O valor social dos dados: Contribuições da avaliação de impacto social do tratamento de dados pessoais

Pedro Dalese[1]

1. Refletindo sobre o valor social dos dados pessoais

O panorama atual da sociedade destaca a relevância dos dados pessoais no acesso a atividades e serviços, desempenhando uma função central na vida das pessoas e nas operações das organizações. Tal importância é impulsionada pela crescente dependência de tecnologias coletoras de dados, que moldam significativamente as interações sociais [1].

Anteriormente considerados recursos escassos, os dados agora emergem como elementos-chave em uma economia digital, caracterizada pela profusão de informações pessoais. A crescente importância dos dados na economia digital contemporânea destaca que a ausência de proteção adequada das informações pode expor as pessoas ao risco de discriminação com base em suas opiniões, crenças religiosas e condições de saúde. A proteção dos dados pessoais, nesse contexto, configura-se como um elemento crucial para a construção de uma sociedade baseada na igualdade. Sem a proteção dos dados referentes às interações com instituições ou afiliação a partidos, sindicatos, associações e movimentos, os cidadãos ficam suscetíveis a serem excluídos dos processos democráticos: assim, tal direito exerce uma influência direta nas oportunidades de inclusão em uma sociedade verdadeiramente participativa [2].

O valor social dos dados cresce à medida que a incessante interconexão digital e a dependência de tecnologias continuam a moldar hábitos e costumes [3]. A cada momento, uma quantidade inestimável de dados pessoais é coletada e utilizada em uma variedade de contextos [4], frequentemente sem a possibilidade de o titular e o corpo social exercerem controle sobre a finalidade, destinatário e duração do tratamento [5].

[1] Bacharel em Direito pela Universidade Federal Fluminense (UFF), advogado especializado em Direito Digital e Proteção de Dados pela Escola Superior de Advocacia da OAB-RJ.

No âmago da questão, a manipulação indevida de dados pessoais pode expor sobremaneira o(s) titular(es), sujeitando-o(s) a riscos potenciais de magnitude e variedade superiores aos relacionados meramente à privacidade, tais como vigilância, discriminação e até mesmo danos econômicos [6]. Este fenômeno, impulsionado pelo desenvolvimento tecnológico e pela expansão da internet, resultou em uma multiplicação exponencial da informação, conferindo aos dados pessoais um valor econômico substancial. A mudança de paradigma não apenas desencadeou uma preocupação crescente com a privacidade, mas também estabeleceu os dados como ferramentas estratégicas para organizações públicas e privadas obterem vantagens pecuniárias, políticas e outras [7].

2. Desafios e regulamentação na era digital

A compreensão das interconexões entre a proteção dos dados pessoais, tanto individualmente quanto coletivamente considerados, e diversos outros direitos e interesses tutelados pode ser extraída do texto constitucional vigente. Nesse contexto, destaca-se a importância de reconhecer que a tutela do direito à proteção dos dados pessoais ocorre concomitantemente à salvaguarda de outros bens fundamentais, estabelecendo regiões de interseção e, em alguns casos, de colisão.

Dentre esses bens constitucionais, podem ser mencionados, a modo de exemplo, a dignidade da pessoa humana, a construção de uma sociedade justa e solidária, a intimidade, a privacidade, bem como o direito à igualdade e à não discriminação, a proteção do consumidor, dos idosos e das crianças e adolescentes. Essa correlação é reforçada pela noção de "poder da informação" nas relações sociais, conforme explicitado na exposição de motivos da Convenção 108 do Conselho da Europa, de 1981 [8]. Tal noção destaca as repercussões das atividades de tratamento de dados nos valores fundamentais de uma sociedade democrática, uma vez que muitas decisões que impactam a sociedade são fundamentadas em informações armazenadas em arquivos de dados informatizados.

Essa preocupação também se reflete nas justificativas e discussões dos projetos de lei (4.060/2012; 330/2013, 5.276/2016 e 53/2018) [9, 10, 11, 12] que antecederam a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD),[2] bem como nos

[2] Lei nº 13.709, de 14 de agosto de 2018.

debates da PEC nº 17/2019 [13], que resultou na EC 115/2022,[14] inserindo a proteção de dados pessoais entre os direitos e garantias fundamentais.[3]

Nesse contexto, a Avaliação de Impacto Social do Tratamento de Dados Pessoais (AIST) surge como um procedimento concebido para fortalecer a execução de medidas e mecanismos no âmbito da proteção coletiva dos dados pessoais, englobando, desse modo, a tutela de direitos difusos, coletivos em sentido estrito e individuais homogêneos [15].

Ao reconhecer o valor social dos dados, torna-se imperativo não apenas regular o tratamento de informações pessoais, mas também promover práticas éticas e transparentes que salvaguardam liberdades fundamentais do indivíduo e de grupos diante da era digital.

A era digital representa um período em que a ascendência da tecnologia digital reconfigura substancialmente as estruturas políticas e os processos de tomada de decisões [16]. Nesse cenário, a AIST não se limita a uma abordagem técnica; ela direciona condutas éticas e procedimentais, buscando harmonizar o avanço tecnológico com a proteção de direitos individuais e coletivos. Em consonância com o avanço na era digital, a avaliação não apenas identifica e mitiga vieses em sistemas automatizados alimentados por dados pessoais, mas também considera os benefícios sociais e econômicos associados aos resultados oriundos de atividades de tratamento.

A AIST sinaliza que as ramificações do processamento de dados pessoais transcendem o domínio técnico, configurando-se como uma problemática que incide diretamente sobre as liberdades fundamentais e os direitos da personalidade de maneira abrangente. Nesse contexto, a avaliação destina esforços na detecção e prevenção de práticas discriminatórias, enquanto promove a adoção de ações responsáveis frente aos possíveis impactos sociais decorrentes do tratamento de dados pessoais, notadamente no contexto digital. Desse modo, a avaliação contribui significativamente para a consolidação do princípio da responsabilização e prestação de contas, presente em diversas legislações de proteção de dados ao redor do mundo [17].

3. Os princípios da LGPD como vetores axiológicos para a AIST

[3] CF, art. 5º, LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

A Lei Geral de Proteção de Dados Pessoais (LGPD), promulgada em 2018, traz à luz diretrizes inequívocas para o tratamento de dados pessoais. A conexão entre a LGPD e a AIST se torna evidente ao ponderar os seguintes aspectos.

A norma, em primeiro plano, busca resguardar os direitos fundamentais de liberdade, privacidade e desenvolvimento da personalidade,[4] premissa alinhada diretamente à preocupação central da AIST, que visa assegurar que o processamento de dados pessoais ocorra de maneira ética e equitativa, reduzindo ao mínimo os riscos para os indivíduos e grupos.[5]

Além disso, a LGPD define o tratamento como toda operação realizada com dados pessoais, incluindo a avaliação e o controle da informação.[6] Vale dizer, tal conceituação enfatiza a importância de analisar os efeitos de como os dados são utilizados e como essas operações podem afetar a sociedade como um todo.

Também é importante destacar que a lei brasileira de dados permite que os controladores e operadores estabeleçam regras de boas práticas e de governança relacionadas ao tratamento de dados pessoais.[7] Note-se que isso implica considerar a natureza, escopo, finalidade e riscos associados ao tratamento de dados. Nesse contexto, a AIST confere uma abordagem coerente e responsável na identificação e gerenciamento de riscos sociais, de modo a minimizar ou até mesmo inibir que atividades de tratamento resultem em práticas discriminatórias ou na exploração desproporcional de grupos desfavorecidos.

Por conseguinte, é relevante observar que de acordo com as disposições previstas no artigo 55-J, inciso XIII, é incumbência da Autoridade Nacional de Proteção de Dados (ANPD) elaborar regulamentos relacionados aos relatórios de impacto na proteção de dados pessoais. Nesse sentido, tais diretrizes podem incluir a promoção da AIST como

---

[4] LGPD. Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

[5] LGPD. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (...) III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.

[6] LGPD. Art. 5º Para os fins desta Lei, considera-se: (...) X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[7] LGPD. Art. 50. § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

uma boa prática que soma esforços na garantia da proteção dos direitos individuais e na equidade social no tratamento de dados pessoais.

Ao analisar os comandos e princípios na legislação, é possível discernir convergências com os objetivos do processo da AIST. Destacam-se a importância dada à asseguração da precisão, clareza, relevância e atualização dos dados pessoais (qualidade dos dados), bem como as iniciativas voltadas para a divulgação transparente e de fácil acesso de informações sobre o tratamento de dados, seus propósitos e os agentes envolvidos (transparência). Adicionalmente, as medidas relacionadas à avaliação concentram-se na identificação de possíveis impactos sociais adversos no tratamento de dados, com o intuito de implementar ações preventivas para proteger os direitos dos titulares (prevenção) e garantir que a utilização dos dados não ocorra de maneira discriminatória (não discriminação).

A análise dessas questões torna-se mais evidente quando se dirige a atenção para os elementos centrais da avaliação.

4. Elementos Centrais da AIST

Na avaliação de impacto social do tratamento de dados pessoais é crucial compreender a complexidade das ramificações desse processo na sociedade. Por meio da AIST, pode-se explorar de forma abrangente os potenciais impactos sociais do tratamento de dados pessoais, avaliando não apenas os riscos, mas também os benefícios associados. Ela deve se estender à conformidade legal, assegurando que o tratamento de dados esteja em total aderência às regulamentações específicas do setor, bem como à legislação nacional e internacional aplicável. Além disso, uma análise específica dos riscos para grupos vulneráveis, como a comunidade LGBTQ+, pessoas com deficiência, portadores de doenças, idosos, pessoas de diferentes religiões e opiniões políticas, assim como grupos raciais, étnicos e questões identitárias, é essencial para evitar discriminação e garantir a igualdade de direitos.

A subjetividade e complexidade das características individuais, quando mal interpretadas por algoritmos e seres humanos falíveis, podem ter impactos sociais extremamente nocivos. Portanto, é de suma importância levar em conta as particularidades desses grupos

em um contexto tecnológico que tem o potencial de promover vigilâncias discriminatórias e ampliar problemas sociais significativos [18].

A AIST também deve priorizar a minimização de riscos sociais e a promoção de boas práticas éticas por parte dos agentes de tratamento,[8] garantindo, assim, a proteção das atividades de tratamento numa perspectiva coletiva.

Nesse sentido, a AIST deve abranger os seguintes elementos:

a) Garantia de conformidade legal sob o prisma social: A AIST deve assegurar não apenas a conformidade legal estrita no tratamento de dados, mas também incorporar uma vertente de análise social. Neste panorama, a ênfase recai além da verificação da aderência às regulamentações específicas do setor e na legislação nacional e internacional aplicável, mas também na avaliação dos impactos sociais que emanam do tratamento de dados. A análise social visa compreender como as práticas de processamento de dados influenciam e interagem com as comunidades, buscando compreender e mitigar possíveis efeitos adversos, promovendo, assim, uma abordagem que considera os efeitos sociais dessa atividade na proteção coletiva dos dados pessoais.

b) Consideração dos benefícios sociais e econômicos: A avaliação deve abranger não apenas os riscos e impactos negativos, mas também os benefícios sociais e econômicos associados ao tratamento de dados. Por essa razão, permite-se uma avaliação equitativa e imparcial dos efeitos do tratamento.

c) Avaliação dos riscos para grupos vulneráveis: A AIST deve incluir uma análise específica dos riscos associados ao tratamento de dados pessoais de grupos vulneráveis, tais como a comunidade LGBTQ+, pessoas com deficiência, portadores de doenças, idosos, pessoas de diferentes religiões e opiniões políticas, assim como grupos raciais, étnicos, e ligados a questões identitárias. Neste eixo, a análise visa garantir que o tratamento de dados não resulte em discriminação, preconceito ou violações dos direitos desses grupos, contribuindo para a proteção e igualdade de direitos na sociedade.

d) Minimização de riscos e promoção de boas práticas: A avaliação deve focar na identificação de riscos potenciais para os direitos e liberdades das pessoas e na implementação de medidas preventivas para mitigar esses riscos. Além disso, prima-se

[8] LGPD. Art. 5º Para os fins desta Lei, considera-se: (...) IX - agentes de tratamento: o controlador e o operador.

pela promoção de boas práticas éticas no tratamento de dados, desde a origem e por padrão.

A AIST, ao abordar elementos como a avaliação dos impactos sociais, a consideração dos benefícios sociais e econômicos, a garantia de conformidade legal e a análise específica dos riscos para grupos vulneráveis, contribui diretamente para o diagnóstico das diversas etapas atinentes ao tratamento de dados pessoais delineadas na lei. A gama de operações descritas no art. 5º, X da LGPD, abrangendo desde a coleta até a eliminação dos dados, evidencia a intrincada natureza das atividades realizadas com informações pessoais.

A respeito dessa característica, os componentes da AIST conferem uma abordagem holística, pois buscam analisar os potenciais impactos sociais do tratamento de dados. Desse modo, a integração dos elementos da AIST com o conceito legal de tratamento emerge como um caminho procedimental que busca a implementação, por parte do agente, de medidas eficazes que atestem a conformidade e o cumprimento das normas de proteção de dados pessoais, incluindo a efetividade dessas medidas na contenção e minimização de danos afetos à coletividade.

Além disso, a AIST se integra de maneira coesa com o § 2º do art. 46 da LGPD. Adotar medidas preventivas desde a concepção das atividades de tratamento, como preconizado pela legislação, é essencial para assegurar a proteção coletiva dos dados pessoais de práticas estigmatizantes, corroborando a vertente proativa existente na AIST.

Dessa forma, a AIST aborda de maneira abrangente os potenciais impactos sociais, considerando tanto os riscos quanto os benefícios associados ao tratamento de dados pessoais. Nessa perspectiva, fundamentada em critérios e metodologias com foco na gestão social de riscos das atividades de tratamento, busca-se, em última instância, garantir um padrão de conformidade legal que proteja grupos sociais vulneráveis contra discriminação e preconceito, promovendo boas práticas éticas no processamento de informações pessoais.

5. A relação de complementaridade entre a AIST e o RIPD

A LGPD se destaca por sua natureza protetiva intencionalmente dual, delineando um cenário regulatório que suplanta a mera salvaguarda de direitos individuais. A legislação adota uma postura afirmativa na tutela dos direitos de personalidade, ao mesmo tempo

em que incorpora dispositivos que asseguram de maneira inequívoca instrumentos de proteção para direitos coletivos e difusos [19]. Essa dualidade estrutural evidencia a complexidade da LGPD, que, ao reconhecer e abordar o valor social dos dados, vai além de uma abordagem estritamente centrada no indivíduo.

No âmbito da análise da relação entre a LGPD e a AIST, é crucial compreender como a LGPD aborda o conceito de Relatório de Impacto à Proteção de Dados Pessoais (RIPD), que se concentra na documentação das atividades de tratamento de dados que possam representar riscos significativos[9] para as liberdades civis e os direitos fundamentais [20]. Desse modo, a relação entre a AIST e o RIPD demonstra-se complexa e crucial para garantir a proteção dos direitos individuais e coletivos no contexto do tratamento de dados pessoais.

Os dois conceitos compartilham áreas de interseção e complementação. A AIST tem como objetivo analisar os impactos sociais decorrentes do tratamento de dados pessoais, enquanto o RIPD focaliza-se em riscos específicos às liberdades civis e aos direitos fundamentais, frequentemente de natureza coletiva, garantindo simultaneamente a conformidade com os princípios da LGPD.

Ambos têm como meta promover a responsabilidade e a prestação de contas, resguardando os direitos fundamentais e as liberdades civis dos titulares de dados. As avaliações estão alinhadas a práticas de conformidade que enfatizam a importância de uma gestão de riscos eficaz e o registro adequado das operações de tratamento de dados pessoais. Dessa forma, mesmo que a AIST não esteja explicitamente prevista na LGPD, ela pode desempenhar um relevante papel na proteção dos interesses individuais e coletivos relacionados ao tratamento de dados pessoais, em conformidade com os objetivos da legislação vigente.

6. A AIST como fator de atenuação de sanções administrativas

A AIST, indo além do estímulo à proteção coletiva de dados pessoais, fomenta a conformidade legal sob uma perspectiva fundamentada em direitos fundamentais e

[9] Quanto às atividades de tratamento de dados pessoais consideradas de alto risco, veja-se o art. 4º da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, que aprovou o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte.

valores éticos, o que pode resultar na redução do valor pecuniário de sanções administrativas.

Diante das disposições da LGPD, a AIST revela-se como um instrumento estratégico na minimização de sanções administrativas. O artigo 52 da norma estabelece parâmetros e critérios para a imposição de sanções, sendo os incisos VIII e IX do § 1º de observância obrigatória nesse contexto. Ao fomentar a implementação consistente de mecanismos internos para reduzir danos e promover a adoção de políticas de boas práticas e governança, a AIST alinha-se diretamente aos requisitos estabelecidos na legislação. Desse modo, ao realizar uma avaliação de impacto social, as organizações não apenas atendem às exigências legais, mas também reforçam sua posição perante a ANPD, demonstrando compromisso efetivo com a promoção de um tratamento legítimo e justo de dados.

Ademais, de acordo com a Resolução CD/ANPD nº 4 de 24 de fevereiro de 2023 [21], a definição das multas por violação da LGPD leva em consideração diversos parâmetros e critérios. Dentre eles, merecem realce a boa-fé do infrator, o benefício já obtido ou almejado pelo mesmo, sua colaboração e a implementação reiterada de procedimentos e mecanismos internos voltados à minimização dos prejuízos aos titulares dos dados. Nesse contexto, a AIST desempenha papel de sobrelevo, pois ao conduzir uma avaliação dos impactos sociais do processamento de informações pessoais, as organizações demonstram seu comprometimento com as diretrizes de prevenção e segurança contidas na norma. A adoção de políticas de boas práticas e governança, respaldada pela AIST, pode resultar na redução das penalidades em até 20%, conforme estabelecido pela mencionada Resolução, proporcionando, assim, um estímulo adicional à implementação efetiva de medidas no âmbito social da proteção de dados.

Dessa maneira, a adoção e implementação da AIST, aliadas à proteção dos dados pessoais numa perspectiva social e coletiva, igualmente podem resultar em impactos financeiros significativos, ao reduzir o montante das penalidades em casos de infração à LGPD.

7. Os impactos sociais dos dados e desafios algorítmicos nos Países Baixos

O escândalo dos Países Baixos, conhecido como o "*toeslagenaffaire*" ou o escândalo relacionado à fraude nos auxílios sociais destinados às crianças, é um exemplo dos

impactos adversos que podem ocorrer quando algoritmos são usados de maneira inadequada [22]. Em 2019, foi revelado que a autoridade tributária holandesa utilizou um algoritmo de aprendizado de máquina para criar perfis de risco a fim de detectar fraudes nos benefícios infantis. Isso resultou na penalização de milhares de famílias com base em suspeitas de fraude, com indicadores de risco do sistema. Muitas dessas famílias, frequentemente de baixa renda ou pertencentes a minorias étnicas, foram empurradas para a pobreza devido a dívidas exorbitantes com a agência tributária. Alguns dos afetados chegaram ao extremo de cometer suicídio, e mais de mil crianças foram retiradas do convívio de suas famílias. Com efeito, o incidente ilustra de forma trágica o impacto devastador de sistemas automatizados encarregados do processamento de dados pessoais para propósitos de assistência social quando não existem salvaguardas adequadas em vigor, e que carecem de respaldo por avaliações de cunho social antes de sua implementação.

O episódio ocorrido nos Países Baixos é apenas um exemplo dos impactos adversos do uso inadequado de algoritmos diante da ausência de avaliação de impacto no tratamento de dados sociais.

Ao ponderarmos sobre os elementos da AIST em relação ao caso específico, torna-se manifesta a maneira pela qual a abordagem poderia ter prevenido ou reduzido os impactos adversos.

Inicialmente, a garantia de conformidade legal sob o prisma social demandaria a observância conjunta das regulamentações específicas e dos impactos decorrentes do algoritmo responsável pela seleção de famílias num programa de assistência social tão sensível. A análise específica dos riscos para grupos vulneráveis, conforme o terceiro elemento, identificaria de forma proativa os impactos discriminatórios sobre famílias de baixa renda e minorias étnicas, atenuando ou até mesmo evitando os resultados trágicos. Por fim, a minimização de riscos, quarto elemento da AIST, atuaria como uma medida protetiva voltada a identificar antecipadamente possíveis consequências decorrentes da interrupção do programa assistencial na vida das crianças e suas famílias, contribuindo para evitar o desencadeamento do incidente humanitário nos Países Baixos.

Nesse contexto, o Relatório de Riscos Algorítmicos dos Países Baixos [23], divulgado em setembro de 2023 pela Autoridade de Proteção de Dados Pessoais (*Autoriteit Persoonsgegevens*), enfatiza a importância da supervisão abrangente dos algoritmos e

propõe a criação de um registro de algoritmos para organizações governamentais. O documento destaca a necessidade não apenas de avaliar os benefícios, mas também os riscos associados ao uso dessas tecnologias. Salienta que é viável desenvolver e empregar algoritmos de maneira responsável, proporcionando assim valor social. Por fim, destaca a premência de ações efetivas por parte do governo e do setor empresarial de medidas proativas em direção a uma maior transparência e explicabilidade, especialmente considerando a rápida integração das inovações de IA na sociedade.

Diante dos trágicos desdobramentos no episódio dos Países Baixos, é incontestável que a implementação irresponsável de algoritmos no âmbito do tratamento de dados sociais pode acarretar consequências devastadoras. O caso ilustra a importância de abordagens cautelosas, como a AIST, na proteção dos direitos fundamentais e na prevenção de discriminações sistêmicas. A reflexão sobre o Relatório de Riscos Algorítmicos dos Países Baixos destaca a necessidade de uma supervisão rigorosa, não apenas focada nos benefícios, mas considerando minuciosamente os riscos associados.

A proposição de um registro de algoritmos para organizações governamentais surge como um passo crucial em direção à transparência e responsabilidade no desenvolvimento e aplicação dessas tecnologias. Afinal, o desenvolvimento e uso responsável de algoritmos podem proporcionar valor social, desde que acompanhados por ações proativas do governo e de agentes privados.

Em última análise, é imperativo o reconhecimento de que o uso ético e responsável de algoritmos é essencial para preservar a equidade e a integridade de comunidades afetadas por decisões automatizadas.

8. A AIST em diálogo com as iniciativas de inteligência artificial do Brasil

A utilização de sistemas de inteligência artificial (IA) suscita questões acerca da privacidade e do tratamento de dados pessoais. A avaliação da extensão em que os sistemas de IA processam dados pessoais é uma consideração sensível, dependente do momento da análise: a identificabilidade das pessoas naturais pode ser latente desde o início ou apenas se manifestar posteriormente, com a aquisição de informações adicionais. Desse modo, torna-se imperativo examinar os métodos de aprendizado de

máquina empregados, bem como a probabilidade de (re)identificação de indivíduos por meio de intervenções atípicas nos sistemas.

Apesar de a utilização da IA prometer um amplo potencial para a sociedade, não está imune a desafios.

Diante da amplitude do conceito de tratamento delineado na LGPD, abarcando praticamente todo o procedimento relacionado a dados pessoais, as operações de processamento pertinentes à proteção de dados no contexto da IA apresentam uma notável diversidade. A título exemplificativo, destacam-se modalidades como: (i) a coleta e estruturação de dados para treinamento e aplicações em IA; (ii) o processamento de dados durante o desenvolvimento de sistemas de IA; (iii) o fornecimento de aplicações de IA treinadas com dados pessoais; (iv) sistemas de IA que processam de forma contínua os dados de treinamento a cada utilização; e (v) sistemas de IA generativa de imagens e informações pessoais [24].

No que diz respeito ao enfoque brasileiro na regulamentação e avaliação de impacto relacionadas à inteligência artificial (IA) e dados pessoais, é importante analisar a relevância e a compatibilidade da AIST com as políticas públicas e iniciativas legislativas no âmbito da IA e da gestão de dados pessoais, tais como a Estratégia Brasileira de Inteligência Artificial (EBIA) e o projeto de lei n° 2.338/2023 [25, 26].

A Estratégia Brasileira de Inteligência Artificial (EBIA) reconhece a importância da regulamentação e avaliação de impacto em relação à inteligência artificial (IA) e dados pessoais. Assim como na AIST, a EBIA destaca a necessidade de um "teste de equilíbrio de riscos/benefícios" que esteja centrado no ser humano, alinhando a busca por soluções para problemas específicos e, simultaneamente, potencializando os benefícios sociais que a inteligência artificial (IA) tem a oferecer à sociedade.

Além disso, EBIA destaca que a análise de riscos da IA, por meio da elaboração de relatórios de impacto, tem o potencial de moldar a abordagem das organizações ao avaliar questões de justiça, direitos humanos e transparência, uma abordagem que vai ao encontro da AIST.

No contexto da regulamentação e avaliação de impacto relacionadas à IA e dados pessoais, as avaliações de impacto se apresentam como um instrumento fundamental para a gestão de riscos associados ao desenvolvimento e utilização de sistemas de IA [27].

Desse modo, abordagens regulatórias centradas no ser humano e nas repercussões sociais resultantes das atividades de tratamento de dados pessoais refletem, em grande medida, o compromisso de harmonizar o progresso tecnológico com a proteção dos direitos associados à promoção do bem-estar social [28].

Em razão da regulamentação da IA ter historicamente dependido de ferramentas *ex post*, reativas, uma parcela da doutrina já sustenta a necessidade de implementação de mecanismos de governança de dados *ex ante* por meio de um regime de licenciamento social ("*social license*"), especialmente em contextos nos quais a IA apresenta altos riscos aos direitos fundamentais e pode perpetuar e até amplificar vieses e discriminações [29]. O que se busca é desencorajar usos inadequados que prejudicam pessoas e comunidades vulneráveis, bem como direcionar o desenvolvimento da IA em direções mais socialmente úteis, num mundo que é cada vez mais visto através das lentes dos algoritmos e dos valores sociais e pontos de vista de seus desenvolvedores, frequentemente sem questionar a real necessidade de tais sistemas [30].

Nesse cenário, o projeto de lei nº 2.338/2023 traz à tona a avaliação de impacto algorítmico em sistemas de IA de alto risco. No contexto brasileiro, as considerações previamente abordadas acerca da diversidade de operações de processamento relacionadas à proteção de dados no âmbito da IA ganham uma relevância ainda maior.

A proposta legislativa estipula que, antes da introdução no mercado ou utilização em serviço, todo sistema de IA passará por uma avaliação preliminar conduzida pelo fornecedor para a classificação de seu grau de risco. Adicionalmente, a avaliação de impacto algorítmico torna-se obrigatória para sistemas considerados de alto risco, conforme determinado pela avaliação preliminar. A metodologia dessa avaliação, conforme delineada no projeto de lei, engloba fases como preparação, compreensão do risco, mitigação dos riscos identificados e monitoramento. Tais diretrizes convergem com a abordagem discutida anteriormente sobre a importância das avaliações de impacto no contexto da regulamentação e gestão de riscos associados à IA, uma vez que buscam identificar e mitigar eventuais impactos adversos desses sistemas na sociedade.

9. Conclusão

A era digital, marcada pela ascensão tecnológica, evidencia a intrincada natureza do valor social dos dados pessoais e sua abrangente influência nas interações sociais e nas operações organizacionais. Enquanto a interconexão digital permeia uma vasta gama de aspectos da vida cotidiana, a dependência crescente de tecnologias exige uma abordagem que vá além do técnico, transcendendo para condutas éticas e procedimentos que equilibrem o avanço tecnológico com a salvaguarda dos direitos individuais e coletivos.

Nesse cenário, o direito fundamental à proteção dos dados pessoais pode ser compreendido como um direito que abrange tanto aspectos individuais quanto coletivos.

A proteção dos dados pessoais transcende a esfera individual, estendendo-se a uma dimensão coletiva que demanda uma abordagem jurídica abrangente. As regras constitucionais, concebidas para resguardar não apenas a liberdade individual, mas também o exercício da racionalidade coletiva, tornam-se fundamentais na definição dos contornos desse direito. Nesse contexto, a salvaguarda dos dados pessoais não é apenas um direito, mas também implica deveres que abarcam não apenas os Estados, mas também indivíduos e a sociedade como um todo. A concepção jurídica deve, portanto, abranger uma perspectiva coletiva, reconhecendo que tanto direitos quanto deveres desempenham um papel crucial na construção de um ambiente digital ético e equitativo. A negligência ou a insuficiência na tutela e promoção da proteção coletiva dos dados pessoais não apenas comprometem direitos individuais, mas emergem como uma preocupação política central no século XXI, destacando a necessidade premente de um arcabouço legal que promova uma sociedade digital justa, inclusiva e livre de restrições indevidas.

Nesse sentido, a AIST se configura como mais um elemento que visa somar esforços na construção de um futuro equilibrado entre a proteção social e o progresso tecnológico no tratamento de dados pessoais, de modo a estimular a adoção de padrões ético-sociais nessas atividades, minimizando os riscos e discriminações para os titulares, em sua multiplicidade, e considerando os benefícios sociais e econômicos associados às atividades de tratamento.

Referências

1. Sobre a proteção dos dados pessoais e os efeitos sociais decorrentes do tratamento irregular de dados pessoais realizado por empresas e setor público no âmbito da União Europeia, veja-se, em especial, CHAVES, João Guilherme Pereira. Sanção aplicada pela inspetoria estatal de proteção de dados lituana no 'caso karantinas': Tratamento de dados pessoais ilícito em aplicativos de saúde pública; PACCOLA, Amanda Thereza Lenci; PELEGRINI, Emília Garbuio. 'Caso Clearview AI': A aplicação de sanção por uso ilegal de software de reconhecimento facial pela polícia finlandesa; LANZILLO, Anderson Souza da Silva; LEMOS, Luana Andrade de; FEITOSA, Lukas Darien Dias. Supervisão de exames universitários on-line e a proteção de dados pessoais no contexto da Covid-19: Uma análise da decisão da DPA dinamarquesa à luz do GDPR; In: TOMASEVICIUS FILHO, Eduardo; FALEIROS JUNIOR, José Luiz de Moura; DALESE, Pedro (Coord.). GDPR - Regulamento Geral sobre a Proteção de Dados da União Europeia. Análise de casos sobre a aplicação das sanções administrativas. Indaiatuba: Foco, 2023, p. 124-268.

2. RODOTÀ, Stefano. Discorso del Presidente Stefano Rodotà - Relazione 2004 - 9 febbraio 2005. Garante per la protezione dei dati personali (GPDP), 2005, p. 2.

3. FRAZÃO, Ana; SANTOS, Luiza Mendonça da Silva Belo. Plataformas digitais e o negócio de dados: necessário diálogo entre o direito da concorrência e a regulação dos dados. Revista de Direito Público, Brasília, v. 17, n. 93, p. 58-81, maio/jun. 2020. p. 59-61.

4. TEPEDINO, Gustavo; TEFFÉ, Chiara Spadaccini de. O consentimento na circulação de dados pessoais. Revista Brasileira de Direito Civil, Belo Horizonte, v. 25, 2020, p. 84-86.

5. SIQUEIRA, Dirceu Pereira; MOREIRA, Mayume Caires. Autodeterminação informativa na sociedade pós-panóptico: novas formas de panoptismo e os direitos da personalidade. Prisma Juridico, [S. l.], v. 22, n. 1, 2023, p. 82–91.

6. DONEDA, Danilo. Registro da sustentação oral no julgamento da ADI 6389, sobre a inconstitucionalidade do art 2º, caput e §§ 1º e 3º da MP 954/2020. civilistica.com, v. 9, n. 1, 12, 2020, p. 2.

7. VÉLIZ, Carissa. Privacy is power Why and How You Should Take Back Control of Your Data. Londres, Reino Unido: Bantam Press, 2020, p. 71.

8. Council of Europe. Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. European Treaty Series - No. 108. Strasbourg, 28.I.1981. p.1.

9. BRASIL. Câmara dos Deputados. Projeto de Lei nº 4.060/2012. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Inteiro teor, p. 7. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: 09 nov. 2023.

10. BRASIL. Senado Federal. Projeto de Lei nº 330/2013. Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências. Texto inicial, p. 13. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/113947. Acesso em: 09 nov. 2023.

11. BRASIL. Câmara dos Deputados. Projeto de Lei nº 5.276/2016. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Inteiro teor, p. 20-21. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378. Acesso em: 09 nov. 2023.

12. BRASIL. Senado Federal. Projeto de Lei nº 53/2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/133486. Acesso em: 09 nov. 2023.

13. BRASIL. Senado Federal. Proposta de Emenda à Constituição nº 17/2019. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757. Acesso em: 09 nov. 2023.

14. BRASIL. Emenda Constitucional nº 115/2022. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Disponível em:

https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 09 nov. 2023.

15. A respeito da tutela coletiva de dados pessoais no sistema de tutela coletiva brasileiro, ROQUE, André. A tutela coletiva dos dados pessoais na Lei Geral de Proteção de Dados Pessoais (LGPD). Rio de Janeiro: Revista Eletrônica de Direito Processual – REDP, Ano 13. Volume 20. Número 2. 2019, p. 4-11. Disponível em: https://www.e-publicacoes.uerj.br/index.php/redp/article/view/42138/30270. Acesso em: 09 nov. 2023.

16. LAOURIS, Yiannis. Reengineering and Reinventing both Democracy and the Concept of Life in the Digital Era. In: FLORIDI, Luciano (Ed.). The Onlife manifesto: Being human in a hyperconnected era. Springer, 2015, p. 125-130.

17. Para uma visão abrangente sobre o assunto, MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E; ROTENBERG, Marc (Org.). Technology and privacy: the new landscape. Cambridge: The MIT Press, Cambridge: The MIT Press, 1997, p. 219–241. Em uma análise contemporânea das normativas internacionais acerca da privacidade e proteção de dados, GREENLEAF, Graham. Global Data Privacy Laws 2023: 162 National Laws and 20 Bills. 181 Privacy Laws and Business International Report (PLBIR), v. 2, n. 1, 2023, p. 2-4.

18. COSTA, Ramon Silva; KREMER, Bianca. Inteligência artificial e discriminação: desafios e perspectivas para a proteção de grupos vulneráveis frente às tecnologias de reconhecimento facial. Revista Brasileira de Direitos Fundamentais & Justiça, v. 16, n. 1, 2022, p. 156-159.

19. ZANATTA, Rafael. Capítulo 13. Tutela coletiva e coletivização da proteção de dados. In: PALHARES, Felipe (Org.). Temas Atuais de Proteção de Dados. São Paulo: Revista dos Tribunais. 2020, p. 345-374.

20. Enunciado 679: "O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) deve ser entendido como uma medida de prevenção e de accountability para qualquer operação de tratamento de dados considerada de alto risco, tendo sempre como parâmetro o risco aos direitos dos titulares". IX Jornada Direito Civil: comemoração dos 20 anos da Lei n. 10.406/2002 e da instituição da Jornada de Direito Civil. Brasília: Conselho da Justiça Federal, Centro de Estudos Judiciários, 2022.

21. BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Resolução CD/ANPD nº 4. Diário Oficial da União, Brasília, 24 fev. 2023.

22. POLITICO. Dutch scandal serves as a warning for Europe over risks of using algorithms. 29 mar. 2022. Disponível em: https://www.politico.eu/article/dutch-scandal-serves-as-a-warning-for-europe-over-risks-of-using-algorithms/. Acesso em: 05 nov. 2023.

23. PAÍSES BAIXOS. Autoriteit Persoonsgegevens. First Algorithmic Risks Report Netherlands calls for additional action to control algorithmic and AI risks. 01 Set. 2023. Disponível em: https://www.autoriteitpersoonsgegevens.nl/en/current/first-algorithmic-risks-report-netherlands-calls-for-additional-action-to-control-algorithmic-and-ai-risks. Acesso em: 05 nov. 2023.

24. ALEMANHA. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg. Rechtsgrundlagen im Datenschutz beim Einsatz von Künstlicher Intelligenz. Unsere Freiheiten: Daten nützen – Daten schützen. Version 1.0, 2023, p. 7-9.

25. BRASIL. Estratégia Brasileira de Inteligência Artificial (EBIA). Ministério da Ciência, Tecnologia e Inovações Secretaria de Empreendedorismo e Inovação. 2021, p.22-26. Disponível em: https://www.gov.br/mcti/pt-br/acompanhe-o-mcti/transformacaodigital/arquivosinteligenciaartificial/ebia-documento_referencia_4-979_2021.pdf. Acesso em 09 de nov. 2023.

26. BRASIL. Projeto de Lei n° 2338, de 2023. Dispõe sobre o uso da Inteligência Artificial. Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/157233. Acesso em 09 de nov. 2023.

27. AVILA NEGRI, Sergio et al. Sistemas de Inteligência Artificial e Avaliações de Impacto para Direitos Humanos. Revista Culturas Jurídicas, v. 10, Ahead of Print, 2023, p. 22-23.

28. LAPIN. Relatório sobre avaliação de impacto algorítmico para proteção dos direitos fundamentais. 2023, p. 16-29.

Disponível em: https://lapin.org.br/2023/04/13/avaliacao-de-impacto-algoritmico-para-protecao-dos-direitosfundamentais/. Acesso em: 19 abr. 2023.

29. MALGIERI, Gianclaudio; PASQUALE, Frank. Licensing high-risk artificial intelligence: Toward ex ante justification for a disruptive technology. Computer Law & Security Review, v. 52, 2024, p. 11-15.

30. MANTELERO, Alessandro. Beyond data: Human rights, ethical and social impact assessment in AI. Information Technology and Law Series. T.M.C. ASSER PRESS, 2022. p. 195.