da possível criação de comitês ou grupos; e estabeleceu um prazo de 180 dias para a elaboração deste relatório.

Em relação ao desenvolvimento e à implementação de sistemas de IA, definiu o papel da Agesic na elaboração de recomendações específicas para entidades dos setores público e privado, incluindo recomendações para a fiscalização de seu cumprimento, tudo isso sem prejuízo das competências próprias da Urcdp e de outras entidades públicas em seus respectivos âmbitos de atuação.

Este relatório foi elaborado a partir de uma metodologia predefinida e por meio de um processo que contou com a participação de servidores e consultores de diversos órgãos públicos. Após diferentes reuniões com eles, foi definido um documento de consulta, disponibilizado a outros atores (organismos e entidades privadas, academia e sociedade civil) previamente identificados, utilizando-se, para isso, a plataforma de participação cidadã gerida pela Agesic.

Estrutura do relatório

O relatório está estruturado em três capítulos e três anexos. O primeiro capítulo descreve os antecedentes do relatório, seus objetivos, pressupostos, os antecedentes internacionais considerados, as definições básicas e as entidades que contribuíram na primeira fase do processo.

O segundo capítulo desenvolve os eixos temáticos considerados por esta Agência, indicando, em cada um deles, algumas considerações preliminares, uma seleção de antecedentes internacionais específicos e um diagnóstico preliminar, que incluiu opiniões não apenas da Agência, mas também das contribuições de outras entidades. Foram incluídos ainda neste capítulo outros eixos temáticos surgidos do processo de elaboração.

Por fim, o terceiro capítulo apresenta as recomendações elaboradas por esta Agência, divididas em recomendações gerais e específicas, vinculadas a três aspectos centrais: institucionalidade e governança da IA; ética, direitos humanos e democracia; e inovação responsável.

Foram acrescentados também três anexos ao relatório: o primeiro contém um breve mapeamento das normas mais relevantes aplicáveis aos eixos temáticos considerados; o segundo detalha normas internacionais em diferentes âmbitos; e o terceiro reúne as contribuições recebidas das instituições que colaboraram no processo de consulta realizado pela plataforma de participação cidadã.

Orientações para a elaboração deste relatório

O artigo 74 mencionado estabelece que as recomendações elaboradas devem estar voltadas a:

- O desenvolvimento ético da IA.
- A proteção dos direitos humanos.
- A promoção da inovação tecnológica.

Nos capítulos seguintes, será especificado como se procurou incorporar essas orientações às análises e às recomendações formuladas.

O desenvolvimento ético da IA, a proteção dos direitos humanos e o sistema democrático

O desenvolvimento ético da IA

No documento atualmente em processo de revisão “Estratégia de IA para o Governo Digital” [1], a Agesic define a IA como “um termo usado para descrever um campo de estudo e um conjunto de tecnologias que estudam e desenvolvem sistemas capazes de realizar tarefas normalmente atribuídas à inteligência humana.”.

Hoje existem outras definições que contemplam aspectos não considerados quando essa Estratégia foi concebida. De fato, o relatório destaca a importância de considerar definições reconhecidas e atualizadas pela Organização para a Cooperação e Desenvolvimento Econômico (OCDE). Assim, pode-se adiantar que esta Agência entende por sistema de IA o: “sistema baseado em máquina que, para objetivos explícitos ou implícitos, infere, a partir das entradas que recebe, como gerar resultados, como previsões,

[1] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-inteligencia-artificial-para-gobierno-digital/estrategia-2 . Último acesso em 09/02/2024.

conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais. Os diferentes sistemas de IA variam em seus níveis de autonomia e adaptabilidade após a implantação". Essa definição será retomada adiante.

Ao analisar os vínculos entre privacidade e IA, SOLOVE [2] afirma que esta última é uma tecnologia "antiga", não diferente das que começaram a gerar preocupações com a privacidade na segunda metade do século XX. A diferença é que, atualmente, há uma quantidade maior de dados tratados, maior poder computacional e melhores mecanismos de análise.

O documento "The governance of artificial intelligence: interim report" [3], do Comitê de Ciência, Inovação e Tecnologia da Câmara dos Comuns do Parlamento britânico, indica claramente que a IA tem sido um campo de interesse desde os anos 1950. No entanto, foi somente com a expansão dos grandes modelos de linguagem (Large Language Models ou LLMs) [4] que a IA se tornou uma tecnologia de propósito geral, acessível a todos.

O Comitê apresenta 12 desafios para os responsáveis pela elaboração de marcos e políticas de IA: vieses, privacidade, deturpação, acesso aos dados, acesso ao poder computacional, "caixas-pretas", código aberto, propriedade intelectual e direitos autorais, responsabilidade, emprego, coordenação internacional e, por fim, o desafio existencial — este último associado à crença de algumas pessoas de que a IA é uma ameaça à vida no mundo.

[2] SOLOVE, Daniel. "Artificial Intelligence and Privacy". 77 Florida Law Review, GWU Legal Studies Research Paper. Disponível em SSRN: https://ssrn.com/abstract=4713111 ou http://dx.doi.org/10.2139/ssrn.4713111 . Último acesso: 20/06/2024.

[3] https://committees.parliament.uk/work/6986/governance-of-artificial-intelligence-ai/news/197236/ai-offers-significant-opportunities-but-twelve-governance-challenges-must-be-addressed-says-science-innovation-and-technology-committee/ . Último acesso: 20/05/2024.

[4] O relatório deste ano do Comitê de Comunicações e Digitalização da Câmara dos Lordes, também do Parlamento britânico, intitulado "Large language models and generative AI", definiu os grandes modelos de linguagem como um subconjunto dos modelos fundacionais — aqueles que usam técnicas de aprendizado profundo e são treinados com grandes bases de dados — voltado ao texto escrito. O relatório está disponível em: https://publications.parliament.uk/pa/ld5804/ldselect/ldcomm/54/54.pdf . Último acesso: 20/05/2024.

O relatório citado começa com um resumo gerado por IA. Com essa inspiração, após a consideração de todos os eixos temáticos e a conclusão da elaboração deste relatório, pediu-se ao ChatGPT — um dos LLMs mais conhecidos — que sugerisse, em menos de 150 palavras, o que recomendar para uma regulação da IA voltada ao desenvolvimento ético, à proteção dos direitos humanos e à promoção da inovação.

Sua resposta foi: “Para uma regulação da IA que promova o desenvolvimento ético e a proteção dos direitos humanos, é essencial estabelecer marcos normativos claros e robustos. Eles devem incluir princípios de transparência, responsabilidade e prestação de contas, garantindo que as decisões automatizadas sejam compreensíveis e justificáveis. É fundamental que os sistemas de IA respeitem a privacidade e a segurança dos dados, implementando mecanismos para evitar vieses e discriminação. Além disso, deve haver supervisão constante e mecanismos de auditoria para assegurar o cumprimento dessas normas, com sanções adequadas para as violações.

Quanto à promoção da inovação, as regulações devem ser flexíveis e adaptáveis, permitindo a experimentação e o desenvolvimento tecnológico sem impor encargos excessivos. É crucial incentivar a colaboração entre os setores público e privado, assim como o investimento em pesquisa e desenvolvimento. As políticas devem promover um ecossistema inclusivo, no qual startups e pequenas empresas tenham acesso a recursos e oportunidades para inovar. Além disso, a educação e a capacitação em IA devem ser prioridades para preparar a força de trabalho do futuro e assegurar que o avanço tecnológico beneficie toda a sociedade”.

É claramente possível concordar com o que foi expresso, mas a realidade revela outras complexidades, sobretudo no contexto latino-americano.

Um dos desafios mais importantes, dado o potencial da IA para afetar a maneira como as pessoas vivem e se relacionam na sociedade, é gerar uma abordagem que contemple determinados princípios incontornáveis, hoje refletidos em instrumentos emanados de diferentes entidades nacionais, regionais e internacionais.

Em particular, diferentes instrumentos internacionais se manifestam a favor do desenvolvimento ético da IA, entendido como o cumprimento de determinados princípios e valores éticos associados, entre outros aspectos, ao respeito à pessoa humana, à prevenção de riscos e à proteção de grupos vulneráveis.

Em uma perspectiva crítica, CRAWFORD [5] observa que "(…) quando a rápida expansão da IA é vista como inevitável, só é possível improvisar restrições legais e técnicas aos sistemas depois dos fatos: limpar conjuntos de dados, fortalecer leis de privacidade ou criar comitês de ética. Mas essas sempre serão respostas parciais e incompletas, nas quais a tecnologia é tomada como dada e todo o resto precisa se adaptar a ela. Mas o que acontece se invertermos essa polaridade e começarmos com o compromisso com um mundo mais justo e sustentável? Como podemos intervir para enfrentar os problemas interdependentes das injustiças sociais, econômicas e climáticas? Onde a tecnologia serve a essa visão? Existem lugares em que a IA não deve ser usada, onde ela enfraquece essa justiça?".

As perguntas da autora levam a pensar na busca da motivação subjacente ao uso da IA e em políticas coletivas voltadas à conservação dos bens comuns, construídas a partir da discussão com múltiplos atores.

Quanto ao desenvolvimento ético da IA como orientação do relatório, esta Agência considerou especialmente a Recomendação sobre a Ética da Inteligência Artificial da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), adotada em 23 de novembro de 2021 e à qual nosso país aderiu em 8 de junho de 2023 [6], que contém princípios, mas também ferramentas práticas de grande relevância.

Em seu âmbito de aplicação, a recomendação detalha que a ética da IA é abordada "como uma reflexão normativa sistemática, baseada em um marco integral, global, multicultural e evolutivo de valores, princípios e ações

[5] CRAWFORD, Kate. "Atlas de Inteligencia Artificial. Poder, política y costos planetarios". Fondo de Cultura Económica. Primeira edição. 2022. P. 342 e seguintes.

[6] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/uruguay-adhiere-recomendacion-etica-inteligencia-artificial-unesco . Último acesso: 25/06/2024.

interdependentes, que pode orientar as sociedades a enfrentar de maneira responsável os efeitos conhecidos e desconhecidos das tecnologias de IA nos seres humanos, nas sociedades, no meio ambiente e nos ecossistemas, oferecendo-lhes uma base para aceitar ou rejeitar as tecnologias de IA."

O artigo 74 da Lei nº 20.212 consagra um conjunto de princípios alinhados aos que resultam da recomendação citada e de outros instrumentos internacionais que serão mencionados: equidade, não discriminação, responsabilidade, prestação de contas, transparência, auditoria e inovação segura, respeito à dignidade humana, ao sistema democrático e à forma republicana de governo, além dos princípios de proteção de dados consagrados na Lei nº 18.331, de 11 de agosto de 2008 (legalidade, veracidade, finalidade, consentimento prévio informado, segurança dos dados, sigilo e responsabilidade).

Entendendo que a ética da IA se relaciona com o cumprimento desses princípios, que viabilizam um desenvolvimento seguro e responsável de sistemas baseados nessa tecnologia, esta Agência considera que devemos nos deter em sua aplicação efetiva, oferecendo exemplos concretos.

A proteção dos direitos humanos e da democracia no contexto do desenvolvimento da IA

A segunda orientação do artigo 74 é a proteção dos direitos humanos. Esta tecnologia, ou qualquer outra tecnologia passada ou futura, não deveria enfraquecer um sistema jurídico construído a partir do reconhecimento de direitos inerentes à pessoa humana e à forma republicana de governo, consagrados em instrumentos nacionais e internacionais vigentes.

Nessa perspectiva, e como será mencionado adiante, esta Agência considera necessário partir do conjunto de obrigações que decorrem, para os Estados, do direito internacional dos direitos humanos: o dever de respeitar, o dever de proteger e o dever de cumprir, adotando todas as medidas ao seu alcance para assegurar a realização dos direitos. Em consonância com essa abordagem, considera-se pertinente destacar a necessidade não apenas de resguardar as pessoas de eventuais efeitos nocivos da IA, mas também de aproveitar seu

potencial para promover efeitos benéficos na vida delas e no desenvolvimento de nossas sociedades.

Nos instrumentos regionais e internacionais, existe consenso em colocar a pessoa humana e a defesa de seus direitos no centro de qualquer desenvolvimento normativo. PEREZ COMENALE [7] aponta a ênfase na proteção dos direitos fundamentais, com o ser humano no centro da regulação, e destaca a necessidade de preservar princípios vinculados à proteção dos dados pessoais, à proteção dos setores vulneráveis, à inclusão digital, à conectividade e à educação digital, tudo de maneira consistente com guias e recomendações internacionais.

Em particular, esta Agência quer enfatizar os impactos da IA no sistema democrático, seguindo a opinião de INNERARITY [8], que procura concretizar as recomendações de ética da UNESCO com esse foco. Nessa perspectiva, ele aborda como os sistemas automáticos de decisão afetam os princípios normativos do autogoverno democrático, afirmando expressamente: “O problema é até que ponto e de que modo o institucionalismo algorítmico, caracterizado pela utilização de sistemas de decisão automatizada (ADS), é compatível com o que consideramos um sistema político de tomada de decisões.”

O autor oferece diferentes recomendações, como educação e conscientização; regulação e legislação — nas quais atribui papel preponderante às comissões parlamentares de futuro para desenvolver um trabalho prospectivo —; participação pública e proteção da democracia por meio de instrumentos que melhorem a qualidade da conversa democrática; regulação e legislação sobre dados; transparência, explicabilidade e contestabilidade; inclusão; estratégias nacionais integrais; abordagem multiator; e desenvolvimento de marcos globais.

7 PEREZ COMENALE, Agustina. “ChatGPT. Retos y oportunidades de la Inteligencia Artificial Generativa. Desafíos de su regulación”. Livro digital, EPUB. Granero H. e outros. 2023. P. 105.

8 INNERARITY, Daniel. “Inteligencia artificial y democracia”. Ano 2024. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000389736_spa

A capacidade das pessoas de participar livremente da vida democrática também tem sido considerada ao analisar o impacto da IA em outros âmbitos, como o da neurotecnologia. É verdade que a sinergia entre IA e neurociência permitiu avanços substanciais que devem ser promovidos com responsabilidade, mas também aumentou os riscos de manipulação das pessoas e de sua autonomia individual. Essas reflexões integram o Documento de Trabalho “Rumo a um texto preliminar de uma recomendação sobre a ética da neurotecnologia”, elaborado pelo Grupo Ad Hoc de Especialistas constituído no âmbito da UNESCO [9][10].

Focar na neurotecnologia, na IA e no impacto sobre a forma como as pessoas analisam e tomam decisões permite visualizar que os usos potenciais deixarão para trás qualquer tentativa regulatória que não se sustente em instrumentos flexíveis e adaptáveis.

O Parlamento Europeu [11], por sua vez, destaca a relevância da aplicação de ferramentas de IA para melhorar o engajamento político e empoderar as pessoas, dando aos operadores políticos a possibilidade de entender melhor suas demandas por meio de diferentes sistemas e de oferecer respostas personalizadas. Também aponta riscos, como a desinformação, os deepfakes e outros mecanismos que podem afetar as campanhas políticas e influenciar a opinião pública.

O Parlamento Europeu propõe, assim, um conjunto de ferramentas para neutralizar os impactos negativos da IA, entre as quais se destacam as ferramentas de detecção automática de conteúdo gerado por IA, as marcas-d’água,

[9] Documento em inglês disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000389438 . Último acesso: 18/06/2024.

[10] Além disso, cabe indicar que a UNESCO disponibilizou uma primeira versão da recomendação sobre a ética da neurotecnologia, aberta a consulta pública e disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000389768 . Último acesso: 19/06/2024.

[11] European Parliament. “Artificial intelligence, democracy and elections”. Disponível em: https://www.europarl.europa.eu/RegData/etudes/BRIE/2023/751478/EPRS_BRI(2023)751478_EN.pdf . Último acesso: 15/6/2024.

os instrumentos de checagem de informações nas redes sociais e, em particular, as normas voltadas à mitigação dos riscos da IA.

A Convenção-Quadro sobre Inteligência Artificial do Conselho da Europa (CoE) [12] afirma que devem ser adotadas medidas para proteger as pessoas nos processos democráticos e no acesso ao debate público, resguardando-as de influências externas prejudiciais ou mal-intencionadas (artigo 5). O item 43 do relatório explicativo da Convenção esclarece que a IA tem potencial para gerar novas formas de participação cidadã e de comunicação entre cidadãos e representantes, mas também para fragmentar a esfera pública e enfraquecer a participação cidadã e a confiança na democracia.

Compartilhamos o que foi expresso nesse relatório explicativo: a integridade da democracia e de seus processos se baseia na capacidade das pessoas de formar uma opinião e agir de acordo com ela, assim como de influenciar as decisões adotadas por seus representantes. Por isso, algumas recomendações do relatório merecem consideração, como a adoção de medidas de cibersegurança diante de interferências estrangeiras mal-intencionadas em processos eleitorais ou da difusão de desinformação, cuidando para não afetar direitos fundamentais preexistentes, como a liberdade de expressão, de associação e de reunião.

Trata-se, portanto, de ter a capacidade de reconhecer e avaliar os impactos da IA nas pessoas, em seus direitos e em nosso sistema em geral, promovendo o desenvolvimento e a aplicação de ferramentas que facilitem a discussão democrática sem influências indevidas no comportamento das pessoas, e de outras que ajudem o espectro político a entender as necessidades delas e da sociedade para adotar decisões informadas e justas.

A promoção da inovação tecnológica e a busca da soberania em IA

Por fim, a promoção da inovação tecnológica se relaciona precisamente com os benefícios que essa tecnologia pode oferecer ao desenvolvimento econômico, mas

[12] https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence . Último acesso: 18/06/2024.

também social de nossas populações, particularmente no âmbito nacional e regional latino-americano.

Em nosso país, a inovação tecnológica surge como fundamento para a adoção de diferentes estratégias e a promoção de diversos benefícios incluídos em disposições legais e regulamentares vigentes.

O Decreto nº 216/023, de 17 de julho de 2023, que cria o programa Uruguay Innovation Hub (UIH), refere-se à inovação como a "(…) atividade que, apoiada em conhecimento novo, é capaz de incorporar mudanças significativas em produtos ou processos que resultem em maior valor econômico."

Neste ponto, a Agência quer destacar alguns aspectos que considera centrais para essa orientação: institucionalidade, objetivos estratégicos, instrumentos ou ferramentas, apoio financeiro e infraestrutura.

Quanto à institucionalidade, cabe mencionar primeiro a Agência Nacional de Pesquisa e Inovação, criada pelo artigo 256 da Lei nº 17.930, de 19 de dezembro de 2005, cuja estrutura teve diferentes aspectos modificados pela Lei nº 18.084, de 28 de dezembro de 2006. Esta criou também o Conselho Nacional de Inovação, Ciência e Tecnologia (CONICyT), integrado por entidades vinculadas à ciência, à tecnologia e à inovação.

Mais recentemente, o citado Decreto nº 216/023 criou o programa Uruguay Innovation Hub (UIH), que inclui, entre seus múltiplos objetivos, o fortalecimento do ecossistema inovador.

Essa institucionalidade é complementada por diversas outras entidades públicas voltadas ao desenvolvimento da inovação, como a Universidad de la República, a Universidad Tecnológica del Uruguay, o Centro Ceibal, o Laboratorio Tecnológico del Uruguay, a Direção Nacional de Inovação, Ciência e Tecnologia do Ministério da Educação e Cultura, a Agência Nacional de Desenvolvimento, a Agência de Monitoramento e Avaliação de Políticas Públicas e a própria Agesic, entre outras, que, de uma forma ou de outra, têm entre suas atribuições a promoção da inovação dentro e fora do setor público.

Por sua vez, quando falamos em objetivos estratégicos, referimo-nos à intenção, manifestada preferencialmente por normas jurídicas, de promover determinadas áreas de atividade.

A título de exemplo, o Decreto nº 216/023, que cria o programa UIH, estabelece como prioritárias as tecnologias digitais avançadas (Deep Tech), a biotecnologia (Bio Tech) e as tecnologias verdes (Green Tech).

O programa também serve para canalizar os recursos previstos no artigo 461 da Lei nº 20.075, de 20 de outubro de 2022, com o objetivo de promover projetos de ciência, tecnologia e inovação. A disponibilização de recursos para esse tipo de projeto é essencial e deve integrar a discussão sobre a promoção da inovação em IA.

Normas posteriores à Lei nº 16.906, de 7 de janeiro de 1998, também incluíram aspectos de inovação tecnológica na concessão dos benefícios previstos nessa lei, no âmbito da promoção de investimentos.

Quanto às ferramentas para inovação, merece destaque a figura dos ambientes controlados de testes — sandboxes regulatórios —, prevista no artigo 75 da Lei nº 20.212, em vias de regulamentação, que se constituirá em instrumento fundamental para testar e desenvolver produtos e serviços de forma controlada antes de sua entrada em produção.

Mas a promoção da inovação depende também de uma infraestrutura adequada, que deveria buscar garantir ao país a capacidade não apenas de produzir tecnologias, mas também de mantê-las e fazê-las evoluir, gerando internamente as capacidades técnicas e educacionais necessárias.

Relacionado a isso, embora de forma mais ampla, desenvolveu-se o conceito de Soberania em IA. BELLI [13] a descreveu como "(…) a capacidade de um determinado país para entender, desenvolver e regular sistemas de IA (…) deveria ser

[13] BELLI, Luca. "Exploring the Key AI Sovereignty Enablers (KASE) of Brazil, to build an AI Sovereignty Stack" em "THE QUEST FOR AI SOVEREIGNTY, TRANSPARENCY AND ACCOUNTABILITY. Official Outcome of the UN IGF Data and Artificial Intelligence Governance Coalition" disponível em https://www.intgovforum.org/en/filedepot_download/288/26421 . Último acesso em 30/04/2024.

vista como essencial para reter o controle, o uso e a autodeterminação sobre os sistemas de IA" [14].

O autor propõe um marco de elementos interconectados (denominado KASE, da expressão em inglês "Key AI Sovereignty Enablers") que permitirá a um país determinar sua soberania na matéria e que se referem a: governança adequada de dados pessoais e de algoritmos, forte capacidade computacional, conectividade significativa, energia elétrica confiável, população com educação digital, cibersegurança sólida e marco regulatório apropriado.

O Fórum Econômico Mundial [15], por sua vez, considerou a aplicação de 6 pilares para alcançar essa soberania: infraestrutura digital, desenvolvimento da força de trabalho, pesquisa, desenvolvimento e inovação (P&D&I), marco regulatório e ético, estímulo à indústria de IA e cooperação internacional.

O argumento da soberania em IA deve ser especialmente considerado ao promover iniciativas regulatórias. A esse respeito, a Declaração de Montevidéu sobre Inteligência Artificial e seu impacto na América Latina [16], assinada em 10 de março de 2023 por ocasião do evento Khipu, sustenta que é imprescindível fortalecer a soberania dos países latino-americanos em questões estratégicas e regulatórias de IA, considerando cruciais a formação de pessoas no mais alto nível e o desenvolvimento do pensamento crítico.

[14] No original mencionado, BELLI indica que define "AI Sovereignty as the capacity of a given country to understand, develop and regulate AI systems. I argue that AI Sovereignty should be seen as essential to retain control, agency, and self-determination over AI systems".

[15] https://www.weforum.org/agenda/2024/04/sovereign-ai-what-is-ways-states-building/ . Último acesso: 30/04/2024.

[16] https://khipu.ai/ . Último acesso: 20/06/2024.

Pressupostos deste relatório

A pergunta que inevitavelmente se coloca e que esta Agência não pretende evitar é: nosso país precisa de uma lei de Inteligência Artificial?

Esta Agência considera que a lei não é o único instrumento regulatório aplicável e que uma eventual regulação legal deveria se concentrar não na regulação de uma tecnologia em si, mas em seus impactos positivos e negativos, potenciais e efetivos, nas pessoas e na sociedade, sem limitar a inovação e o desenvolvimento tecnológico.

É preciso reconhecer que o Uruguai conta com uma base normativa em vários dos aspectos envolvidos no desenvolvimento ético da tecnologia, nos direitos humanos e na promoção da inovação. É necessário continuar a discussão e nos apoiar em disposições e compromissos internacionais assumidos por nosso país, que oferecem um marco de proteção e incentivo à inovação e ao desenvolvimento de uma IA responsável. Devemos pensar em uma regulação complementar nos aspectos que impactem significativamente a vida das pessoas e o desenvolvimento de nossas sociedades. Por isso, procuraremos oferecer uma proposta de orientações sobre como conduzir essa discussão.

DANESI [17] observa que “precisamos de uma legislação sobre inteligência artificial, mas não de qualquer uma, pois, caso contrário, corremos o risco de frear a inovação e deixar nossos países fora do progresso”, propondo uma série de espaços de diálogo, análise e diagnóstico com a participação de múltiplos atores e foco nos sistemas de IA de alto risco.

Em suma, na opinião da Agência, não se trata de uma dicotomia entre regular ou não regular, mas de responder à pergunta: o que regular? A partir dessa base, as recomendações apresentadas neste relatório se fundamentam em três pressupostos:

1. O que entendemos por “regulação tecnológica” não deve estar associado à regulação de uma tecnologia em si, mas à mitigação de impactos

[17] DANESI, Cecilia. “El Imperio de los Algoritmos”. Versão Kindle. P. 215-216.

negativos ou à promoção de impactos positivos nas pessoas e/ou na sociedade. Como consequência dessa concepção, cabe afirmar que o conceito de “regulação” compreende um leque de instrumentos normativos em sentido amplo, não limitado a leis ou regulamentos, mas que abrange outros instrumentos “brandos”, como protocolos, guias, recomendações, códigos etc.

2. Uma eventual regulação dos impactos negativos da tecnologia em geral e da IA em particular deve se concentrar na pessoa e se fundamentar na defesa de nossa sociedade e de nosso sistema democrático. As limitações deveriam ser fixadas expressamente por lei, ser estritamente necessárias e proporcionais para assegurar objetivos legítimos em uma sociedade democrática.

3. Uma eventual regulação dos impactos positivos, por sua vez, deverá se concentrar no cumprimento dos objetivos que definirmos como estratégicos em nível nacional, para aumentar a eficiência na alocação dos recursos limitados disponíveis e gerar e promover as condições estruturais necessárias a esse cumprimento. As medidas adotadas podem ter diferentes alcances, de gerais a setoriais, e nosso nível de sucesso dependerá de sua adequada definição.

Instrumentos internacionais em IA e lições aprendidas

A importância da IA em nossa sociedade tem sido reconhecida em diferentes instrumentos internacionais, nos quais também foram elaborados conceitos úteis aos objetivos deste relatório.

Em particular, a Recomendação do Conselho da OCDE sobre Inteligência Artificial [18] estabelece definições sobre o que devemos entender por Sistema de IA, Ciclo de Vida da IA, Conhecimento em IA e Atores da IA — às quais

[18] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 . Último acesso em 09/02/2024.

será feita referência nos capítulos seguintes —, assim como um conjunto de princípios aplicáveis a ela [19].

Essa organização também fez recomendações para o desenvolvimento de políticas nacionais e de cooperação internacional voltadas especialmente às pequenas e médias empresas (PMEs), a saber:

1. investir em pesquisa e desenvolvimento de IA (incluindo investimento público de longo prazo e promoção do investimento privado em pesquisa e desenvolvimento, com foco na inovação em IA responsável e no uso de dados abertos que respeite a proteção de dados, sem vieses, melhorando a interoperabilidade e o uso de padrões);

2. promover o ecossistema digital para IA (promovendo, em particular, mecanismos como os fideicomissos de dados para compartilhar informações de forma legal, ética e segura);

3. definir e viabilizar um marco de políticas de uso da IA (permitir, assim, a transição da pesquisa e desenvolvimento para a implantação e operação por mecanismos como os ambientes controlados, e revisar e adaptar os marcos regulatórios e de políticas e os mecanismos de análise aplicáveis para promover a inovação e a concorrência em IA confiável);

4. gerar capacidades e preparar a transformação do mercado de trabalho (trabalhar com vários atores na preparação da sociedade e do mundo do trabalho por meio do empoderamento das pessoas, elaborar programas de capacitação, melhorar a segurança dos trabalhadores e promover o empreendedorismo, entre outras medidas);

5. cooperar internacionalmente para uma IA confiável (cooperação com outros países e atores, trabalho em iniciativas comuns, uso de métricas internacionalmente comparáveis e coleta de evidências, entre outras medidas).

[19] Na data de elaboração deste documento, o Uruguai está em processo de adesão a esses princípios.

Os princípios da OCDE serviram de base para desenvolvimentos posteriores, como os onze princípios orientadores para IA Avançada ratificados pelo G7 e conhecidos como Princípios de Hiroshima [20], que, por sua vez, deram origem a um código de conduta para desenvolvedores.

Apenas como referência [21], o marco político global do Processo de IA de Hiroshima tem quatro pilares: 1. análise dos riscos prioritários, dos desafios e das oportunidades da IA generativa; 2. os Princípios Orientadores Internacionais do Processo de Hiroshima para todos os atores da IA no ecossistema de IA; 3. o Código de Conduta Internacional do Processo de Hiroshima para Organizações que Desenvolvem Sistemas Avançados de IA; e 4. cooperação baseada em projetos em apoio ao desenvolvimento de ferramentas e boas práticas de IA responsável.

Como mencionado, o Uruguai aderiu recentemente [22] à Recomendação sobre a Ética da IA da UNESCO [23], marco adotado por seus 193 membros e baseado em 4 valores fundamentais: 1. Direitos humanos e dignidade humana; 2. Viver em sociedades pacíficas, justas e interconectadas; 3. Garantir a diversidade e a inclusão; 4. Florescimento do meio ambiente e dos ecossistemas. Essa recomendação promove uma compreensão dinâmica da IA, definindo-a como "aqueles sistemas com capacidade de processar dados de forma semelhante a um comportamento inteligente."

Para os fins do relatório solicitado, interessa destacar dois aspectos da Recomendação. Primeiro, a definição de 11 áreas significativas para a adoção de ações relevantes pelos governos, de modo a passar de princípios de alto nível a estratégias práticas. Essas áreas de ação e as estratégias propostas pela UNESCO contribuem para determinar os passos a

[20] https://www.mofa.go.jp/files/100573466.pdf . Último acesso em 12/02/2024.
[21] https://digital-strategy.ec.europa.eu/en/library/g7-leaders-statement-hiroshima-ai-process . Último acesso em 11/02/2024.
[22] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/uruguay-adhiere-recomendacion-etica-inteligencia-artificial-unesco . Último acesso em 09/02/2024.
[23] https://www.unesco.org/es/artificial-intelligence/recommendation-ethics . Último acesso em 09/02/2024.

seguir para estruturar um marco normativo que contemple outros aspectos, além do institucional, afetados pela IA em nossas sociedades.

Segundo, cabe apontar que a Recomendação propõe duas metodologias práticas que contribuem para sua implementação: a Metodologia de Avaliação de Prontidão (Readiness Assessment Methodology ou RAM) e a Avaliação de Impacto Ético (Ethical Impact Assessment ou EIA). A RAM, em particular, apresenta perguntas sobre temas como a regulação de IA e a infraestrutura nacional para viabilizar a acessibilidade das tecnologias de IA. Seu objetivo é contribuir para determinar as mudanças normativas e institucionais necessárias para aproveitar essas tecnologias e também se resguardar em seu uso [24].

Na data de elaboração deste documento, o Uruguai está sendo avaliado no âmbito dessa metodologia, com a colaboração do Banco de Desenvolvimento da América Latina (CAF) [25].

Mais recentemente, cabe mencionar, por sua relevância, a adoção da Resolução A/RES/78/265 pela Assembleia Geral da ONU [26], que insta todos os Estados partes e outras organizações do setor privado, da sociedade civil, entre outros, a desenvolver e apoiar abordagens e marcos normativos e de governança em favor de um uso seguro e confiável da IA.

Existe outro conjunto de iniciativas que afetam a forma como os sistemas de IA serão tratados internacionalmente e que serão mencionadas em mais detalhes ao longo deste relatório.

---

[24] https://www.unesco.org/es/articles/la-unesco-ayudara-mas-de-50-paises-elaborar-una-politica-etica-en-materia-de-ia-este-ano . Último acesso em 09/02/2024.

[25] https://www.unesco.org/es/articles/unesco-apoya-proceso-de-revision-de-la-estrategia-de-etica-de-la-inteligencia-artificial-en-uruguay . Último acesso em 09/02/2024.

[26] ONU — Assembleia Geral. Resolução aprovada pela Assembleia Geral em 21 de março de 2024. 78/265. “Aproveitar as oportunidades de sistemas seguros e confiáveis de inteligência artificial para o desenvolvimento sustentável”. A/RES/78/265. Disponível em: https://documents.un.org/doc/undoc/gen/n24/087/86/pdf/n2408786.pdf?token=hxXvAKO8RS5xFkIlcb&fe=true . Último acesso:29/4/2024.

Definições básicas para o relatório

O objetivo aqui é definir o que se considera um sistema de inteligência artificial para fins da análise e das recomendações deste documento, assim como apresentar conceitos fundamentais que contribuam para compreender as características e o funcionamento desses sistemas.

Os primórdios do desenvolvimento da inteligência artificial remontam à metade do século passado, mas a velocidade vertiginosa dos avanços tecnológicos na construção e no funcionamento desses sistemas faz com que responder à pergunta sobre o que é inteligência artificial seja um desafio permanente.

Diante da necessidade de uma definição técnica que reflita o que os sistemas de IA são atualmente e, ao mesmo tempo, seja flexível frente aos avanços constantes da tecnologia, em 8 de novembro de 2023 a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) atualizou a definição de sistemas de inteligência artificial incluída na Recomendação da OCDE sobre IA adotada em 2019. A definição revisada e consensuada nesse âmbito constituiu a base técnica de diferentes processos internacionais e regionais.

Como indicado, para fins deste documento será adotada a definição revisada da OCDE: “sistema baseado em máquina que, para objetivos explícitos ou implícitos, infere, a partir das entradas que recebe, como gerar resultados, como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais. Os diferentes sistemas de IA variam em seus níveis de autonomia e adaptabilidade após a implantação [27]” (Tradução não oficial [28]).

[27] OCDE, Recomendação da OCDE sobre IA, OECD/LEGAL/0449, 2019, alterada em 2023. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 . Último acesso: 16/4/2024.

[28] Texto original em inglês: “An AI system is a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment”.

Como analisado recentemente pelo Comitê de Inteligência Artificial (CAI) do Conselho da Europa, essa definição atualizada busca identificar as características principais que permitem distinguir os sistemas de inteligência artificial de outros sistemas de software mais simples, capazes de executar operações automaticamente a partir de regras definidas por pessoas físicas [29]. Ela constituiu a base para as definições de sistemas de IA estabelecidas pelo Regulamento de Inteligência Artificial da União Europeia [30] e pela minuta da Convenção-Quadro sobre Inteligência Artificial, Direitos Humanos, Democracia e Estado de Direito [31] adotada no âmbito do CAI, do qual o Uruguai participa como observador.

Evolução da definição

A Recomendação da OCDE sobre IA adotada em 2019 [32] definia os sistemas de inteligência artificial "como um sistema baseado em máquinas que pode, para um conjunto determinado de objetivos definidos pelo ser humano, realizar previsões, recomendações ou decisões que afetam ambientes reais ou virtuais. Os

[29] COE (2024). Draft Explanatory Report, Draft Framework Convention on artificial intelligence, human rights, democracy and the rule of law. CM(2024)52-addprov), Par. 24. Disponível para download em: https://www.coe.int/en/web/artificial-intelligence/cai. Último acesso: 16/4/2024.

[30] O artigo 3 do Regulamento de Inteligência Artificial da União Europeia estabelece a seguinte definição: "«sistema de IA»: sistema baseado em máquina, concebido para funcionar com diferentes níveis de autonomia, que pode apresentar adaptabilidade após a implantação e que, para objetivos explícitos ou implícitos, infere, a partir das informações de entrada que recebe, a maneira de gerar informações de saída, como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais". Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf . Último acesso: 16/4/2024.

[31] O artigo 2 da Convenção-Quadro sobre Inteligência Artificial, Direitos Humanos, Democracia e Estado de Direito oferece a seguinte definição: "For the purposes of this Convention, "artificial intelligence system" is a machine-based system that for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that may influence physical or virtual environments. Different artificial intelligence systems vary in their levels of autonomy and adaptiveness after deployment". Disponível em: https://rm.coe.int/-1493-10-1b-committee-on-artificial-intelligence-cai-b-draft-framework/1680aee411 . Último acesso: 16/4/2024.

[32] OCDE, C/MIN(2019)3/FINAL disponível em https://one.oecd.org/document/C/MIN(2019)3/FINAL/en/pdf . Último acesso: 26/4/2024.

sistemas de IA são concebidos para operar com diferentes níveis de autonomia" (tradução não oficial [33]).

Segundo o organismo, as modificações introduzidas em 2023 para refletir as características e o funcionamento atuais dos sistemas de inteligência artificial buscam [34]:

- Esclarecer os objetivos de um sistema de IA, que podem ser explícitos ou implícitos.
- Refletir que a entrada recebida pelo sistema pode ser fornecida por seres humanos ou máquinas.
- Especificar que a Recomendação se aplica a sistemas de IA generativa.
- Substituir o termo "real" por "físico" para se referir aos ambientes.
- Refletir o fato de que alguns sistemas de IA podem continuar evoluindo após sua concepção e implementação.

A esse respeito, o memorando explicativo indica que [35]:

- Embora a definição e o desenvolvimento dos objetivos de um sistema de IA sempre possam ser rastreados até um ser humano que dá origem ao processo de desenvolvimento do sistema, alguns tipos de sistemas podem desenvolver subobjetivos implícitos e, às vezes, estabelecer objetivos para outros sistemas.
- Embora a supervisão humana possa ocorrer em qualquer fase do ciclo de vida do sistema de IA, alguns sistemas de IA podem gerar resultados

[33] Texto original em inglês: "AI system: An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy"

[34] Ver informações de contexto (Background information) em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#backgroundInformation . Último acesso:16/4/2024.

[35] OCDE (2024), "Memorando explicativo sobre a definição atualizada de um sistema de IA da OCDE", OECD Artificial Intelligence Papers, nº 8, OECD Publishing, Paris. Disponível em: https://doi.org/10.1787/623da898-en . Último acesso:16/4/2024.

sem que estes sejam descritos explicitamente no objetivo do sistema de IA e sem instruções específicas dos seres humanos.

• Alguns sistemas podem desenvolver a capacidade de realizar novas formas de inferência não previstas inicialmente quando foram programados, isto é, modificar seu comportamento por meio da interação direta com entradas e dados, antes ou depois de sua implantação.

• A referência a “inferir” deve ser entendida como “gerar saídas” a partir de entradas. O conceito de saída(s), por sua vez, refere-se aos resultados gerados por um sistema de IA, que variam em função das diferentes capacidades e funcionalidades desempenhadas.

Em suma, as definições da OCDE que serão consideradas são:

Sistema de IA: um sistema de IA é um sistema baseado em máquina que, para objetivos explícitos ou implícitos, infere, a partir das entradas que recebe, como gerar resultados, como previsões, conteúdos, recomendações ou decisões que podem influenciar ambientes físicos ou virtuais. Os diferentes sistemas de IA variam em seus níveis de autonomia e adaptabilidade após a implantação.

Ciclo de vida do sistema de IA: as fases do ciclo de vida do sistema de IA envolvem: i) “concepção, dados e modelos”, uma sequência dependente do contexto que abrange planejamento e concepção, coleta e processamento de dados, assim como construção de modelos; ii) “verificação e validação”; iii) “implantação”; e iv) “operação e acompanhamento”. Essas fases costumam ocorrer de forma iterativa, não necessariamente sequencial. A decisão de retirar um sistema de IA de operação pode ocorrer a qualquer momento durante a fase de operação e monitoramento.

Conhecimento de IA: refere-se às habilidades e aos recursos, como dados, códigos, algoritmos, modelos, pesquisas, conhecimentos técnicos, programas de capacitação, governança, processos e boas práticas, necessários para compreender o ciclo de vida do sistema de IA e participar dele.

Atores de IA: são aqueles que desempenham um papel ativo no ciclo de vida do sistema de IA, incluindo as organizações e os indivíduos que implementam ou operam IA.

A seguir, são abordados outros conceitos fundamentais que contribuem para compreender as características e o funcionamento dos sistemas de IA.

Machine learning

O aprendizado de máquina, ou Machine learning (ML), é um campo da Inteligência Artificial.

Nas palavras da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO), “é um conjunto de técnicas que permite às máquinas aprender automaticamente usando padrões e deduções, em vez de instruções diretas de uma pessoa. As técnicas de ML frequentemente ensinam as máquinas a alcançar um resultado fornecendo numerosos exemplos de resultados corretos. No entanto, também podem especificar um conjunto de padrões e deixar que a máquina os descubra por si mesma nos dados” [36].

O modelo é treinado a partir de dados de entrada que podem ser rotulados (aprendizado de máquina supervisionado) ou não rotulados (aprendizado de máquina não supervisionado). Um terceiro tipo é o chamado aprendizado por reforço, que envolve a melhoria contínua do modelo com base na retroalimentação [37].

A eficácia dos modelos de aprendizado de máquina depende, entre outros fatores, do volume e da qualidade dos dados de treinamento.

[36] UNESCO (2023). Kit global de ferramentas sobre IA e Estado de Direito para o Poder Judiciário. CI/DIT/2023/AIRoL/01. Glossário. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000387331_spa . Último acesso:16/4/2024.

[37] UNESCO (2021). Inteligência artificial e educação: guia para formuladores de políticas, P.9. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000379376 . Último acesso:16/4/2024.

Redes neurais artificiais

Uma rede neural artificial (RNA) inspira-se na estrutura das redes neurais do cérebro humano.

Segundo a descrição da UNESCO, as redes neurais artificiais “são um tipo de técnica de aprendizado de máquina que permite aos computadores aprender a realizar tarefas por meio da análise de exemplos de treinamento” 38. Uma RNA é concebida com nós de processamento interconectados, geralmente organizados em camadas. Cada nó recebe dados dos nós da camada inferior e envia dados aos nós da camada superior [39].

Deep Learning

O aprendizado profundo (Deep Learning) foi definido pela UNESCO como uma técnica de ponta do aprendizado de máquina que “permite à máquina reconhecer, por si mesma, conceitos complexos, como rostos, corpos humanos ou imagens de gatos, examinando milhões de imagens extraídas da Internet, sem que essas imagens tenham sido previamente rotuladas por humanos. Nascido da combinação de algoritmos de aprendizado de máquina com redes neurais formais e com o uso de grandes volumes de dados, o Deep Learning revolucionou a inteligência artificial” [40].

IA Generativa

A inteligência artificial generativa é um subconjunto do Deep Learning. A IA generativa aprende padrões em um conteúdo para gerar conteúdo novo. A saída (output) da IA será baseada nos grandes volumes de dados com os quais o modelo foi

[38] UNESCO (2023). Kit global de ferramentas sobre IA e Estado de Direito para o Poder Judiciário. CI/DIT/2023/AIRoL/01. Glossário. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000387331_spa . Último acesso:16/4/2024.
[39] UNESCO (2023). Kit global de ferramentas sobre IA e Estado de Direito para o Poder Judiciário. CI/DIT/2023/AIRoL/01. Glossário. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000387331_spa . Último acesso:16/4/2024.
[40] UNESCO. Léxico da Inteligência Artificial. Disponível em: https://www.unesco.org/es/articles/lexico-de-la-inteligencia-artificial-0 . Último acesso:16/4/2024.

treinado. O novo conteúdo pode se apresentar em diferentes formatos: textos escritos em linguagem natural, imagens, áudio e código de software.

Nas palavras da UNESCO, “a IA generativa é uma tecnologia de inteligência artificial que gera conteúdos automaticamente em resposta a instruções escritas em interfaces conversacionais de linguagem natural (prompts)” [41].

As técnicas utilizadas na IA generativa variam.

Assim, por exemplo, explica a UNESCO, a IA generativa de textos “utiliza um tipo de rede neural artificial conhecido como transformador de propósito geral, e um tipo de transformador de propósito geral chamado grande modelo de linguagem. Por isso, os sistemas de inteligência artificial generativa de texto costumam ser denominados grandes modelos de linguagem (ou LLMs). O tipo de grande modelo de linguagem utilizado pela inteligência artificial generativa é conhecido como transformador generativo pré-treinado, ou GPT, na sigla em inglês” (UNESCO, 2023).

Em sentido semelhante, a Ordem Executiva de outubro de 2023 dos Estados Unidos sobre o desenvolvimento e o uso da inteligência artificial de forma segura e confiável define IA generativa como “a classe de modelos de IA que emulam a estrutura e as características dos dados de entrada para gerar conteúdos sintéticos derivados. Isso pode incluir imagens, vídeos, áudio, texto e outros conteúdos digitais” (tradução não oficial) [42].

Modelos fundacionais ou de uso geral

São modelos com amplas capacidades que se adaptam a diferentes cenários.

No Regulamento de IA da União Europeia, são definidos como um modelo de IA treinado com um grande volume de dados, utilizando autossupervisão em grande

[41] UNESCO (2023). Kit global de ferramentas sobre IA e Estado de Direito para o Poder Judiciário. CI/DIT/2023/AIRoL/01. Glossário. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000387331_spa . Último acesso:16/4/2024.

[42] Ver artigo 3, alínea p. Disponível em: 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/ Último acesso: 22/06/2024.

escala, que apresenta um grau considerável de generalidade e é capaz de realizar competentemente uma ampla variedade de tarefas distintas; pode ser integrado a diversos sistemas ou aplicações posteriores [43].

Entidades que contribuíram para a elaboração do relatório

Para elaborar este relatório, a Agesic contou com contribuições de representantes de diferentes unidades executoras e entidades que participaram dos grupos de trabalho associados aos eixos temáticos mencionados a seguir, incluindo: Presidência da República (Subsecretaria da Presidência e Secretaria de Direitos Humanos), Ministério da Educação e Cultura (Conselho de Direitos Autorais), Ministério da Economia e Finanças (Unidade de Defesa do Consumidor), Ministério da Indústria, Energia e Mineração (Direção Nacional de Telecomunicações e Direção Nacional da Propriedade Industrial), Ministério do Trabalho e Seguridade Social (Inspeção-Geral do Trabalho e da Seguridade Social), Unidade Reguladora de Serviços de Comunicações, Agência Nacional de Pesquisa e Inovação, Programa Uruguay Innovation Hub, Unidade Reguladora e de Controle de Dados Pessoais e Instituição Nacional de Direitos Humanos e Defensoria do Povo.

Também foram recebidas contribuições no processo de consulta da Asociación de Escribanos del Uruguay (AEU), do Laboratorio de Datos y Sociedad (DATYSOC), da DATA Uruguay, da Cámara Uruguaya de Tecnologías de la Información (CUTI) e da Instituição Nacional de Direitos Humanos e Defensoria do Povo (INDDHH).

Embora nem todas as recomendações de quem respondeu à consulta tenham sido incorporadas, considerou-se necessário acrescentar a documentação enviada para ilustrar as diferentes perspectivas apresentadas. Ela consta do Anexo a este relatório.

[43] Ver artigo 3. Item 63. Disponível em: Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf . Último acesso: 22/06/2024.

Eixos temáticos considerados

Aspectos gerais

Na elaboração do relatório, considerando os avanços e os subsídios obtidos dos processos de revisão e criação das Estratégias Nacionais de Dados e de IA, respectivamente, foram definidos os seguintes eixos temáticos:

- Institucionalidade e governança
- Direitos humanos
- Trabalho e capacitação
- Propriedade intelectual
- Responsabilidade civil e relações de consumo
- Infraestrutura e cibersegurança
- Medidas de promoção

As páginas seguintes reproduzem o alcance desses eixos.

Eixo de institucionalidade e governança

Considerações preliminares

O objetivo deste eixo é determinar os aspectos fundamentais para assegurar uma institucionalidade adequada da IA em nosso país.

A institucionalidade da IA e a institucionalidade dos dados, assim como a governança da IA e a governança dos dados, estão inevitavelmente ligadas, em razão da relação de dependência da primeira em relação aos segundos. Neste eixo, a Agesic propõe abordar a institucionalidade pela perspectiva da estrutura necessária para desenvolver, monitorar e auditar uma política pública de IA e dados, das competências exigidas no âmbito interno das organizações públicas e das normas que já regulam a forma de governar os dados em nível nacional.

Quanto à institucionalidade para IA, é importante considerar antecedentes internacionais, mas sob o prisma das características locais, pois estruturas que em outros países ou regiões possam ter aplicação

efetiva podem não ser eficientes ou ser diretamente inadequadas para nosso país, e vice-versa.

Um exemplo de estruturas diferentes ligadas à gestão de dados e também à IA é a forma como se regulou a organização da proteção dos dados pessoais. Em nosso país, a Lei nº 18.331, de 11 de agosto de 2008, cria um órgão desconcentrado da Agesic, denominado Unidade Reguladora e de Controle de Dados Pessoais (Urcdp), com competência para determinar seu próprio orçamento e autonomia técnica, sem deixar de integrar a estrutura hierárquica da Presidência da República.

Em outros países da América Latina, existem entidades autárquicas — como a Agência de Acesso à Informação Pública da República Argentina, a Autoridade Nacional de Proteção de Dados do Brasil ou o Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais do México — ou entidades subordinadas a ministérios — como na Colômbia, onde a entidade de proteção de dados é uma unidade delegada da Superintendência de Indústria e Comércio do Ministério do Comércio, Indústria e Turismo. Algumas dessas entidades têm competências compartilhadas de proteção de dados e acesso à informação pública; algumas dispõem de poderes sancionatórios para todo o conjunto de responsáveis, enquanto outras distinguem entre públicos e privados.

Esse conjunto de diferenças não impede que desenvolvam suas atividades nas respectivas jurisdições nacionais, representem seus países na matéria, façam recomendações e imponham as sanções cabíveis pelo descumprimento da lei.

O objetivo desta exposição é esclarecer que a institucionalidade da IA no Uruguai deverá, sim, contemplar os antecedentes internacionais e nacionais associados ao tema, mas, reiteramos, analisados à luz das características locais.

Juntamente com a institucionalidade da IA, é fundamental considerar a governança dos dados, por ser esta um dos elementos essenciais para o desenvolvimento dos sistemas de IA. A governança dos dados inclui diferentes tipos

de dados — pessoais e não pessoais —, sua gestão, as entidades que geram e gerem esses dados, sua reutilização, a interoperabilidade e, em suma, os padrões que tanto o setor público quanto o privado devem cumprir no uso de dados que alimentem ou sejam gerados por sistemas de IA.

Seleção de antecedentes internacionais

O texto atual da Convenção de IA do Conselho da Europa (CoE) [44] estabelece, em seu artigo 1, que as partes devem adotar e manter medidas legislativas, administrativas ou outras apropriadas para dar efetividade às disposições da convenção. Essas medidas devem ser graduadas e diferenciadas conforme a gravidade e a probabilidade de impactos adversos nos direitos humanos, na democracia e no Estado de Direito. A Convenção prevê, com nuances, a aplicabilidade de suas disposições nos âmbitos público e privado.

Quanto à inovação, a Convenção prevê a possibilidade de estabelecer ambientes controlados para o desenvolvimento e a experimentação de sistemas de inteligência artificial sob a supervisão de autoridades competentes. Cabe lembrar que o artigo 75 da Lei nº 20.212 previu a possibilidade de criar ambientes controlados de testes ou sandboxes regulatórios, em processo de regulamentação pela Agesic com a colaboração de outras entidades.

A transparência é um princípio central no âmbito da Convenção: o conhecimento efetivo das pessoas de que estão interagindo com um sistema de IA e os mecanismos de supervisão são partes integrantes dessa transparência.

Quanto ao Regulamento Europeu de IA [45], seu Título VI trata da governança da IA, criando, em seus capítulos, o Comitê Europeu de Inteligência Artificial (órgão comunitário integrado por autoridades nacionais de supervisão), com poderes para auxiliar as autoridades nacionais, coordenar orientações e análises e contribuir para uma cooperação efetiva.

[44] https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence . Último acesso: 13/06/2024.
[45] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52021PC0206 . Último acesso: 19/03/2024.

O capítulo 2 do Título VI do Regulamento trata das Autoridades Nacionais Competentes, cuja finalidade é garantir sua aplicação e execução e que deverão preservar a objetividade e a imparcialidade de suas atividades e funções. Elas deverão contar com recursos financeiros e humanos adequados e conhecimento aprofundado em tecnologias de IA, dados, computação de dados, riscos para os direitos fundamentais, saúde e segurança, além de conhecimento sobre normas e requisitos legais vigentes.

O Regulamento Europeu de IA, ou Lei de IA da UE, integra um conjunto de regulações sobre governança dos dados que buscam — no âmbito da Estratégia Europeia de Dados [46] — criar um mercado único em que os dados circulem livremente entre diferentes setores da sociedade. Esse ecossistema é composto pela Digital Services Act, pela Digital Governance Act, pela Digital Markets Act, pela Data Act, pela e-Privacy Regulation e pelo GDPR (Regulamento Europeu de Proteção de Dados).

Nos Estados Unidos, há a Ordem Executiva sobre o desenvolvimento e o uso seguro, confiável e fidedigno de sistemas de Inteligência Artificial [47]. Ela enfatiza 8 princípios que devem ser cumpridos pelas entidades do Governo Federal para alcançar os objetivos pretendidos e estabelece ações relacionadas à IA que diferentes agências do governo federal devem adotar em seus respectivos âmbitos de competência. Não se prevê uma autoridade central exclusiva com competências em IA, mas uma distribuição das questões de IA entre as instituições legalmente competentes.

Não se pode ignorar a influência da República Popular da China na matéria. Além de normas preexistentes de cibersegurança e proteção de dados pessoais, ela promoveu medidas para regular a IA em geral e a IA generativa em particular. Preveem-se, assim, medidas específicas de transparência no uso de sistemas de IA, salvaguardas para determinados usos, aprovação

46 Mais informações sobre essa estratégia estão disponíveis em: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_en . Último acesso: 21/06/2024.

47 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/ . Último acesso: 19/3/2024.

governamental para usos incluídos em listas, prevenção da discriminação, exercício de direitos pelos usuários e responsabilidades sujeitas a sanções de multa [48].

O Reino Unido, por sua vez, publicou um documento com uma abordagem favorável à inovação na regulação de IA [49], após uma consulta pública realizada durante 1 ano. Além disso, criou um Escritório de Inteligência Artificial, vinculado ao Departamento de Ciência, Inovação e Tecnologia, e uma Unidade de Adoção Responsável de Tecnologia. Esta última tem como objetivo promover a inovação responsável nos setores público e privado, desenvolvendo ferramentas para gerar confiança, no âmbito interno das organizações, nos sistemas de IA e de gestão de dados. Antes disso, e até junho de 2023, havia um Conselho de IA composto por especialistas de múltiplos setores, com o objetivo de contribuir para o desenvolvimento da estratégia de IA.

Atualmente, o governo do Reino Unido também possui um Escritório Central Digital e de Dados, que lidera as funções digitais, de dados e de tecnologias do governo e trabalha particularmente no desenvolvimento da política e da estratégia de IA, incluindo padrões para o uso governamental.

Todas essas disposições demonstram uma ênfase particular na forma de usar os dados e nos princípios que devem orientar as regulações. Também existe uma tendência a gerar esquemas de governança com a participação de múltiplos atores, sem prejuízo da liderança de um órgão dentro da estrutura estatal.

[48] Uma síntese do que esperar da legislação chinesa pode ser encontrada no Observatório Parlamentar, Programa Ásia-Pacífico da Biblioteca Nacional do Chile, disponível em https://www.bcn.cl/observatorio/asiapacifico/noticias/andamiaje-institucional-inteligencia-artificial-china . Último acesso: 21/06/2024. Além disso, uma tradução para o inglês da proposta legislativa pode ser encontrada no site do “Center for Security and Emerging Technology - Georgetown University’s Walsh School of Foreign Service” https://cset.georgetown.edu/publication/china-ai-law-draft/ . Último acesso: 21/06/202.

[49] https://www.gov.uk/government/consultations/ai-regulation-a-pro-innovation-approach-policy-proposals/outcome/a-pro-innovation-approach-to-ai-regulation-government-response . Último acesso: 19/3/2024.

Observa-se também a necessidade de enfatizar fortemente o componente da inovação responsável e de garantir a proteção dos direitos humanos, sendo a capacitação dos quadros técnicos vinculados a essa entidade reguladora um elemento central.

Diagnóstico sobre institucionalidade e governança da IA

De acordo com as normas levantadas, do ponto de vista institucional existem duas entidades com atribuições para estabelecer critérios gerais na matéria: a Agesic e a Urcdp.

O artigo 74 da Lei nº 20.212 determina a concepção e a implementação da Estratégia de Dados e de Inteligência Artificial, atribuindo sua liderança à Agesic. No âmbito dessas competências, a Agência pode criar grupos de trabalho e outros espaços com diferentes atores que colaborem na implementação das estratégias.

Com base nesse artigo, a Agesic criou recentemente o Comitê Estratégico do Setor Público para Inteligência Artificial e Dados, composto por representantes da Agência, do Ministério da Indústria, Energia e Mineração, do Ministério da Educação e Cultura, do Ministério do Trabalho e Seguridade Social, do Ministério da Economia e Finanças, do Instituto Nacional de Estatística, do Instituto Nacional de Direitos Humanos e Defensoria do Povo, da Agência Nacional de Pesquisa e Inovação e da Unidade Reguladora e de Controle de Dados Pessoais.

Além disso, o último parágrafo do artigo 74 prevê uma atribuição que vai além da estratégia e se refere ao desenvolvimento de sistemas de inteligência artificial, para o qual a Agesic poderá estabelecer critérios e definir mecanismos de fiscalização de seu cumprimento. Esse parágrafo estabelece especificamente: “A AGESIC fará recomendações específicas a entidades do setor público e do setor privado para o desenvolvimento e a implementação dos sistemas de inteligência artificial mencionados e para a fiscalização de seu cumprimento, sem prejuízo das competências próprias da URCDP e de outras entidades públicas em seus respectivos âmbitos de atuação”.

Em conformidade com essa disposição, estabelece-se que essa competência é exercida sem prejuízo, em primeiro lugar, das competências da Urcdp, que pode definir critérios para o uso de dados pessoais em qualquer operação de tratamento, especialmente naquelas previstas no artigo 16 da Lei nº 18.331 — tratamentos automatizados que gerem, entre outros resultados, perfis das pessoas —, de acordo com o artigo 34 dessa lei.

Quanto à institucionalidade, cabe mencionar neste diagnóstico as reflexões surgidas do processo de consulta. A INDDHH propõe que, diante das atribuições de estabelecer critérios gerais e fiscalizar atribuídas à Agesic e à Urcdp, seu âmbito de atuação deveria se situar fora do Poder Executivo, sugerindo especificamente a forma jurídica de serviço descentralizado.

A esse respeito, esta Agência considera que, embora a proposta seja compreensível e mereça consideração, a institucionalidade existente permitiria uma governança adequada da IA, pelo menos atualmente. Sem prejuízo disso, a proposta completa da INDDHH é anexada para consideração pelo Poder Legislativo.

Em suas contribuições, a CUTI afirma que a institucionalidade existente no Uruguai seria adequada para tratar os desafios apresentados, sem prejuízo da necessidade de grupos consultivos com a participação de múltiplos atores e papel relevante na definição das políticas.

Para que a governança da IA e a adoção dessa tecnologia ocorram de forma confiável e responsável, também devem ser consideradas medidas para uma governança e gestão adequadas dos dados. Os dados são um dos principais insumos dessa tecnologia e seu principal resultado. Para que sejam confiáveis e possam ser utilizados, é importante assegurar uma gestão adequada, definindo e adotando normas, políticas e diretrizes. Para isso, é relevante considerar padrões nacionais, regionais e internacionais na matéria.

Embora nosso país não conte com uma governança de dados plenamente estabelecida no setor público, há avanços que contribuem para sua construção.

A Agesic possui determinadas competências nesse campo, como as normas de intercâmbio de informações e interoperabilidade, governo aberto e dados abertos, compiladas no Decreto nº 184/015, de 14 de julho de 2015. Além disso, as unidades desconcentradas da Agência, a Urcdp e a Unidade de Acesso à Informação Pública (Uaip), têm competência nacional sobre a gestão das informações pessoais e das informações públicas, respectivamente.

As contribuições à consulta sugeriram mecanismos específicos de proteção dos dados (como a análise dos fideicomissos de dados propostos pela INDDHH), a adoção de mecanismos para resolver conflitos entre a promoção da inovação no desenvolvimento de serviços públicos e o impacto de um eventual fracasso nesse âmbito (CUTI) e a geração de padrões que permitam avaliar soluções uruguaias e "exportá-las" (CUTI).

Quanto à forma de utilizar os sistemas de IA, a AEU menciona a importância de considerar setores ou usos específicos, particularmente no âmbito judicial (propondo sistemas de "caixa branca" baseados em técnicas para realizar previsões, classificações e detecções inteligentes), do scoring (enfatizando a impossibilidade de usar dados que não integrem aqueles empregados para a finalidade determinada e a necessidade de explicabilidade) e contratual e notarial (nos quais desaconselha o uso de dados sintéticos).

Eixo de direitos humanos

Considerações preliminares

O objetivo deste eixo é apresentar os riscos que não podem ser ignorados no desenvolvimento de uma política pública de IA e que podem exigir — se considerado necessário — medidas especiais em razão de seu impacto nos direitos das pessoas.

Além disso, o objetivo é identificar medidas para aproveitar os sistemas de IA em benefício das pessoas e de seus direitos, particularmente medidas de natureza normativa.

Para isso, serão consideradas as normas e obrigações internacionais conexas do direito internacional dos direitos humanos ratificadas pelo país, as recomendações específicas sobre IA feitas por organismos internacionais e a regulação vigente ou em elaboração nos âmbitos regional e internacional.

Os impactos da IA nos direitos humanos têm sido analisados em diferentes fóruns. No Evento Paralelo de Alto Nível do 53º Período de Sessões do Conselho de Direitos Humanos [50], o Alto Comissário das Nações Unidas para os Direitos Humanos, Volker Turk, observou que, no mundo e no momento atuais, os direitos humanos estão sendo postos à prova e que a pergunta sobre os limites da IA é uma das "(…) questões mais urgentes para nossa sociedade, para os governos e para o setor privado". O Alto Comissário aponta duas correntes sobre a regulação da IA: a) uma se concentra nos riscos, na autorregulação e na autoavaliação pelos desenvolvedores, atribuindo responsabilidade muito grande ao setor privado; b) a segunda integra os direitos humanos em todo o ciclo de vida da IA, incorporando seus princípios desde "(…) a coleta e a seleção de dados, assim como à concepção,

[50] O discurso do Alto Comissário pode ser encontrado em: https://www.ohchr.org/es/statements/2023/07/artificial-intelligence-must-be-grounded-human-rights-says-high-commissioner . Último acesso: 20/03/2024.

ao desenvolvimento, à implementação e ao uso dos modelos, instrumentos e serviços resultantes".

Nesse ponto, o Alto Comissário apresenta algumas propostas: 1) ouvir os grupos mais vulneráveis ao uso dessa tecnologia; 2) prestar atenção ao uso da IA nos serviços públicos e privados em que haja maior risco de abuso de poder ou intrusão na privacidade; 3) exigir avaliação de riscos e impactos nos direitos humanos antes, durante e depois do uso de sistemas de IA (transparência, supervisão independente e acesso a recursos efetivos); 4) proibir ou suspender tecnologias de IA que não cumpram as normas internacionais de direitos humanos; 5) aplicar a regulação de proteção de dados e outras legislações setoriais de proteção já existentes; 6) não permitir uma abordagem baseada apenas na autorregulação; 7) criar um órgão consultivo internacional.

Em nosso país, quanto à política de direitos humanos, deve ser especialmente mencionado o Plano Nacional de Direitos Humanos 2023-2027, que inclui o impacto da inteligência artificial, entre outros temas, e a necessidade de avançar rumo aos ideais da Declaração Universal dos Direitos Humanos. Esse Plano complementa os objetivos mencionados acima ao estabelecer mecanismos de articulação, marcos normativos e protocolos de atuação que permitam incorporar a abordagem de direitos humanos a políticas públicas como a que se pretende institucionalizar no tema da IA. Assim, parece relevante acompanhar o desenvolvimento das diretrizes apresentadas para incluir a IA nos objetivos definidos.

Seleção de antecedentes internacionais

A já mencionada "Recomendação sobre a Ética da Inteligência Artificial" destaca o papel da proteção dos direitos humanos no desenvolvimento ético de sistemas de IA, baseado em princípios de transparência e equidade.

A recomendação também considera os seguintes instrumentos: a Declaração Universal dos Direitos Humanos (1948), os instrumentos do marco internacional dos direitos humanos, entre eles a Convenção relativa ao

Estatuto dos Refugiados (1951), a Convenção sobre Discriminação em Matéria de Emprego e Ocupação (1958), a Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Racial (1965), o Pacto Internacional sobre Direitos Civis e Políticos (1966), o Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais (1966), a Convenção sobre a Eliminação de Todas as Formas de Discriminação contra a Mulher (1979), a Convenção sobre os Direitos da Criança (1989), a Convenção sobre os Direitos das Pessoas com Deficiência (2006), a Convenção relativa à Luta contra a Discriminação no Campo do Ensino (1960) e a Convenção sobre a Proteção e Promoção da Diversidade das Expressões Culturais (2005), assim como quaisquer outros instrumentos, recomendações e declarações internacionais pertinentes. Registra-se ainda a Declaração sobre o Direito ao Desenvolvimento (1986); a Declaração sobre as Responsabilidades das Gerações Presentes em Relação às Gerações Futuras (1997); a Declaração Universal sobre Bioética e Direitos Humanos (2005); a Declaração das Nações Unidas sobre os Direitos dos Povos Indígenas (2007); a resolução da Assembleia Geral das Nações Unidas sobre a revisão da Cúpula Mundial sobre a Sociedade da Informação (A/RES/70/125) (2015); a resolução da Assembleia Geral das Nações Unidas intitulada “Transformar nosso mundo: a Agenda 2030 para o Desenvolvimento Sustentável” (A/RES/70/1) (2015); a Recomendação referente à Preservação do Patrimônio Documental, Incluindo o Patrimônio Digital, e ao Acesso a Ele (2015); a Declaração de Princípios Éticos em Relação à Mudança Climática (2017); a Recomendação sobre a Ciência e os Pesquisadores Científicos (2017); os indicadores de universalidade da Internet (aprovados em 2018 pelo Programa Internacional para o Desenvolvimento da Comunicação da UNESCO), incluindo os princípios ROAM (aprovados pela Conferência Geral da UNESCO em 2015); a resolução do Conselho de Direitos Humanos sobre “O direito à privacidade na era digital” (A/HRC/RES/42/15) (2019); e a resolução do Conselho de Direitos Humanos intitulada “As tecnologias digitais novas e emergentes e os direitos humanos” (A/HRC/RES/41/11) (2019).

Com base nesses antecedentes, a UNESCO recomenda aos Estados-membros a aplicação de medidas adequadas — legislativas e outras — para dar efetividade aos

princípios e às normas desenvolvidos, em conformidade com o direito internacional e, em especial, com o direito internacional dos direitos humanos.

A recomendação explicita, em particular, que os sistemas de IA devem melhorar a qualidade de vida dos seres humanos, que não devem sofrer nenhum tipo de dano em qualquer etapa de seu ciclo de vida. Destaca também a necessidade de meios para promover, defender e exercer os direitos humanos. Para isso, propõe os princípios de proporcionalidade e não causar danos; segurança e proteção; equidade e não discriminação; sustentabilidade; direito à privacidade e proteção de dados; supervisão e decisão humanas; transparência e explicabilidade; responsabilidade e prestação de contas; conscientização e educação; e governança e colaboração adaptativas de múltiplas partes interessadas. Esses princípios estão associados a medidas concretas que serão analisadas adiante, destacando-se a chamada Avaliação de Impacto Ético.

A Avaliação de Impacto Ético propõe que os Estados-membros estabeleçam "(…) marcos de avaliação de impacto, como avaliações de impacto ético, para determinar e analisar os benefícios, os problemas e os riscos dos sistemas de IA, assim como medidas adequadas de prevenção, mitigação e acompanhamento dos riscos, entre outros mecanismos de garantia. Essas avaliações de impacto deveriam revelar as repercussões nos direitos humanos e nas liberdades fundamentais, particularmente, mas não exclusivamente, nos direitos das pessoas marginalizadas, vulneráveis ou em situação de vulnerabilidade, nos direitos trabalhistas, no meio ambiente e nos ecossistemas, assim como as consequências éticas e sociais, e facilitar a participação cidadã, em conformidade com os valores e princípios enunciados nesta Recomendação".

Como mencionado anteriormente, a recente resolução da Assembleia Geral da ONU [51] para a promoção de sistemas de IA seguros e confiáveis que

[51] Mais informações podem ser obtidas em: https://news.un.org/es/story/2024/03/1528511#:~:text=La%20Asamblea%20General%20de%20la%20ONU%20adopt%C3%B

permitam alcançar os Objetivos de Desenvolvimento Sustentável (ODS) contém, em particular, recomendações de medidas a serem adotadas pelos Estados-membros.

Também no âmbito da ONU, merece destaque especial o documento de dezembro de 2023 “Interim Report: Governing AI for Humanity” [52], que contém, entre outros elementos, uma categorização dos riscos sob a perspectiva da vulnerabilidade existente ou potencial das pessoas, dos grupos, da economia, dos (eco)sistemas, dos valores e normas e da sociedade. Isso além de considerar, como princípio orientador da governança da IA, as normas internacionais de direitos humanos e os compromissos assumidos nos ODS.

Ainda nos antecedentes internacionais, a regulação comunitária da União Europeia, aprovada pelos países membros em 13 de março de 2024, estabelece alguns aspectos relevantes destacados pela própria organização [53]:

1) Regras para diferentes tipos de riscos:

    a. Riscos inaceitáveis, proibidos por constituírem uma ameaça às pessoas: manipulação cognitiva do comportamento de grupos vulneráveis, “scoring” social, identificação e categorização biométrica de pessoas e sistemas de identificação biométrica remota e em tempo real — neste caso, existem exceções baseadas em finalidades policiais.

    b. Riscos altos, divididos em duas categorias e que exigem uma avaliação antes de sua entrada em produção: i. sistemas utilizados em produtos abrangidos pela legislação de segurança de produtos da UE (brinquedos, aviação, automóveis, dispositivos médicos e elevadores); ii. sistemas de áreas

3%20por,que%20beneficien%20tambi%C3%A9n%20al%20desarrollo%20sostenible%20para%20todos . Último acesso: 25/03/2024.

[52] Disponível em https://www.un.org/sites/un2.un.org/files/un_ai_advisory_body_governing_ai_for_humanity_interim_report.pdf . Último acesso: 02/04/2024.

[53] Ver a respeito: https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence . Último acesso: 24/03/2024.

específicas que devem ser registrados em uma base de dados da UE (gestão e operação de infraestrutura crítica, capacitação profissional e educação, trabalho, gestão de trabalhadores e acesso ao emprego, acesso e usufruto de serviços privados essenciais e serviços públicos e benefícios, aplicação da lei, migração, asilo e gestão do controle de fronteiras, assistência na interpretação e aplicação jurídica da lei)

2) Requisitos de transparência. Alguns sistemas de IA, como a IA generativa, mesmo quando não são considerados de alto risco, devem cumprir requisitos de transparência e normas de propriedade intelectual, a saber:

a. Revelar que o conteúdo foi gerado por IA

b. Conceber o modelo para evitar que gere conteúdo ilícito

c. Publicar resumos dos dados sujeitos à propriedade intelectual usados no treinamento

Modelos de IA de uso geral de alto impacto que possam gerar risco sistêmico deverão ser avaliados e, se sofrerem incidentes graves, estes devem ser comunicados à Comissão Europeia.

Da mesma forma, o conteúdo gerado e modificado com ajuda de IA deve ser identificado para que os usuários tomem conhecimento dessa circunstância.

3) Apoio à inovação. Por meio da criação de condições que estimulem o teste de modelos de IA antes de sua entrada em produção.

No Reino Unido, a proposta regulatória apresentada e submetida a consulta pública ao longo do ano passado teve como objetivo alcançar uma abordagem favorável à inovação e à segurança.

Essa proposta distingue 3 categorias de riscos: 1) riscos sociais; 2) riscos de mau uso; 3) riscos de autonomia. Entre os primeiros, menciona o mundo do trabalho, a inovação e a propriedade intelectual, a proteção das pessoas contra vieses e discriminação, a proteção dos dados pessoais, a confiança e a segurança no conteúdo on-line, a garantia da concorrência nos

mercados digitais e as boas práticas no setor público. Quanto ao segundo tipo de risco, menciona resguardar a democracia contra interferências nos processos eleitorais e prevenir o mau uso da tecnologia. Por fim, o último tipo de risco se refere ao alcance do controle das pessoas sobre os sistemas de IA.

A distinção entre riscos também está presente em projetos discutidos na América do Sul, como o Projeto nº 2338 [54] da República Federativa do Brasil, que distingue sistemas de risco alto e excessivo e prevê a possibilidade de impor medidas rigorosas para seu desenvolvimento e implementação. O governo chileno, por sua vez, enviou ao Parlamento, em 7 de maio de 2024, um projeto de lei [55] que também distingue sistemas de IA de risco inaceitável e de alto risco e acrescenta os de risco limitado.

Em outubro de 2023, o governo dos Estados Unidos emitiu uma Ordem Executiva sobre o Desenvolvimento Seguro e Confiável da Inteligência Artificial, aplicável pelas agências governamentais [56]. As medidas previstas incluem a criação de padrões de segurança; a proteção da privacidade dos estadunidenses; avanços em direitos civis e equidade; proteção a consumidores, pacientes e estudantes; apoio aos trabalhadores; promoção da inovação e da concorrência; fortalecimento da liderança dos Estados Unidos no exterior; e garantia do uso governamental responsável e efetivo da IA (o anexo de normas internacionais apresenta as medidas em mais detalhes).

[54] https://legis.senado.leg.br/sdleg-getter/documento?dm=9347622&ts=1718367327465&disposition=inline . Último acesso: 13/06/2024.

[55] https://www.camara.cl/verDoc.aspx?prmID=17048&prmTIPO=INICIATIVA . Último acesso: 14/06/2024.

[56] 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/ Último acesso: 24/03/2024.

Diagnóstico sobre IA e direitos humanos

O diagnóstico deste eixo se concentra em 5 aspectos centrais, vinculados aos pontos mencionados pelo Alto Comissário das Nações Unidas para os Direitos Humanos e detalhados acima.

1. É necessário reforçar a aplicação das normas e dos princípios de direitos humanos preexistentes por meio de instrumentos normativos que explicitem e especifiquem sua aplicação transversal no âmbito da IA e/ou como pilares da política nacional, além da previsão do Art. 74 para a Estratégia Nacional de IA?

2. A autorregulação pode se constituir em recurso efetivo para orientar as ações de entidades públicas e privadas no desenvolvimento da IA?

3. A abordagem de riscos é suficiente? Como consequência, existem sistemas de IA que, por seu impacto nos direitos das pessoas, devam ser proibidos ou limitados, ou exijam medidas especiais?

4. Quais garantias de transparência e explicabilidade devem ser estabelecidas no desenvolvimento de sistemas de IA centrados nas pessoas?

5. Quais critérios devem orientar a definição de uma política pública associada ao desenvolvimento da IA em nosso país que também permita ampliar seu impacto positivo nos direitos humanos?

Quanto ao alcance da aplicação dos princípios, atualmente, conforme o artigo 74 da Lei nº 20.212, eles se aplicam à concepção e ao desenvolvimento da Estratégia Nacional de Inteligência Artificial e de Dados. Entretanto, sem prejuízo da plena aplicação das normas de direito internacional dos direitos humanos ratificadas pelo país e das obrigações internacionais decorrentes, na medida em que esses princípios foram previstos para o desenvolvimento das referidas Estratégias, cabe considerar se é pertinente explicitá-los normativamente com alcance mais

amplo. Isto é, especificar seu conteúdo normativo pontualmente em relação à política de IA.

Como mencionado, os princípios incluídos no artigo 74 estão alinhados aos consagrados na primeira Convenção Internacional sobre o tema elaborada pelo CoE. Nessa convenção, destacam-se os princípios de dignidade humana e autonomia individual, transparência e supervisão, responsabilidade e prestação de contas, equidade e não discriminação, privacidade e proteção de dados pessoais, confiança e segurança e inovação segura. Segundo a própria definição da convenção, esses princípios se aplicam a todos os sistemas de IA durante todo o seu ciclo de vida.

Quanto à abordagem de riscos, essa perspectiva já está presente na regulação da proteção dos dados pessoais, que também pode ser aplicável aos sistemas de IA quando utilizem ou gerem esse tipo de dado.

Assim, o artigo 12 da Lei nº 18.331, com a redação dada pelo artigo 39 da Lei nº 19.670, de 15 de outubro de 2018, prevê avaliações de impacto na proteção de dados pessoais. O artigo 6 do Decreto nº 64/020, de 17 de fevereiro de 2020, prevê essas avaliações nos tratamentos de dados pessoais que gerem maiores riscos às pessoas, e o artigo 7 indica o conteúdo mínimo do instrumento, enfatizando a avaliação do risco e as medidas de segurança a adotar.

A título de exemplo, o artigo 6, alínea c, do decreto mencionado exige avaliações de impacto nos tratamentos que impliquem “(…) uma avaliação de aspectos pessoais dos titulares para criar ou utilizar perfis pessoais, particularmente por meio da análise ou previsão de aspectos referentes a seu desempenho no trabalho, situação econômica, saúde, preferências ou interesses pessoais, confiabilidade do comportamento e solvência financeira e localização”. A alínea d acrescenta que essas avaliações são obrigatórias quando se tratar de “(…) tratamento de grandes volumes de dados pessoais”.

O vínculo com a IA é inegável, e a aplicação dessas disposições a sistemas de IA que realizem perfilamento de pessoas ou empreguem grandes volumes de

dados para seu treinamento é indiscutível, tanto no âmbito público quanto no privado. É verdade que existem circunstâncias nas quais o âmbito de aplicação dessa lei pode não alcançar algumas situações, como aponta a sociedade civil na resposta à consulta e como será visto adiante.

Quanto à autorregulação, há múltiplos exemplos. Em particular, as normas de proteção dos dados pessoais podem ilustrar como funcionam esses mecanismos (ver, por exemplo, os códigos de conduta previstos no artigo 36 da Lei nº 18.331).

A adoção de esquemas de corregulação que estabeleçam normativamente determinadas linhas vermelhas e mecanismos de supervisão parece um caminho mais conveniente. Essas definições podem ser observadas no trabalho de MANTELERO [57], que propõe considerar os diferentes âmbitos de atuação dos governos e o alcance da regulação, comparando as propostas do Conselho da Europa e da Comissão Europeia. O autor indica que, além da abordagem corregulatória, as propostas dessas organizações se inclinam a uma abordagem baseada em riscos, mais do que em princípios.

A eventual imposição de medidas especiais também se vincula à análise dos impactos nos direitos das pessoas, com outras medidas para uma supervisão mais efetiva do funcionamento dos sistemas. A criação de registros de algoritmos, a exigência de autorização especial prévia ou mesmo a obrigação de realizar testes em ambientes controlados podem ser instrumentos úteis para determinados tipos de sistemas e tipos específicos de riscos.

Quanto ao princípio de transparência e explicabilidade, o Grupo de Especialistas de Alto Nível em Inteligência Artificial da Comissão Europeia (AI HLEG), em suas “Diretrizes Éticas para uma IA Confiável” [58], aponta que a explicabilidade — elemento central da transparência, junto à rastreabilidade e à comunicação — é a

[57] MANTELERO, Alessandro. “Beyond Data – Human Rights, Ethical and Social Impact Assessment in AI” em “IT&LAW 36”. Disponível em: https://link.springer.com/chapter/10.1007/978-94-6265-531-7_4 . Último acesso: 25/03/2024.
[58] https://digital-strategy.ec.europa.eu/es/library/ethics-guidelines-trustworthy-ai . Último acesso: 14/06/2024.

capacidade de explicar tanto os processos técnicos de um sistema de IA quanto as decisões humanas associadas. Em nosso direito, a explicabilidade está expressamente consagrada em duas disposições da Lei nº 18.331: os artigos 13 e 16.

O artigo 13 dessa lei prevê o Direito à Informação e, em sua alínea G, estabelece que a obrigação dos responsáveis e operadores de fornecer informações aos titulares dos dados abrange, no caso de "(…) tratamentos automatizados de dados regulados pelo artigo 16 desta lei, os critérios de avaliação, os processos aplicados e a solução tecnológica ou o programa utilizado".

O artigo 16, por sua vez, consagra o direito de impugnar avaliações pessoais, afirmando que: "As pessoas têm o direito de não ser submetidas a uma decisão com efeitos jurídicos que as afete significativamente e se baseie em tratamento automatizado de dados destinado a avaliar determinados aspectos de sua personalidade, como desempenho profissional, crédito, confiabilidade, conduta, entre outros.

A pessoa afetada poderá impugnar os atos administrativos ou decisões privadas que envolvam uma avaliação de seu comportamento cujo único fundamento seja um tratamento de dados pessoais que ofereça uma definição de suas características ou personalidade.

Nesse caso, a pessoa afetada terá direito a obter do responsável pela base de dados informações tanto sobre os critérios de avaliação quanto sobre o programa utilizado no tratamento que serviu para adotar a decisão manifestada no ato".

Sem prejuízo do exposto, é necessário considerar efetivamente soluções mais amplas para sistemas de IA que não realizem tratamentos de dados pessoais ou para destinatários que devam ter conhecimento de sua interação com esses sistemas, mesmo quando não sejam seus próprios dados os utilizados por eles.

Quanto ao uso de sistemas de IA na Administração Pública, cabe mencionar a Lei nº 18.381, de 17 de outubro de 2008, que tem como objetivo

promover a transparência da função administrativa de todo órgão público, estatal ou não, e garantir o direito fundamental das pessoas de acesso à informação pública (artigo 1). Seu Decreto regulamentador nº 232/010, de 2 de agosto de 2010, estabelece, no artigo 6, o princípio da máxima publicidade, para que os sujeitos obrigados forneçam as informações da forma mais ampla possível. Seu artigo 38 inclui, entre as informações que devem obrigatoriamente divulgar em seus sites, "qualquer outra informação que possa ser útil ou relevante para o conhecimento e a avaliação das funções e políticas públicas de responsabilidade do sujeito obrigado".

Assim, a obrigação de dar transparência e, sobretudo, explicar as decisões adotadas pelas entidades públicas quando usam sistemas de IA tem fundamento não em uma, mas em duas leis fundadoras do ambiente digital.

Os possíveis critérios orientadores da política pública sobre o tema poderiam se associar ao cumprimento de princípios e à disponibilização de ferramentas práticas que permitam o desenvolvimento inovador, o controle da conformidade com as normas de direitos humanos e mecanismos de supervisão.

Nesse ponto, a competência para formular recomendações sobre o tema foi atribuída por lei à Instituição Nacional de Direitos Humanos e Defensoria do Povo, pelo artigo 4 da Lei nº 18.446, de 24 de dezembro de 2008, e à Secretaria de Direitos Humanos, conforme o artigo 67 da Lei nº 19.149, de 24 de outubro de 2013; e, em matéria de dados pessoais, à Unidade Reguladora e de Controle de Dados Pessoais, pelo artigo 34 da Lei nº 18.331, de 11 de agosto de 2008.

Podemos afirmar que a maioria das preocupações recebidas das entidades participantes da consulta se concentrou neste eixo temático. Assim, por exemplo, a CUTI afirma que, embora o marco legal e institucional atual seja adequado à gestão dos riscos potenciais decorrentes do uso da IA — considerando também as atualizações da lei de proteção de dados pessoais —, seria necessário um comitê ou grupo específico para avaliar o impacto nos

direitos humanos e uma abordagem cautelosa da classificação de riscos, de modo a não afetar a inovação e o investimento em IA.

O diagnóstico das instituições da sociedade civil sobre a suficiência ou não das normas aponta que as disposições da lei de proteção de dados pessoais não são suficientes porque, entre outras razões, se dirigem exclusivamente ao tratamento de dados pessoais. Deveriam, portanto, ser incluídas disposições que especifiquem o conceito de "supervisão humana significativa", viabilizem o exercício de direitos coletivos, a publicação de avaliações de impacto, os requisitos de explicabilidade, rastreabilidade e auditabilidade de algoritmos, a garantia de interação humana e presencial com a administração pública e as relações entre direitos autorais, segredo comercial e auditabilidade de sistemas de IA (propostas da DATYSOC).

A DATA destaca a importância do direito previsto no artigo 16 da lei de proteção de dados pessoais, mas esclarece que é necessário aplicar esses padrões à administração pública por meio de modificações na Lei nº 18.381. Também enfatiza a discussão sobre sistemas de alto risco e o estabelecimento de garantias básicas, além da necessidade de apoiar o trabalho da INDDHH.

A AEU propõe, neste eixo, considerar se é necessária uma regulação geral ou setorial e avalia como conveniente a abordagem de riscos, levando em conta também a atribuição e a distribuição da responsabilidade por danos. Tudo isso com foco no ser humano, contemplando a obrigação de as empresas explicitarem onde e como usam IA e considerando o dever de prevenir a discriminação, assegurar que não se reproduzam atitudes discriminatórias e evitar riscos. Também propõe avaliações de impacto nos direitos humanos dos desenvolvimentos de IA e o fortalecimento do papel do consentimento informado e do princípio de finalidade previstos na Lei nº 18.331.

As respostas da sociedade civil à consulta revelam a necessidade de se deter na análise do uso da IA na vigilância pelas forças de segurança, tema que será considerado em outro capítulo.

Eixo de propriedade intelectual

Considerações preliminares

A Organização Mundial da Propriedade Intelectual (OMPI) [59] aponta que o conceito de Propriedade Intelectual se refere às criações do intelecto, das obras de arte às invenções, aos programas de computador, às marcas e a outros sinais comerciais. Ela se divide em duas categorias: a propriedade industrial (patentes de invenção, marcas, desenhos industriais e indicações geográficas) e os direitos autorais e conexos (obras literárias, artísticas e científicas, incluindo interpretações, execuções e radiodifusões). Os segredos comerciais serão incluídos na discussão.

As conexões entre a Propriedade Intelectual e a inovação são inegáveis [60], assim como os impactos da Inteligência Artificial sobre ela [61]. O Plano Nacional de Inteligência Artificial da República Argentina [62], por exemplo, indicou que a propriedade intelectual, a proteção de dados pessoais e os direitos dos consumidores são regulações em tensão, entre as quais se deve buscar um equilíbrio regulatório, por sua importância para o desenvolvimento e a aplicação da IA.

Nesse sentido, a OMPI [63] publicou recentemente um documento que busca refletir sobre esses aspectos e propõe que o ponto de partida seja o seguinte:

1) Entender se as leis nacionais permitem que um sistema de IA seja nomeado como inventor ou se é necessária a intervenção humana;

[59] "O que é Propriedade Intelectual?" disponível em: https://www.wipo.int/publications/es/details.jsp?id=4528 . Último acesso: 25/03/2024.

[60] "Relatório Mundial sobre a Propriedade Intelectual 2022: A direção da inovação", publicado pela OMPI em 2022 e disponível em: https://www.wipo.int/edocs/pubdocs/es/wipo-pub-944-2022-es-world-intellectual-property-report-2022-the-direction-of-innovation.pdf . Último acesso: 25/03/2024.

[61] "Getting the Innovation Ecosystem Ready for AI An IP policy toolkit", publicado por IMPO e disponível em: https://www.wipo.int/about-ip/es/frontier_technologies/ . Último acesso: 26/03/2024.

[62] https://oecd-opsi.org/wp-content/uploads/2021/02/Argentina-National-AI-Strategy.pdf Último acesso: 26/03/2024.

[63] https://www.wipo.int/edocs/pubdocs/es/wipo-pub-rn2023-11-es-ai-inventions.pdf . Último acesso: 13/06/2024.

2) Analisar se a situação atual permite incentivos, considerando os benefícios econômicos e sociais pretendidos.

Também apresenta perguntas relacionadas à forma de responder às invenções geradas por IA.

No primeiro ponto, a OMPI propõe ir além da pergunta sobre quem deve ser o inventor e oferece uma lista de alternativas: 1) reconhecer apenas invenções realizadas por humanos; 2) permitir que a IA seja nomeada como inventora ou coinventora; 3) exigir que uma pessoa jurídica seja criada e designada inventora ou coinventora quando a criação for realizada pela IA; 4) estabelecer um novo esquema de leis de Propriedade Intelectual para as criações geradas por IA.

Em qualquer caso, a proposta da OMPI é trabalhar em uma perspectiva de múltiplos atores que permita considerar as diferentes opiniões antes de estabelecer modificações na legislação.

Quanto à IA e às criações intelectuais, seguindo o mesmo documento da OMPI, devem ser distinguidas as criações assistidas por IA, baseadas em IA e geradas por IA. Nesse ponto, MANTEGNA [64] propõe alternativas para regular as criações assistidas por IA e as geradas por IA, em linha com as alternativas da OMPI.

Considerando o que aponta a autora, o alcance deste eixo se relaciona à autoria nos direitos autorais, à propriedade industrial e aos segredos comerciais; ao vínculo destes últimos com as medidas de transparência e explicabilidade — que integram os princípios considerados pela lei para a IA —; à propriedade das bases de dados empregadas para gerar as criações; e às medidas a adotar, do ponto de vista regulatório, nas etapas de desenvolvimento e implementação de sistemas generativos de IA.

[64] MANTEGNA, Micaela. “ARTEficial: Creatividad, Inteligencia Artificial y Derechos de Autor”. Ed. CDYT, 2022. P. 299 e seguintes..

Por sua vez, e por seu impacto, é necessário avaliar a questão da propriedade intelectual nos desenvolvimentos aplicados pelo Estado ao utilizar IA para prestar serviços e cumprir suas atribuições.

Seleção de antecedentes internacionais

Recentemente, foi apresentado um projeto de lei para modificar as normas de propriedade intelectual na França em razão do impacto da IA [65], que está em análise em seu Parlamento. Em poucos artigos, o projeto apresenta disposições significativas:

- O artigo 1 estabelece que a integração e a exploração posterior, por um sistema de IA, de obras protegidas por direitos autorais estão sujeitas às disposições gerais sobre a autorização dos autores das obras utilizadas;

- O artigo 2 indica que, quando as obras são criadas por sistemas de IA sem intervenção humana, pertencem aos autores ou titulares dos direitos das obras originais e acrescenta que sua gestão pode ser realizada por sociedades de autores ou outros organismos de gestão coletiva;

- O artigo 3 exige uma menção específica na obra criada por um sistema de IA, indicando que ela foi gerada por essa tecnologia, além dos nomes dos autores das obras originais;

- O artigo 4 prevê uma forma específica de compensação nos casos em que não seja possível determinar a origem das obras que serviram de base à nova criação do sistema de IA, em benefício de organismos de gestão coletiva, deixando sua definição à regulamentação.

Na legislação do Reino Unido, o artigo 9 (3) da Lei de Direitos Autorais, Desenhos e Patentes de 1988 [66] estabelece, em matéria de autoria, que, quando a obra literária, dramática, musical ou artística foi gerada por

[65] https://www.assemblee-nationale.fr/dyn/16/textes/l16b1630_proposition-loi . Último acesso: 26/03/2024.
[66] https://www.legislation.gov.uk/ukpga/1988/48/contents . Último acesso: 27/03/2024.

computador — definida como aquela em que não existe um autor humano —, deve-se entender como autor a pessoa que realizou os arranjos necessários para produzir essa obra.

Essa posição não é compartilhada em todas as jurisdições, e a dificuldade atual é que existe um conjunto de propostas a respeito, mas o tema tem sido sobretudo objeto de diferentes pronunciamentos de órgãos administrativos e judiciais, com respostas distintas conforme o caso. A nova regulação de IA da União Europeia, por exemplo, não se pronuncia sobre essa questão — embora contenha disposições sobre mineração de dados.

A citada Resolução A/RES/78/265 [67] da Assembleia Geral da ONU destaca a Propriedade Intelectual ao estabelecer: “Incentivando, quando apropriado e pertinente, a aplicação de salvaguardas adequadas para respeitar os direitos de propriedade intelectual, incluindo o conteúdo protegido por direitos autorais, promovendo ao mesmo tempo a inovação”.

Diante do exposto, parece razoável apoiar-se nas opiniões dos diferentes organismos internacionais e regionais sobre a necessidade de explorar alternativas sob uma perspectiva multissetorial e favorável à inovação.

Diagnóstico sobre IA e propriedade intelectual

Como primeiro ponto, deve-se mencionar que nosso país possui, de fato, normas que regulam o registro de programas de computador, compilações de dados ou outros materiais que constituam criações intelectuais, expressão de ideias, informações e algoritmos formulados em sequências originais ordenadas para uso por um dispositivo de processamento de informações ou de controle automático. A legislação vigente se pronuncia pela proteção por meio dos direitos autorais.

A legislação vigente permite ainda que o registro desses direitos seja feito por pessoa física ou jurídica, incluindo o Estado. A norma também prevê a situação de obras anônimas e, seguindo as

[67] https://documents.un.org/doc/undoc/gen/n24/087/86/pdf/n2408786.pdf?token=q7sbXbo0iQB4sT9YhT&fe=true . Último acesso: 14/06/2024.

disposições da Convenção de Berna, coloca o editor, ou o empresário, conforme o caso, como titular do direito autoral enquanto o autor não revelar sua identidade. Mesmo nesse caso, porém, não se discute a originalidade ou a suposta autoria da obra por uma pessoa, mas o desconhecimento dos detalhes de sua identidade.

Como apontam Alexander CUNTZ e outros [68], não se trata apenas de determinar quem elaborou a obra, mas de como as criações geradas integralmente por IA mudam a natureza do processo de inovação e de como essa mudança afeta o equilíbrio das necessidades de recursos e incentivos no ecossistema inovador.

No entanto, embora possa ser prudente perguntar se é possível atribuir a titularidade dos direitos ao sistema de IA — por uma espécie de personalidade eletrônica —, a uma pessoa física ou jurídica específica — desenvolvedor, usuário ou outros —, a um conjunto de pessoas ou entender que a obra deva estar em domínio público, não parecem estar dadas as condições para responder neste momento.

O emprego de dados de treinamento nos modelos de IA é outro ponto a esclarecer, para determinar se a legislação vigente — tanto sobre o potencial uso de dados protegidos por direitos de propriedade intelectual quanto sobre o uso de informações pessoais protegidas pelas normas de proteção de dados pessoais — é suficiente para atender às necessidades desses sistemas ou se são necessárias exceções especiais — como no projeto de lei de IA do Brasil [69].

Também é importante determinar como as exigências de transparência e explicabilidade se relacionam com os direitos de propriedade intelectual.

[68] CUNTZ, Alexander e outros. “Artificial Intelligence and Intellectual Property: An Economic Perspective”. Publicado pela OMPI no âmbito dos Documentos de Trabalho em Pesquisa Econômica. Nº 77/2024. Disponível em: https://www.wipo.int/publications/en/details.jsp?id=4715 . Último acesso: 26/03/2024.

[69] https://www25.senado.leg.br/web/atividade/materias/-/materia/157233 . Ver particularmente o artigo 42. Último acesso: 27/03/2024.

Quanto ao segredo comercial, existem diferentes normas relacionadas ao tema [70] — como o artigo 39 do Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio (ADPIC).

Quanto aos dados pessoais, o alcance das informações que empresas e organizações devem divulgar em determinados tipos de tratamento automatizado de dados pessoais está previsto nos artigos 13 e 16 da Lei nº 18.331.

Por fim, é pertinente determinar se as normas de propriedade intelectual no uso de aplicações pelo Estado, refletidas indiretamente nas disposições sobre Software Público, devem ser aplicadas aos sistemas de IA.

Na discussão sobre o alcance deste eixo, a DNPI apresentou alguns aspectos que merecem menção. Apontou que o sistema de propriedade intelectual constitui um mecanismo de incentivos para capturar valor, permitindo aos criadores negociar e evitar o aproveitamento indevido de suas criações. Indica, em particular, que não é possível, neste momento, transferir esse fundamento às criações da IA.

Essa Direção também sustenta que, por seguir a tradição europeia continental, nosso país considera o direito autoral uma extensão dos direitos da personalidade, consagrando direitos morais inalienáveis e irrenunciáveis em favor do autor; a originalidade, por sua vez, é entendida como expressão da personalidade do autor. No caso das patentes, os direitos inalienáveis se referem ao reconhecimento como inventor, conforme o artigo 2 da Lei nº 17.164, de 2 de setembro de 1999.

Assim, conforme a legislação vigente, para conceder ao inventor direitos exclusivos sobre a invenção, ele deve fornecer uma descrição clara, detalhada e

[70] Um detalhamento das normas sobre segredos comerciais e industriais pode ser encontrado na seguinte publicação da Unidade de Acesso à Informação Pública: https://www.gub.uy/unidad-acceso-informacion-publica/politicas-y-gestion/informacion-secreta-definida-ley . Último acesso: 26/03/2024.

completa da invenção; com a intervenção de algoritmos ou outros mecanismos de IA, a questão está na possibilidade de fornecer efetivamente uma descrição completa de como esses algoritmos chegam a um resultado ou outro, ou de gerar um efeito “black box”.

A DATYSOC também apresentou considerações sobre Propriedade Intelectual em suas respostas à consulta. Mencionou a omissão da legislação vigente quanto ao uso de obras para análise computacional (incluindo a restrição de que esses usos não concorram com a exploração normal das obras nem prejudiquem injustificadamente os interesses dos autores, para a qual também propõe uma redação), a necessidade de regular as relações entre direitos autorais, segredo comercial e auditabilidade dos sistemas (o que, especificamente em propriedade intelectual, implicaria exceções que permitissem acessar, copiar e analisar sistemas para auditá-los a pedido de um juiz ou quando a lei assim dispusesse) e de estabelecer proibições de usos competitivos ou que prejudiquem injustificadamente o autor ou titular dos direitos das obras.

A DATA se alinha à necessidade de maior apoio às decisões de aquisição de software ou soluções baseadas em IA pela Administração Pública, indicando a possibilidade de adaptar a Lei nº 19.179, de 27 de dezembro de 2014, e seu Decreto regulamentador nº 44/015, de 30 de janeiro de 2015. Também propõe considerar um mecanismo de intervenção para que a Agesic possa determinar o risco e assessorar entidades públicas na realização de avaliações de impacto antes de adquirir soluções baseadas em IA para alguns setores.

Eixo de infraestrutura e cibersegurança

Considerações preliminares

O desenvolvimento da IA depende de vários fatores. Um deles é uma infraestrutura adequada, para a qual o Estado assume papel central.

O Ministério da Inteligência Artificial dos Emirados Árabes Unidos publicou, em novembro de 2020, um relatório [71] sobre a situação da infraestrutura de hardware para IA no país, indicando que os elementos essenciais para apoiar a inovação na matéria se resumem a três: a) infraestrutura de dados — especialmente sua disponibilidade e a existência de plataformas de armazenamento de alto desempenho —; b) rede — especialmente sistemas especializados de redes de alto desempenho que conectem os servidores entre si e às unidades de armazenamento —; e c) infraestrutura de hardware — especialmente plataformas computacionais e chips de computador que acelerem o treinamento e o desenvolvimento de aplicações de IA e suportem grandes quantidades de memória.

Em fevereiro de 2023, a OCDE publicou seu relatório nº 350 [72] da série de economia digital, apresentando recomendações para construir capacidades computacionais para a Inteligência Artificial e reconhecendo esse eixo como elemento central para o desenvolvimento e a evolução da tecnologia. O documento destaca a necessidade de que os países que desenvolvam planos de IA analisem adequadamente as capacidades computacionais nacionais para alcançar os objetivos definidos.

A partir da análise da OCDE, cabe, neste ponto: 1) avaliar a revisão das capacidades computacionais, especialmente para IA, dos atores dos setores público e privado, considerando o uso de serviços de nuvem no país ou no exterior; 2) considerar o número de centros de dados existentes, definir padrões relativos aos dados e analisar as capacidades de processamento e as necessidades de hardware do país, entre outros aspectos; 3) determinar a demanda

[71] https://ai.gov.ae/infrastructure_report/ . Último acesso: 28/03/2024.

[72] https://www.oecd-ilibrary.org/science-and-technology/a-blueprint-for-building-national-compute-capacity-for-artificial-intelligence_876367e3-en . Último acesso: 28/03/2024.

potencial de processamento para IA, antecipando as necessidades e planejando de acordo com elas; 4) distinguir as necessidades de processamento para IA das demais; 5) oferecer capacitação e treinamento aos trabalhadores; 6) mapear e analisar as cadeias de suprimentos necessárias para construir planos de contingência e resiliência.

As alternativas consideradas pela OCDE merecem, sem dúvida, atenção para assegurar a efetividade da estratégia a ser concebida. No entanto, o alcance deste documento se relaciona a possíveis recomendações de natureza normativa e, nesse sentido, cabe considerar a existência e a suficiência ou não de normas associadas a:

1) infraestrutura para a gestão e o intercâmbio de dados

2) armazenamento de informações

3) cibersegurança

4) redes de telecomunicações

Seleção de antecedentes internacionais

Não se observam antecedentes normativos que contemplem expressamente essa circunstância em nível internacional, além da menção isolada a aspectos específicos nas normas e nos projetos existentes. O tema não está presente nas diferentes estratégias de IA levantadas. Confirma-se, assim, o que afirma o relatório nº 350 da OCDE: muitos países desenvolveram estratégias nacionais de IA sem analisar integralmente se possuem infraestrutura computacional e software de IA suficientes para alcançar seus objetivos.

A iniciativa de Infraestrutura Pública Digital promovida pelo PNUD [73], mencionada anteriormente, está vinculada, segundo essa entidade, a uma combinação de padrões abertos construídos com uma finalidade de interesse público, condições para a governança e uma comunidade de atores de mercado competitivos e inovadores para promover a inovação, especialmente ao longo de diferentes programas públicos.

[73] https://www.undp.org/digital/digital-public-infrastructure , Último acesso: 02/05/2024.

Os impactos dessa forma de considerar determinados mecanismos aplicáveis a soluções de transformação digital foram levantados em diferentes documentos e podem ajudar a determinar a orientação dos esforços para uma IA sustentada em infraestrutura segura, soberana e favorável à inovação.

Diagnóstico sobre infraestrutura e cibersegurança para IA

Nosso país possui uma institucionalidade forte em políticas de telecomunicações, cibersegurança, interoperabilidade e dados. A distribuição de competências entre as entidades públicas envolvidas parece adequada, sem prejuízo da necessidade de maior coordenação entre elas.

Por outro lado, não foram encontradas análises atuais sobre compras de infraestrutura física, normas que regulem especificamente os requisitos para a aquisição de sistemas de IA por entidades públicas, planos de adoção de IA sob a perspectiva deste documento ou informações objetivas associadas ao uso das infraestruturas físicas para essas atividades por entidades públicas ou privadas [74].

Aqui, os processos planejados de compras e a determinação das necessidades das entidades são um ponto central a considerar. Duas normas poderiam ser relevantes: a) o artigo 74 da Lei nº 19.149, de 24 de outubro de 2013, que atribui à Agesic a tarefa de emitir parecer obrigatório sobre os planos de desenvolvimento e aquisições de informática dos órgãos da Administração Central e propor ao Poder Executivo requisitos técnicos gerais para as aquisições de bens e serviços de informática; e b) o Decreto nº 431/022, de 27 de dezembro de 2022, que cria o Comitê de Governança de Processos e Soluções Transversais — integrado por várias entidades públicas, entre elas a Agesic — para exercer a direção funcional e tecnológica dos sistemas de

[74] Isso sem prejuízo de informações setoriais que podem contribuir para definir políticas, como o “Informe de Mercado de Telecomunicaciones de Uruguay”, publicado periodicamente pela URSEC e disponível em: https://www.gub.uy/unidad-reguladora-servicios-comunicaciones/datos-y-estadisticas/estadisticas/informes-mercado-del-sector-telecomunicaciones . Último acesso: 29/03/2024.

informação transversais e das plataformas tecnológicas compartilhadas, vinculados à gestão interna das seções orçamentárias da Administração Central.

O planejamento das compras associadas à infraestrutura necessária para desenvolver a IA também contribuiria para o cumprimento de outras normas, como o Decreto nº 339/021, de 4 de outubro de 2021 (Plano Anual de Contratações).

Quanto ao armazenamento de informações, o Decreto nº 92/014, de 7 de abril de 2014, tem sido aplicado pelas entidades públicas em geral — não apenas pelas da Administração Central, seja por referência expressa a suas previsões, seja pela adoção de normas semelhantes em seus respectivos âmbitos — como argumento para evitar a contratação de serviços de processamento de dados em nuvem. A Agesic procurou esclarecer melhor o alcance do decreto [75], mas deveria ser considerada uma atualização em consonância com os critérios definidos pela Agência [76].

Quanto à infraestrutura que viabiliza o intercâmbio de informações, a Agesic disponibiliza a Plataforma de Interoperabilidade, criada pelo artigo 17 do Decreto nº 178/013, de 11 de junho de 2013, para garantir intercâmbios de informações em meio eletrônico de forma segura e confiável. Embora a plataforma seja voltada a entidades públicas, também poderia ser usada por entidades privadas, que deveriam cumprir as condições estabelecidas pela Agesic e pelas entidades que nela exponham seus serviços para o consumo de informações.

Por fim, quanto à cibersegurança, a Estratégia Nacional está em desenvolvimento, de modo que se deverá observar o que nela for definido. Pode-se, contudo,

[75] "Guía de interpretación del Decreto 92/014 en Ciberseguridad", disponível em https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/guia-interpretacion-decreto-92014-ciberseguridad/guia-interpretacion e documento "Uso de la Nube en la Administración Pública", disponível em https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/uso-nube-administracion-publica/uso-nube-administracion-publica . Último acesso: 30/03/2024.

[76] "Principios generales de la Nube Pública en el Estado". Disponível em: https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/principios-generales-nube-publica-estado#:~:text=Con%20el%20fin%20de%20guiar%20a%20las%20entidades,este%20documento%20principios%20generales%20a%20tener%20en%20cuenta . Último acesso: 30/03/2024.

indicar que, além de uma regulação extensa e preexistente na matéria, houve uma atualização recente pelos artigos 78 e seguintes da Lei nº 20.212.

Nas discussões sobre a elaboração do relatório, a DINATEL enviou propostas relacionadas ao alcance e ao diagnóstico realizado neste eixo temático.

Propôs-se considerar a situação das normas atuais sobre infraestrutura para a gestão e o intercâmbio de dados, armazenamento de informações, obrigações de cibersegurança, redes de telecomunicações (robustez e qualidade do serviço), identificação de infraestrutura crítica, acordos internacionais de intercâmbio de dados e normas de responsabilidade civil, além da infraestrutura de nuvem e da atualização da regulação atual dos dados na nuvem.

A DINATEL indicou que o desenvolvimento da IA deve incorporar necessidades de infraestrutura além do setor de telecomunicações, uma visão de impacto social e uma regulação não restritiva ou leis de promoção para a instalação no país e o uso de data centers públicos e privados para finalidades públicas. Isso além de outras contribuições anexadas a este documento.

Eixo de trabalho e capacitação em IA

Considerações preliminares

Os impactos da IA no mundo do trabalho e nos trabalhadores precisam ser avaliados e abordados sob diferentes perspectivas para aproveitar as oportunidades e enfrentar os desafios emergentes.

Neste eixo específico, o relatório procurou identificar medidas para fortalecer as habilidades das pessoas no campo da IA, voltadas à prevenção e à mitigação dos impactos negativos no emprego e no mercado de trabalho e ao maior aproveitamento da IA em benefício da sociedade.

O relatório da OCDE intitulado “Perspectivas do Emprego da OCDE 2023: A inteligência artificial e o mercado de trabalho” [77] indica que o impacto da IA mudará as necessidades de habilidades, das quais já existe escassez atualmente. Por isso, as políticas públicas terão papel importante no incentivo à capacitação pelos empregadores, assim como no âmbito da educação formal.

Essa visão é compartilhada pela UNESCO na Recomendação sobre a Ética da Inteligência Artificial, que, em sua área de ação nº 10, estabelece a necessidade de ampliar as competências básicas e interdisciplinares em todos os níveis educacionais associados ao uso ético da IA, apoiar acordos de colaboração com instituições de ensino, indústria, sociedade civil e organizações de trabalhadores para reduzir lacunas e gerar estratégias de capacitação em médias empresas, entre outras medidas. Também propõe trabalhar com empresas para apoiar transições justas de empregados em situação de risco por meio de programas de aperfeiçoamento e reconversão profissional, entre outros. Inclui ainda medidas relacionadas à pesquisa, à competitividade dos mercados e à proteção dos consumidores, à oferta de financiamento quando necessário etc.

[77] Ver particularmente o capítulo 5 sobre habilidades, disponível em: https://www.oecd-ilibrary.org/sites/638df49a-en/index.html?itemId=/content/component/638df49a-en . Último acesso: 31/03/2024.

Seleção de antecedentes internacionais

O governo espanhol, por meio do Decreto-Lei nº 2/2023, de 8 de março de 2023, estabeleceu medidas urgentes de incentivo à IA na comunidade autônoma da Extremadura [78]. Seu primeiro artigo define como finalidade principal e geral elevar a capacidade técnica em IA por meio da alfabetização da população, incluindo a formação da população economicamente ativa e dos empregados públicos. Para isso, propõe promover capacidades empreendedoras, criativas, sociais e culturais; incentivar medidas de apoio a empresas que realizem planos de formação e capacitação na matéria; e incluir essa formação para pessoas desempregadas e servidores públicos.

A Ordem Executiva sobre o Desenvolvimento Seguro e Confiável da IA do governo dos Estados Unidos, na Seção 10 (Avançando no uso da IA no Governo Federal), propõe, no mais alto nível das agências do governo federal, a implementação de programas de treinamento e familiarização em IA para empregados, gerentes e líderes, entre outros. Esses programas deverão capacitar os empregados e outros a desenvolver e manter conhecimentos operacionais sobre tecnologias emergentes de IA. Também propõe que as agências ofereçam oportunidades de desenvolvimento profissional, bolsas e recursos para seu pessoal.

Diagnóstico sobre trabalho e capacitação para IA

Há diferentes disposições nacionais que preveem a promoção da capacitação dos trabalhadores. No entanto, as normas inicialmente analisadas não demonstram ênfase particular em aspectos de IA e na forma de gerir seus impactos, embora a capacitação digital esteja presente em programas como os do Instituto Nacional de Emprego e Formação Profissional (INEFOP) ou da Escola Nacional de Administração Pública (ENAP), no caso dos trabalhadores do setor público.

[78] https://www.boe.es/buscar/doc.php?id=BOE-A-2023-8795 . Último acesso: 31/03/2024.

Diante do exposto, estima-se que a institucionalidade existente permitiria implementar políticas e programas relacionados a esse tema e explorar alternativas de cooperação entre entidades públicas e privadas.

Dar visibilidade ao problema, estabelecer ações coordenadas, definir uma política específica e implementar uma cooperação contínua entre os diferentes atores do ecossistema são aspectos a considerar para conduzir uma estratégia bem-sucedida na matéria.

Eixo de responsabilidade civil e direitos do consumidor

Considerações preliminares

A IA apresenta questões de difícil solução para muitos operadores jurídicos que, em países como o nosso, procuram interpretar normas que — embora claramente ofereçam a segurança jurídica necessária — foram aprovadas em uma realidade muito diferente da atual.

Este eixo trata de dois aspectos bem regulados normativamente: a responsabilidade civil e as relações de consumo.

Ao analisar a função preventiva da responsabilidade civil em nosso direito, DE CORES [79] indica que o próprio conceito apresenta "(…) grande polissemia, mas que, em sentido amplo, pode ser definido como a consequência que decorre do descumprimento de uma norma, podendo, assim, existir responsabilidade não apenas civil, mas também penal, administrativa e até política ou moral".

JOSÉ DOS SANTOS [80] afirma que "(…) a responsabilidade civil tem a função de restabelecer o equilíbrio comprometido pela ocorrência de danos morais ou materiais causados pelo agente causal" e destaca que, no direito brasileiro, há responsabilidade civil subjetiva — que exige conduta dolosa ou culposa, ou omissão de seu autor — e responsabilidade objetiva — para a qual basta a prova do nexo causal entre a conduta e o dano, sem considerar a intenção ou a culpa de quem o causou.

A autora questiona o que ocorre com a responsabilidade civil da IA e conclui pela necessidade de considerar se os institutos atuais podem responder à sua evolução.

[79] DE CORES, Carlos. "La denominada función preventiva de la responsabilidad civil. Una crítica a su ubicación dogmática". Disponível em: https://eva.fder.udelar.edu.uy/mod/resource/view.php?id=49243&redirect=1 . Último acesso: 30/03/2024.
[80] JOSÉ DOS SANTOS, Sonia. "Inteligencia Artificial y Responsabilidad Civil" em "Inteligencia Artificial y Derecho". 1ª ed. Ed. Hammurabi. 2020. P. 179 e seguintes.

No conceito de responsabilidade civil, a distinção mais comum é entre a contratual — decorrente do descumprimento de um contrato entre duas ou mais partes — e a extracontratual — decorrente do prejuízo causado a alguém sem esse vínculo contratual. No Uruguai, o regime de responsabilidade civil está regulado principalmente em nosso Código Civil.

As relações de consumo são definidas no artigo 4 da Lei nº 17.250, de 11 de agosto de 2000, como o vínculo entre o fornecedor que, a título oneroso, fornece um produto ou presta um serviço e quem o adquire ou utiliza como destinatário final. Do ponto de vista subjetivo, encontram-se as figuras do fornecedor e do consumidor.

ARAMENDIA [81] aponta que, no uso da IA e nos eventuais danos decorrentes da utilização desses sistemas, existem 2 extremos a considerar: a insegurança das pessoas prejudicadas pelo produto ou serviço que contém IA sobre como proceder para serem indenizadas e a insegurança dos projetistas, desenvolvedores, produtores, financiadores e demais integrantes da cadeia que levou esse produto ou serviço ao mercado quanto a seu papel na produção do evento danoso.

A autora apresenta três desafios: 1) a complexidade dos sistemas e a diversidade de fatores que podem causar o erro que, por sua vez, causou o dano; 2) a multiplicidade e a diversidade de atores na cadeia, dificultando a rastreabilidade; 3) o mecanismo para continuar incentivando o investimento, a pesquisa e o desenvolvimento em IA e, ao mesmo tempo, assegurar a quem sofre um dano o acesso a uma indenização justa.

É precisamente a resposta a esses três desafios que se procurará considerar, sob uma perspectiva estritamente normativa. Ficam fora do alcance os impactos da IA nas relações de consumo, pois este eixo tratará do problema associado à responsabilidade dos fornecedores e à reparação de danos aos consumidores.

[81] ARAMENDIA, Mercedes. “La Inteligencia Artificial ¿y la responsabilidad?” em “Estudios sobre los Desafíos Jurídicos ante la Digitalización”, Tomo III. Coord. Mercedes Aramendía e Agustina Pérez Comenale. Ed. UM. Ano 2023. P. 557 e seguintes.

Seleção de antecedentes internacionais

Neste ponto, é relevante considerar a proposta de Diretiva sobre Responsabilidade da IA da União Europeia [82], que complementa o Regulamento recentemente aprovado.

CASALS [83] observa que "a atual proposta de Diretiva, por sua vez, refere-se apenas à responsabilidade por dolo ou culpa por danos causados por sistemas de IA, que continua sujeita às regras substantivas nacionais. Por isso, não entra em conflito nem com a aplicação das normas nacionais nem com as decorrentes da Diretiva sobre responsabilidade por danos causados por produtos defeituosos e, como apontado, seu âmbito objetivo é muito mais amplo".

Nesse ponto, a Comissão Europeia [84] afirmou que: "A Diretiva simplifica o processo jurídico para as vítimas demonstrarem que a culpa de uma pessoa causou os danos, introduzindo duas características principais: primeiro, quando uma culpa relevante tiver sido comprovada e parecer razoavelmente provável a existência de um nexo causal com o desempenho da IA, a chamada «presunção de causalidade» enfrentará as dificuldades das vítimas para explicar detalhadamente como o dano foi causado por uma culpa ou omissão específica, o que pode ser especialmente difícil ao tentar compreender e lidar com sistemas complexos de IA. Segundo, as vítimas terão mais ferramentas para solicitar reparação judicial graças à introdução de um direito de acesso às provas apresentadas por empresas e fornecedores nos casos que envolvam IA de alto risco". [85]

---

[82] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52022PC0496 . Último acesso: 30/03/2024.

[83] CASALS, Miguel Martín. "Las propuestas de la Unión Europea para regular la responsabilidad civil por los daños causados por sistemas de inteligencia artificial". Disponível em: https://indret.com/las-propuestas-de-la-union-europea-para-regular-la-responsabilidad-civil-por-los-danos-causados-por-sistemas-de-inteligencia-artificial/ . Último acesso: 30/03/2024.

[84] https://ec.europa.eu/commission/presscorner/detail/es/ip_22_5807 . Último acesso: 30/03/2024.

[85] Uma análise mais extensa pode ser encontrada em La Ley Digital, no artigo de Gonzalo ITURMENDI MORALES "Responsabilidad civil por el uso de sistemas de inteligencia artificial", disponível em https://laleydigital.laleynext.es/Content/Documento.aspx?params=H4sIAAAAAAAEAMtMSbF1CTEAAmNDCwsjI7Wy1KLizPw8WyMDIwNDQyMDkEBmWqVLfnJlZUGqbVpiTnEqANKvjtI1AAAAWKE . Último acesso: 30/03/2024.

Um projeto de lei apresentado na República Argentina [86] estabelece, em seus artigos 19 a 23, um regime de responsabilidade por dano ou erro de uso. O projeto prevê a responsabilidade dos desenvolvedores e fornecedores pelos erros de uso de seus sistemas que causem dano quando não tiverem adotado medidas razoáveis para evitar o erro ou tiverem descumprido as regulações e os padrões estabelecidos, devendo implementar medidas de segurança e testes. Prevê também a responsabilidade dos usuários pelo uso adequado dos sistemas, conforme as instruções fornecidas e com a devida diligência; caso contrário, eles responderão por danos a terceiros. Inclui ainda a obrigação de manter seguro de responsabilidade civil adequado para cobrir possíveis danos. Por fim, há normas sobre transparência e capacitação e um mecanismo de denúncia de erros de uso da inteligência artificial.

Também não existem antecedentes normativos relevantes nesse tema, além das disposições da proposta de diretiva da União Europeia. Isso leva a refletir sobre a necessidade de uma análise específica e multiator da legislação uruguaia, dada a sensibilidade da estrutura de responsabilidade civil para a segurança jurídica.

Diagnóstico sobre responsabilidade civil e direitos do consumidor

O primeiro ponto do diagnóstico é que as normas não estabelecem uma regulação específica para o problema dos danos que os sistemas de IA podem causar. A menos que o regime de responsabilidade esteja claramente estabelecido nos termos de um contrato, a regulação geral de responsabilidade civil que poderia se aplicar por analogia nesses casos — nos quais existe grande complexidade para determinar os integrantes da cadeia que leva à entrada em produção de um produto ou serviço de IA — é o artigo 1330 do Código Civil, que regula uma espécie de responsabilidade coletiva associada a coisa que cai de um edifício. Essa análise em termos gerais e sua

[86] https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2023/PDF2023/TP2023/2505-D-2023.pdf . Último acesso: 30/03/2024.

aplicação por analogia foram elaboradas por BORDOLI [87], embora não especificamente em relação ao tema aqui tratado, mas à atribuição de responsabilidade quando existe um grupo identificado com várias pessoas, sem ser possível identificar concretamente quem causou o dano.

Esse regime parece insuficiente para atribuir adequadamente a responsabilidade a quem causou o evento danoso e reparar o dano efetivo às pessoas.

Nas relações de consumo, aplica-se o mencionado artigo 34 da Lei nº 17.250, de 11 de agosto de 2000, que dispõe: “Se do vício ou risco da coisa ou da prestação do serviço resultar um dano ao consumidor, o fornecedor será responsável conforme o regime previsto no Código Civil.

O comerciante ou distribuidor só responderá quando o importador e o fabricante não puderem ser identificados. Da mesma forma, serão responsáveis se o dano resultar da conservação inadequada do produto ou da alteração de suas condições originais”.

Outro aspecto a considerar é o dano causado quando o produto ou serviço é oferecido pelo Estado, situação na qual se aplicam os artigos 24 e 25 da Constituição, como indicado.

[87] BORDOLI, Carlos Rubens. “Responsabilidad Extracontractual Colectiva por Daño Causado por un Miembro Indeterminado de un Grupo”, disponível em Revista de la FDER (30). Ano 2014. P. 65 e seguintes. Disponível em formato eletrônico em: https://revista.fder.edu.uy/index.php/rfd/article/view/87 . Último acesso: 30/03/2024.

Eixo de medidas de promoção da IA

Considerações preliminares

O objetivo deste eixo é considerar o alcance e a definição de possíveis medidas de promoção associadas a uma política pública de IA.

Por que propor medidas de promoção da IA? A resposta está nos benefícios comprovados que essa tecnologia pode oferecer à sociedade. Embora haja ênfase em alertar para os riscos potenciais às pessoas, também é relevante ponderar suas múltiplas vantagens.

Pode-se considerar, a esse respeito, o relatório provisório do Órgão Consultivo de Inteligência Artificial da ONU de dezembro de 2023 [88], que estabelece recomendações preliminares baseadas em 5 princípios: 1) governança inclusiva, por todos e em benefício de todos; 2) governança voltada ao interesse público; 3) governança construída em conjunto com a governança de dados e a promoção dos bens comuns; 4) governança universal, em rede e enraizada na colaboração de múltiplas partes interessadas; 5) governança ancorada na Carta das Nações Unidas, no direito internacional dos direitos humanos e em outros compromissos internacionais acordados, como os Objetivos de Desenvolvimento Sustentável. Quanto à promoção da IA para a Humanidade, o documento aponta, entre outras necessidades, que o acesso e os benefícios devem caminhar juntos, por meio do investimento nacional em talentos, dados e recursos computacionais. Para isso, são consideradas relevantes a cooperação e a assistência internacional nos setores público e privado.

A pertinência e o alcance de eventuais medidas de promoção da IA devem levar em conta: 1) a definição dos objetivos aos quais se dirige a promoção efetiva da Inteligência Artificial, colocando no centro os desenvolvimentos que contribuam para construir uma sociedade mais justa e equitativa; 2) os instrumentos concretos que poderiam ser empregados para conceder benefícios que ajudem no desenvolvimento dos sistemas identificados como seus destinatários.

[88] https://www.un.org/sites/un2.un.org/files/ai_advisory_body_interim_report.pdf . Último acesso: 04/04/2024.

Seleção de antecedentes internacionais

Entre os pontos mais relevantes da Ordem Executiva sobre o Desenvolvimento Seguro e Confiável da Inteligência Artificial, aplicável pelas agências governamentais dos Estados Unidos [89], está a promoção da inovação e da concorrência por meio de:

> a) Catalisar a pesquisa em IA nos Estados Unidos por meio de um projeto-piloto de Recurso Nacional de Pesquisa em IA.
>
> b) Promover um ecossistema justo, aberto e competitivo mediante assistência técnica e recursos para pequenos desenvolvedores.
>
> c) Utilizar autoridades existentes para ampliar as possibilidades de imigrantes e não imigrantes altamente especializados, com experiência em áreas críticas, estudarem, permanecerem e trabalharem nos Estados Unidos.

Isso sem prejuízo de outros pontos, como a cooperação internacional e a colaboração entre entidades dentro do governo.

A proposta de "Lei de IA" da União Europeia [90], por sua vez, aponta expressamente o vínculo entre a governança de dados, os dados abertos e a promoção da inovação impulsionada pela IA. As medidas de apoio à inovação incluem ambientes controlados de testes de IA, a autorização de tratamentos de dados com determinadas finalidades e medidas para fornecedores e usuários de pequena escala, que vão do acesso prioritário aos ambientes controlados, de atividades de conscientização e de canais específicos de comunicação até, eventualmente, valores diferenciados de taxas para determinados serviços.

[89] O conteúdo da Ordem Executiva pode ser consultado em: 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/ Último acesso: 04/04/2024.

[90] https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex:52021PC0206 . Último acesso: 04/04/2024.

No Brasil, o Projeto de Lei nº 2338/2023 [91] enfatiza a promoção da pesquisa e do desenvolvimento para estimular a inovação nos setores produtivos e no poder público. As medidas previstas também incluem a criação de sandboxes regulatórios e bases de dados públicas de IA.

Existem outras disposições internacionais que compartilham os critérios de promoção aqui refletidos, incluindo o conceito de desenvolvimento da inovação e destacando o papel dos ambientes controlados de testes nesse sentido.

Diagnóstico preliminar sobre medidas de promoção da IA

Atualmente, algumas disposições tratam especificamente da promoção da inovação no campo da IA. Na data deste documento, está em elaboração a regulamentação do artigo 75 da Lei nº 20.212, de modo que serão consideradas as observações feitas nesta análise.

Há também outros tipos de medidas que poderiam ser eficientes para promover a inovação e seus desenvolvimentos, como isenções tributárias e a análise e promoção de selos que comprovem a realização de auditorias e avaliações que, por sua vez, permitam acessar determinados benefícios, entre outras. Todos esses elementos exigem uma análise específica.

[91] https://legis.senado.leg.br/sdleggetter/documento?dm=9347622&ts=1702407086098&disposition=inline&_gl=1*1wg6j22*_ga*NTk0MjQwOTMwLjE3MDE3OTA5MTc.*_ga_CW3ZH25XMK*MTcwNjYxODMwOS4yLjEuMTcwNjY0NDgxOC4wLjAuMA . Último acesso: 04/04/2024.

Outros eixos temáticos identificados a partir das contribuições recebidas

O uso de sistemas de IA para vigilância

Entre as preocupações e recomendações apresentadas pela sociedade civil ao responder ao documento de consulta disponibilizado por esta Agência, estão questões associadas ao uso de sistemas de IA para vigilância pelas forças de segurança.

A Lei nº 19.696, de 29 de outubro de 2018, regulamentada pelo Decreto nº 157/022, de 23 de maio de 2022, estabelece e regula o Sistema Nacional de Inteligência do Estado (SNIE), impondo a seus órgãos o cumprimento de princípios voltados ao respeito à Constituição, aos princípios do regime democrático republicano de governo e aos direitos humanos.

Nesse marco, o artigo 20 da Lei determina que a busca de informações por procedimentos especiais que possam afetar a liberdade e a privacidade dos cidadãos deve ser autorizada pelo Poder Judiciário. Quanto aos controles, destaca-se o artigo 25, que prevê a criação, na Assembleia Geral, de uma comissão parlamentar bicameral encarregada de controlar e supervisionar a atuação do sistema.

O Decreto nº 157/022 aprova a Política Nacional de Inteligência, especificando ações e medidas, mas, além de referências genéricas ao cumprimento dos direitos humanos, não faz nenhuma previsão sobre a aplicação da IA nas atividades de vigilância das pessoas.

Em sua resposta à consulta, a sociedade civil propõe sugestões como impor uma moratória à aquisição de software de vigilância até que exista uma base legal que regule adequadamente o ecossistema de vigilância policial, ou exigir auditabilidade e explicabilidade algorítmicas, rastreabilidade, protocolos de controle de acesso e descrição detalhada das responsabilidades de quem usa esses sistemas.

A sociedade civil também propõe linhas vermelhas sobre os usos estritamente proibidos à polícia e os que exigem ordem judicial; a proibição da vigilância biométrica em tempo real e sem ordem judicial em espaços públicos; e uma regulação específica da admissibilidade, valoração e produção dos matches biométricos como métodos de investigação e prova digital, entre outras medidas.

Por fim, as recomendações da sociedade civil incluem treinamento adequado de policiais, juízes e promotores — mediante certificação obrigatória — e uma regulação urgente do uso da IA para vigilância pelo Ministério do Interior.

Esta Agência compartilha a preocupação com o uso adequado dos sistemas de IA nas atividades das forças de segurança, mas também quer enfatizar a necessidade de um diálogo multissetorial para contemplar um equilíbrio adequado entre as necessidades de segurança interna e a proteção dos direitos fundamentais das pessoas.

Inserção e cooperação internacional

Outro aspecto que não integrou os eixos iniciais, mas tem enorme relevância, é a inserção internacional do país. Como outros temas na agenda de nossos países, a IA apresenta desafios globais que nos motivam a buscar soluções globais.

Por outro lado, como os sistemas de IA aplicados na região são “importados” de outras partes do mundo, devemos fazer um esforço adicional para gerar mecanismos de cooperação regional que contemplem nossas próprias necessidades.

Como parte da Agenda Comum [92] apresentada pelo Secretário-Geral da ONU em 2021, essa organização lançou, no ano passado, a iniciativa “Global Digital

[92] https://www.un.org/en/content/common-agenda report/assets/pdf/Common_Agenda_Report_English.pdf . Último acesso: 22/06/2024.

Compact – an Open, Free and Secure Digital Future for All” [93] — atualmente em consulta e que se espera seja acordada na Cúpula do Futuro a ser realizada neste ano —, que, em seu objetivo 5, inclui a melhoria da governança internacional das tecnologias emergentes, incluindo a IA, em benefício da humanidade. O documento propõe uma governança internacional ágil, multidisciplinar e multiator e iniciativas concretas, como estabelecer um Painel Científico Internacional sobre IA e Tecnologias Emergentes e um Grupo de Contato Internacional sobre Governança da IA.

É interessante que esse documento também propõe promover a cooperação Norte-Sul e Sul-Sul no desenvolvimento de conjuntos de dados, capacidade computacional, soluções locais, casos de uso e ecossistemas empresariais em países em desenvolvimento.

No âmbito internacional, já foi mencionada a Convenção-Quadro de IA promovida pelo Conselho da Europa, que se constitui no primeiro tratado internacional sobre o tema, com uma perspectiva de princípios e também de riscos. Como nosso país participou como observador de sua elaboração, pode tornar-se membro da Convenção, o que deverá ser avaliado com a assessoria do Ministério das Relações Exteriores. Desde já, esta Agência afirma compartilhar as disposições da Convenção e apoiar a adesão.

Por fim, no âmbito regional, devem ser especialmente destacados os esforços da UNESCO e do CAF para incorporar a voz regional à discussão sobre o futuro da IA. Da Primeira Cúpula Ministerial e de Altas Autoridades sobre a Ética da IA da América Latina e do Caribe, organizada por essas instituições com apoio do governo do Chile, resultou a já mencionada Declaração de Santiago [94], que aprovou a criação de um Grupo de Trabalho para constituir um Conselho Intergovernamental de IA para a América Latina e o Caribe, no marco da Recomendação sobre a Ética da IA da UNESCO, a fim de fortalecer as capacidades regionais na matéria.

[93] https://www.un.org/techenvoy/global-digital-compact . Último acesso: 22/06/2024.

[94] https://minciencia.gob.cl/uploads/filer_public/40/2a/402a35a0-1222-4dab-b090-5c81bbf34237/declaracion_de_santiago.pdf . Último acesso: 22/06/2024.

Contribuições de outras entidades públicas levantadas na primeira etapa de discussão

Durante a elaboração deste relatório, foram realizadas várias reuniões com as entidades mencionadas neste documento, cujas contribuições podem ser resumidas da seguinte forma:

Eixo de institucionalidade e governança

• Necessidade de uma abordagem transversal, sem prejuízo da importância de contar com um órgão líder na matéria.

• Contar com um comitê consultivo, com papel de assessoria em temas específicos e a integração de diferentes atores conforme os temas a abordar (por exemplo, setor privado, organizações da sociedade civil, empresas de telecomunicações e empresas ligadas ao desenvolvimento de sistemas de IA, entre outros). Propõe-se que o Comitê constitua grupos ad hoc de acordo com o tema específico ou convoque especialistas do setor ou da área a considerar.

• Incluir na análise a defesa do consumidor, a defesa do usuário e a consideração da pessoa como cidadã digital (geradora e usuária de IA)

• Integrar os dados de telecomunicações e contemplar esse ponto como serviço crítico.

• Incluir nas discussões o Ministério da Defesa Nacional (MDN) pela defesa e pelo uso da IA para esse fim, assim como o Ministério do Interior (MI) pelos aspectos de segurança pública.

• Aplicar o mecanismo de consultas públicas para ampliar os atores envolvidos, obtendo e/ou integrando outras visões.

• Incluir e trabalhar no fortalecimento das pequenas e médias empresas.

Eixo de direitos humanos

• Considerar a criação de políticas para os sistemas de IA.

• Quanto à população vulnerável, prestar atenção especial a meninas, meninos, adolescentes e pessoas idosas.

• Especificar que a decisão final deve ser tomada por um ser humano, não pelo algoritmo, e a possibilidade de incorporar auditorias para analisar o impacto da aplicação da IA, institucionalizando essas auditorias.

• Analisar em qual etapa do ciclo do processo deveria ocorrer uma eventual auditoria.

• Definir um órgão e/ou instituição que exerça controle independente para determinados casos de riscos e/ou alto impacto.

• Analisar a viabilidade e/ou pertinência de atribuir maiores competências à INDDHH ou estabelecer algum mecanismo de garantia dos direitos humanos.

• Incorporar um eixo de trabalho que integre a IA para facilitar o acesso aos serviços do Estado.

• Reconhecendo a importância do setor de trabalho, analisar como as empresas poderiam ter um papel propositivo, apresentando alternativas à substituição do trabalho humano pela IA, por exemplo, mediante capacitações para outras tarefas e para o uso de novas tecnologias.

• Analisar a abordagem dos impactos ambientais.

• Considerar a abordagem de riscos.

Eixo de trabalho e capacitação para IA

• Enfatizar o impacto especificamente no emprego e, em termos gerais, no mundo do trabalho.

• Contemplar toda a legislação trabalhista vigente (em particular normas de combate à discriminação no trabalho).

Eixo de propriedade intelectual

• Ampliar a discussão sobre autoria e incorporar o tema do plágio.

• Analisar o desenvolvimento de exceções para o uso de determinados dados no treinamento e estabelecer salvaguardas quando houver direitos autorais, definindo seu alcance e sua finalidade.

• Discutir uma reforma da Lei de Direitos Autorais nº 9739 para contemplar a incidência da IA na matéria.

• Quanto às patentes com intervenção de IA, analisar a necessidade ou não de indicar no pedido de patente como a IA intervém no processo inventivo.

• Incentivar ações para desenvolver a propriedade intelectual.

Eixo de responsabilidade civil e direitos do consumidor

• Determinar o alcance das normas vigentes para contemplar os eventuais danos causados pelo uso de sistemas de IA e aprofundar sua análise antes de formular propostas normativas.

• Analisar a possibilidade de conscientizar a população para que as pessoas identifiquem quando estão em uma relação de consumo vinculada à IA e quais mecanismos existem para reclamações e/ou denúncias.

Eixo de infraestrutura e cibersegurança

• Definir claramente o conceito de IA aplicado à infraestrutura e à cibersegurança.

• Considerar temas como o uso de repositórios de dados em nível internacional, nos âmbitos público e privado.

• Considerar e analisar a qualidade do Software e do Hardware nas instituições públicas.

• Identificar outros tipos de empresas, como as de serviços de armazenamento.

• Considerar a IA aplicada à normalização da infraestrutura de telecomunicações.

• Analisar a possibilidade de centros de capacidade computacional por região.

• Avaliar aspectos ambientais e de uso dos recursos naturais.

• Avaliar as capacidades do país em cada um dos seguintes pontos:

- Normas de gestão e intercâmbio de dados
- Capacidade de armazenamento e de computação
- Cibersegurança

- Capacidade de conectividade e infraestrutura: escalabilidade, flexibilidade e adaptabilidade às mudanças

Eixo de medidas de promoção

• Analisar e definir objetivos estratégicos nacionais para o uso da IA.

• Levantar medidas de promoção existentes nessa matéria e em diferentes aspectos relacionados à IA.

• Analisar a possibilidade de contar com infraestrutura nacional para realizar testes (sandboxes e outros).

• Analisar a possibilidade de isenções e incentivos tributários associados à promoção do desenvolvimento e do uso da IA voltados a objetivos estratégicos do país em diferentes âmbitos.

Recomendações

Conceitos preliminares

Nos capítulos anteriores, apresentou-se uma visão do processo e do marco aplicado na elaboração do relatório atribuído a esta Agência conforme o artigo 74 da Lei nº 20.212.

As recomendações apresentadas resultam da análise institucional realizada a partir do diagnóstico desenvolvido previamente sobre os desafios identificados em cada eixo temático, considerando:

1. as orientações decorrentes do artigo 74 da Lei nº 20.212;
2. o marco jurídico nacional, incluindo as normas de direito internacional aplicáveis e as obrigações jurídicas de respeitar, proteger, garantir e promover os direitos humanos dentro e fora do ambiente digital;
3. os princípios e recomendações decorrentes dos antecedentes internacionais de soft law;
4. a revisão dos antecedentes regulatórios gerados por outros países;
5. as contribuições recebidas de entidades públicas, da sociedade civil e do setor privado no processo de trabalho deste relatório e no de construção das Estratégias lideradas por esta Agência;
6. as orientações da política digital do país decorrentes do Plano de Governo Digital 2025 [95], da Agenda Uruguay Digital 2025 [96] e da Estratégia de IA para o Governo Digital [97].

95 https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/plan-gobierno-digital-2025 . Último acesso: 20/06/2024.

96 https://www.gub.uy/uruguay-digital/comunicacion/publicaciones/agenda-uruguay-digital-2025-actualizacion-medio-termino. Último acesso: 20/06/2024.

97 https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-inteligencia-artificial. Último acesso: 20/06/2024.

Dada a transversalidade dos sistemas de IA e seus impactos positivos e negativos atuais e potenciais em todos os setores da sociedade, estas recomendações não devem ser interpretadas como uma lista exaustiva.

Elas refletem o resultado da análise institucional alcançada na data de apresentação deste relatório sobre aspectos gerais, e não setoriais, em um contexto marcado pelo desenvolvimento vertiginoso das tecnologias — que exige uma análise contínua de seus potenciais e riscos —, por processos em curso nos âmbitos regional e internacional, pela revisão da Estratégia de IA e pela construção das Estratégias Nacionais de Dados e de Cibersegurança.

Tudo isso torna previsível que esses elementos possam, no futuro, afetar os desafios públicos a que se referem estas recomendações e que precisem ser atendidos no processo de trabalho eventualmente iniciado pelo Poder Legislativo.

As análises também partem do conhecimento e da experiência desta Agência em transformação e política digital e das contribuições de outras entidades públicas em âmbitos específicos. Contudo, em vários dos temas analisados, é necessário um debate aprofundado com essas entidades e outros atores antes de adotar qualquer medida.

Recomendações gerais.

O número crescente de instrumentos internacionais desenvolvidos nos últimos anos reflete um cenário de consenso cada vez maior sobre a necessidade de regular as atividades em todo o ciclo de vida dos sistemas de IA, para garantir sua plena coerência com os direitos humanos, a democracia e o Estado de Direito e, ao mesmo tempo, ampliar as oportunidades dessas tecnologias para a humanidade e assegurar o acesso equitativo entre os países e no interior deles.

Como exposto neste relatório, esses instrumentos incluem, entre outros: a Recomendação da OCDE sobre IA e seus princípios adotados em 2019 e atualizados em 2024; a Recomendação sobre a Ética da Inteligência Artificial adotada pela UNESCO em 2021; os princípios de IA e o "Código de Conduta Internacional para Organizações que Desenvolvem Sistemas Avançados de IA", desenvolvido pelo G7 em 2023 no Processo de IA de Hiroshima; o Regulamento de IA da União Europeia, aprovado em março de 2024; a Convenção-Quadro sobre Inteligência Artificial adotada pelo Conselho da Europa em maio de 2024; e a recente Resolução "Sistemas de inteligência artificial seguros e confiáveis para o desenvolvimento sustentável", adotada pela Assembleia Geral das Nações Unidas em março de 2024.

No âmbito interamericano, podem ser citadas, entre outros exemplos, a Declaração de Santiago para promover uma inteligência artificial ética na América Latina e no Caribe, resultante, em 2023, da Cúpula Ministerial e de Altas Autoridades da América Latina e do Caribe, e a Carta Regional sobre Inteligência Artificial na Administração, adotada no Centro Latino-Americano de Administração para o Desenvolvimento (CLAD) em 2023. O Uruguai tem acompanhado esses esforços e, em vários casos, participou de sua elaboração ou aderiu a eles.

Desses antecedentes decorre um apelo claro aos Estados para respeitarem e atuarem proativamente na proteção e promoção dos direitos humanos durante todo o ciclo de vida da IA, adotando marcos regulatórios adequados e efetivos, sob uma abordagem equilibrada que integre os riscos e as oportunidades da IA e promova uma inovação responsável e segura.

Os antecedentes apresentados reconhecem que a governança da IA é um campo em evolução, que exige avançar na construção de marcos comuns e, ao mesmo tempo, contemplar a margem de cada Estado para estabelecer abordagens e instrumentos regulatórios nacionais conforme seus contextos e prioridades, de maneira consistente com seu marco normativo e as obrigações do direito internacional aplicável.

Diante de tudo isso, esta Agência considera pertinente, em primeiro lugar, respaldar a importância de que nosso país mantenha uma abordagem proativa para a

regulação dos sistemas de IA por diferentes instrumentos de política pública:

1. Atualizando, sob uma abordagem de múltiplas partes interessadas, sua Estratégia de Inteligência Artificial para responder ao novo contexto gerado particularmente — e não apenas — pela expansão dos modelos mais avançados, como a IA generativa; e com o objetivo de ampliar o alcance ao setor privado, conforme determinou o artigo 74 da Lei 20.212. Esse processo está em curso e se espera sua conclusão no segundo semestre deste ano.

2. Revisando, quando pertinente, as normas vigentes para:
   i) Reforçar o desenho institucional para a governança da IA no país, incluindo mecanismos para a participação e a colaboração de múltiplas partes interessadas;
   ii) Garantir que as atividades em todo o ciclo de vida dos sistemas de IA sejam plenamente consistentes com os direitos humanos, a democracia e o Estado de Direito, por meio de marcos que permitam identificar, prevenir, avaliar e mitigar os riscos e impactos negativos nesses direitos.

   iii) Impulsionar o aproveitamento equitativo das oportunidades e dos benefícios da IA em favor da sociedade e do desenvolvimento sustentável do país em suas diferentes dimensões (social, cultural, ambiental e econômica), promovendo a pesquisa e a inovação segura em função do interesse público;
   iv) Garantir o desenvolvimento e o uso éticos, respeitosos dos direitos humanos, responsáveis e seguros dos sistemas de IA no setor público;

   v) Fortalecer a soberania digital e a soberania em IA do país com visão de futuro.
3. Desenvolvendo, a partir do setor público, entre outros instrumentos possíveis, protocolos consensuados, guias e recomendações técnicas para os setores e âmbitos críticos para a sociedade e os interesses nacionais e promovendo, quando pertinente, a adoção de instrumentos como diretrizes, códigos e outros mecanismos de autorregulação

alinhados às orientações nacionais; e implementando as políticas e medidas definidas no marco da Estratégia Nacional de Cidadania Digital, da Estratégia Nacional de Dados, da Estratégia Nacional de IA e da Estratégia Nacional de Cibersegurança.

Em segundo lugar, considerando as preocupações e contribuições recebidas da sociedade civil e do setor privado no processo de elaboração deste relatório, esta Agência também gostaria de destacar, como recomendação geral, a importância de que as medidas regulatórias adotadas:

1. sejam precedidas e sustentadas por um processo de discussão pública baseado na abordagem de múltiplas partes interessadas;
2. considerem tanto o impacto da regulação insuficiente quanto o impacto da regulação excessiva;
3. sejam analisadas de forma interdisciplinar, envolvendo diferentes conhecimentos especializados.

O Uruguai tem uma trajetória extensa e contínua em espaços internacionais como a Parceria para Governo Aberto (OGP, na sigla em inglês), por meio da qual impulsionou e implementou iniciativas para integrar os princípios do governo aberto à sua política digital, ao mesmo tempo que definiu os pilares do governo aberto como parte dos objetivos dessa política.

Nesse sentido, e em consonância com outras abordagens internacionais, como a Recomendação da UNESCO sobre a Ética da IA, propõe-se que o país continue e aprofunde o caminho da criação participativa e transparente de suas políticas digitais por meio de políticas de governo aberto e parlamento aberto.

Entre as sugestões e contribuições recebidas por esta Agência durante a elaboração do relatório constam as seguintes medidas específicas propostas, que são levadas ao conhecimento do Poder Legislativo:

- Criar um fórum para identificar prioridades e formular recomendações por diferentes atores sociais.
- Realizar uma audiência pública perante o Poder Legislativo com a participação de empresas, academia e sociedade civil especializada.

- Criar grupos consultivos com a participação de todos os atores, que funcionem regularmente.

Por fim, em terceiro lugar, esta Agência gostaria de destacar, como recomendação geral, a importância de que novos instrumentos regulatórios, caso sejam criados, contemplem um processo de revisão e atualização periódicas em função dos desafios emergentes.

Recomendações específicas

Apresenta-se uma síntese das recomendações com base nas orientações definidas e nos eixos temáticos abrangidos.

Institucionalidade e governança da IA

Como mencionado acima, esse é um aspecto central em muitos instrumentos internacionais. Há várias fórmulas aplicadas em diferentes jurisdições que procuram estabelecer uma institucionalidade específica para a IA, apoiando-se em instituições preexistentes ou criando novas. A definição da institucionalidade da IA no país também afeta os mecanismos de governança de dados — que devem ser estabelecidos — e, portanto, o próprio desenvolvimento da IA.

O papel da Agesic na institucionalidade da IA

Quanto ao papel da Agesic, propõe-se avaliar a possibilidade de ampliar as capacidades atuais da Agência, instituindo uma nova estrutura interna que contemple o eixo de Inteligência Artificial e Dados, incluindo os papéis definidos no último parágrafo do artigo 74 da Lei nº 20.212.

Isso esclareceria a expansão atual das competências da Agência para além da concepção e da implementação da Estratégia Nacional de IA. Também aproveitaria as potencialidades da Agesic, já que aspectos da gestão de dados dentro das entidades públicas são atualmente de sua competência.

Poderia ser apropriado — embora não estritamente necessário — estabelecer uma disposição normativa de nível legal que atribua à Agência competências adicionais às existentes — previstas no artigo 74, parte final, e no artigo 75 da Lei nº 20.212 —, incluindo seu papel na coordenação com outras entidades nacionais e na representação internacional do país sobre o tema. Além disso, cabe lembrar que a liderança da Agência em transformação e política digital decorre de várias disposições preexistentes já resenhadas.

Sem prejuízo da liderança da Agesic na matéria, é necessária a participação de outros atores dentro e fora do setor público para colaborar na concepção e implementação de políticas públicas integrais. Desde sua criação, a Agesic conta com Conselhos Consultivos e lidera diferentes comitês estratégicos.

Quanto à estratégia de adoção de uma política de inteligência artificial e dados, propõe-se institucionalizar normativamente o atual Comitê Estratégico do Setor Público para Inteligência Artificial e Dados, para que coordene com a Agência não apenas o desenvolvimento da Estratégia Nacional de IA e Dados, mas também o planejamento dos planos de ação que permitam sua implementação.

Entre os papéis fundamentais do Comitê estaria colaborar com a Agesic na elaboração de políticas gerais na matéria, além da atuação com outras entidades públicas competentes na elaboração de políticas setoriais. Nesse modelo, caberia às entidades públicas setoriais conduzir a elaboração de normas e recomendações setoriais, o monitoramento e a fiscalização do cumprimento, alertando a Agesic e o Comitê em caso de desvios.

Outro aspecto a considerar, que pode motivar uma composição diferente do Comitê, é a definição de outros temas surgidos do processo participativo de criação das Estratégias Nacionais de IA e de Dados que orientem a política pública nessas áreas.

Conforme o artigo 74, parte final, da Lei nº 20.212, os processos de fiscalização setorial atribuídos a entidades públicas de controle contarão com a colaboração da Agesic — e eventualmente do Comitê — quando houver uso de sistemas de IA.

Além de composições pontuais, esta Agência entende que algumas entidades devem integrar essa institucionalidade (por exemplo, ANII, MIEM, URCDP e INDDHH), para cumprir as orientações do Poder Legislativo sobre o desenvolvimento de uma IA baseada na ética, que promova a inovação e respeite os direitos humanos.

A institucionalidade da IA no âmbito interno das organizações

Sugerem-se duas frentes de ação dentro das entidades públicas: i. capacitação e fortalecimento em IA e Dados; e ii. fortalecimento estrutural para dotar cada instituição das capacidades de gerir, monitorar e controlar as políticas implementadas, assim como executar planos estratégicos e operacionais alinhados a elas.

Existem atualmente funções que devem ser obrigatoriamente instituídas pelas entidades públicas e se relacionam à governança dos dados: o delegado de proteção de dados pessoais — instituído pelo artigo 40 da Lei nº 19.670, de 15 de outubro de 2019 —; o responsável pela transparência — instituído pelos artigos 41 e 57 do Decreto nº 232/010, de 2 de agosto de 2010, que regulamenta a Lei nº 18.381, de 17 de outubro de 2008 —; e o responsável pela segurança da informação — instituído legalmente pelo artigo 78, alínea B, da Lei nº 20.212, de 6 de novembro de 2023.

A particularidade das funções de delegado de proteção de dados e responsável pela segurança da informação é que se estendem não apenas a entidades públicas, mas também a algumas entidades privadas:

- a primeira função se estende àquelas entidades privadas que tratam dados sensíveis como atividade principal — sendo a definição de dados sensíveis taxativa e prevista no artigo 4, alínea E, da Lei nº 18.331, de 11 de agosto de 2008 — e às que tratam grandes volumes de dados — definidos como dados de mais de 35.000 pessoas pelo artigo 10, alínea c, do Decreto nº 64/020, de 17 de fevereiro de 2020 —;

- a segunda se refere a entidades privadas ligadas a serviços ou setores críticos do país — o que depende da definição da regulamentação, que ainda não havia sido editada.

A isso deve ser acrescentada a necessidade de responsáveis que implementem as políticas de dados abertos nas entidades públicas, vinculadas ao cumprimento do artigo 82 da Lei nº 19.355, de 12 de dezembro de 2015.

Esta Agência entende ser possível reconverter as funções já existentes, especialmente a do delegado de proteção de dados, mediante capacitação em IA e governança de dados. Parece, sim, conveniente criar, dentro das organizações públicas, um Comitê Interno de Dados que inclua o delegado de proteção de dados, o responsável pela segurança da informação, o responsável pela transparência e o ponto focal de dados abertos.

Perspectiva multissetorial e multidisciplinar

Ao longo deste relatório, mencionou-se reiteradamente a necessidade de definir as políticas sob uma perspectiva de múltiplos atores, incluindo entidades públicas, privadas, academia e sociedade civil e considerando também os diferentes setores produtivos.

Também se propôs que os órgãos contem com papéis estratégicos em IA e Dados que viabilizem o desenvolvimento das políticas e ampliem as oportunidades oferecidas por ambos os temas.

Para isso, propõe-se partir das institucionalidades existentes na Agesic, modificando as competências do Conselho Consultivo Honorário da Sociedade da Informação e incorporando, eventualmente, novos atores, em um esquema semelhante ao que existe atualmente em cibersegurança. A multidisciplinaridade também deverá ser contemplada.

Existem atualmente na Agesic dois espaços relacionados à IA que convém manter e fortalecer: 1) a Comunidade de IA na Administração Pública [98], integrada por representantes técnicos de diferentes entidades públicas; 2) o Observatório do Uso de IA no Estado [99], criado como parte de um compromisso

[98] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/comunidad-inteligencia-artificial-administracion-publica . Último acesso: 29/03/2023.

[99] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/observatorio-uso-inteligencia-artificial-estado . Último acesso: 29/03/2024.

assumido no 5º Plano de Ação de Governo Aberto. Ambos os espaços viabilizam a participação de diferentes atores do ecossistema, com finalidades complementares e de grande valor para o desenvolvimento da IA, destacando-se a participação da sociedade civil e de técnicos especializados.

Governança de dados

Por fim, quanto à governança de dados, deve-se continuar avançando nas obrigações das entidades públicas de publicar dados com segurança — pela plataforma prevista na regulamentação — e respeitando a proteção dos dados pessoais, indo além da obrigação estabelecida no artigo 5 da Lei nº 18.381, de 17 de outubro de 2008.

Devemos também continuar avançando rumo a um modelo de governança de dados que dê sustentabilidade à política definida na matéria.

Também é importante continuar promovendo a obrigatoriedade do intercâmbio de informações — dentro do marco vigente — entre entidades públicas (artigo 157 e seguintes da Lei nº 18719), para incentivar a reutilização dos dados, e avançar na definição dos responsáveis pelos dados mestres de Governo.

O uso de dados de entidades privadas também pode fazer diferença. Para isso, poderiam ser promovidas medidas de incentivo caso essas entidades decidam compartilhar dados — não necessariamente pessoais, mas úteis à definição de políticas públicas. Esses incentivos não estão presentes nas normas vigentes, mas poderiam incluir isenções tributárias e melhorias na prestação de serviços, além de aspectos estritamente reputacionais.

No âmbito internacional, o Regulamento (EU) 2023/2854 (Data Act) [100] estabelece direitos dos usuários de dispositivos para acessar e compartilhar seus dados, obrigações das empresas privadas de compartilhar informações quando solicitadas por entidades públicas e de cumprir requisitos mínimos que

[100] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854&qid=1704709568425 . Último acesso: 21/06/2024.

assegurem a interoperabilidade — em consonância com a estratégia de padronização para um mercado único, resiliente, verde e digital —, entre outros pontos.

Essa regulação também é um dos pilares da estratégia europeia de dados e de sua política de transformação digital, complementando-se com o Regulamento (EU) 2022/868 (Data Governance Act) [101], que estabelece as bases dos processos de intercâmbio de dados e prevê conceitos interessantes, como o "altruísmo de dados", que permite compartilhar informações para objetivos de interesse geral, com salvaguardas apropriadas.

Nos aspectos de uso de dados no mercado, deve ser incluída a perspectiva da Unidade de Defesa do Consumidor e da Comissão de Promoção e Defesa da Concorrência, ambas do Ministério da Economia e Finanças.

Quanto aos dados pessoais e ao treinamento de sistemas, parece necessário discutir a regulação atual das bases legítimas de tratamento de dados pessoais. O artigo 9 da Lei nº 18.331, de 11 de agosto de 2008, omite bases de tratamento existentes internacionalmente, e as bases atuais podem gerar dificuldades interpretativas ao serem aplicadas ao treinamento de sistemas de IA. Embora isso não impeça necessariamente o uso dos dados, a ausência de uma base de legitimação, como o legítimo interesse, acrescenta complexidade e leva a considerar se outras bases podem ser usadas para esses fins.

Outros instrumentos, como os fideicomissos de dados sugeridos pela INDDHH, começaram a integrar a discussão. No entanto, o delicado equilíbrio do tratamento de dados pessoais previsto na Lei nº 18.331 motiva que essa discussão seja liderada pela Urcdp.

[101] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0868 , Último acesso: 21/06/2024.

Resumo das recomendações sobre institucionalidade e governança	
Recomendações voltadas a eventuais modificações ou atualizações normativas	- Criar Comitês Internos de Dados nas entidades públicas, incluindo responsáveis pela transparência, delegados de proteção de dados, responsáveis pela informação e pontos focais de dados abertos. - Promover o uso de dados abertos e interoperáveis, considerando novas obrigações para as entidades públicas sobre a publicação de dados em formato aberto, estabelecendo prazos e condições para essa publicação
Outras iniciativas recomendadas	- Especificar as atribuições da Agesic ligadas à liderança em IA e Dados - Criar uma nova institucionalidade dentro da Agesic encarregada da política de IA e Dados. - Institucionalizar o Comitê Estratégico do Setor Público para IA e Dados. - Reformular o Conselho Consultivo Honorário da Sociedade da Informação para incorporar novos atores e funções. - Definir um modelo de governança de dados de governo. - Fortalecer a capacitação das entidades públicas e dotá-las das capacidades necessárias para assegurar a implementação de políticas, estratégias e planos operacionais de IA e dados

	- Oferecer capacitação em dados e IA a delegados de proteção de dados e outras funções relacionadas à gestão de dados nas entidades públicas. - Promover incentivos para que entidades privadas compartilhem dados, respeitando as normas de proteção dos dados pessoais e de propriedade intelectual e por mecanismos seguros. - Promover a criação de bases de dados públicas que contenham informações que contemplem o idioma e as características locais e possam servir como dados de treinamento para sistemas de IA. - Viabilizar o uso da plataforma de interoperabilidade prevista no Decreto nº 178/013, de 11 de junho de 2013, por entidades privadas.

Ética, direitos humanos e democracia

O ponto de partida para a proteção dos direitos humanos

O Uruguai mantém vínculo estreito com os Sistemas Interamericano e Universal de proteção dos direitos humanos, ratificou os tratados de direitos humanos decorrentes desses sistemas e participa ativamente de seus espaços. As recomendações deste tópico partem do conjunto de obrigações (respeitar, proteger e garantir) que a proteção internacional dos direitos humanos impõe aos Estados.

Na mesma linha, a recente Resolução sobre IA da Assembleia Geral das Nações Unidas destaca “que os direitos humanos e as liberdades fundamentais devem ser respeitados, protegidos e promovidos durante todo o ciclo de vida dos sistemas de inteligência artificial” e “insta todos os Estados-membros e, quando cabível,

outros interessados a se absterem de usar ou deixarem de usar sistemas de inteligência artificial que sejam impossíveis de operar em conformidade com o direito internacional ou que representem riscos indevidos para o gozo dos direitos humanos, especialmente de quem se encontra em situações vulneráveis, e reafirma que os direitos das pessoas também devem ser protegidos na Internet, inclusive durante o ciclo de vida dos sistemas de inteligência artificial" [102].

A proteção jurídica dos direitos humanos em nosso país se apoia na Constituição da República, nas normas do direito internacional dos direitos humanos que foram ratificadas e em um amplo e diversificado conjunto de leis que especificam a proteção e regulam o exercício de determinados direitos. No entanto, em alguns casos, a proteção jurídica dos direitos humanos neste campo seria fortalecida com o desenvolvimento de normas que especificassem a proteção neste âmbito.

Medidas especiais voltadas à proteção dos direitos humanos

Em função do exposto na seção anterior, e partindo do que já foi alcançado por meio da Lei Nº 20.212, a primeira recomendação aponta para ampliar a especificação de princípios voltados à Estratégia de IA feita pelo artigo 74 dessa norma, indicando-os como princípios orientadores das políticas de IA e de seus diferentes instrumentos regulatórios.

Esses princípios podem ser complementados com medidas que lhes deem conteúdo substantivo e permitam colocá-los em prática, tomando como base os artigos 6° a 12° da Lei N° 18.331, que não apenas enumeram o alcance dos princípios, mas também determinam certas ações que devem ser realizadas na prática pelos responsáveis e operadores do tratamento de dados pessoais.

Complementarmente, e a partir da orientação que decorre do próprio artigo 74 da Lei Nº 20.212, devem ser abordados os riscos e impactos adversos atuais e potenciais sobre os direitos humanos envolvidos no ciclo de vida dos

[102] https://documents.un.org/doc/undoc/gen/n24/087/86/pdf/n2408786.pdf?token=ZTiBbJsISYXoE5uIOW&fe=true

sistemas de IA, nos setores público e privado, por meio da regulação e de outras medidas.

Em função da necessidade de abordar os riscos e impactos mencionados, sugere-se avaliar a adoção de uma abordagem baseada no risco com o objetivo de:

1. Analisar e definir as aplicações dos sistemas de IA que sejam

   inaceitáveis para a sociedade por seu impacto sobre os direitos das pessoas, avaliando as proibições ou moratórias que sejam adequadas e compatíveis com a obrigação de proteger os direitos humanos; e

2. Identificar e definir as aplicações da IA que representem um

   alto risco para os direitos das pessoas em função do contexto e do uso previsto, da gravidade e da probabilidade dos possíveis impactos, com o objetivo de definir as medidas específicas aplicáveis.

Para abordar os riscos, diferentes modelos e abordagens vêm sendo desenvolvidos no direito comparado. Por exemplo:

• O Regulamento de IA da União Europeia estabelece um conjunto de aplicações proibidas (Título II do Regulamento), entre as quais se incluem a manipulação cognitiva do comportamento de pessoas que afete a autonomia e a capacidade de escolher livremente, os sistemas de categorização biométrica baseados em dados biométricos e os usos de sistemas de IA para a identificação biométrica remota em tempo real de pessoas físicas em espaços de acesso público para fins de aplicação da lei, estabelecendo exceções.

• A Ordem Executiva adotada em 2023 pelo Governo dos Estados Unidos determina que as entidades governamentais, de acordo com suas respectivas competências, adotem diferentes medidas destinadas a dispor de diretrizes e padrões para o desenvolvimento e a implementação responsável da IA segundo sua área de atividade, e estabelece um conjunto de obrigações voltadas ao fornecimento de informações a diferentes agências nacionais pelas empresas que desenvolvam determinados modelos de IA.

• Da mesma forma, o artigo 16 da Convenção-Quadro adotada em março pelo Conselho da Europa estabelece que cada Parte avaliará a necessidade de uma moratória ou proibição ou de outras medidas apropriadas em relação a determinados usos dos sistemas de IA quando considerar que esses usos são incompatíveis com o respeito aos direitos humanos, o funcionamento da democracia ou o Estado de Direito.

Assim, sugere-se avaliar, para determinados tipos de riscos que exijam medidas especiais:

1. Estabelecer, de forma obrigatória e prévia, uma avaliação de impacto sobre os direitos humanos;

2. Estabelecer o dever de inscrição do sistema em um Registro estatal de acesso público a cargo da entidade que lidere a política de IA no país;

3. Submeter os sistemas a um processo de autorização ou certificação prévia segundo a finalidade ou o tipo de sistema em questão;

4. Prever mecanismos de auditoria periódica dos sistemas e eventual encaminhamento dos resultados à entidade responsável por sua revisão;

5. Complementar as normas que garantem a transparência e a explicabilidade dos sistemas de IA utilizados para tomar decisões ou apoiar a tomada de decisões e a supervisão humana relacionada ao funcionamento e aos resultados desses sistemas.

Por outro lado, como destacou o relatório preliminar do Órgão Consultivo de Alto Nível sobre IA da ONU, a IA oferece importantes oportunidades para a humanidade e a realização dos direitos das pessoas, por seu potencial de melhorar a prestação de serviços públicos e facilitar o acesso ao conhecimento, à educação, à assistência à saúde, ao desenvolvimento produtivo, à agricultura etc.

Consequentemente, além de abordar os riscos, recomenda-se considerar a promoção do desenvolvimento de sistemas de IA que tenham como finalidade o bem comum

por meio da determinação de finalidades consideradas compatíveis com esse propósito, definindo também apoios e medidas de promoção, entre outros.

Implementação de direitos

Da perspectiva das pessoas, sugere-se considerar a implementação, por meio de disposições legais, de determinados direitos, como:

1. O direito de saber que se está interagindo com um sistema de IA;

2. O direito de obter informações básicas sobre o funcionamento do sistema e os resultados esperados, por meio de uma pessoa física, se necessário; e

3. Eventualmente, o direito de recorrer quando uma decisão for adotada com base nesse sistema, complementando o direito de contestação de avaliações pessoais e o direito à informação previstos na Lei Nº 18.331 de proteção de dados pessoais.

Igualdade e não discriminação

A atual Estratégia Nacional de Cidadania Digital [103] assinala que os "impactos que podem surgir no contexto do desenvolvimento de tecnologias disruptivas, como a inteligência artificial (IA), vão além do individual, abrangendo efeitos coletivos e sociais. Ou seja, pode-se falar de impactos sistêmicos de muitas dessas tecnologias digitais. Por exemplo, os relacionados a seus efeitos sobre o futuro dos trabalhos e a democracia como elementos-chave".

No trabalho de pesquisa "Construyendo ciudadanía en entornos digitales. Perspectivas transversales de abordaje [104]", seguindo o documento da CEPAL "Ciudadanía digital en América Latina. Revisión conceptual de iniciativas",

[103] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-nacional-ciudadania-digital-para-sociedad-informacion . Último acesso: 20/06/2024.

[104] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/construyendo-ciudadania-entornos-digitales-perspectivas-transversales-3 . Último acesso: 20/04/2024.

afirma-se que o conceito de exclusão digital hoje está associado a desigualdades nos usos e benefícios das tecnologias digitais (decorrentes de diferenças no nível socioeconômico, na idade, no gênero, no capital cultural e nas habilidades digitais).

Esse trabalho afirma a necessidade de incorporar uma perspectiva de inclusão ou igualdade digital e de desenvolver as habilidades necessárias para superar as limitações de acesso e de capacidades, assim como para compreender as regras do jogo e refletir sobre nossos próprios comportamentos.

As medidas adotadas em função das recomendações deste documento deveriam integrar uma abordagem que considere especialmente a maior vulnerabilidade enfrentada por diversos grupos da sociedade, adotando marcos e políticas para abordar os vieses que possam aprofundar as desigualdades, proteger as pessoas contra todas as formas de discriminação e zelar para que os resultados discriminatórios não sejam transferidos aos sistemas de IA e, quando for o caso, sejam detectados e corrigidos.

Enfrentar os desafios para as democracias

Em âmbito global, cresce cada vez mais a preocupação com os impactos da desinformação, a proteção da integridade dos processos democráticos e a capacidade das pessoas de formar sua opinião livremente.

Nesse sentido, por exemplo, ao analisar os impactos e riscos envolvidos na Inteligência Artificial, o relatório provisório do Órgão Consultivo de Alto Nível sobre IA da ONU [105] analisa que alguns riscos da IA se originam nas limitações técnicas desses sistemas, como no caso dos vieses prejudiciais ou das chamadas alucinações na IA generativa, enquanto outros são produto do uso humano, como as deep fakes, que “podem representar grave risco para a confiança social e o debate democrático”.

A Resolução AG/RES. 3004 (LIII-O/23) sobre “Fortalecimento da Democracia” [106], aprovada na quarta sessão plenária de 23 de junho de 2023 da

[105] https://www.un.org/sites/un2.un.org/files/ai_advisory_body_interim_report.pdf. Último acesso: 20/06/2024.
[106] https://scm.oas.org/doc_public/SPANISH/HIST_23/AG08884S03.docx . Último acesso: 20/06/2024.

Organização dos Estados Americanos (OEA), resolveu encarregar a Secretaria-Geral do desenvolvimento de uma agenda interamericana sobre tecnologias emergentes, particularmente no que se refere ao uso ético de políticas de IA, algoritmos e governança de dados, no âmbito de um conjunto de medidas destinadas precisamente ao fortalecimento democrático.

A preocupação internacional diante dos desafios mencionados se refletiu na última atualização dos Princípios sobre IA da OCDE, realizada em 2024, na qual um dos objetivos foi precisamente refletir a crescente importância de abordar esses fenômenos no contexto da IA generativa. Nesse sentido, os princípios propõem "abordar a desinformação amplificada pela IA, respeitando, ao mesmo tempo, a liberdade de expressão e outros direitos e liberdades protegidos pelo direito internacional aplicável" [107].

Enquanto continuam os esforços globais para compreender esse fenômeno e como abordá-lo, é necessário pensar em medidas não apenas restritivas — sem dúvida necessárias —, mas também de alfabetização digital e informacional, gerando habilidades instrumentais e fundamentais para a interação crítica das pessoas no ambiente digital.

Como parte dessas medidas, podem ser promovidos mecanismos para identificar a manipulação de informações e os conteúdos gerados por IA, bem como políticas para fortalecer as habilidades digitais das pessoas — neste último caso, apoiadas, em nosso país, na Estratégia Nacional de Cidadania Digital —.

Mecanismos e recursos acessíveis, adequados e efetivos

Existem em nosso ordenamento jurídico diferentes entidades públicas com competências em matéria de direitos humanos fora do âmbito do sistema de justiça, como a Instituição Nacional de Direitos Humanos e Defensoria do Povo, a Unidade Reguladora e de Controle de Dados Pessoais e a Unidade de Acesso à Informação Pública, entre outras.

[107] https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449#mainText. Último acesso: 20/06/2024.

Para garantir que as eventuais violações dos direitos humanos resultantes do uso da IA sejam atendidas por mecanismos e recursos acessíveis, adequados e efetivos, sugere-se realizar uma análise dos mecanismos atuais para identificar se existe a necessidade de fortalecer as competências específicas dos organismos existentes ou de criar novos mecanismos necessários, assim como a articulação de suas competências.

Regulação do desenvolvimento, uso e aquisição de IA no setor público

A Carta Ibero-Americana de Inteligência Artificial na Administração Pública, adotada em 2023 no âmbito do CLAD, tem "como objetivo principal promover um modelo compartilhado de desenvolvimento da Inteligência Artificial a partir das e nas administrações públicas do âmbito ibero-americano [108]". Como base para esse marco comum, o capítulo 3 propõe um conjunto de princípios gerais da IA na Administração Pública: autonomia humana; transparência, rastreabilidade e explicabilidade; prestação de contas, responsabilidade e auditabilidade; segurança e robustez técnica; confiabilidade, precisão e reprodutibilidade; confiança, proporcionalidade e prevenção de danos; privacidade e proteção dos dados pessoais; qualidade e integridade dos dados; equidade, inclusão e não discriminação; centralidade das pessoas, valor público e responsabilidade social; e sustentabilidade e proteção ambiental.

Ao identificar as dimensões-chave para a adoção da IA na Administração Pública, a Carta propõe como componente das estratégias nacionais que: "as legislações nacionais deveriam atender a questões que tornem os sistemas algorítmicos seguros, transparentes, rastreáveis, não discriminatórios e ambientalmente sustentáveis. Também deveria ser adaptada a normativa de proteção dos dados pessoais, assim como do uso e da reutilização dos dados públicos em geral. Adicionalmente, deve-se garantir que os sistemas de Inteligência Artificial sejam supervisionados por humanos, em vez de serem completamente autônomos, minimizando os potenciais danos e eliminando situações de risco extremo. Além disso, devem ser estabelecidos mecanismos robustos de cibersegurança para manter a integridade dos dados e a

[108] https://clad.org/wp-content/uploads/2023/10/Borrador-CIIA-V1-ES-08-2023.pdf. Último acesso: 20/05/2024.

inviolabilidade das infraestruturas tecnológicas. Finalmente, seria necessário garantir que os algoritmos públicos sejam transparentes e não proprietários ou sujeitos a patentes, promovendo infraestruturas tecnológicas baseadas em arquiteturas abertas".

São princípios compartilhados com a Estratégia de IA atualmente em processo de revisão, na qual também se destaca que "toda solução tecnológica que utilize IA deve respeitar os Direitos Humanos, as liberdades individuais e a diversidade".

Em função do caminho que o Uruguai já vem percorrendo no âmbito de sua política digital nacional, centrada nas pessoas por definição, recomenda-se continuar fortalecendo os instrumentos regulatórios referentes ao âmbito público, integrando os componentes da nova Estratégia de IA a ser adotada em 2024 relativos ao uso e ao desenvolvimento dessas tecnologias especificamente nesse âmbito.

Nesse sentido, uma medida pontual a considerar é a realização de avaliações de impacto sobre os direitos humanos como requisito para a aquisição, o desenvolvimento e/ou o uso dos sistemas de IA por entidades públicas em áreas em que se determine que possa existir alto risco para os direitos das pessoas. Em função do que já foi exposto, e em particular, recomenda-se analisar, como parte do conjunto de medidas a avaliar, a regulação do desenvolvimento, da aquisição e da aplicação de sistemas de vigilância para fins de segurança pública.

Adicionalmente, e considerando que está em curso a elaboração das estratégias de Dados e Cibersegurança, também será relevante considerar as diretrizes ali definidas para identificar os elementos que exijam uma regulação legal que complemente os marcos gerais preexistentes.

Capacitação e educação para a IA

Como foi mencionado ao considerar o eixo temático de trabalho e capacitação para IA, este relatório identifica medidas concretas voltadas especificamente à formação das pessoas e ao fortalecimento de suas habilidades.

Outros aspectos relacionados ao impacto da IA no mundo do trabalho exigirão desenvolvimentos mais abrangentes e uma discussão aberta com a participação do Estado, dos empregadores, dos trabalhadores e dos sindicatos, de modo a alcançar acordos que potencializem os benefícios da aplicação dessa tecnologia e mitiguem os efeitos adversos.

No entanto, da perspectiva deste relatório, podem ser feitas as seguintes recomendações, sugerindo-se:

1. a promoção de programas de capacitação por meio de entidades do ensino técnico, superior e universitário em temas de IA e gestão de dados, em colaboração com câmaras empresariais, sindicatos e outros agrupamentos;

2. estabelecer apoios específicos ou benefícios particulares para as empresas que realizem cursos voltados à IA para seus trabalhadores e quadros gerenciais, em setores predefinidos;

3. avaliar a obrigação de os empregadores capacitarem os trabalhadores que devam aplicar ou que possam ser afetados por sistemas de IA, antes de sua implementação, em setores predefinidos.

Resumo de recomendações em ética, direitos humanos e democracia	
Recomendações voltadas a eventuais modificações ou atualizações normativas	- Explicitar os princípios enumerados no artigo 74 da Lei 20.2012 como princípios orientadores da política nacional de IA e de sua implementação. - Definir riscos que sejam inaceitáveis para a sociedade; e identificar os usos que representem alto risco e exijam medidas

	especiais, definindo também essas medidas. - Avaliar a adoção de medidas voltadas a combater a desinformação e proteger a integridade dos processos democráticos e a capacidade das pessoas de formar sua opinião livremente. - Analisar o fortalecimento dos mecanismos existentes ou a criação de novos mecanismos para resolver violações dos direitos humanos resultantes de sistemas de IA. - Regular direitos instrumentais em favor da transparência, da explicabilidade e da possibilidade de contestação.
Outras iniciativas recomendadas	- Estabelecer normas específicas com relação ao desenvolvimento, uso e aquisição da IA no Setor público. - Avaliar os instrumentos regionais e internacionais de cooperação na matéria. - Analisar a adoção de medidas com o objetivo de continuar abordando as desigualdades digitais e fortalecer o desenvolvimento da cidadania digital.

	- Promover iniciativas de uso da IA para o bem da sociedade. - Promover a capacitação especialmente de trabalhadores, em colaboração com câmaras empresariais, sindicatos e outros agrupamentos, e estabelecer apoios específicos ou benefícios particulares para as empresas que realizem cursos voltados à IA, em setores predefinidos. - Avaliar a obrigação de os empregadores capacitarem os trabalhadores que devam aplicar ou que possam ser afetados por sistemas de IA, antes de sua implementação, em setores predefinidos.

Inovação responsável

Segurança jurídica nos aspectos da responsabilidade civil e da Propriedade Intelectual

Das análises realizadas surge a necessidade de revisar o regime nacional de responsabilidade civil, pois não parece razoável recorrer a interpretações ou integrações de normas que não correspondem à realidade atual, para assim oferecer maior certeza a desenvolvedores, usuários e outros atores do sistema.

Sugere-se considerar as seguintes alternativas: i. determinar, com as entidades competentes, sugestões de conteúdos mínimos em contratos firmados entre quem disponibiliza sistemas e quem os utiliza. Nesse sentido, poderão ser consideradas como antecedentes as normas em matéria de responsabilidade proativa da proteção de dados pessoais; ii. estabelecer uma comissão de

análise que se concentre especificamente em uma eventual reforma do regime de responsabilidade civil na matéria.

A segurança jurídica também está associada a um sistema adequado de atribuição de direitos no caso de criações nas quais esteja envolvido, de alguma forma, um sistema de IA.

Esta Agência sugere:

1. Incluir, no caso de obras geradas por IA sem intervenção humana direta, uma indicação dessa circunstância na própria obra e, em alguns casos, a referência ao sistema utilizado para a criação da obra. Poderiam ser propostas exceções relacionadas ao uso doméstico ou a outras finalidades;

2. Iniciar um processo de consulta sobre como serão consideradas as obras geradas exclusivamente por IA. Atualmente, não existe uma consolidação da opinião de que essas obras possam ser atribuídas a esses sistemas, de modo que a consulta deveria ser realizada com todos os atores envolvidos, considerando não apenas os aspectos associados à atribuição da titularidade, mas também as compensações econômicas correspondentes;

3. Considerar uma definição sobre o sistema a aplicar às obras assistidas por IA, por exemplo, atribuindo-o a quem dirige o processo criativo da obra finalizada [109];

4. Reafirmar que o alcance do tratamento dos dados utilizados por esses sistemas para a geração de novas obras dependerá da normativa vigente — artigo 35 da Lei N° 9.376 e artigo 9° bis da Lei N° 18.331 —.

Em outros aspectos relacionados à propriedade intelectual, sugere-se considerar que:

[109] Podem ser vistas diferentes alternativas a respeito em MANTEGNA. Op. Cit. Pág. 309.

1. No que se refere à inscrição registral, continuar com o processo já iniciado pela Lei N° 20.212 e avaliar a possibilidade de comunicação entre esse registro, outros registros e a publicação de software público indicada no artigo 7° do decreto N° 44/015, no caso das entidades públicas;

2. Ampliar o alcance do artigo 2° da Lei N° 19.179 aos programas de computador (programas-fonte ou programas-objeto), compilações de dados ou de outros materiais, em qualquer forma, que, em razão da seleção ou disposição de seus conteúdos, constituam criações de caráter intelectual, e à expressão de ideias, informações e algoritmos, formulada em sequências originais ordenadas de forma apropriada para ser usada por um dispositivo de processamento de informações ou de controle automático.

Infraestrutura e cibersegurança

Este relatório já apresentou a necessidade de contar com uma infraestrutura adequada para o desenvolvimento da IA e o papel relevante do Estado para alcançar esse objetivo.

Seguindo o relatório da OCDE examinado ao analisar este eixo, parece necessário adotar um conjunto de medidas associadas à revisão das capacidades computacionais nos setores público e privado, considerar o número, a capacidade e a disponibilidade dos centros de dados existentes, definir padrões em matéria de gestão de dados, analisar as capacidades de processamento e as necessidades de hardware no país, determinar a demanda potencial de processamento para IA, distinguir as necessidades de processamento para IA, oferecer capacitação e treinamento, mapear e analisar as cadeias de suprimentos.

Considera-se necessário gerar ou atualizar instrumentos normativos que facilitem a aquisição, a operação e a manutenção dessas infraestruturas, de modo a impulsionar uma gestão da capacidade que se adapte rapidamente ao avanço exponencial apresentado por essa tecnologia em particular.

Para os fins deste relatório, cujo objetivo é oferecer recomendações ao Poder Legislativo, as análises realizadas também devem estar voltadas à determinação de se as disposições normativas vigentes estão alinhadas às necessidades na matéria.

Dessa perspectiva, esta Agência deseja destacar que existe legislação e regulamentação abundante em aspectos como o intercâmbio de dados, a cibersegurança, o tratamento de informações — pessoais e não pessoais —, as redes de telecomunicações e as aquisições no âmbito público, entre outros. Pode-se reconhecer, sim, a dificuldade gerada pela dispersão normativa existente, de modo que poderia ser relevante organizar as normas mencionadas por meio de um texto consolidado ou de instrumentos semelhantes.

A cibersegurança, em particular, é objeto de regulação desde a criação da Agesic e, recentemente, sua relevância foi destacada com a sistematização de diferentes disposições e a atualização das competências da Agência e das obrigações de entidades públicas em geral e de algumas privadas em particular, em vários artigos da Lei N° 20.212.

Os resultados do processo de construção da Estratégia Nacional de Cibersegurança e os objetivos estratégicos decorrentes desse processo — como já foi mencionado repetidas vezes neste relatório — serão um insumo central para a determinação de novas medidas que contribuam para um ecossistema seguro para o desenvolvimento da IA e de outras tecnologias.

Em matéria de infraestrutura, e considerando as contribuições recebidas ao longo do processo de elaboração deste relatório, a Agesic propõe promover um diálogo com outros atores nesse aspecto, para o que são sugeridas como alternativas:

1. Acrescentar como atribuição específica do Conselho Consultivo de Informática Pública a de colaborar na definição de recomendações;

2. Articular ações com o Comitê de Governança de Processos e Soluções Transversais criado pelo decreto N° 431/022, de 27 de dezembro de 2022,

3. Definir, juntamente com a Agência Reguladora de Compras Estatais (ARCE), requisitos específicos para contratações associadas ao desenvolvimento de sistemas de IA.

Em particular, nos aspectos de fundamentação normativa para o intercâmbio de dados de forma segura, recomenda-se habilitar o uso da Plataforma de Interoperabilidade criada pelo decreto N° 178/013 para o consumo de serviços por entidades privadas e avaliar a modificação do decreto N° 92/014, para esclarecer normativamente as hipóteses associadas ao uso de serviços de provedores de nuvem.

Uma perspectiva integral da infraestrutura e dos processos para a transformação digital

É necessário trabalhar em uma perspectiva integral, repensando a forma como se propõe o uso da infraestrutura e dos processos do Estado, facilitando a implantação de tecnologias como a IA.

Nesse sentido, deveria ser buscada a promoção do aproveitamento da IA como uma oportunidade para melhorar os serviços públicos, a eficiência do Estado e a tomada de decisões baseadas em dados.

Propostas como a Infraestrutura Pública Digital (DPI, na sigla em inglês) permitem uma abordagem integral para realizar processos de transformação digital mais eficientes. Recentemente, foi lançada a iniciativa denominada “Salvaguardas da DPI”. Essa iniciativa tem como objetivo compartilhar lições aprendidas, criando um marco para minimizar riscos nos níveis técnico, normativo e organizacional e, em última análise, um ambiente para uma implementação segura, inclusiva, prática e adaptável da DPI [110].

Nessa perspectiva, a melhoria da infraestrutura do Estado, que dá suporte a tecnologias como a IA, deve resultar em benefício para a inovação e a

110 O relatório provisório da iniciativa pode ser acessado em: https://safedpi.gitbook.io/safeguards/working-group-documents/reports . Último acesso: 22/06/2024.

pesquisa nos setores público e privado, contribuindo para o desenvolvimento econômico e social do país.

Nessa lógica, deveria ser buscado que os componentes da infraestrutura, quando cabível, possam ser aproveitados por atores do ecossistema de inovação, científico e empreendedor, considerando especialmente as diferentes características desses atores.

Impactos ambientais da infraestrutura

Embora o aspecto ambiental não tenha feito parte dos eixos temáticos centrais deste relatório, é indispensável fazer alguma referência aos impactos que o desenvolvimento acelerado da tecnologia em geral e da IA em particular tem sobre o meio ambiente.

O uso da IA pode gerar grandes benefícios para mitigar os impactos das mudanças climáticas e, de fato, diferentes iniciativas, inclusive em âmbito nacional, promovem desenvolvimentos que enfrentem esse problema [111].

No entanto, existem aspectos de impacto negativo relacionados à extração de materiais para a criação de componentes de hardware, ao uso da água e ao consumo de energia, entre outros, o que torna necessário trazer as autoridades e os atores relevantes a essa discussão.

A recomendação sobre a ética da IA da UNESCO assinala claramente a necessidade de que todos os participantes do ciclo de vida dos sistemas de IA respeitem as normas e práticas nacionais e internacionais relacionadas à precaução, concebidas para a proteção e a restauração do meio ambiente e dos ecossistemas e para o desenvolvimento sustentável.

O CLAD inclui entre os princípios de sua carta o da sustentabilidade e proteção ambiental, defendendo o uso de tecnologias ambientalmente sustentáveis e energeticamente não poluentes, fundamentadas na aplicação de materiais e

111 Ver, como exemplo: https://www.anii.org.uy/apoyos/innovacion/309/fondo-de-investigacion-e-innovacion-en-cambio-climatico/ . Último acesso: 20/06/2024.

dispositivos reutilizáveis e fontes de energia renováveis, tudo em consonância com os ODS.

Diante do exposto, a perspectiva ambiental deve estar presente em toda iniciativa associada ao desenvolvimento de infraestrutura para a IA.

Medidas de promoção

As medidas de promoção são múltiplas e deveriam se concentrar não na promoção da tecnologia, mas em objetivos a alcançar por meio dela. Na análise realizada, foram mencionadas algumas medidas decorrentes de normas vigentes e as entidades responsáveis por realizá-las.

Em janeiro deste ano, a Comissão Europeia lançou um conjunto de medidas de apoio a startups europeias e pequenas e médias empresas para o desenvolvimento de IA segura. Esse conjunto inclui a instalação de fábricas de IA com supercomputadores acessíveis às PMEs, apoio ao uso de modelos de IA de propósito geral, a criação de um escritório de IA na Comissão, apoio financeiro por meio de diferentes programas e o desenvolvimento de espaços de dados, entre outros.

Do processo de construção das estratégias lideradas por esta Agência surge, de forma reiterada, a necessidade de que o desenvolvimento de infraestrutura contemple instrumentos como benefícios tarifários, isenções tributárias e incentivos à importação de componentes e à exportação de serviços a partir de nosso país, entre outros.

Algumas medidas de promoção, como incentivos, isenções e outros benefícios que já existem em normas vigentes, podem ser orientadas ou reorientadas ao fomento de atividades que, graças à IA, possam resultar em benefício para a economia, a sociedade e, em última análise, as pessoas.

Em matéria de apoio à IA no Setor Público, já em 2021 o Banco Mundial [112] sugeria a instalação de um hub central de inovação para IA no governo,

[112] https://documents1.worldbank.org/curated/en/746721616045333426/pdf/Artificial-Intelligence-in-the-Public-Sector-Summary-Note.pdf . Último acesso: 21/06/2024.

semelhante ao programa da UIH com que nosso país conta atualmente. Nesse documento, o Banco Mundial assinala que os investimentos devem ser direcionados ao capital humano e à infraestrutura digital, priorizando a pesquisa, o empreendedorismo, as tecnologias digitais fundamentais e as habilidades digitais.

Os objetivos traçados a esse respeito estão relacionados, entre outros e a critério desta Agência, aos objetivos já definidos na Agenda Digital Uruguay 2025 e aos que resultem do processo de construção das estratégias nacionais de Dados e Cibersegurança e da atualização da Estratégia Nacional de Inteligência Artificial.

Além das alternativas de apoio financeiro sustentadas em normas vigentes, existem outros tipos de medidas que promovem o uso responsável da IA, entre os quais encontramos os sandboxes regulatórios e os espaços de dados, instrumentos que possibilitam a experimentação segura, um marco de responsabilidade delimitado e a colaboração de múltiplas partes (setor público, privado, academia e sociedade civil).

Por sua vez, deve ser continuado o caminho da cooperação internacional na matéria, assim como a assinatura de acordos que possibilitem um melhor posicionamento do país em inovação e pesquisa segura em IA, como ocorre com a assinatura do recente Tratado de Cooperação em Matéria de Patentes.

Resumo de recomendações em matéria de fomento à inovação em IA	
Recomendações voltadas a eventuais modificações ou atualizações normativas	- Impulsionar a extensão da atribuição prevista no artigo 74 da Lei N° 19.149, de 24 de outubro de 2013, a toda a Administração.

	- Ampliar o alcance do artigo 2° da Lei N° 19.179, de 27 de dezembro de 2013.
Outras iniciativas recomendadas	- Estabelecer uma comissão interdisciplinar de análise para uma eventual reforma do regime de responsabilidade civil na matéria. - Analisar, juntamente com os organismos competentes, propostas de conteúdos mínimos de alcance da responsabilidade nos contratos firmados entre desenvolvedores, usuários e outros atores de sistemas de IA. - Em matéria de Propriedade Intelectual, promover uma discussão sobre as alternativas para a geração de obras por IA sem intervenção humana direta e para as obras assistidas por IA. - Continuar com o processo de inscrição iniciado pela Lei N° 20.212, de 6 de novembro de 2023, e avaliar a comunicação entre esse registro, outros registros e a publicação de software público. - Avaliar a inclusão, como atribuição específica do Conselho Consultivo de Informática Pública, de colaborar com a Agesic na definição das recomendações necessárias para o desenvolvimento adequado da infraestrutura para IA em âmbito nacional.

	- Considerar a elaboração de uma análise relacionada à infraestrutura atual e integral na matéria, que considere especialmente medidas de investimento público e de promoção do investimento privado. - Avaliar a definição de uma nova política de uso de nuvem em relação à determinada no decreto N° 92/014, de 7 de abril de 2014. - Estabelecer a colaboração entre entidades responsáveis pela promoção de iniciativas em matéria de infraestrutura de IA, incluindo, em especial, a perspectiva ambiental. - Consolidar as ferramentas necessárias para realizar as ações definidas na Estratégia Nacional de Cibersegurança. - Finalizar a proposta de regulamentação dos ambientes controlados de teste e de outras medidas de promoção da inovação e realizar sua implementação. - Avaliar, juntamente com o MEF, o MIEM, a ANII e outras entidades públicas competentes, a determinação das medidas de apoio necessárias.

Anexo 1: Antecedentes nacionais

Mapeamento da legislação nacional

Para a elaboração deste relatório, foi considerada a existência de um conjunto de disposições de nível legal e regulamentar, que procurou se concentrar estritamente nos aspectos relacionados aos eixos temáticos definidos e à sua relação com a IA.

A seguir, apresenta-se uma tabela com as disposições identificadas, diferenciadas segundo o eixo temático associado e uma breve descrição de cada uma delas.

Institucionalidade da IA

Normas aplicáveis	Resumo do conteúdo
Artigo 74 Lei N° 20.212, de 6 de novembro de 2023	Atribui à Agesic a concepção e o desenvolvimento de uma estratégia nacional de dados e de IA. Além disso, o parágrafo final estabelece expressamente que ela fará recomendações específicas a entidades dos setores público e privado para o desenvolvimento e a implementação dos sistemas de inteligência artificial mencionados e para a fiscalização de seu cumprimento, sem prejuízo das competências próprias da URCDP e de outras entidades públicas em seus respectivos âmbitos de atuação.
Artigo 34 Lei N° 18.331, de 11 de agosto de 2008, na redação dada pelo artigo 63 da Lei N° 20.075, de	Estabelece, entre as atribuições da URCDP, a de definir os critérios e procedimentos que devem ser observados pelos responsáveis e operadores no tratamento automatizado de dados pessoais indicado no artigo 16 da lei N° 18.331.

20 de outubro de 2022.	

Governança de dados

Normas aplicáveis	**Tema**	Resumo do conteúdo
Lei N° 18.331, de 11 de agosto de 2008, suas alterações e normas correlatas, e N° 19.670, de 15 de outubro de 2018. Regulamentadas por decretos N° 414/009, de 31 de agosto de 2009, e 64/020, de 17 de fevereiro de 2020.	Dados Pessoais	São estabelecidas as formas de tratamento dos dados pessoais nos setores público e privado, associadas a um conjunto de princípios.
Lei N° 18.381, de 17 de outubro de 2008. Norma regulamentada pelo decreto N° 232/010, de 2 de agosto de 2010.	Informação Pública	Estabelece-se o caráter público das informações em poder do Estado, assim como suas exceções.
Artigos 157 a 160 da Lei N° 18.719,	Interoperabilidade e intercâmbio	São estabelecidas as condições para a interoperabilidade e o intercâmbio de informações públicas e privadas nos termos da regulamentação. Norma regulamentada

de 27 de dezembro de 2010		pelo decreto N° 178/013, de 11 de junho de 2013.
Decreto N° 259/012, de 13 de agosto de 2012	Dados abertos e Governo Aberto	O Uruguai adere à “Declaração sobre Governo Aberto” da “Parceria para Governo Aberto” e é estabelecido o primeiro plano de ação, sucedido por outros planos posteriores.
Artigo 82 da Lei N° 19.355, de 19 de dezembro de 2015	Dados Abertos e Governo Aberto	Estabelece-se a obrigação dos organismos públicos de publicar as informações contidas no artigo 5° da Lei N° 18.381 em formato de dados abertos. Norma regulamentada pelo decreto N° 54/017, de 20 de fevereiro de 2017.
Artigo 76 da Lei N° 19.355, de 19 de dezembro de 2015 na redação dada pelo artigo 2 da Lei N° 19.670, de 15 de outubro de 2018	Interoperabilidade e intercâmbio	Estabelece-se a obrigação dos organismos públicos de não solicitar certificados, declarações, certidões ou outra documentação de natureza semelhante emitida por outra entidade pública quando for possível acessar as informações contidas nesses documentos por meio de sistemas informatizados fornecidos pelas entidades competentes. Norma regulamentada pelo decreto N° 353/023, de 9 de novembro de 2023.
Decreto N° 357/016, de 7 de novembro de 2016	Dados Abertos e Governo Aberto	É criado o Grupo de Trabalho de Governo Aberto, integrado por um representante de cada um dos seguintes organismos: Agesic, OPP, UAIP. MEF, MRREE, MIEM e INE. Também são estabelecidas suas atribuições.

Aplicação de princípios em IA

Normas	Resumo do conteúdo
Artigo 74 Lei N° 20.212, de 6 de novembro de 2023	Atribui à Agesic a concepção e o desenvolvimento de uma estratégia nacional de dados e de IA. O artigo, em seu segundo parágrafo, estabelece que "(a) estratégia deverá se fundamentar em princípios de equidade, não discriminação, responsabilidade, prestação de contas, transparência, auditoria e inovação segura, respeitando a dignidade humana, o sistema democrático e a forma republicana de governo. Os princípios da proteção de dados pessoais incluídos na Lei N° 18.331, de 11 de agosto de 2008, serão parte dessa estratégia".
Artigo 5° Lei N° 18.331, de 11 de agosto de 2008.	O artigo estabelece como princípios da proteção de dados pessoais, que o artigo 74 inclui na Estratégia de IA, os seguintes: legalidade, veracidade, finalidade, consentimento informado prévio, segurança dos dados, sigilo e responsabilidade (proativa).

Propriedade Intelectual

Normas aplicáveis	Resumo do conteúdo
Constituição Nacional, art. 33	Estabelece que o trabalho intelectual e o direito do autor, do inventor ou do artista serão reconhecidos e protegidos pela lei

Lei N° 9.739, de 17 de dezembro de 1937, alterada pelas Leis N° 17.616, de 10 de janeiro de 2003, 19.857, de 23 de dezembro de 2019 e 20.212, de 6 de novembro de 2023. Regulamentada pelos Decretos N° 154/004, de 3 de maio de 2004, 295/017, de 16 de outubro de 2017, 404/023, de 12 de dezembro de 2023	Reconhece aos autores o domínio sobre as produções de seu pensamento, ciência e arte. Incluem-se na proteção da lei os programas de computador ou software e as compilações de dados que, por seu conteúdo, constituam uma criação intelectual. São previstos direitos, um prazo determinado de proteção, condutas lícitas e ilícitas e eventuais sanções. As obras são registradas na Biblioteca Nacional, com exceção dos programas de computador, compilações de dados ou outros materiais que constituam criações intelectuais, expressão de ideias, informações e algoritmos formulados em sequências originais ordenadas para serem usadas por um dispositivo de processamento de informações ou de controle automático e as transmissões dos direitos patrimoniais sobre essas obras, que serão inscritas no Registro de Software da DNPI.
Lei N° 14.910, de 19 de julho de 1979	Por essa Lei, são aprovadas as convenções para a proteção da propriedade industrial, para a proteção das obras literárias e artísticas e para a propriedade intelectual (Convenções de Paris e Berna).
Lei N° 16.671, de 13 de dezembro de 1994	São aprovados os acordos assinados resultantes da Rodada Uruguai de Negociações Comerciais Multilaterais, contidos na Ata Final assinada em Marrakech em 15 de abril de 1994 e, em particular, o Acordo sobre os Aspectos dos Direitos de Propriedade Intelectual Relacionados ao Comércio (ADPIC).

Lei N° 17.011, de 25 de setembro de 1998. Regulamentada pelo decreto N° 34/999, de 3 de fevereiro de 1999.	Regula a proteção conferida às marcas, definidas como sinal apto a distinguir os produtos ou serviços de uma pessoa física ou jurídica dos de outra. São estabelecidos tipos de marcas, direitos, prazos de proteção, registro e nulidades absolutas e relativas em relação a determinados sinais. Regula também os nomes comerciais, as indicações geográficas, as denominações de origem e as indicações de procedência.
Lei N° 17.164, de 2 de setembro de 1999. Regulamentada pelo decreto N° 11/000, de 13 de janeiro de 2000.	Regulam-se os direitos e obrigações relativos a patentes de invenção, modelos de utilidade e desenhos industriais. São estabelecidos, assim como no caso anterior, direitos, nulidades, prazos de proteção, registro e eventuais sanções.
Lei N° 18.036, de 20 de outubro de 2006.	É aprovado o Tratado da Organização Mundial da Propriedade Intelectual (OMPI) sobre Direito de Autor e as Declarações Acordadas relativas ao Tratado da OMPI sobre Direito de Autor.
Lei 18.253, de 20 de fevereiro de 2008	Aprovação do Tratado da Organização Mundial da Propriedade Intelectual sobre interpretações ou execuções e fonogramas e das declarações acordadas relativas a ele.
Lei N° 19.179, de 27 de dezembro de 2013. Regulamentado pelo decreto N° 44/015,	Regula o formato para o processamento e o armazenamento de informações digitais em determinadas entidades públicas e privadas.

de 30 de janeiro de 2015.	

Infraestrutura e Cibersegurança

Normas aplicáveis	Resumo do conteúdo
Lei N° 17.296, de 21 de fevereiro de 2001, artigos 70 a 94 bis, na redação dada pelos artigos 143 e 418 da Lei N° 18.719, de 27 de dezembro de 2010 e 256 a 273 da Lei N° 19.889, de 9 de julho de 2020, entre outros. Regulamentado pelo decreto N° 212/001, de 4 de maio de 2001.	São estabelecidas as competências da Unidade Reguladora de Serviços de Comunicações (URSEC) — atualmente serviço descentralizado —, do Ministério da Indústria, Energia e Mineração (MIEM) e, em particular, da Direção Nacional de Telecomunicações e Serviços de Comunicação Audiovisual (DINATEL) em matéria de telecomunicações. Quanto à URSEC, foram estabelecidas como principais atribuições a regulação e o controle das atividades e dos setores referentes às telecomunicações e aos serviços postais. A definição de políticas cabe ao MIEM.
Lei N° 18.331, de 11 de agosto de 2008. Regulamentada pelos decretos N° 414/009, de 31 de agosto de 2009 e	Estabelece-se o marco geral para a comunicação de dados pessoais entre entidades dos âmbitos público e privado, assim como os requisitos básicos que devem ser cumpridos para dar segurança aos tratamentos de dados pessoais. O decreto N° 64/020, de 17 de fevereiro de 2020, em particular, recomenda a adoção de determinadas medidas de segurança em seus artigos 3° e

64/020, de 17 de fevereiro de 2020.	4°, sugerindo expressamente a adoção do Marco de Cibersegurança da Agesic.
Lei N° 18.719, de 27 de dezembro de 2010, artigo 149, na redação dada pelo artigo 84 da Lei N° 19.924, de 18 de dezembro de 2020.	A Agesic é encarregada de dirigir as políticas, metodologias e melhores práticas e de regular a segurança da informação e a cibersegurança em âmbito nacional, assim como de fiscalizar e auditar seu cumprimento e oferecer apoio nas etapas de sua implementação em todas as entidades públicas e, também, nas entidades privadas vinculadas a serviços ou setores críticos do país.
Lei N° 18.719, de 27 de dezembro de 2010, artigos 157 a 160. Regulamentados pelo decreto N° 178/013, de 11 de junho de 2013.	São estabelecidas regras para a interoperabilidade entre organismos públicos. São definidos o papel da Agesic na matéria e suas competências. A regulamentação determina a criação de uma plataforma de interoperabilidade gerenciada por essa agência para o intercâmbio de informações entre entidades públicas.
Decreto 92/014, de 7 de abril de 2014	Para o âmbito da Administração Central, estabelece-se a obrigação de que os centros de dados seguros estejam situados em território nacional, excetuando-se os que não constituam um risco para o organismo. Da mesma forma, em Anexo, são estabelecidas as condições físicas de segurança que devem ser colocadas em prática pelas entidades públicas. Também é prevista a possibilidade de contemplar exceções, cuja concessão compete à Agesic.
Lei N° 19.924, de 18 de dezembro de 2020, artigos 372	É extinta a Secretaria Nacional de Ciência e Tecnologia e são modificadas, no âmbito do Ministério da Educação e Cultura, a denominação e as competências da Direção

a 375, que extinguem a entidade criada pela Lei N° 19.355, de 19 de dezembro de 2015, artigo 34, cujas competências estavam regulamentadas pelo decreto N° 324/017, de 10 de novembro de 2017.	para o Desenvolvimento da Ciência e do Conhecimento, que passa a se chamar Direção Nacional de Inovação, Ciência e Tecnologia. A regulamentação da Secretaria mencionada havia estabelecido, entre suas competências, as de propor projetos de políticas de ciência, tecnologia e inovação, promover o maior desenvolvimento das capacidades de conectividade e telecomunicações e propor infraestruturas no campo da ciência, da tecnologia e da inovação, em áreas estratégicas para o desenvolvimento do país.
Lei N° 20.075, de 20 de outubro de 2022, artigo 461, regulamentado pelo decreto N° 216/023, de 17 de julho de 2023	O artigo dispõe uma dotação orçamentária para o programa de pesquisa, inovação e desenvolvimento experimental para promover projetos em ciência, tecnologia e inovação, sendo regulamentada pelo decreto citado a criação do Programa Uruguay Innovation Hub, na Agência Nacional de Pesquisa e Inovação (ANII). Entre seus instrumentos encontram-se, por exemplo, a instalação de laboratórios abertos, mediante apoios financeiros e operacionais.
Lei N° 20.212, de 6 de novembro de 2023, artigos 78 a 84.	Embora existam múltiplas normas que regulam aspectos de cibersegurança, tanto em nível legal quanto regulamentar, destaca-se o impulso que esses artigos dão à matéria, impondo determinadas obrigações de nível legal a entidades públicas e a entidades privadas vinculadas a setores ou serviços críticos do país, assim como instrumentos para o controle e a fiscalização de seu cumprimento a cargo da Agesic. Por outro lado, estabelece-se a composição de duas entidades

	consultivas da Agesic em matéria de cibersegurança e a definição das bases para uma Estratégia Nacional.

Trabalho e capacitação para a IA

Normas aplicáveis	Resumo do conteúdo
Lei N° 18.046, de 24 de outubro de 2008. Regulamentada pelo decreto N° 52/021, de 8 de fevereiro de 2021.	Lei de criação do Instituto Nacional de Emprego e Formação Profissional (INEFOP). Inclui entre suas atribuições o assessoramento na definição de políticas de capacitação e formação para gerar e melhorar o emprego.
Lei N° 18.437, de 12 de dezembro de 2008. Regulamentada pelos decretos N° 334/009, de 20 de julho de 2009 e 294/013, de 11 de setembro de 2013.	Declara-se de interesse geral a promoção do gozo e do efetivo exercício do direito à educação como direito humano fundamental.
Lei N° 19.121, de 20 de agosto de 2013.	Regula o Estatuto do Funcionário Público da Administração Central, promovendo a capacitação dos funcionários públicos, o que é considerado fundamental para o acesso e a progressão no cargo.

Decreto N° 340/018, de 22 de outubro de 2018.S	É criada a Comissão Nacional de Certificação Ocupacional no âmbito do INEFOP.
Lei N° 19.973, de 13 de agosto de 2021. Regulamentada pelo decreto N° 308/021, de 10 de setembro de 2021.	São estabelecidas políticas de emprego para favorecer a atividade remunerada de jovens, adultos e pessoas com deficiência, incluindo sua capacitação e formação.

Responsabilidade civil e direitos do consumidor

Normas aplicáveis	Resumo do conteúdo
Código Civil	As normas em matéria de responsabilidade estão nos artigos 1246 e seguintes do Código Civil, prevendo-se a responsabilidade contratual e extracontratual na forma mencionada e, salvo exceções, um regime de responsabilidade subjetiva para todos os tipos. Em particular, cabe considerar, neste tema, o artigo 1330.
Lei N° 17.250, de 11 de agosto de 2000. Regulamentada pelo decreto N° 244/000, de 23 de agosto de 2000.	No caso específico das relações de consumo, também é previsto um regime de responsabilidade subjetiva. Estabelece algumas especificidades relacionadas à responsabilidade nos artigos 34 a 36.

Medidas de promoção

Normas aplicáveis	Resumo do conteúdo
Lei N° 16.906, de 7 de janeiro de 1998. Regulamentada pelo decreto N° 92/998, de 21 de abril de 1998.	Lei de investimentos e promoção industrial.
Artigo 461 da Lei N° 20.075, de 20 de outubro de 2022	É destinada uma dotação anual de $ 400.000.000 (quatrocentos milhões de pesos uruguaios), com recursos das Receitas Gerais, com o objetivo de promover projetos em ciência, tecnologia e inovação aprovados pelo Ministério da Economia e Finanças, com o assessoramento do Escritório de Planejamento e Orçamento, por proposta da Agência Nacional de Pesquisa e Inovação.
Decreto N° 216/023, de 17 de julho de 2023	É criado o Programa Uruguay Innovation Hub para promover o ecossistema empreendedor e inovador.
Lei N° 20.121, de 23 de agosto de 2023. Regulamentada pelo decreto N° 360/023, de 14 de novembro de 2023.	Lei relacionada ao incentivo ao estabelecimento, no Uruguai, de técnicos e profissionais do setor de tecnologias da informação

Artigo 75 Lei N° 20.212, de 6 de novembro de 2023	Promove-se a criação de ambientes controlados de teste para projetos que tenham como objetivo, entre outros, a construção de sistemas que apliquem a IA.

Anexo 2: Antecedentes internacionais

Princípios e recomendações internacionais

A atenção aos sistemas de inteligência artificial tornou-se onipresente na agenda dos organismos e fóruns internacionais, abrangendo os mais diversos temas e áreas: desde como a Inteligência Artificial pode ajudar a alcançar os Objetivos de Desenvolvimento Sustentável até os debates sobre sua aplicação no âmbito militar.

Em meio a essa diversidade, no entanto, é possível identificar um ponto de partida comum em vários dos esforços internacionais concluídos ou em curso voltados à governança da inteligência artificial: a ênfase na necessidade de construir uma governança orientada a potencializar as oportunidades e os benefícios da inteligência artificial para a humanidade, assegurando o acesso equitativo a esses benefícios e abordando, ao mesmo tempo, os desafios e riscos decorrentes dessas tecnologias.

Para isso, como se depreende dos antecedentes apresentados a seguir, boa parte dos esforços em curso enfatiza a necessidade de adotar uma abordagem que: coloque as pessoas no centro; proteja os direitos humanos, a democracia e o Estado de Direito; esteja fundamentada no direito internacional e no direito internacional dos direitos humanos; promova sistemas de inteligência artificial seguros e confiáveis, desenvolvidos e utilizados de maneira ética; e promova a inovação para aproveitar o potencial da IA em benefício da humanidade e do desenvolvimento sustentável.

O objetivo deste anexo do Relatório é apresentar uma síntese dos princípios orientadores e das recomendações que buscam orientar as ações dos Estados na formulação de sua legislação, políticas ou outros instrumentos relacionados à IA provenientes do âmbito internacional, em função da revisão dos antecedentes internacionais realizada no contexto da preparação deste relatório. Esses princípios e recomendações devem ser entendidos como um complemento às obrigações internacionais de direitos humanos decorrentes, para os Estados, do direito internacional vigente.

A seleção dos antecedentes apresentados foi realizada em função de sua relevância internacional e de seu impacto no Uruguai; eles são apresentados em cada subseção em ordem cronológica.

Nações Unidas

No âmbito da Organização das Nações Unidas, está em curso um processo voltado à governança internacional da Inteligência Artificial, impulsionado pelo Secretário-Geral, ao mesmo tempo em que está em negociação o Pacto Digital Global, que incluiria um capítulo específico sobre Inteligência Artificial. Prevê-se que o Pacto seja adotado no âmbito da Cúpula do Futuro, que ocorrerá em setembro próximo. Os processos em curso têm como antecedentes, entre outros, os marcos no âmbito da Organização das Nações Unidas indicados a seguir nesta seção.

Recomendação da UNESCO sobre a ética da IA (2021)

A Recomendação sobre a Ética da Inteligência Artificial foi adotada em novembro de 2021 pela Conferência Geral da Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO) [113]. Tem o propósito de orientar os Estados na formulação de suas leis e políticas relativas à inteligência artificial. Para isso, a Recomendação promove um conjunto de valores [114], princípios e ações de política.

O texto analisa “as repercussões positivas e negativas profundas e dinâmicas da inteligência artificial” sobre as sociedades, o ambiente e a vida humana e propõe que “o fato de considerar os riscos e as preocupações éticas não deveria impedir a inovação e o desenvolvimento”, mas, ao contrário, estimular

[113] UNESCO. Recomendação sobre a Ética da Inteligência Artificial, adotada em 23 de novembro de 2021. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa . Último acesso:29/4/2024.

[114] Os valores indicados são: Respeito, proteção e promoção dos direitos humanos, das liberdades fundamentais e da dignidade humana. Prosperidade do meio ambiente e dos ecossistemas. Garantir a diversidade e a inclusão. Viver em sociedades pacíficas, justas e interconectadas.

uma pesquisa e uma inovação realizadas de maneira ética e baseadas nos direitos humanos [115].

Em 2023, o Uruguai aderiu à Recomendação da UNESCO, reforçando assim o compromisso do país com sua implementação no âmbito da nova Estratégia de Inteligência Artificial e da primeira Estratégia Nacional de Dados 116. Diante do exposto e de sua importância como marco de referência para a elaboração deste Relatório, apresenta-se, a seguir, uma síntese dos 10 princípios orientadores promovidos pela Recomendação.

Princípios da UNESCO [117]

Princípio	**Alcance**
Proporcionalidade e não causar danos.	A Recomendação propõe que se deveria garantir a aplicação de procedimentos de avaliação de riscos e medidas para impedir danos aos seres humanos, ao ambiente e aos ecossistemas. Da mesma forma, deveria ser garantido que os processos relacionados ao ciclo de vida dos sistemas de IA se restrinjam a propósitos ou objetivos legítimos. A Recomendação sustenta que os sistemas de IA não deveriam ser utilizados para fins de pontuação social ou vigilância em massa.
Segurança e proteção.	A Recomendação indica que os riscos de segurança e proteção deveriam ser identificados,

[115] Ibíd. Preâmbulo.

[116] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/uruguay-adhiere-recomendacion-etica-inteligencia-artificial-unesco . Último acesso 09/02/2024.

[117] Com base nos parágrafos 25 a 47 da Recomendação sobre a Ética da IA da UNESCO.

	prevenidos e eliminados ao longo do ciclo de vida da IA.
Equidade e não discriminação	A Recomendação destaca que deveria ser adotada uma abordagem inclusiva para assegurar que os benefícios das tecnologias de IA estejam disponíveis e sejam acessíveis a todas as pessoas, considerando as necessidades específicas dos diferentes grupos. Também sustenta que deveriam ser abordadas as desigualdades digitais dentro dos países e entre eles e os vieses ao longo do ciclo de vida dos sistemas de IA.
Sustentabilidade	A Recomendação destaca a necessidade de avaliar os impactos das tecnologias da IA sobre a sustentabilidade, isto é, a avaliação contínua dos efeitos humanos, sociais, culturais, econômicos e ambientais envolvidos nessa tecnologia.
Direito à privacidade e proteção de dados.	A Recomendação propõe que a privacidade deve ser respeitada, protegida e promovida ao longo do ciclo de vida dos sistemas de IA. Sustenta que os sistemas algorítmicos exigem avaliações adequadas do impacto sobre a privacidade e assinala que deveriam ser estabelecidos marcos de proteção de dados e mecanismos de governança de dados adequados, de acordo com a abordagem de múltiplas partes interessadas.
Supervisão e decisão humanas	A Recomendação sustenta que os Estados-Membros deveriam zelar para que, em qualquer etapa do ciclo de vida dos sistemas de IA, sempre

	seja possível atribuir a responsabilidade ética e jurídica a pessoas físicas ou a entidades jurídicas existentes.
Transparência e explicabilidade	A Recomendação afirma que as pessoas deveriam ser plenamente informadas quando uma decisão se basear em algoritmos de IA ou for tomada a partir de seus resultados, particularmente quando afetar seus direitos, e propõe que deveriam existir mecanismos adequados para revisar e corrigir a decisão. Sustenta que os atores da IA deveriam informar os usuários de maneira adequada e oportuna quando um produto ou serviço for fornecido diretamente ou com a ajuda de um sistema de IA. A Recomendação define que a explicabilidade consiste em tornar inteligíveis os resultados dos sistemas de IA e fornecer informações sobre eles. Também se refere à inteligibilidade da entrada, da saída e do funcionamento de cada componente algorítmico e à forma como contribui para os resultados dos sistemas (rastreabilidade).
Responsabilidade e prestação de contas	A Recomendação propõe que os atores da IA e os Estados-Membros deveriam respeitar, proteger e promover os direitos humanos e fomentar a proteção do meio ambiente e dos ecossistemas, assumindo sua respectiva responsabilidade ética e jurídica. Para isso, deveriam ser elaborados mecanismos adequados de supervisão, avaliação de impacto, auditoria e devida diligência, inclusive no que se refere à proteção dos denunciantes de

	irregularidades, para garantir a prestação de contas em relação aos sistemas de IA e a seu impacto ao longo de seu ciclo de vida.
Conscientização e educação.	A Recomendação enfatiza que a conscientização e a compreensão pública sobre as tecnologias da IA, seu funcionamento e impacto deveriam ser promovidas por meio de uma educação aberta e acessível, da participação cívica, das competências digitais, da capacitação em ética da IA e da alfabetização midiática e informacional.
Governança e colaboração adaptativas e de múltiplas partes interessadas.	A Recomendação propõe que, para assegurar uma abordagem inclusiva na governança da IA, é necessário garantir a participação das diferentes partes interessadas (os governos, as organizações intergovernamentais, a academia, a sociedade civil, o setor privado e as instituições de direitos humanos, entre outras).

Para a implementação desses princípios, a Recomendação da UNESCO promove um conjunto de ações específicas a serem implementadas pelos Estados e por outros atores. Em função do objeto deste relatório, destacam-se as seguintes:

- Zelar para que os mecanismos de governança da IA sejam inclusivos, transparentes, multidisciplinares e contem com múltiplas partes interessadas.
- Assegurar que a legislação em matéria de sistemas de IA se ajuste às obrigações dos Estados-Membros em matéria de direitos humanos

e promova os direitos humanos e as liberdades fundamentais ao longo do ciclo de vida desses sistemas.

• Elaborar ou adaptar, conforme apropriado, marcos regulatórios para alcançar a prestação de contas e a responsabilidade pelo conteúdo e pelos resultados dos sistemas de IA nas diferentes etapas de seu ciclo de vida. Esses marcos deveriam considerar que a responsabilidade e a prestação de contas devem sempre recair, em última instância, sobre pessoas físicas ou jurídicas e que não se deve conceder personalidade jurídica aos próprios sistemas de IA. Esses marcos deveriam também incorporar o princípio da supervisão humana.

• Contar com marcos para proteger os dados pessoais e garantir uma supervisão eficaz e independente no âmbito de um mecanismo de governança de dados.

• Estabelecer requisitos claros de transparência e explicabilidade dos sistemas de IA para ajudar a garantir a confiabilidade desses sistemas durante todo o seu ciclo de vida. Esses requisitos deveriam abranger a concepção e a aplicação de mecanismos de avaliação de impacto que considerem a natureza do âmbito de aplicação, a utilização prevista, os destinatários e a viabilidade de cada sistema de IA em particular.

• Assegurar o cumprimento das leis, políticas e práticas ambientais por todos os atores da IA.

• Destinar recursos específicos do orçamento público ao financiamento de planos com perspectiva de gênero, zelar para que as políticas digitais nacionais incluam um plano de ação em matéria de gênero e elaborar políticas pertinentes.

• Promover programas gerais de conscientização sobre os avanços da IA, particularmente sobre os dados, as oportunidades oferecidas e os desafios apresentados pelas tecnologias da IA, o impacto dos sistemas de IA nos direitos humanos, incluindo os direitos das crianças, e suas repercussões. Esses programas deveriam ser acessíveis tanto aos grupos técnicos quanto aos não técnicos.

• Promover a pesquisa e incentivar as empresas do setor privado a facilitar o acesso da comunidade científica a seus dados para pesquisa.

• Garantir que os atores da IA respeitem e promovam a liberdade de expressão e o acesso à informação no que se refere à geração, moderação e conservação automáticas de conteúdos, por meio de marcos adequados, inclusive regulamentares, que propiciem a transparência, zelem para que os usuários tenham acesso a pontos de vista diversos e prevejam processos de notificação rápida aos usuários sobre os motivos da remoção ou de outro tratamento dos conteúdos, assim como mecanismos de recurso que permitam aos usuários solicitar reparação.

• Avaliar e abordar o impacto dos sistemas de IA sobre os mercados de trabalho e suas consequências para as necessidades educacionais de cada país.

• Impulsionar e apoiar os esforços de outros atores para adequar os programas e as estratégias de capacitação às implicações futuras do trabalho e às necessidades da indústria, incluindo as pequenas e médias empresas, implementar programas de aperfeiçoamento e requalificação profissional e explorar programas de proteção social para aqueles que não possam se requalificar.

• Adotar as medidas adequadas para garantir a competitividade dos mercados e a proteção dos consumidores, considerando possíveis medidas e mecanismos nos planos nacional, regional e internacional, a fim de impedir os abusos de posição dominante no mercado, incluindo os monopólios, em relação aos sistemas de IA durante seu ciclo de vida.

Princípios e recomendações preliminares do Órgão Consultivo de Alto Nível sobre Inteligência Artificial (2023).

Este antecedente decorre do Relatório provisório: Governar a IA para a humanidade (Interim Report: Governing AI for Humanity), elaborado pelo Órgão Consultivo sobre Inteligência Artificial das Nações Unidas, publicado em dezembro

de 2023 [118]. O órgão foi criado nesse mesmo ano por iniciativa do Secretário-Geral, com o objetivo de tratar dos riscos, das oportunidades e da governança internacional da IA, e é integrado por especialistas independentes [119].

O relatório do órgão consultivo descreve um conjunto de oportunidades e riscos envolvidos nos sistemas de IA e analisa que o déficit de governança global leva a uma distribuição desigual dos benefícios e riscos no mundo. Destaca a necessidade de identificar e abordar os riscos da IA, incluindo a construção de consenso sobre quais riscos são inaceitáveis e como podem ser prevenidos ou antecipados.

As recomendações do Órgão Consultivo enfatizam a necessidade de uma governança global internacional da IA baseada em cinco princípios orientadores, resumidos a seguir.

Princípios para a governança internacional da IA promovidos pelo Órgão Consultivo sobre IA da ONU

Princípio	**Alcance**
A IA deve ser governada de forma inclusiva, por e para o benefício de todos.	O relatório propõe que a IA deve ser governada de modo que todas as pessoas e todos os países, independentemente de seu nível de desenvolvimento, possam se beneficiar dela.
A IA deve ser regida pelo interesse público.	O relatório sustenta que são necessárias normas vinculantes aplicadas de forma consistente pelos

[118] https://www.un.org/sites/un2.un.org/files/un_ai_advisory_body_governing_ai_for_humanity_interim_report.pdf . Último acesso:29/4/2024.

[119] A lista completa de integrantes está disponível no seguinte link: https://www.un.org/en/ai-advisory-body/members Último acesso:29/4/2024.

	Estados-membros para garantir que os interesses públicos prevaleçam.
A governança da IA deve ser construída de maneira conjunta com a governança dos dados e a promoção dos dados comuns.	O relatório propõe a necessidade de considerar como os dados são coletados, armazenados e compartilhados, para assegurar que sejam compartilhados e utilizados de uma maneira que beneficie a sociedade como um todo.
A governança da inteligência artificial deve ser universal, em rede e estar enraizada em uma colaboração adaptativa entre múltiplas partes interessadas.	O relatório destaca que qualquer esforço de governança da inteligência artificial deve priorizar o apoio universal de diferentes Estados-Membros e partes interessadas e a participação inclusiva do Sul Global, considerando os diferentes contextos culturais.
A governança da IA deve se basear nas normas e compromissos internacionais.	O relatório promove que a governança da IA deve se basear na Carta das Nações Unidas, no direito internacional dos direitos humanos e em outros compromissos internacionais acordados, como os Objetivos de Desenvolvimento Sustentável.

Foi anunciado que o relatório final do Órgão Consultivo seria apresentado em meados de 2024 e que seria um insumo fundamental para a definição dos compromissos e das ações específicas em matéria de Inteligência Artificial que os Estados-Membros assumirão no âmbito do Pacto Digital Global em setembro

de 2024. O Uruguai participou das instâncias de consulta promovidas pelo Órgão Consultivo sobre IA e participa da negociação em curso do Pacto Digital Global.

Resolução A/RES/78/265 da Assembleia Geral da ONU (2024)

A resolução da Assembleia Geral das Nações Unidas 78/265, “Aproveitar as oportunidades de sistemas seguros e confiáveis de inteligência artificial para o desenvolvimento sustentável” [120], foi adotada em 21 de março deste ano, após ter sido copatrocinada por mais de 120 Estados, entre eles o Uruguai.

A Resolução abrange os “sistemas de inteligência artificial no âmbito não militar, cujo ciclo de vida inclui as etapas de pré-concepção, concepção, desenvolvimento, avaliação, teste, implantação, utilização, venda, aquisição, operação e retirada de serviço”.

O texto define as características que distinguem os sistemas seguros e confiáveis de IA nos seguintes termos: “(…) são centrados nas pessoas, confiáveis, explicáveis, éticos e inclusivos, respeitam plenamente a promoção e a proteção dos direitos humanos e o direito internacional, preservam a privacidade, são orientados ao desenvolvimento sustentável e responsáveis” [121].

A Resolução afirma que [122] “os direitos humanos e as liberdades fundamentais devem ser respeitados, protegidos e promovidos durante todo o ciclo de vida dos sistemas de inteligência artificial” e “exorta todos os Estados-Membros e, conforme o caso, outros interessados a se absterem de usar ou deixarem de usar sistemas de inteligência artificial que sejam impossíveis de operar em conformidade com o direito internacional ou que representem riscos indevidos para o gozo dos direitos humanos”.

---

[120] ONU – Assembleia Geral. Resolução aprovada pela Assembleia Geral em 21 de março de 2024. 78/265. Aproveitar as oportunidades de sistemas seguros e confiáveis de inteligência artificial para o desenvolvimento sustentável. A/RES/78/265. Disponível em: https://documents.un.org/doc/undoc/gen/n24/087/86/pdf/n2408786.pdf?token=hxXvAKO8RS5xFkIlcb&fe=true . Último acesso:29/4/2024.

[121] Ibíd. Considerandos.

[122] Ibíd. Item 5.

A resolução da ONU incentiva os Estados-Membros a promover sistemas seguros e confiáveis de inteligência artificial por diferentes meios, entre outros:

• Promovendo a elaboração e a aplicação de abordagens e marcos regulatórios e de governança nacionais, em consonância com suas respectivas políticas e prioridades e com suas obrigações em virtude do direito internacional, a fim de apoiar a inovação e o investimento responsáveis e inclusivos em inteligência artificial, promovendo, ao mesmo tempo, sistemas seguros e confiáveis de IA [123].

• Fomentando o desenvolvimento, a aplicação e a divulgação de mecanismos de acompanhamento e gestão de riscos, mecanismos para a proteção dos dados, incluindo a proteção dos dados pessoais e políticas de privacidade, e avaliações de impacto, conforme apropriado, durante todo o ciclo de vida dos sistemas de inteligência artificial [124].

• Incentivando o desenvolvimento e a implantação de ferramentas técnicas, normas ou práticas eficazes, acessíveis, adaptáveis e interoperáveis em âmbito internacional, incluindo mecanismos confiáveis de autenticação do conteúdo e da origem, como marcas-d'água ou rotulagem, nos casos em que seja tecnicamente possível ou apropriado, que permitam aos usuários identificar quando houve manipulação de informações, distinguir ou determinar a origem do conteúdo digital autêntico e do gerado por inteligência artificial ou manipulado, e aumentando a alfabetização midiática e informacional [125].

• Facilitando a elaboração e a aplicação de marcos, práticas e normas eficazes e interoperáveis em âmbito internacional para o treinamento e o teste dos sistemas de inteligência artificial, a fim de melhorar a formulação de políticas, ajudar a proteger as pessoas contra todas as formas de discriminação, viés, uso indevido ou outros danos e evitar reforçar ou perpetuar as aplicações e os resultados discriminatórios ou

[123] Ibíd. Item 6. Alínea a)
[124] Ibíd. Item 6. Alínea e)
[125] Ibíd. Item 6. Alínea g).

enviesados durante todo o ciclo de vida dos sistemas de inteligência artificial [126].

• Incentivando, quando apropriado e pertinente, a aplicação de salvaguardas adequadas para respeitar os direitos de propriedade intelectual, incluindo o conteúdo protegido por direitos autorais, promovendo, ao mesmo tempo, a inovação [127].

• Promovendo a transparência, a previsibilidade, a confiabilidade e a facilidade de compreensão ao longo de todo o ciclo de vida dos sistemas de inteligência artificial utilizados para tomar decisões ou apoiar a tomada de decisões que afetem os usuários finais, entre outras coisas, fornecendo informações e explicações e promovendo a supervisão humana, por exemplo, por meio do exame das decisões automatizadas e dos processos relacionados ou, nos casos em que seja apropriado e pertinente, por meio da previsão de alternativas de tomada de decisões por pessoas ou de meios eficazes de reparação e prestação de contas para aqueles afetados negativamente pelas decisões automáticas dos sistemas de inteligência artificial [128].

• Fortalecendo o investimento na elaboração e na aplicação de salvaguardas eficazes, incluindo avaliações de riscos e de impacto, ao longo de todo o ciclo de vida dos sistemas de inteligência artificial, para proteger o gozo pleno e efetivo dos direitos humanos e das liberdades fundamentais e mitigar o possível impacto sobre ele [129].

[126] Ibíd. Item 6. Alínea h).
[127] Ibíd. Item 6. Alínea i).
[128] Ibíd. Item 6. Alínea k).
[129] Ibíd. Item 6. Alínea l).

Outros processos intergovernamentais

No âmbito da Organização para a Cooperação e Desenvolvimento Econômico (OCDE), assim como no Conselho da Europa, no G7 e no G20, nos últimos anos ocorreram diferentes processos voltados a impulsionar um marco comum para a governança da IA. Esta seção apresenta uma síntese dos princípios e das orientações de política decorrentes desses esforços.

Recomendação da OCDE sobre Inteligência Artificial (2019)

A Recomendação do Conselho da OCDE sobre IA [130] foi adotada originalmente pelo Conselho da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) em maio de 2019. Para responder aos avanços nas tecnologias de Inteligência Artificial e, particularmente, no campo da IA generativa, desde então foi alterada em duas ocasiões: em 2023 e, recentemente, em 2024.

Os princípios buscam facilitar a interoperabilidade das políticas globais e defendem uma IA inovadora e confiável, que proteja os direitos humanos e os valores democráticos. Em 2024, o Uruguai solicitou formalmente a adesão aos Princípios da OCDE, estando o processo atualmente em andamento.

Princípios da OCDE sobre Inteligência Artificial

Princípio	**Alcance**
Crescimento inclusivo, desenvolvimento sustentável e bem-estar	A Recomendação propõe que as partes interessadas [131] devem participar de maneira proativa de uma gestão responsável da IA em benefício das pessoas e do planeta, favorecendo o crescimento

[130] OCDE. Recomendação do Conselho sobre Inteligência Artificial. OCDE/LEGAL/0449. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 Último acesso, 13/05/2024.

[131] A Recomendação define partes interessadas indicando que “abrangem todas as organizações e indivíduos envolvidos ou afetados pelos sistemas de IA, direta ou indiretamente”.

	inclusivo, o bem-estar, o desenvolvimento sustentável e a sustentabilidade ambiental.
Respeito ao Estado de Direito, aos direitos humanos e aos valores democráticos, incluindo a equidade e a privacidade.	A Recomendação sustenta que os atores da IA [132] devem respeitar o Estado de direito, os direitos humanos e os valores democráticos durante todo o ciclo de vida do sistema de IA, para o que devem aplicar mecanismos e salvaguardas para enfrentar os riscos decorrentes dos usos fora da finalidade prevista, do uso indevido intencional ou do uso indevido não intencional, de maneira adequada ao contexto. Isso também inclui abordar a desinformação amplificada pela IA, respeitando, ao mesmo tempo, a liberdade de expressão e outros direitos e liberdades protegidos pelo direito internacional aplicável.
Transparência e explicabilidade	A Recomendação destaca que os atores da IA devem se comprometer com a transparência e a divulgação responsável dos sistemas de IA, para o que devem fornecer informações significativas, adequadas ao contexto e coerentes com o estado da técnica. Essas informações devem permitir uma compreensão geral dos sistemas de IA, incluindo suas capacidades e limitações, saber quando se está interagindo com sistemas de IA e, quando viável e útil, informações simples e fáceis de entender sobre as fontes de dados/entradas, fatores,

[132] A Recomendação define que “os atores da IA são aqueles que desempenham um papel ativo no ciclo de vida do sistema de IA, incluindo as organizações e os indivíduos que implementam ou operam IA”.

	processos e/ou lógica que permitam compreender o resultado e, quando for o caso, questioná-lo, para aqueles afetados negativamente pelo resultado.
Robustez, segurança e proteção	A Recomendação propõe que os sistemas de IA devem ser robustos, seguros e protegidos ao longo de todo o seu ciclo de vida, de modo que, em qualquer condição de uso, não representem riscos irrazoáveis para a segurança. Quando for tecnicamente viável, para reforçar a integridade da informação e, ao mesmo tempo, garantir o respeito à liberdade de expressão.
Responsabilidade	A Recomendação propõe que os atores da IA devem ser responsáveis pelo funcionamento correto dos sistemas de IA e pelo respeito aos princípios anteriores. Para isso, devem garantir a rastreabilidade, inclusive em relação aos conjuntos de dados, aos processos e às decisões tomadas durante o ciclo de vida do sistema de IA, aplicar uma abordagem sistemática de gestão de riscos a cada fase do ciclo de vida do sistema de IA de forma contínua e adotar uma conduta empresarial responsável para abordar os riscos relacionados aos sistemas de IA.

Princípios de Inteligência Artificial do G20 (2019)

Em 2019, por meio de uma resolução, o Grupo dos Vinte (G20) explicitou seu apoio aos Princípios da OCDE e tomou nota de suas recomendações [133]. A resolução reproduz esses princípios, já comentados na seção anterior.

Princípios orientadores internacionais para as organizações que desenvolvem sistemas avançados de IA, Princípios de Hiroshima (2023)

Os princípios da OCDE também serviram de base para outros desenvolvimentos, como os Princípios orientadores internacionais para as organizações que desenvolvem sistemas de IA avançada, adotados pelo G7, denominados Princípios de Hiroshima [134]. Sua adoção ocorreu em 2023, no âmbito do Processo de Hiroshima [135], e eles buscam abordar os avanços recentes dos sistemas mais avançados de IA, incluindo a IA generativa, oferecendo orientação às organizações que desenvolvem e utilizam os sistemas de IA mais avançados. O conceito de organizações no contexto dos Princípios inclui, entre outras, entidades do meio acadêmico, da sociedade civil, do setor privado e do setor público.

Os Princípios de Hiroshima deram origem a um código de conduta para desenvolvedores.

[133] https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/documents/en/annex_08.pdf Último acesso 2/5/2024.
[134] G7 Leaders' Statement on the Hiroshima AI Process. 30 de outubro de 2023. Disponível em: https://digital-strategy.ec.europa.eu/es/library/hiroshima-process-international-guiding-principles-advanced-ai-system . Último acesso, 02/05/2024.
[135] O Processo de IA de Hiroshima consiste em quatro pilares: 1. Análise dos riscos prioritários, dos desafios e das oportunidades da IA generativa. 2. Os Princípios Orientadores Internacionais do Processo de Hiroshima para todos os agentes da IA no ecossistema da IA. 3. Código de conduta internacional do Processo de Hiroshima para as organizações que desenvolvem sistemas avançados de IA. 4. Cooperação baseada em projetos em apoio ao desenvolvimento de ferramentas e melhores práticas de IA responsáveis (Cf. (https://digital-strategy.ec.europa.eu/en/library/g7-leaders-statement-hiroshima-ai-process),

Princípios de Hiroshima

Princípio	**Alcance**
Identificação, avaliação e mitigação de riscos em todo o ciclo de vida da IA.	Propõe-se adotar as medidas adequadas durante todo o desenvolvimento dos sistemas avançados de IA, inclusive antes e durante sua implantação, para identificar, avaliar e mitigar os riscos existentes ao longo do ciclo de vida da IA.
Identificação e mitigação das vulnerabilidades e, quando for o caso, dos incidentes e usos indevidos.	Propõe-se monitorar vulnerabilidades, incidentes, riscos emergentes e uso indevido após a implementação e tomar as medidas adequadas para abordá-los. Os mecanismos para informar sobre vulnerabilidades, quando cabível, devem ser acessíveis a um conjunto diverso de partes interessadas.
Transparência.	Propõe-se informar publicamente por meio de informações claras e precisas sobre as capacidades, limitações e âmbitos de uso apropriado e inapropriado dos sistemas avançados de IA, para contribuir para garantir transparência suficiente e aumentar a prestação de contas.
Intercâmbio de informações.	Propõe-se trabalhar por um intercâmbio responsável de informações e de notificação de incidentes entre as organizações que desenvolvem sistemas avançados, incluindo a indústria, os governos, a sociedade civil e a academia.

Políticas de gestão de riscos e governança da IA.	Propõe-se desenvolver, implementar e divulgar políticas de governança e gestão de riscos de inteligência artificial, fundamentadas em uma abordagem baseada no risco, incluindo políticas de privacidade e medidas de mitigação. Isso deveria incluir processos de prestação de contas e governança para avaliar e mitigar os riscos, quando viável, durante todo o ciclo de vida da IA.
Segurança	Propõe-se investir e aplicar controles de segurança robustos, incluindo segurança física, cibersegurança e proteção contra ameaças internas em todo o ciclo de vida da IA.
Mecanismos de autenticação de conteúdos	Propõe-se desenvolver e implementar mecanismos confiáveis de autenticação e procedência de conteúdo, quando tecnicamente viável, como marcas-d'água ou outras técnicas para permitir aos usuários identificar conteúdo gerado por IA.
Pesquisa para mitigar os riscos sociais e de segurança e investimento em medidas de mitigação efetivas.	Propõe-se realizar, colaborar e investir em pesquisas que apoiem o avanço da segurança e da confiança da IA e abordar riscos-chave, assim como investir no desenvolvimento de ferramentas adequadas de mitigação.
Desenvolver sistemas avançados de IA centrados no ser humano e nos desafios globais e no apoio ao alcance dos ODS.	Propõe-se priorizar o desenvolvimento de sistemas avançados de IA para abordar os maiores desafios do mundo, particularmente, entre outros, a crise climática, a saúde global e a educação. Apoiar o progresso nos Objetivos de Desenvolvimento Sustentável das Nações Unidas. As organizações devem priorizar a gestão responsável de uma IA confiável e

	centrada no ser humano e também apoiar iniciativas de alfabetização digital.
Desenvolvimento e adoção de padrões e normas técnicas internacionais relativas à IA.	Propõe-se contribuir para o desenvolvimento e, quando cabível, o uso de padrões técnicos e melhores práticas internacionais, incluindo as marcas-d'água, e trabalhar com organizações de desenvolvimento de padrões.
Implementação de medidas para a proteção dos dados pessoais e da propriedade intelectual	Propõe-se implementar medidas apropriadas de entrada de dados e proteções para dados pessoais e propriedade intelectual. Gerenciar a qualidade dos dados, incluindo os dados de treinamento e a coleta de dados, para mitigar os vieses. Apoiar a transparência adequada dos conjuntos de dados de treinamento e o cumprimento dos marcos legais aplicáveis.

Convenção-Quadro do Conselho da Europa (2024)

A Convenção-Quadro sobre Inteligência Artificial, Direitos Humanos, Democracia e Estado de Direito [136] foi adotada formalmente pelo Comitê de Ministros do Conselho da Europa (COE) em maio de 2024 e será aberta à assinatura dos Estados-Membros e não membros do Conselho em setembro próximo. O texto da Convenção foi negociado no âmbito do Comitê sobre Inteligência Artificial do COE, em um processo que se estendeu entre 2021 e março de 2024. Em outubro de 2023, o Uruguai passou a integrar o Comitê na qualidade de observador, condição que permite aos Estados não membros aderir ao tratado.

[136] Disponível em: https://rm.coe.int/-1493-10-1b-committee-on-artificial-intelligence-cai-b-draft-framework/1680aee411

No caso deste antecedente, trata-se de um instrumento de natureza jurídica vinculante para os Estados que o assinarem e ratificarem.

A Convenção-Quadro tem como objetivo garantir que as atividades dentro do ciclo de vida dos sistemas de inteligência artificial cumpram e sejam compatíveis com as obrigações, os padrões e os compromissos internacionais de direitos humanos dos Estados e sejam plenamente compatíveis com a democracia e o Estado de Direito.

O tratado obriga todas as partes a abordar os riscos decorrentes das atividades relacionadas ao ciclo de vida da IA, tanto do setor público quanto do setor privado, estabelecendo nuances quanto ao alcance das obrigações dos Estados em relação ao setor privado no contexto da Convenção.

O Relatório Explicativo que acompanha o Tratado sustenta que ele garante que as obrigações aplicáveis existentes de cada Parte em matéria de direitos humanos, democracia e Estado de Direito também se apliquem às atividades dentro do ciclo de vida da inteligência artificial. Nesse sentido, a Convenção-Quadro está alinhada ao sistema e aos mecanismos de proteção dos direitos humanos aplicáveis de cada Parte, incluindo suas obrigações de direito internacional, outros compromissos internacionais e seu direito interno aplicável.

Assim, nenhuma disposição desta Convenção-Quadro tem como objetivo criar novos direitos humanos ou obrigações de direitos humanos ou prejudicar o alcance e o conteúdo das proteções aplicáveis existentes, mas sim, ao estabelecer várias obrigações juridicamente vinculantes contidas em seus Capítulos II a VI, facilitar a implementação efetiva das obrigações de direitos humanos aplicáveis de cada Parte no contexto dos novos desafios apresentados pela inteligência artificial [137].

Quanto ao setor privado, o Relatório explica que o tratado obriga todas as Partes a abordar os riscos e impactos para os direitos humanos, a democracia e o Estado de direito no setor privado e esclarece que abordar os riscos não

[137] COE – CAI. Explanatory Report. Par. 13 (tradução não oficial). Disponível em: https://www.coe.int/en/web/artificial-intelligence/cai . Último acesso. 2/5/2024.

significa simplesmente reconhecer esses riscos, mas exige a adoção ou a manutenção de medidas legislativas, administrativas ou de outro tipo apropriadas para dar efeito a essa disposição, assim como a cooperação entre as Partes segundo o previsto nas disposições sobre o mecanismo de acompanhamento e a cooperação internacional. Esclarece, no entanto, que a obrigação não exige necessariamente legislação adicional e que as Partes podem utilizar outras medidas apropriadas, incluindo medidas administrativas e voluntárias. Assim, embora a obrigação seja vinculante e todas as Partes devam cumpri-la, a natureza das medidas adotadas pelas Partes poderia variar [138].

São excetuadas do alcance da Convenção as atividades dentro do ciclo de vida dos sistemas de inteligência artificial relacionadas à proteção de seus interesses de segurança nacional. O Relatório Explicativo esclarece que essa exceção se aplica apenas se e na medida em que as atividades se relacionem com a proteção dos interesses de segurança nacional, de modo que todas as atividades regulares de aplicação da lei para a prevenção, detecção, investigação e persecução de crimes, incluindo as ameaças à segurança pública, também permanecem no alcance da Convenção-Quadro, desde que os interesses de segurança nacional das Partes não estejam em jogo.

A Convenção-Quadro consiste em 36 artigos e 8 capítulos.

O capítulo II estabelece as obrigações gerais dos Estados-Partes de: adotar ou manter medidas para garantir que as atividades dentro do ciclo de vida dos sistemas de inteligência artificial sejam compatíveis com as obrigações de proteger os direitos humanos, conforme consagrado no direito internacional aplicável e em seu direito interno (artigo 4), e de adotar ou manter medidas que busquem garantir a integridade, a independência e a eficácia das instituições e dos processos democráticos (artigo 5). Já o capítulo III estipula os princípios comuns que orientarão a implementação da Convenção.

Como foi indicado, exige-se que as Partes apliquem os marcos nacionais e internacionais existentes ao contexto das atividades dentro do ciclo de vida dos

[138] Ibíd. Par. 29.

sistemas de inteligência artificial, adotando ou mantendo, de maneira compatível com esses marcos, medidas para garantir a disponibilidade de recursos acessíveis e efetivos para as violações dos direitos humanos resultantes das atividades dentro do ciclo de vida dos sistemas de inteligência artificial (artigo 14).

Da mesma forma, a Convenção propõe que os Estados-Partes deverão adotar ou manter medidas prévias e, conforme apropriado, de forma iterativa ao longo do ciclo de vida do sistema de inteligência artificial, para a identificação, avaliação, prevenção e mitigação dos riscos, considerando os impactos reais e potenciais sobre os direitos humanos, a democracia e o Estado de direito. Indica-se que essas medidas deverão ser graduais e diferenciadas, adequadas ao contexto e ao uso.

A esse respeito, o Relatório Explicativo esclarece que essa disposição concede flexibilidade às Partes nas abordagens e metodologias para realizar a avaliação. Assinala que “em particular, as Partes poderão optar por implementar essa avaliação em diferentes níveis, como no nível regulatório, prescrevendo diferentes categorias de classificação de riscos e/ou no nível operacional pelos atores relevantes aos quais tenham sido atribuídas responsabilidades pelas atividades dentro do ciclo de vida do sistema de inteligência artificial. Da mesma forma, cada parte avaliará a necessidade de uma moratória, uma proibição ou outras medidas apropriadas em relação a certos usos dos sistemas de inteligência artificial quando considerar que esses usos são incompatíveis com o respeito aos direitos humanos, o funcionamento da democracia ou o Estado de Direito (artigo 15).

Princípios enunciados na Convenção-Quadro sobre Inteligência Artificial, Direitos Humanos, Democracia e Estado de Direito

Princípio	**Alcance**
Dignidade humana e autonomia individual	Adotar ou manter medidas para respeitar a dignidade humana e a autonomia individual

	relacionadas às atividades dentro do ciclo de vida dos sistemas de inteligência artificial.
Transparência e supervisão	Adotar ou manter medidas para garantir que existam requisitos adequados de transparência e supervisão adaptados aos contextos e riscos específicos em relação às atividades dentro do ciclo de vida dos sistemas de inteligência artificial, inclusive quanto à identificação do conteúdo gerado pelos sistemas de inteligência artificial.
Prestação de contas e responsabilidade	Adotar ou manter medidas para garantir a prestação de contas e a responsabilidade pelos impactos adversos sobre os direitos humanos, a democracia e o Estado de direito resultantes de atividades dentro do ciclo de vida dos sistemas de inteligência artificial.
Igualdade e não discriminação	Adotar ou manter medidas para garantir que as atividades relacionadas ao ciclo de vida dos sistemas de inteligência artificial respeitem a igualdade, incluindo a igualdade de gênero, e a proibição da discriminação, e adotar ou manter medidas destinadas a superar as desigualdades.
Privacidade e proteção de dados pessoais	Adotar ou manter medidas para garantir a proteção da privacidade das pessoas e dos dados pessoais dentro do ciclo de vida dos sistemas de IA, inclusive por meio de leis, padrões e marcos nacionais e internacionais, e estabelecer garantias e salvaguardas efetivas para as pessoas.

Confiabilidade	Adotar medidas para promover a confiabilidade dos sistemas de inteligência artificial, que poderiam incluir requisitos relacionados a uma qualidade e segurança adequadas durante todo o ciclo de vida dos sistemas de inteligência artificial.
Inovação segura	Estabelecer, quando apropriado, ambientes controlados para desenvolver, experimentar e testar sistemas de IA sob a supervisão de autoridades competentes para fomentar a inovação, evitando, ao mesmo tempo, impactos adversos sobre os direitos humanos, a democracia e o Estado de Direito.

Processos na América Latina e no Caribe

Agenda digital para a América Latina e o Caribe, e-LAC (2022)

A Agenda digital para a América Latina e o Caribe (e-LAC 2024), adotada no âmbito da Oitava Conferência Ministerial sobre a Sociedade da Informação da América Latina e do Caribe, realizada de 16 a 18 de novembro de 2022 e organizada conjuntamente pela Comissão Econômica para a América Latina e o Caribe (CEPAL) e pelo Governo do Uruguai, organiza um conjunto de prioridades de política e ações estratégicas em âmbito regional em quatro eixos.

O eixo 3 do instrumento aborda a transformação digital produtiva e sustentável e estabelece como um dos objetivos da agenda regional “impulsionar o uso efetivo de tecnologias digitais emergentes para promover a produtividade e fomentar a inovação e o empreendedorismo, prevendo-se especialmente soluções de Internet das coisas, inteligência artificial e tecnologias amigáveis ao

meio ambiente, com a proteção dos direitos humanos e o uso ético da tecnologia” [139].

No âmbito da implementação dos objetivos da Agenda, foram estabelecidos grupos de trabalho. Os grupos de trabalho são um espaço de cooperação no âmbito da eLAC2024, com o objetivo de cumprir uma determinada meta sob a condução de um país coordenador.

O Grupo de trabalho sobre inteligência artificial é um dos grupos estabelecidos para o período 2023 – 2024 sob a coordenação do Centro Nacional de Inteligência Artificial do Chile e da Agência de Governo Eletrônico e Sociedade da Informação e do Conhecimento do Uruguai (AGESIC).

Declaração de Santiago (2023)

A Declaração de Santiago para “Promover uma inteligência artificial ética na América Latina e no Caribe” [140] foi adotada em outubro de 2023 pelos governos participantes — entre eles o Governo do Uruguai —, no âmbito do Fórum sobre a Ética da Inteligência Artificial na América Latina e no Caribe e da Cúpula Ministerial e de Altas Autoridades da América Latina e do Caribe, organizada pela UNESCO, pela CAF e pelo Governo do Chile.

A Declaração aprova a criação de um Grupo de Trabalho para a constituição de um Conselho Intergovernamental de Inteligência Artificial para a América Latina e o Caribe, para fortalecer as capacidades regionais em matéria de ética e governança da IA no âmbito da Recomendação sobre a Ética da IA da UNESCO.

Por meio desse instrumento, os países signatários concordaram em “iniciar uma análise diante da necessidade de elaborar e adotar novos marcos jurídicos e agendas regulatórias para a concepção, o desenvolvimento e o uso responsável da IA. A análise

[139] CEPAL (2022). Agenda digital para a América Latina e o Caribe, e-LAC 2024, Objetivo 13. Disponível em: https://repositorio.cepal.org/server/api/core/bitstreams/1fae5881-feba-42b4-a0b0-53ba8fa1f679/content . Último acesso, 15/5/2024.
[140] Disponível em: https://minciencia.gob.cl/uploads/filer_public/40/2a/402a35a0-1222-4dab-b090-5c81bbf34237/declaracion_de_santiago.pdf .

deveria considerar todos os princípios transversais de direitos humanos, especialmente os princípios da proporcionalidade e de não causar danos, da segurança e proteção, da equidade e não discriminação, da inclusão, da diversidade de gênero, da diversidade cultural, da acessibilidade, da sustentabilidade — social, cultural, econômica e ambiental —, do direito à privacidade e à proteção de dados pessoais, da supervisão e decisão humanas, da transparência e explicabilidade, da responsabilidade e prestação de contas, da conscientização e educação e da governança inteligente e colaboração adaptativas e de múltiplas partes interessadas" [141]

A Declaração sustenta que é urgente integrar as particularidades das culturas da América Latina e do Caribe à criação de tecnologias de IA para a região e propõe que é fundamental incentivar maiores investimentos na região para aproveitar integralmente a IA na solução de suas diversas problemáticas e promover o uso inovador dessa tecnologia, desenvolvendo os incentivos necessários para esse fim.

As recentes regulações nos Estados Unidos e na União Europeia

Ordem Executiva de 2023 dos Estados Unidos

Em outubro de 2023, o governo dos Estados Unidos emitiu uma Ordem Executiva para o Desenvolvimento e o uso da inteligência artificial de forma segura e confiável [142], na qual explicita o propósito de impulsionar uma "abordagem que trate dos riscos da IA sem reduzir indevidamente seus benefícios" [143].

[141] Cúpula Ministerial e de Altas Autoridades da América Latina e do Caribe (2023). Declaração de Santiago, "Para promover uma inteligência artificial ética na América Latina e no Caribe", item resolutivo 2. Disponível em: https://minciencia.gob.cl/uploads/filer_public/40/2a/402a35a0-1222-4dab-b090-5c81bbf34237/declaracion_de_santiago.pdf Último acesso. 16/5/2024.
[142] O conteúdo da Ordem Executiva pode ser consultado em: 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/ Último acesso: 24/03/2024.
[143] Artigo 2, alínea (a).

A regulação determina que diferentes entidades federais adotem múltiplas medidas para estabelecer salvaguardas em torno das tecnologias de inteligência artificial e impõe novas normas a determinados desenvolvedores de sistemas de IA. A Ordem Executiva propõe oito princípios orientadores e prioridades em relação à política de inteligência artificial, resumidos a seguir:

1. Segurança e proteção: A Ordem Executiva promove a garantia de avaliações robustas, confiáveis, repetíveis e padronizadas dos sistemas de IA, assim como políticas, instituições e, quando cabível, outros mecanismos para testar, compreender e mitigar os riscos desses sistemas antes de colocá-los em uso.

2. Inovação responsável e concorrência: A Ordem Executiva promove um conjunto de medidas para atrair talentos ao país, investimentos em educação, formação, desenvolvimento, pesquisa e capacidade relacionados à IA e a necessidade de abordar questões de propriedade intelectual (PI) para proteger os inventores e criadores.

3. Apoio aos trabalhadores: A Ordem Executiva analisa que é necessário adaptar a formação e a educação para o trabalho para apoiar uma força de trabalho diversa, ajudar a facilitar o acesso às oportunidades criadas pela IA e zelar para que a IA não seja implantada de forma que prejudique os direitos dos trabalhadores.

4. Equidade e proteção dos direitos civis: A Ordem Executiva propõe que as políticas de Inteligência Artificial devem ser compatíveis com as políticas de promoção da equidade e com os direitos civis.

5. Proteção do consumidor: A Ordem Executiva propõe a proteção dos interesses dos consumidores que interagem com os sistemas de IA, particularmente em áreas críticas, juntamente com a promoção do uso responsável da IA.

6. Privacidade: A Ordem Executiva propõe a necessidade de proteger a privacidade à medida que a IA continua avançando.

7. Gerenciar os riscos do uso da IA pelas entidades federais: A Ordem Executiva propõe aumentar a capacidade interna para regular, governar e apoiar o uso responsável da IA para oferecer melhores resultados.

8. Liderança internacional e cooperação: A Ordem Executiva propõe que os Estados Unidos devem ser líderes mundiais em IA e pioneiros nos sistemas e garantias necessários para implantar a tecnologia de forma responsável e propõe liderar

os esforços regulatórios voltados a estabelecer marcos comuns para a garantia e a gestão de riscos e promover padrões técnicos globais para a IA.

Entre as medidas específicas previstas pela Ordem Executiva para alcançar os objetivos mencionados, encontram-se:

1. Padrões em matéria de Segurança.

   • Exigir que os desenvolvedores de determinados sistemas compartilhem informações com o governo dos Estados Unidos.

   • Desenvolver padrões, ferramentas e testes para assegurar que os sistemas sejam seguros e confiáveis antes de sua entrada em produção.

   • Proteção contra os riscos do uso da IA em materiais biológicos perigosos.

   • Proteção contra fraudes e enganos possibilitados pela IA. Para isso, serão elaboradas diretrizes de autenticação de conteúdo e marcas-d'água para identificar conteúdo gerado por IA.

   • Estabelecer um programa avançado de cibersegurança para desenvolver ferramentas de IA e colaborar na detecção e resolução de vulnerabilidades em software crítico.

   • Determinar o desenvolvimento de um Memorando de Segurança Nacional para orientar futuras ações em IA e segurança.

2. Proteção da privacidade.

   • Priorizar o apoio federal para acelerar o desenvolvimento de tecnologias de preservação da privacidade.

   • Reforçar a pesquisa e as tecnologias que preservem a privacidade.

• Avaliar a forma como as agências coletam e usam informações disponíveis e reforçar as diretrizes de privacidade para as agências federais.

• Desenvolver diretrizes para que as agências federais avaliem a efetividade das técnicas de preservação da privacidade.

3. Avançar nos direitos civis e na equidade

• Fornecer diretrizes para locadores, programas de benefícios federais e contratados federais que evitem o uso de algoritmos discriminatórios.

• Combater a discriminação algorítmica por meio de assistência técnica, coordenação e melhores práticas.

• Assegurar a equidade no sistema de justiça criminal

4. Proteger os consumidores, pacientes e estudantes.

• Avançar no uso responsável da IA em matéria de saúde

• Conceber recursos que apoiem a transformação da educação por meio de ferramentas de IA.

5. Apoio aos trabalhadores.

• Desenvolver princípios e boas práticas para mitigar os danos e maximizar os benefícios da IA para os trabalhadores

• Elaborar um relatório sobre o potencial impacto da IA no mercado de trabalho e estudar e identificar opções para reforçar o apoio federal aos trabalhadores afetados pela IA

6. Promover a inovação e a concorrência.

• Catalisar a pesquisa em IA nos Estados Unidos por meio de um projeto-piloto de Recurso Nacional de Pesquisa em IA.

• Promover um ecossistema justo, aberto e competitivo por meio de assistência técnica e recursos para pequenos desenvolvedores.

• Utilizar as competências existentes para ampliar as possibilidades de imigrantes e não imigrantes altamente especializados com experiência em áreas críticas estudarem, permanecerem e trabalharem nos Estados Unidos.

7. Avançar na Liderança dos Estados Unidos no exterior

• Ampliar os compromissos bilaterais, multilaterais e de múltiplos atores para colaborar em IA.

• Acelerar o desenvolvimento e a implementação de padrões de IA vitais

• Promover o desenvolvimento e a implementação seguros, responsáveis e centrados em direitos no exterior para resolver desafios globais.

8. Assegurar o uso governamental responsável e efetivo da IA.

• Estabelecer diretrizes para o uso da IA por órgãos do governo.

• Apoiar as agências do governo na aquisição de produtos e serviços de IA.

• Acelerar a rápida contratação de profissionais de IA no governo.

Lei de Inteligência Artificial da União Europeia

O Regulamento Europeu de Inteligência Artificial [144] foi aprovado pelos países da União Europeia em 13 de março de 2024. Em conformidade com o estabelecido

[144] Regulamento de Inteligência Artificial, 13 de março de 2024. Disponível em: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.html

no artigo 1, seu objetivo é proteger os direitos fundamentais, a democracia, o Estado de direito e a sustentabilidade ambiental diante da IA de alto risco, ao mesmo tempo em que impulsiona a inovação.

O instrumento da União Europeia adota uma abordagem baseada no risco, em função da qual estabelece aplicações proibidas e sistemas de alto risco para os quais regula um conjunto de requisitos e obrigações:

a) Risco inaceitável (Título II).

Estão incluídas nesta classificação as seguintes aplicações proibidas:

• Manipulação cognitiva do comportamento de pessoas que afete a autonomia e a capacidade de escolher livremente ou explore as vulnerabilidades das pessoas decorrentes de sua idade, situação de deficiência, entre outras. A proibição não afeta as práticas legais relacionadas a tratamentos médicos [145].

• Sistemas de categorização biométrica baseados em dados biométricos [146].

• Sistemas de IA que permitem a agentes públicos ou privados realizar uma pontuação cidadã das pessoas físicas com base em vários pontos de dados relacionados a seu comportamento social em múltiplos contextos ou a características pessoais ou de sua personalidade conhecidas, inferidas ou previstas durante determinados períodos de tempo [147].

• Uso de sistemas de IA para a identificação biométrica remota «em tempo real» de pessoas físicas em espaços de acesso público para fins de aplicação da lei (são estabelecidas exceções) [148].

b) Sistemas de IA de alto risco (Título III).

São incluídos nesta classificação aqueles cuja saída produzida seja relevante em uma ação ou decisão com possível risco importante para a

[145] Par. 29.
[146] Par. 30.
[147] Par. 31.
[148] Par. 32 e 33.

saúde, a segurança ou os direitos fundamentais das pessoas. O regulamento indica que a classificação deve ser realizada considerando tanto a gravidade do possível dano quanto a probabilidade de que ele ocorra. Determina que a entrada em serviço ou a utilização de sistemas de IA de alto risco deve estar condicionada ao cumprimento de determinados requisitos obrigatórios.

Entre outros, estão incluídos nesta classificação:

- Vários casos de uso de sistemas de identificação biométrica.
- Os sistemas de IA destinados a serem utilizados como componentes de segurança na gestão e no funcionamento das infraestruturas críticas.
- Os sistemas de IA utilizados na educação ou na formação profissional.
- Os sistemas de IA utilizados nos âmbitos do emprego e da gestão dos trabalhadores, particularmente para o recrutamento e a seleção de pessoal.
- Os sistemas de IA usados para avaliar a classificação de crédito ou a solvência das pessoas físicas, pois decidem se essas pessoas podem acessar recursos financeiros ou serviços essenciais.
- Os sistemas de IA destinados a serem utilizados para fins de aplicação da lei
- Os sistemas de IA utilizados na migração, no asilo e na gestão do controle fronteiriço.
- Sistemas de IA destinados à administração da justiça.
- As implementações com IA de produtos ou componentes de segurança de produtos já abrangidos pela legislação europeia (como, por exemplo, dispositivos médicos, ferrovias, aviões ou máquinas).

O Regulamento define várias autoridades de supervisão. Também estabelece uma série de exigências que os fornecedores de sistemas de alto risco devem cumprir. Entre elas, o artigo 9 indica que será estabelecido, implantado, documentado e mantido um sistema de gestão de riscos. Da mesma forma,

estabelece-se que, quando pertinente, os fornecedores deverão assegurar que as pessoas físicas sejam informadas de que estão interagindo com um sistema de IA.

Anexo 3: Contribuições recebidas no processo de consulta

Institución Nacional de Derechos Humanos y Defensoría del Pueblo

Montevidéu, 11 de junho de 2024.

Ref. Relatório sobre a aplicação do artigo 74 da Lei N° 20.212

i. Antecedentes

De acordo com o estabelecido no artigo 74 da Lei N° 20.212, de 6 de novembro de 2023, é atribuída à AGESIC a concepção e o desenvolvimento de uma estratégia nacional de dados e inteligência artificial baseada em padrões internacionais, nos âmbitos público e privado. Nesse contexto e como parte dessa estratégia, foi estabelecido um prazo de 180 dias para a apresentação ao Poder Legislativo de um relatório e recomendações para sua regulação legal, voltada a seu desenvolvimento ético, à proteção dos direitos humanos e, ao mesmo tempo, ao fomento da inovação tecnológica. Para esse fim, a referida norma prevê que a AGESIC possa estabelecer grupos de trabalho, comitês consultivos e outros mecanismos de participação que incluam as perspectivas de atores do setor público, do setor privado, da academia e da sociedade civil organizada.

Em 30 de abril de 2024, a AGESIC elaborou o documento de Bases para o desenvolvimento do relatório previsto no art. 74 da Lei N° 20.212, convidando diversas entidades públicas a participar, entre elas a Instituição Nacional de Direitos Humanos
e Defensoria do Povo.

Nesse contexto, a INDDHH fará as seguintes contribuições ao documento em questão, no âmbito de suas atribuições e competências institucionais de defesa, promoção e proteção dos direitos humanos, com o objetivo de contribuir para a questão e responder às perguntas formuladas no relatório como elementos de contribuição para as entidades participantes.

> O presente documento não implica uma análise de todos os pontos mencionados no extenso

relatório apresentado, mas de algumas questões que o Conselho Diretor da INDDHH considera mais relevantes mencionar, sem prejuízo da importância de todos os aspectos referidos no documento e da possibilidade de, em ocasiões posteriores, abordar outras questões não mencionadas aqui.

ii. Sobre a institucionalidade e a governança

Segundo consta no documento enviado, um dos primeiros aspectos a analisar está relacionado à institucionalidade e à governança da IA e, especialmente, à questão da posição orgânica e institucional da entidade orientadora na matéria.

Nesse sentido, cita-se como exemplo o caso da própria AGESIC, criada em virtude da Lei N° 17.930 como um órgão desconcentrado da Presidência da República e, posteriormente, da Lei N° 18.331, que criou a Unidade Reguladora e de Controle de Dados Pessoais (URCDP) como um órgão desconcentrado da AGESIC, sempre no âmbito da Presidência da República.

Também são apresentados exemplos do direito comparado, tanto na América Latina quanto na Europa, verificando-se a existência de entidades autárquicas

(que, em nosso direito, corresponderiam ao que o constituinte considerou como Entes Autônomos ou Serviços Descentralizados) e entidades vinculadas a Ministérios, funcionando como uma espécie de secretarias técnicas, em um tipo de mecanismo semelhante ao existente em nosso país (com a ressalva de que, em nosso caso, o vínculo é com a Presidência). Por fim, a respeito desse ponto, faz-se referência ao Regulamento Europeu, ao caso norte-americano e à regulação atualmente existente no Reino Unido.

Quanto a esse ponto, e considerando as previsões da Lei N° 20.212, pela qual compete à AGESIC e à URCDP a fixação de critérios gerais sobre a matéria (que abrangem inclusive a fiscalização), considera-se que seu âmbito de atuação deveria, idealmente, estar situado fora da esfera da Presidência da República (deixando de lado as discussões doutrinárias sobre o papel da Presidência à luz de nossa Constituição e a enorme expansão em temas e atribuições que esse sistema orgânico teve) e, em geral, do próprio Poder Executivo, pois este último, de fato, é o sistema que mais produz e utiliza informações e dados em nosso país.

Considerando a importância cada vez maior do tratamento de dados, da informação e da IA, o ideal deveria ser a existência de uma entidade de controle completamente autônoma, como a Constituição de nosso país reconhece aos três órgãos de controle, dotados também de poder regulamentar autônomo, como ocorre especialmente com o Tribunal de Contas e a Corte Eleitoral.

Como esse cenário é pouco viável, pois implica uma reforma constitucional, são propostos dois possíveis caminhos institucionais para a eventual institucionalização.

Em primeiro lugar, uma opção é situar essa agência no campo de atuação do Poder Legislativo, como uma entidade autônoma e independente, tal como ocorre com a INDDHH, criada a partir da Lei N° 18.446. O caso do Comissário Parlamentar para o Sistema Carcerário, embora também pertença à esfera do Legislativo, possui um papel de prestação de contas direta ao parlamento, o que não ocorre com a INDDHH e tampouco deveria ocorrer no caso de uma agência como a indicada em matéria de IA. Uma vantagem desse ponto, sem dúvida, é o papel representativo do âmbito de atuação do Legislativo e, especialmente, a clara separação da atuação em relação ao Poder Executivo, com as particularidades antes assinaladas.

A segunda opção viável, com fortes antecedentes em nosso direito, seria a possibilidade de seguir o caminho de outras entidades de controle, como URSEC, URSEA e JUTEP, que recentemente (em termos institucionais) se transformaram no que, no direito comparado, se denomina entidades autárquicas e adotaram — nos três casos — a forma de serviços descentralizados, embora eventualmente também pudessem adotar a forma de Entes Autônomos, pois não estão limitadas pelo art. 186 da Constituição, tal como ocorre com o papel de controle do BCU.

A forma de Serviço Descentralizado, que, como indicado, parece ser o caminho adotado para as entidades de controle, considerando a especificidade de suas atribuições e a correta aplicação dos princípios de especialidade e especialização aos organismos públicos e, em particular, a esse tipo de entidade, retirando-as da esfera de atuação hierárquica do Poder Executivo (ou da Presidência da República) e inclusive adotando uma forma de designação da direção que ultrapassa os mandatos governamentais de cinco anos.

> Sem prejuízo disso, naturalmente o controle do sistema continuará existindo, considerando

as características da forma de atuação dos serviços descentralizados e os aspectos relativos à tutela administrativa, ao estatuto dos servidores e à previsão orçamentária no âmbito do art. 220 da Constituição. Este último aspecto, sem dúvida, apresenta um dos desafios mais substanciais, já que uma dotação orçamentária adequada, como reconhecido no relatório, é fundamental para a correta atuação desse tipo de agência de controle.

iii. Outro dos aspectos apresentados no relatório está relacionado ao exemplo dos fideicomissos de dados. Embora claramente a figura do fideicomisso — prevista em nosso país na Lei N° 17.703 — se volte à matéria de bens e finanças (sejam fideicomissos testamentários, de administração, de garantia ou financeiros), sua aplicação ao campo dos dados parece claramente inovadora.

Considerando os exemplos do direito comparado — especialmente a figura do trust do direito anglo-saxão — e as bases substantivas da figura do fideicomisso, isto é, especialmente a existência de fideicomitentes, fiduciário e beneficiários e, por outro lado, uma série de bens ou direitos sob fideicomisso e um mandato, é fundamental que uma regulação que viabilize esse tipo de instrumento tenha uma base normativa legal, a fim de proteger os direitos dos titulares dos dados e regular os papéis de cada uma das partes, especialmente o fiduciário, que preferencialmente deveria ser uma entidade estatal (por exemplo, a agência de controle).

Juntamente com isso, existe um conjunto importante de aspectos de regulação e controle que deverão estar claramente estabelecidos por lei, em particular os poderes de atuação desse fiduciário em relação aos dados que manejar e aos eventuais beneficiários desses dados coletados.

Nesse contexto, a opção do fideicomisso, embora não deva ser descartada, sem dúvida implica um extenso desenvolvimento normativo que permita garantir a segurança das informações e a devida proteção dos direitos das pessoas.

iv. (…..)

Contribuições da Data Uruguay para o desenvolvimento do relatório previsto no art. 74 da Lei N° 20.212

Daniel Carranza Secretário
da Data Uruguay

1. Quais são as recomendações específicas que você poderia fazer, a partir de sua experiência, para promover os eixos definidos neste documento?

Da Data Uruguay, analisamos o documento “Bases para el desarrollo del informe previsto en el art. 74 de la Ley N° 20.212” e destacamos a importância de uma adequação da normativa nacional para regular a inteligência artificial (IA) no Uruguai segundo os padrões internacionais de direitos humanos mais recentes.

Destacamos a importância do trabalho da Agesic no estabelecimento de marcos éticos e normas de soft law por meio da Estratégia de IA para o âmbito público, embora entendamos que essa tarefa deve ser complementada com a atualização da normativa nacional. Os aspectos que exigem uma regulação mais urgente estão relacionados à tomada automatizada de decisões por meio de sistemas de inteligência artificial, especialmente na administração pública. Essas situações incluem não apenas a tomada de decisões totalmente automatizadas, mas também a interação pessoa-máquina e o conceito de supervisão significativa (quando os operadores atuam conscientes dos vieses ou das limitações do sistema).

Com o objetivo de promover os eixos definidos neste documento, entendemos que, após esta consulta, o Parlamento uruguaio deveria considerar a abertura de uma audiência pública na qual nossos legisladores possam interagir com empresas, academia e sociedade civil especializada, já que atualmente se legisla sobre esses temas com base em entendimentos muito superficiais de alguns dos desafios de normatizar esse tema e de suas consequências.

Sugerimos uma lista de possíveis aspectos a discutir nas instâncias de audiência pública sobre regulação da IA propostas, entre eles:

- A determinação de quais são os usos com alto risco de violação de direitos individuais que justificariam uma regulação específica.

- O estabelecimento de garantias básicas, como o direito à explicabilidade, à rastreabilidade, à transparência e à auditabilidade algorítmica em sistemas de alto risco, mesmo que não tratem dados pessoais ou não sejam abrangidos pela Lei de Proteção de Dados Pessoais.

- A aplicação obrigatória de instrumentos para a avaliação de riscos em determinados cenários críticos que não envolvam o uso de dados pessoais ou nos quais as obrigações de proteção de dados pessoais não se apliquem (como na segurança pública ou na defesa).

- A rotulagem obrigatória dos conteúdos sintéticos.

- A conceituação do princípio da supervisão humana significativa.

Por fim, entendemos que, embora a Instituição Nacional de Direitos Humanos e Defensoria do Povo seja o órgão incumbido de fazer recomendações e orientações de política pública sobre direitos humanos ao Parlamento, os membros dessa Instituição não contam com uma massa crítica de conhecimento suficiente para cumprir essa função de recomendação sobre IA. Por isso, seria desejável sugerir algum tipo de apoio à INDDHH para estabelecer convênios com a academia e a sociedade civil especializada em direitos digitais.

2. Existem deficiências ou incongruências do ponto de vista regulatório que impactem os aspectos avaliados nos eixos definidos neste documento e que não tenham sido consideradas?

Em relação à análise desenvolvida sobre os artigos 13 e 16 da Lei de Proteção de Dados Pessoais, no ponto “3.3 Diagnóstico preliminar em matéria de IA e Direitos Humanos do documento”, ressaltamos a importância do direito de contestar decisões automatizadas e de obter informações sobre “os critérios de avaliação, os processos aplicados e a solução tecnológica ou o programa utilizados”. De qualquer forma, essa normativa é insuficiente e precisa ser atualizada para incluir padrões modernos, como os padrões

sobre transparência algorítmica [1] e supervisão humana significativa [2]. Esses mesmos padrões também poderiam ser incluídos por meio de obrigações impostas à administração pública mediante modificações na Lei de Acesso à Informação Pública.

3. Você identificou potenciais melhorias ou modificações na regulação vigente que possam contribuir para o desenvolvimento da IA no Uruguai?

Reforma da Lei N° 19.179 de formatos abertos e software livre e de seu decreto regulamentar (Decreto N° 44/015)

Seguindo a mesma lógica de atualização da normativa existente proposta pela Agesic no documento preliminar, sugere-se implementar um sistema de apoio à tomada de decisões de aquisição de software ou soluções baseadas em IA pela administração pública, introduzindo modificações na Lei N° 19.179 de formatos abertos e software livre e em seu decreto regulamentar (Decreto N° 44/015). Essa lei é um instrumento que já existe em nosso ordenamento jurídico desde antes da expansão da IA e que poderia ser revisado para dar prioridade às soluções de IA Aberta, evitando as caixas-pretas e fomentando as garantias de transparência e explicabilidade. Entendemos que, além de revisar a Lei N° 19.179 e seu decreto para impulsionar a promoção preferencial da utilização de modelos de IA Aberta, também deveria ser incluído um mecanismo de intervenção pelo qual a Agesic determine o risco e assessore os entes públicos para realizar avaliações de impacto antes da aquisição de soluções baseadas em IA, pelo menos para alguns setores ou usos-chave (saúde, segurança pública ou educação, por exemplo).

4. Existem outros aspectos que você não encontra considerados e que devam ser analisados?

Regulação urgente da aquisição e do uso de software de vigilância pelo Ministério do Interior

Basta fazer uma busca na imprensa para constatar que, nos últimos anos, o Ministério do Interior vem adquirindo de forma contínua novas tecnologias para combater o crime. Muitas dessas aquisições utilizam sistemas potentes de IA, seja para detectar disparos

[1] BID (2022), "Auditoría algorítmica para sistemas de toma o soporte de decisiones". Ver: https://publications.iadb.org/publications/spanish/document/Auditoria-algoritmica-para-sistemas-de-toma-o-soporte-de-decisiones.pdf

[2] EU AI Act. Ver: https://www.euaiact.com/key-issue/4

colocando microfones na via pública, seja para identificar as pessoas com base em padrões biométricos. Nenhuma dessas tecnologias está devidamente regulada por lei segundo os padrões reivindicados pelas diferentes Relatorias do sistema internacional de direitos humanos.

O critério do Comitê de Direitos Humanos da ONU quanto à adoção de medidas de vigilância é o seguinte: os governos poderão estabelecer esse tipo de medida sobre seus cidadãos desde que 1) estejam autorizadas por uma lei nacional acessível e precisa, 2) tenham um objetivo legítimo e 3) cumpram os critérios de necessidade e proporcionalidade. Há 10 anos, a Alta Comissária das Nações Unidas para os Direitos Humanos advertiu que esses requisitos não estão sendo cumpridos [3] e que os Estados costumam usar sistemas de vigilância sem leis nacionais adequadas, sem garantias processuais e sem supervisão suficiente. A Alta Comissária assinala "a preocupante falta de transparência governamental associada às políticas, leis e práticas de vigilância, que dificulta qualquer tentativa de avaliar sua compatibilidade com o direito internacional dos direitos humanos e assegurar a prestação de contas".

Compartilhamos a preocupação da Alta Comissária e entendemos que o relatório apresentado pela Agesic ao Parlamento deveria recomendar a regulação urgente do uso da IA para fins de vigilância pelo Ministério do Interior.

[3] O direito à privacidade na era digital. Relatório do Escritório do Alto Comissariado das Nações Unidas para os Direitos Humanos" A/HRC/27/37, par. 48. Ver: https://documents.un.org/doc/undoc/gen/g14/068/74/pdf/g1406874.pdf?token=BBP8Fg822XkzlZAS4c&fe=true

Consulta para o desenvolvimento do relatório previsto no art. 74 da Lei N° 20.212

Documento elaborado por Patricia Díaz, cocoordenadora do Laboratorio de Datos y Sociedad | Datysoc

Questões preliminares

Fazemos algumas sugestões relacionadas à estrutura do documento:

- Como será um documento de extensão considerável, sugerimos gerar um sumário com hiperlinks para melhorar sua navegabilidade e usabilidade.
- Sugerimos colocar, ao final de cada eixo, uma lista com um resumo que apresente de forma específica e clara as recomendações de regulação.

Autorização: autoriza-se a equipe da Agesic a copiar, adaptar e/ou incorporar qualquer parte deste documento à versão final que será apresentada ao Parlamento, sem necessidade de citação.

1. Quais são as recomendações específicas que você poderia fazer, a partir de sua experiência, para promover os eixos definidos neste documento?

Expressamos que, de forma geral, estamos de acordo tanto com a análise apresentada quanto com os aspectos priorizados e as diretrizes gerais da proposta apresentada na versão preliminar “Bases para el desarrollo del informe previsto en el art. 74 de la Ley N° 20.212”. Embora exista um aspecto central que o documento deixa de abordar de forma explícita e clara, trata-se de uma pergunta que certamente vários legisladores têm em mente: Precisamos de uma regulação geral da IA ou devemos regular determinados usos da IA ou seu uso em determinados setores?

Entendemos que ainda não estão dadas as condições para uma regulação generalista baseada na determinação de diferentes níveis de risco, na atribuição de obrigações diferenciadas para cada um desses níveis e na criação de uma nova institucionalidade especializada em IA. É preciso compreender melhor o panorama para regular; por isso, propomos recomendar aos
parlamentares a criação de um fórum para promover os eixos definidos neste documento, detectar outras prioridades em âmbito nacional e formular recomendações por diferentes atores sociais para uma regulação adequada e sustentável.

Paralelamente a essa discussão, sugerimos concentrar os esforços regulatórios **atuais na atualização do corpo normativo nacional vigente e na regulação dos usos atuais da IA pelo governo que impliquem alto risco.**

Dessa forma, e sem descartar a possível existência de outras questões emergentes, destacamos o uso policial da IA como uma questão emergente de alto risco que exige regulação urgente e propomos a criação de um novo eixo: "Eixo uso da IA para fins de vigilância policial e como prova no processo penal" (ver pergunta 4).

2. Existem deficiências ou incongruências do ponto de vista regulatório que impactem os aspectos avaliados nos eixos definidos neste documento e que não tenham sido consideradas?

A seguir, apresentamos alguns aspectos que não foram considerados no documento e que entendemos que deveriam ser acrescentados:

Seção "3. Eixo Direitos Humanos"

Propomos acrescentar as seguintes considerações na seção "3.3 **Diagnóstico preliminar em matéria de IA e Direitos Humanos":**

Sobre a Lei 18331 de Proteção de Dados Pessoais (LPDP) e o Decreto 64/020.

Estamos de acordo com as observações do documento preliminar de que os Arts. 13 e 16 da LPDP deveriam ser revisados. Entendemos que essas disposições não são suficientes pelos seguintes motivos:

1) O direito à contestação de avaliações pessoais baseadas em tratamento automatizado de dados (Art. 16) só se aplica no contexto de dados pessoais, embora exista uma infinidade de contextos nos quais não se aplica. Um exemplo ilustrativo: o mecanismo previsto no Art. 16 não poderia ser utilizado para contestar e obter informações de um sistema de IA que analise dados de poluição da água e do ar no qual se entenda que a saúde de um conjunto de cidadãos está em risco.
2) O Art. 16 só permite contestar decisões "cujo único fundamento seja um tratamento de dados pessoais". Basta "colocar um humano no meio" e dizer que o sistema "assessora", mas que o humano toma a decisão, para que o artigo deixe de ser aplicável. Diante dos conhecidos "vieses de automação" [1], deveria ser considerada a inclusão de alguma disposição que defina o conceito de "supervisão humana significativa"

[1] Relatório "Hacia una supervisión significativa de los sistemas automatizados de toma de decisiones" (2022). Digital Future Society. Disponível em: https://digitalfuturesociety.com/es/report/hacia-una-supervision-significativa-de-los-sistemas-automatizados-de-toma-de-decisiones/

incluindo os aspectos mínimos exigidos, como a formação dos atores que operam o sistema, entre outros fatores.
3) Não devemos esquecer que os mecanismos da LPDP e do Decreto 64/020 não consideram a proteção de dados pessoais como um direito coletivo; por isso, com base nessas disposições, tampouco se poderá exigir de qualquer instituição pública ou privada que preste contas sobre parâmetros básicos de explicabilidade de seus sistemas automatizados diante de um risco potencial aos direitos fundamentais.
4) No Decreto 64/020, os sujeitos obrigados não têm obrigação de publicar suas avaliações de impacto; só são obrigados a compartilhá-las com a URCDP se a avaliação indicar um risco potencial e significativo (Art. 7).
5) Os Arts. 13 e 16 da LPDP não especificam quais são os requisitos exigidos para configurar a explicabilidade e não exigem rastreabilidade nem auditabilidade, de modo que essa obrigação é satisfeita quando a própria administração apresenta explicações de forma unilateral.
6) São necessárias normas que garantam um mínimo de transparência, **interpretabilidade e auditabilidade algorítmica (Stoyanovich, Julia 2020)** [2] entendendo que:

- **A transparência algorítmica não é sinônimo de liberar o código-fonte;** a publicação do código-fonte ajuda, mas às vezes é desnecessária e frequentemente insuficiente. Em alguns casos, a exigência de liberar o código-fonte pode ser excessiva ou lesar direitos.
- **A transparência algorítmica exige transparência de dados; a** explicabilidade só pode ser alcançada no contexto dos dados: os dados usados para treinamento e testes, os dados que serão usados para a implementação e validação do sistema (conjuntos de dados de referência) e os dados sobre desempenho e precisão do sistema. A transparência de dados é necessária para todos os sistemas automatizados, não apenas para sistemas baseados em Machine Learning.
- **A transparência de dados não é sinônimo de tornar públicos todos os dados;** os dados devem ser liberados sempre que possível. Quando isso não for possível (por questões de proteção de dados, confidencialidade ou propriedade intelectual, por exemplo), também é possível: publicar as metodologias de seleção ou coleta, recorrer a conjuntos de dados sintéticos, publicar resumos estatísticos ou amostras, os dados utilizados para o pré-processamento, a procedência dos dados e informações sobre sua qualidade/ representatividade e as fontes conhecidas de viés identificadas.

[2] Stoyanovich, Julia (2020). TransFAT. Translating fairness, accountability, and transparency into data science practice. Disponível em: https://pdfs.semanticscholar.org/061f/de41f92e6bd408b5722428bdcc8b2a7d0858.pdf

- **A transparência acionável exige interpretabilidade ou** compreensibilidade; em última análise, trata-se de explicar os pressupostos e efeitos do sistema (não apenas os detalhes de operação) e de envolver o público — técnico e não técnico.

Sobre a Lei 18381 de Acesso à Informação Pública (LAIP).

A LAIP deveria incluir uma disposição que introduza o direito de ser **informado sobre quais decisões são tomadas de forma automatizada ou com apoio de um sistema automatizado pela administração pública e sobre** como esses sistemas funcionam (considerando o exposto na seção anterior em relação à transparência, interpretabilidade e auditabilidade algorítmica e à conceituação de "intervenção humana significativa"). Também deveria ser incluída uma disposição que garanta o direito à interação humana e presencial com a administração pública.

Seção "4. Eixo Propriedade Intelectual"

Propomos acrescentar as seguintes considerações na seção "4.1 **Considerações preliminares":**

Atualmente, a maioria das atividades de desenvolvimento de IA exige o uso massivo de grandes volumes de dados e costuma incluir o uso de milhares de imagens, áudios, textos etc. protegidos por direitos autorais para fins de análise computacional ou treinamento de modelos. Entre esses usos podemos encontrar a aplicação de técnicas de mineração de texto e dados (como crowling, scraping e parsing), a criação de cópias técnicas ou efêmeras para fins de treinamento de modelos, entre outras. Dessa forma, para incentivar a inovação e gerar um ambiente jurídico seguro para pesquisadores e desenvolvedores locais, é necessário incluir nas leis de direitos autorais uma exceção que permita o uso de obras para fins de análise computacional. Essa exceção deveria incluir como restrição a condição de que esses usos não concorram com a exploração normal das obras nem prejudiquem injustificadamente os interesses dos autores.

Considerando que o software e as bases de dados também são protegidos por direitos autorais e por medidas de proteção tecnológica, será necessário regular de forma clara as relações entre os direitos autorais, o segredo comercial e a auditabilidade dos sistemas. A auditabilidade dos sistemas de IA é de especial interesse público tanto por razões de cibersegurança quanto de transparência e explicabilidade e, muitas vezes, exige contornar medidas de proteção tecnológica para o acesso

aos sistemas, a realização de cópias de teste ou as atividades de engenharia reversa.

Propomos acrescentar as seguintes considerações na seção “4.2 Seleção **de antecedentes internacionais”:**

Quanto às exceções ao direito de autor para fins de análise computacional, o antecedente mais recente no contexto da OMPI é o relatório sobre “Los retos de los centros de investigación y los fines de la investigación en relación con los derechos de autor” (2023) [3]. Esse relatório foi solicitado a Raquel Xalabarder pelo Comitê de Direitos de Autor e Conexos (SCCR/OMPI), e nele a autora afirma: “O papel da leitura não humana (mecânica), como a análise de inteligência artificial (IA), está ganhando cada vez mais importância nas metodologias de pesquisa. A mineração de textos e dados (TDM) ganhou destaque graças às tecnologias digitais. Graças às ferramentas de TDM, os pesquisadores extraem informações de uma grande variedade de obras protegidas, desde trabalhos acadêmicos até música e publicações da imprensa.” (tradução nossa) Nesse mesmo relatório encontramos um Anexo com exemplos de normas nacionais que contêm esse tipo de exceção ao direito de autor para atividades de pesquisa com fins de análise computacional, já presentes em quase todas as legislações do Norte Global. Quanto às exceções ao direito de autor e às medidas de proteção tecnológica para fins de auditabilidade dos sistemas, encontramos o relatório do Grupo de Trabalho sobre Segurança na Economia Digital de 2022 da OCDE [4]. Nesse relatório, afirma-se que “a lei de direitos autorais pode ser infringida quando as informações divulgadas contêm partes do código de software protegido por direitos autorais. Essa proteção de direitos autorais poderia restringir o intercâmbio de informações sobre vulnerabilidades com o fornecedor original, dificultando a implementação das DCV — Divulgação Coordenada de Vulnerabilidades — em muitos casos.” O documento explica que a falta de atualização das exceções ao direito de autor e às medidas de proteção tecnológica implica riscos legais para os auditores e pesquisadores de segurança digital e também afirma que essas normas são usadas pelos proprietários do software que se pretende investigar para ameaçar com procedimentos jurídicos.

[3] Xalabarder, Raquel (2023). “Los retos de los centros de investigación y los fines de la investigación en relación con los derechos de autor”. Disponível em: https://www.wipo.int/meetings/es/doc_details.jsp?doc_id=621815

[4] OECD (2022). OECD Policy Framework on Digital Security. Disponível em: https://www.oecd.org/publications/oecd-policy-framework-on-digital-security-a69df866-en.htm

Propomos acrescentar as seguintes considerações na seção “4.3 **Diagnóstico preliminar em IA e Propriedade Intelectual”:**

> A Lei de Direitos Autorais do Uruguai (Lei 9.739) não prevê exceções ao direito de autor (nem ao regime de medidas de proteção tecnológica) que permitam o desenvolvimento adequado de atividades de análise computacional ou de auditorias, seja para fins de segurança, seja para fins de explicabilidade. Por isso, é necessário incluir uma nova exceção no Art. 45 da Lei de Direitos Autorais (Lei 9739) que permita o uso de obras para fins de análise computacional. Também se sugere acrescentar uma exceção ao direito de autor (e às medidas de proteção tecnológica) para possibilitar o acesso, a cópia e a análise dos sistemas com a finalidade exclusiva de permitir instâncias de auditabilidade quando um juiz ou outra lei assim exigir. Essas exceções deverão explicitar que ficam estritamente proibidos os usos competitivos ou que prejudiquem injustificadamente o autor ou titular dos direitos sobre as obras.

3. Você identificou potenciais melhorias ou modificações na regulação vigente que possam contribuir para o desenvolvimento da IA no Uruguai?

---

4. Existem outros aspectos que você não encontra considerados e que devam ser analisados?

A seguir, propõe-se a inclusão de um novo eixo que constitui a **principal questão emergente de uso da IA com alto risco de violação dos direitos** fundamentais no Uruguai, de modo que deveria ser analisada de forma independente e exige regulação urgente:

Eixo uso da IA para fins de vigilância policial e como prova no processo penal.

Considerações preliminares:

O uso da IA para fins de prevenção do crime e segurança pública coloca em risco os direitos dos cidadãos por seu potencial de discriminação e por se tratar de uma tecnologia altamente intrusiva, além dos possíveis vieses ou falhas que impliquem riscos de discriminação. Algumas das principais

preocupações em torno do uso desses sistemas pela polícia e na justiça criminal são [5]: A violação da presunção de inocência. O direito à presunção de inocência nos processos penais é um direito humano fundamental. No entanto, o crescente uso da IA no âmbito da justiça penal, especialmente o uso de vigilância biométrica a distância e de certos tipos de software policial preditivo, levanta questões sobre o alcance desse direito e sobre como os sistemas de IA devem ser construídos e utilizados para protegê-lo.

A preservação da igualdade processual e do devido processo. Uma das principais preocupações apresentadas nos estudos sobre determinados sistemas de IA é que eles são inacessíveis a um exame adequado pelos acusados e seus advogados. Isso tem graves implicações para o princípio da igualdade de meios processuais e o direito ao contraditório, pois, sem informações sobre como uma decisão é tomada, é difícil prever como os acusados poderão questionar a precisão e a legalidade da decisão. Nesse sentido, um dos principais problemas que impedem a possibilidade suficiente de contestar os sistemas de IA nos processos penais é a falta de notificação. Se uma pessoa não for notificada de que foi objeto de uma decisão automatizada por um sistema de IA, não terá a possibilidade de contestar essa decisão nem as informações nas quais ela se baseou. Por sua vez, o fenômeno das caixas-pretas é outro fator de risco na aplicação da IA, pois, para preservar o devido processo e o direito à igualdade processual, o sistema e seus resultados deverão ser necessariamente explicáveis e comprovadamente livres de viés.

A falta de formação obrigatória dos atores do sistema judicial: a formação dos atores do sistema judicial é imprescindível para determinar a admissibilidade e realizar uma correta avaliação dos meios de prova digital, além de dar sentido ao conceito de “intervenção humana significativa” no contexto judicial. A formação não é necessária apenas para os usuários primários dos sistemas de IA, como juízes e policiais que os utilizam para fundamentar suas próprias decisões. A formação também deve estar disponível para os advogados da defesa penal, para que estejam em melhores condições de contestar os sistemas de IA, quando necessário.

Seleção de antecedentes internacionais

O Relator Especial sobre a promoção e a proteção do direito à liberdade de opinião e expressão da ONU, em seu relatório “La vigilancia y los derechos Humanos” (2019) [6], propõe medidas drásticas. Faz um chamado urgente para

[5] Policy Paper: Regulating Artificial Intelligence for Use in Criminal Justice Systems in the EU (2022). Fair Trials. Disponível em: https://www.fairtrials.org/app/uploads/2022/01/Regulating-Artificial-Intelligence-for-Use-in-Criminal-Justice-Systems-Fair-Trials.pdf

[6] Relator Especial sobre a promoção e a proteção do direito à liberdade de opinião e expressão. «Informe sobre la vigilancia y los derechos humanos», A/HRC/41/35. (Assembleia Geral

estabelecer "uma moratória imediata sobre a venda e a transferência, em âmbito mundial, dos instrumentos utilizados pelo setor de vigilância privada até que sejam estabelecidas salvaguardas rigorosas dos direitos humanos na regulação dessas práticas e se possa garantir que os governos e os agentes não estatais utilizarão esses instrumentos de modo legítimo." Também solicita "uma regulação mais rigorosa das exportações de equipamentos de vigilância e restrições mais estritas de sua utilização".

No "Regulamento de Inteligência Artificial da UE" (Art. 5 do Capítulo II "Práticas de Inteligência Artificial proibidas") [7], proíbe-se o uso, para aplicações policiais ou de ordem pública, da identificação biométrica em tempo real em locais acessíveis ao público pelas forças de segurança, salvo nos seguintes casos: busca de vítimas potenciais de crimes; prevenção de ameaças específicas e substanciais a infraestruturas críticas ou a pessoas físicas; prevenção de ataques terroristas; e persecução de crimes puníveis com mais de cinco anos de privação de liberdade. Antes, será obrigatório avaliar a probabilidade e a escala do dano possível sem esses sistemas e do dano que eles poderiam ocasionar; deverá haver autorização judicial ou administrativa vinculante; e serão impostas limitações temporais, geográficas e pessoais.

Outro antecedente importante é a "Resolução do Parlamento Europeu, de 6 de outubro de 2021, sobre a inteligência artificial no Direito penal e sua utilização pelas autoridades policiais e judiciais em assuntos penais" [8]. Essa resolução aborda o uso da inteligência artificial (IA) no âmbito do direito penal, concentrando-se em sua aplicação pelas autoridades policiais e judiciais. O documento destaca a necessidade de estabelecer um marco regulatório robusto que garanta o respeito aos direitos fundamentais, à privacidade e à proteção de dados. Além disso, enfatiza a importância da transparência, da supervisão humana e da responsabilidade no uso de sistemas de IA para prevenir vieses e discriminações. A resolução também insta à realização de avaliações de impacto e auditorias regulares desses sistemas para assegurar sua conformidade com os padrões éticos e legais da União Europeia.

Nessa Resolução, o Parlamento Europeu destaca o potencial da IA para melhorar a eficiência e a eficácia no combate à criminalidade, mas também adverte sobre os riscos associados, como a possibilidade de erros judiciais e a

das Nações Unidas, 28 de maio de 2019). Disponível em:.
https://www.undocs.org/es/A/HRC/41/35

[7] Regulamento de Inteligência Artificial da União Europeia aprovado por Resolução legislativa do Parlamento Europeu, de 13 de março de 2024. Disponível em:
https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_ES.pdf

[8] Resolução do Parlamento Europeu, de 6 de outubro de 2021, sobre a inteligência artificial no Direito penal e sua utilização pelas autoridades policiais e judiciais em assuntos penais (2020/2016(INI)). Disponível em:
https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_ES.html

violação de direitos humanos. A resolução propõe a criação de um marco legal específico para o uso da IA no âmbito penal, que inclua diretrizes claras sobre a coleta e o processamento de dados, assim como medidas para garantir a equidade e a não discriminação. Além disso, recomenda que as autoridades e os profissionais do direito recebam formação adequada sobre o uso e as implicações da IA, assegurando assim uma aplicação justa e segura dessas tecnologias no sistema judicial.

Diagnóstico preliminar

O Ministério do Interior vem construindo um ecossistema de vigilância automatizada em apoio ao cumprimento de suas atribuições, baseado tanto em IA quanto em outros tipos de sistemas. Esse ecossistema não foi acompanhado da devida regulação nem de critérios de transparência proativa que ofereçam confiança sobre seu funcionamento. Não existe nenhuma regulação relacionada ao uso policial dos sistemas recentemente adquiridos pelo Ministério do Interior. Por exemplo, o de reconhecimento facial automatizado, o software UCINET (software de inteligência sobre fontes abertas, como redes sociais), o sistema ShotSpotter (sistema que implica a colocação de microfones nas ruas para que uma IA detecte disparos) ou inclusive um software de análise de câmeras para "determinar condutas suspeitas que possam alertar o policial antes que o crime ocorra". No Uruguai, o controle do uso das bases de dados pessoais utilizadas nas atividades de "segurança pública, defesa, segurança do Estado e suas atividades em matéria penal, investigação e repressão do crime" não é abrangido pelas obrigações estabelecidas na Lei 18331 de Proteção de Dados Pessoais (LPDP Art. 3 Alínea B e Art. 25) [9].

Quanto ao software de Reconhecimento Facial Automatizado (RFA) adquirido pelo Ministério do Interior em fevereiro de 2020 por licitação pública, ressaltamos que essa aquisição está relacionada à aprovação da criação de uma base de dados de identificação facial para tratamento com fins de segurança pública a cargo da Secretaria do Ministério do Interior (arts. 191 e 192 da Lei Orçamentária 2020). Dessa forma, permite-se o uso das fotografias de rostos (e informações associadas a elas) das carteiras de identidade e dos passaportes da base da Direção Nacional de Identificação Civil (DNIC) para criar uma base biométrica com finalidade diferente da identificação. São muitas as questões que surgem dessa contratação e autorização em massa para o uso de

[9] "No entanto, cabe indicar que, mesmo nos casos indicados no parágrafo anterior, a URCDP interpretou que os princípios da proteção de dados pessoais também são aplicáveis de forma geral." Ver consulta ao Conselho Executivo da URCDP publicada no Relatório "Fuera de Control. Uso policial del reconocimiento facial automatizado en Uruguay". Datysoc (2022), pág. 49. Disponível em:

https://datysoc.org/wp-content/uploads/2022/03/Informe-reconocimiento-facial-automatizado-Uruguay-2022-Datysoc.pdf

dados biométricos de toda a população. Com quais finalidades exatas o sistema foi contratado? Quem autoriza o uso do sistema de RFA? Como o uso do sistema será auditado? Como o acesso ao sistema será controlado? Como um agente deve proceder diante de uma correspondência biométrica nos diferentes contextos de uso? Quando uma correspondência biométrica pode ser aceita como prova? Como essa prova será avaliada? Como será abordada a possibilidade de vieses no sistema? Quando e como o acusado será informado da existência desse tipo de prova? Como serão abordadas as diferenças entre uma correspondência biométrica em ambiente controlado e outra em ambiente não controlado? Como esses dados pessoais serão eliminados quando não forem mais necessários? Nada disso foi definido ainda, e a maioria dessas **decisões deveria ser fixada por meio de normas de nível legal precisas e publicamente acessíveis.**

Também cabe destacar que nem no Código de Processo Penal nem na Lei de Procedimento Policial contamos com qualquer regulação sobre admissibilidade ou avaliação da prova digital, com protocolos públicos sobre o uso da IA adquirida pelo Ministério do Interior ou com a formação dos atores judiciais sobre o funcionamento dessa IA.

Recomendações regulatórias sobre o uso policial da IA

Seguindo as recomendações da Relatoria de Liberdade de Expressão da ONU, sugere-se impor uma moratória à aquisição de software de vigilância até que exista uma base legal que regule adequadamente o ecossistema de vigilância policial.

Com o objetivo de estabelecer uma regulação rigorosa sobre seu uso e oferecer garantias contra atos discriminatórios e contra seu uso abusivo ou arbitrário, deveriam ser introduzidas as modificações necessárias no Código de Processo Penal e na Lei de Procedimento Policial para regular adequadamente o tema, incluindo:

- A obrigação de realizar uma análise de impacto (se possível, pública) sobre os direitos fundamentais antes de adquirir soluções de IA para fins de vigilância, assim como conhecer e declarar previamente as finalidades exatas da contratação.
- O estabelecimento de limites sobre quais usos são estritamente proibidos à polícia e quais exigem ordem judicial.
- A possibilidade de exigir a auditabilidade e a explicabilidade algorítmica, a rastreabilidade, protocolos de controle de acesso e a descrição detalhada das responsabilidades de quem usa esses sistemas de vigilância.
- O treinamento adequado dos agentes policiais, juízes e promotores sobre o funcionamento e as limitações do sistema, mediante certificação obrigatória.

Recomendações específicas relacionadas à vigilância biométrica e ao reconhecimento facial:

- A proibição da inclusão em massa de toda a população no sistema de reconhecimento facial adquirido pelo Ministério do Interior. Isso implica a revogação dos arts. 191 e 192 da Lei Orçamentária 2020, pois esses artigos violam o princípio da presunção de inocência.
- A proibição do uso de vigilância biométrica em tempo real e sem ordem judicial em espaços públicos.
- Os mecanismos obrigatórios de análise de impacto e de avaliação de risco, juntamente com mecanismos de prestação de contas e acompanhamento.
- Regulação específica da admissibilidade, avaliação e produção das correspondências biométricas como métodos de investigação e como prova digital.

CONTRIBUIÇÃO DA COMISSÃO DE DIREITO INFORMÁTICO E TECNOLÓGICO DA ASOCIACIÓN DE ESCRIBANOS DEL URUGUAY.

Consulta: Bases para a discussão de conteúdos do relatório preliminar previsto no art. 74 da Lei No. 20212 (AGESIC)

1. Quais são as recomendações específicas que você poderia fazer a partir de sua experiência para promover os eixos definidos neste documento?

Quanto à governança, uma definição inicial deveria ser se é necessário que a normativa seja geral ou setorial, pois existem setores com alta sensibilidade institucional, social e econômica. Em ambos os casos, e tal como ocorre com o Regulamento de Inteligência Artificial da União Europeia, seria conveniente abordá-lo a partir dos riscos que poderia provocar, assim como da atribuição e distribuição de responsabilidades por danos (dada a multiplicidade de atores que podem participar), para garantir reparações equitativas às pessoas prejudicadas.

Será um desafio resolver a questão da atribuição de responsabilidades pelo uso da IA em um sistema que pode não estar sediado no Uruguai, mas cujas consequências serão suportadas em nosso país.

Em matéria judicial, entendemos que pode ser recomendável “utilizar sistemas de IA de “caixa-branca”, baseados em técnicas que servem para realizar previsões, classificações e detecções inteligentes que apresentam

enormes benefícios para a atividade judicial e a transformação digital das organizações, sem o risco de inexplicabilidade das caixas-pretas” [1]

O sistema “PretorIA”, criado pelo Laboratorio de Innovación e Inteligencia Artificial da Facultad de Derecho da Universidad de Buenos Aires (UBA IALAB), sistema preditivo desenvolvido para ser utilizado pela Corte Constitucional da Colômbia, pode ser altamente recomendável

“PretorIA combina funcionalidades baseadas em sistemas especialistas e técnicas de machine learning (aprendizado de máquina) de caixa-branca” [2]

2. Existem deficiências ou incongruências do ponto de vista regulatório que impactem os aspectos avaliados nos eixos definidos neste documento e que não tenham sido consideradas?

Para determinar esses critérios e, por meio deles, colocar a IA a serviço do cidadão e alcançar maior bem-estar social, deveríamos pensar, como país, quais são os limites que estamos dispostos a estabelecer para os diferentes desenvolvimentos de IA e, assim, regulá-los.

Estabelecer as avaliações de impacto correspondentes de um desenvolvimento de IA para minimizar os riscos aos direitos humanos.

[1] Tratado de inteligencia artificial y derecho : tomo II / Juan Gustavo Corvalan... [et al.] ; dirigido por Juan Gustavo Corvalan. - 2a ed. - Ciudad Autónoma de Buenos Aires : La Ley, 2023. Livro digital, Book "app" for Android Arquivo Digital: download e online ISBN 978-987-03-4642-5 [2] Obra citada

Nesses temas, será avaliada a adoção como base do recente Regulamento de IA da UE

> 3. Você identificou potenciais melhorias ou modificações na regulação vigente que possam contribuir para o desenvolvimento da IA no Uruguai?

Na seção 3.3. "Diagnóstico preliminar em matéria de IA e Direitos Humanos" do documento submetido à consulta, são destacados "7 aspectos centrais, relacionados aos pontos mencionados pelo Alto Comissário das Nações Unidas para os Direitos Humanos e detalhados acima…"

Neste relatório, vamos nos deter em duas das perguntas ali explicitadas:

1.- Qual é o alcance da transparência e da explicabilidade a serem garantidas no âmbito do desenvolvimento de sistemas de IA centrados na pessoa?

Respondendo a essa pergunta, dizemos que, embora em nossa normativa vigente pudéssemos aplicar a lei No. 18331 no que se refere a dados pessoais, utilizando os princípios de finalidade e de consentimento informado prévio, dado o impacto que a IA, tanto em seu desenvolvimento quanto em sua aplicação, tem sobre a pessoa e a sociedade, eles deveriam ser reforçados em sua definição e aplicação. O consentimento informado prévio deveria estabelecer claramente as informações que devem ser fornecidas tanto ao consumidor de um serviço de IA quanto a quem compra um produto de IA. (jogos para crianças, óculos, chat GPT) Não é suficiente o estabelecido pelo art.9 da lei No. 18331.

Chega-se a essa conclusão pelo tipo de dados pessoais que podem ser utilizados no treinamento da IA, que podem ser dados biométricos e dados sensíveis, os quais podem ser violados no momento de seu tratamento. Quanto ao princípio da finalidade, sua definição mais explícita e voltada ao desenvolvimento da IA ajudaria a obter maior transparência.

“Entendemos ser imprescindível que um esquema regulatório” coloque no centro o ser humano e “contemple a obrigação das empresas de explicitar onde e como são utilizadas as tecnologias de inteligência artificial e as técnicas automatizadas em suas plataformas, serviços e aplicativos, assim como o dever de prevenir a discriminação e assegurar que os equipamentos e sistemas de IA reflitam atitudes não discriminatórias e evitem vieses”[3]

“Em matéria de scoring realizado por IA, não poderão ser considerados dados pessoais que não façam parte do conjunto de dados correspondente à finalidade para a qual o estudo é realizado.

O resultado do scoring deverá contar com todos os princípios da IA, para que seja devidamente explicado por um ser humano à pessoa por ele afetada

Não poderão ser utilizados dados sintéticos no âmbito notarial ou contratual.

[3] Tratado de inteligencia artificial y derecho : tomo II / Juan Gustavo Corvalan... [et al.] ; dirigido por Juan Gustavo Corvalan. - 2a ed. - Ciudad Autónoma de Buenos Aires : La Ley, 2023. Livro digital, Book "app" for Android Arquivo Digital: download e online ISBN 978-987-03-4642-5 1. Inteligência Artificial. 2. Direito. I. Corvalan, Juan Gustavo, dir. CDD 346.002

As políticas de privacidade deverão explicitar se são utilizados dados sintéticos e como são utilizados” [4]

4. Existem outros aspectos que não foram considerados e que devam ser analisados?

Deverá ser prevista uma nova desigualdade tecnológica, muito mais profunda que as anteriores, na qual muitas pessoas ficarão pelo caminho, com o perigo de cair em situações de vulnerabilidade.

Por outro lado, “a adaptabilidade e a aquisição de novas habilidades sempre foram imperativas no mundo em mudança do direito. No entanto, na era digital e da inteligência artificial, essas habilidades evoluem e devem se adaptar aos desafios e às oportunidades oferecidos pelas novas tecnologias

“Um exemplo disso é o legal prompt engineering, uma habilidade emergente que se refere à capacidade de interagir e se comunicar eficazmente com agentes conversacionais baseados em IA, como é o caso do ChatGPT.

Nesse entendimento, veremos que o legal prompt engineering é uma habilidade crucial que abrange e melhora vários aspectos da prática jurídica na era digital, não apenas na busca de informações, mas também na elaboração de textos jurídicos, na argumentação eficaz de casos ou na concepção de estratégias jurídicas aprimoradas por meio da interação precisa e efetiva com agentes conversacionais sofisticados. Essa adaptação

[4] Ob.citada

não apenas é necessária, mas pode oferecer grandes oportunidades para acentuar o caminho da reconversão e otimizar o curso da prática jurídica e o desenvolvimento da justiça inteligente na era das máquinas” [5]

Tabeliã Elisabeth Bouvier Villa
Tabelião Javier Wortman

[5] Obra citada

Neste documento, reunimos as contribuições do Grupo Consultivo de IA para apresentar ao Poder Legislativo, conforme previsto no art. 74 da Lei N° 20.212, a cargo da Agesic.

As contribuições são feitas pelo Grupo Consultivo em Inteligência Artificial da Cámara Uruguaya de Tecnologías de la Información

Institucionalidade e Governança (Ref. Capítulo 2 do documento)
O objetivo deste eixo é determinar os aspectos fundamentais para assegurar uma institucionalidade adequada da Inteligência Artificial em nosso país.
Comentários
O documento mostra que a institucionalidade existente é adequada para tratar dos desafios apresentados. É fundamental, sim, contar com grupos consultivos com a participação de todos os atores, que funcionem de forma regular.
O conceito de grupos de trabalho é claro, mas eles deveriam ter maior influência na definição de políticas, que são articuladas, gerenciadas e lideradas pela AGESIC. Seria bom dar a eles maior relevância e poder de decisão do que a um grupo de trabalho. Compartilha-se o papel da URDCDP. A Agesic deve impulsionar o desenvolvimento de sistemas de inteligência artificial, mas não será conveniente que os desenvolva. Também me parece adequado definir critérios e mecanismos de fiscalização de que os critérios sejam bem aplicados.
O caminho para incorporar a IA como um aspecto central da criação de soluções inovadoras implica assumir riscos (como toda inovação). Quando uma solução é desenvolvida para oferecer um serviço público (e, em muitos casos, em temas sensíveis), o impacto do fracasso é maior, e isso pode desacelerar a inovação por não se assumirem esses riscos. Devem ser incorporados à governança mecanismos para resolver esse tipo de "conflito".
Buscar avaliar as soluções desenvolvidas pelo ecossistema uruguaio segundo padrões internacionais de impacto da solução, qualidade dos dados etc., de modo que as soluções avaliadas localmente segundo esse padrão possam ser "exportadas" para outros países que utilizem o mesmo padrão.

Direitos Humanos (Ref. Capítulo 3 do documento)
O objetivo deste eixo é apresentar quais são os riscos que não podem ser ignorados no âmbito do desenvolvimento de uma política pública em Inteligência Artificial e que devem exigir — caso seja considerado necessário — medidas especiais por seu impacto sobre os direitos das pessoas, e quais medidas poderiam ser pertinentes para aproveitar os sistemas de IA em benefício das pessoas e de seus direitos, identificando aquelas de ordem normativa.
Comentários

É importante identificar os casos aos quais está sendo aplicada. Deveriam ser consideradas diferentes ciências para avaliar o impacto nos DH. Seria aconselhável formar um comitê ou grupo de trabalho específico sobre esse tema e as implicações que pode ter no longo prazo.

A abordagem de classificação de riscos, embora apropriada, exige muita cautela para não se tornar uma barreira à inovação e ao investimento em IA. As definições precisam ser suficientemente precisas para dar garantias jurídicas e suficientemente flexíveis para se adaptar aos contextos. Por exemplo: um sistema de reconhecimento facial para vigiar os cidadãos não é o mesmo que um sistema de reconhecimento facial para encontrar crianças desaparecidas.

Como descrito no documento da Agesic, o marco legal e institucional atual já é apropriado para lidar com a maioria dos riscos potenciais.
Atualizações feitas na lei de proteção de dados pessoais já previnem alguns dos problemas potenciais.

Propriedade intelectual (Ref. Capítulo 4 do documento)

A Organização Mundial da Propriedade Intelectual (OMPI)27 assinala que o conceito de Propriedade Intelectual se refere às criações do intelecto, desde as obras de arte até as invenções, os programas de computador, as marcas e outros sinais comerciais.

SEM COMENTÁRIOS.

Infraestrutura e Cibersegurança (Ref. Capítulo 5 do documento)

O desenvolvimento da Inteligência Artificial depende de vários fatores. Um dos mais relevantes é contar com uma infraestrutura adequada, tendo o Estado um papel central para esse fim.

Comentários

A infraestrutura e a arquitetura tecnológica devem acompanhar a estratégia do país em políticas de IA. O processamento dos algoritmos e o controle sobre ela são fundamentais para gerar capacidades em âmbito nacional e ter independência para impulsionar essa tecnologia.

Em nível de Infraestrutura, é preciso diferenciar aquela com disponibilidade para prestar serviços de outra destinada à pesquisa e à Inovação.

É importante aprofundar uma estratégia nacional sobre o que pode ser autorizado a ir para a nuvem e utilizar seus algoritmos e o que não pode.

Por fim, são necessárias plataformas de interoperabilidade para melhorar a qualidade dos dados e, dessa forma, a interoperabilidade dos sistemas.

Eixo trabalho e Capacitação em IA (Ref. Capítulo 6 do documento)
Os impactos da Inteligência Artificial no mundo do trabalho e nos trabalhadores precisam ser avaliados e abordados a partir de diferentes perspectivas para aproveitar as oportunidades e enfrentar os desafios emergentes.
Comentários
Neste campo, há três grandes grupos a capacitar: • Em relação à requalificação, é necessário familiarizar os trabalhadores com essas tecnologias para que as incorporem em seus ambientes de trabalho. Isso é necessário para ter empresas e uma indústria mais competitivas. • Pessoal que desenvolverá os modelos, que não precisa pertencer a áreas técnicas. • Conscientizar a população sobre as vantagens proporcionadas pelo bom uso e as ameaças que podem surgir se houver mau uso.

Eixo responsabilidade civil e direitos do consumidor (Ref. Capítulo 7 do documento)
O eixo proposto neste ponto se refere a dois aspectos bem regulados normativamente: a responsabilidade civil e as relações de consumo.
Comentários
Em um país produtor de tecnologia como o Uruguai, que aposta no crescimento da participação dessa indústria na economia, é importante oferecer proteção adequada aos desenvolvedores e fabricantes das aplicações de IA. A responsabilidade deve estar associada ao descumprimento das normas legais vigentes e a casos de negligência comprovada. O excesso de regulação neste ponto pode gerar responsabilidades que imponham uma barreira elevada aos empreendedores.

Eixo de medidas de promoção para a IA (Ref. Capítulo 8 do documento)
O objetivo deste eixo é considerar o alcance e a determinação de eventuais medidas de promoção associadas a uma política pública em IA.
Comentários
Entende-se ser importante gerar espaços com políticas públicas que impulsionem a inclusão dessa tecnologia em indústrias que queremos fortalecer em âmbito nacional. Por exemplo, o setor agropecuário. Definir políticas e práticas de bom uso dos dados e de seus treinamentos. Gerar selos que validem as empresas que as aplicam. Esses selos podem

ser reconhecidos globalmente, melhorando a qualidade dos serviços prestados pelas empresas; por outro lado, oferecem garantias à população de que as boas práticas são aplicadas.