O PRINCÍPIO DA PRECAUÇÃO NA REGULAÇÃO DE INTELIGÊNCIA ARTIFICIAL: SERIAM AS LEIS DE PROTEÇÃO DE DADOS O SEU PORTAL DE ENTRADA?

Bruno Ricardo Bioni[1]
Maria Luciano[2]

PALAVRAS-CHAVE: princípio da precaução; dano; incerteza; risco; responsabilidade; decisões automatizadas

KEY WORDS: precautionary principle; damage; uncertainty; risk; responsibility; automated decisions

---

[1] Doutorando em Direito Comercial e Mestre em Direito Civil pela Universidade de São Paulo. Professor e Fundador do Data Privacy Brasil.
[2] Mestranda e Bacharela em Direito pela Universidade de São Paulo. Pesquisadora no InternetLab.

I.Introdução e apontamentos metodológicos

Concessões de crédito, apólices de seguro, direcionamento de anúncios em redes sociais, autocorretor em aplicativos de mensageria, reconhecimento facial e etc. Decisões automatizadas estão cada vez mais presentes no dia-a-dia das pessoas. Elas compreendem uma das técnicas de Inteligência Artificial (IA), que, em geral, procuram identificar padrões a partir da análise de dados por meio de uma lógica matemática (algoritmo) e aprendizado de máquina (*machine learning*).

Contudo, acreditar que algoritmos sejam isentos de subjetividade, erro ou manipulação é uma "ficção cuidadosamente construída" (GILLESPIE, 2014). A escolha de quais dados importam e porquê importam nesse processamento depende de suposições prescritas a esses sistemas. Problemas decorrentes de algoritmos enviesados têm sido frequentes.[3] Eles parecem indicar o abismo entre os desenvolvedores desse tipo de tecnologia e aqueles que são impactados por ela. Dentre as razões para isso têm sido apontadas a falta de regulação, monopólios no setor de IA, estruturas de governança insuficientes dentro de empresas de tecnologia, assimetrias de poder entre empresas e usuários, a distância cultural entre os responsáveis por pesquisas em tecnologia e a diversidade das populações nas quais essa tecnologia é utilizada (AI Now, 2018). Esse diagnóstico tem suscitado demandas sociais por maior transparência no uso de IA.

Como o emprego dessa tecnologia, em geral, demanda o processamento de dados pessoais, essas questões têm sido endereçadas em leis de proteção de dados. A Lei Geral de Proteção de Dados no Brasil (Lei no. 13.709/2018 - LGPD), por exemplo, prevê o fornecimento informações sobre o tratamento desses dados, incluindo os critérios utilizados, e a possibilidade de solicitar revisão de decisões automatizadas. Nesse sentido também a Regulação Geral de Proteção de Dados da União Europeia (RGPD) prevê o fornecimento de informações sobre a lógica do processamento automatizado, seu significado e consequências para o titular.

A discussão de transparência nesse caso, contudo, não parece tão simples. A transparência pura e simples dos sistemas automatizados empregados parece gerar outros problemas: perpetuação dos problemas caso as informações apreendidas não sejam utilizadas

---

[3] "Bias in criminal risk scores is mathematically inevitable, researches say". Disponível em <https://www.propublica.org/article/bias-in-criminal-risk-scores-is-mathematically-inevitable-researchers-say>. Facebook has been charged with housing discrimination by the US government". Disponível em <https://www.theverge.com/2019/3/28/18285178/facebook-hud-lawsuit-fair-housing-discrimination>. "Self-driving cars may be more likely to hit you if you have dark skin". Disponível em <https://www.technologyreview.com/the-download/613064/self-driving-cars-are-coming-but-accidents-may-not-be-evenly-distributed/>.

para mudança, podendo aprofundar assimetrias de poder já existentes; danos à privacidade e exposição de grupos já marginalizados; fornecimento de informações pouco úteis que podem se sobrepor a informações realmente úteis; criação do falso binário segredo/transparência; a invocação de modelos liberais que pressupõem plena capacidade de todos os indivíduos entenderem e processarem as informações fornecidas; a crença na causalidade, ainda pouco comprovada empiricamente, de que a transparência, sozinha, aumenta a confiança nas instituições; a impossibilidade de se disponibilizar *toda* a informação, sem considerá-las em seus contextos e histórias específicas; a preferência por *ver* uma informação ao invés de *entendê-la*; a desconsideração de que, por vezes, existem limitações técnicas à transparência (Ananny e Crawford, 2018). A *accountability* desses sistemas parece demandar, assim, um tipo de transparência *qualificada*. E, nesse cenário, o princípio da precaução, há muito invocado no campo da proteção ambiental, parece um *framework* útil para se pensar essa questão.

Nesse sentido, o presente artigo pretende investigar se leis gerais de proteção de dados são possíveis vetores de entrada para a aplicação do princípio da precaução como parte da empreitada regulatória de Inteligência Artificial. Para tanto, analisa-se se o princípio da *accountability*, relatórios de impacto à proteção de dados pessoais e o direito à revisão de decisões automatizadas carregam consigo expressões normativas do princípio precaução. Em particular, qual é o grau de abertura nos processos de tomadas de decisão quanto ao emprego dessa tecnologia, bem como na ação ou inação em lançar mão de IA frente aos riscos que lhes são subjacentes. Analisa-se, ainda, a regulação efervescente de tecnologias de reconhecimento facial como um caso de fronteira que atrai diversos graus de aplicação do princípio da precaução.

O artigo está dividido em duas seções. A primeira delas mapeia o debate normativo em torno do princípio da precaução, buscando compreender sua racionalidade e verificar a procedência, ou não, das críticas feitas a ele. E a segunda seção pretende averiguar de que forma o princípio da *accountability*, relatórios de impacto à proteção de dados pessoais, o direito à revisão de decisões automatizadas poderiam servir como ferramentas à aplicação concreta desse princípio e, por fim, de que forma e a regulação de tecnologias de reconhecimento facial também internaliza conotações normativas do referido princípio.

II. Aplicação do Princípio da Precaução em Discussões Regulatórias: definindo os termos do debate

Durante a década de 1970, desenvolveu-se na Europa um movimento em defesa de políticas públicas baseadas em evidência ("*evidence-based policy*"). Buscava-se com isso a promoção de análises rigorosas de políticas, com vistas a fornecer informação e conhecimento aos reguladores para sua implementação. Contudo, o reconhecimento de que essas discussões ocorrem em uma arena política, permeada por valores, persuasão e negociação entre diversos atores, em que evidências e conhecimento científico são inevitavelmente valorados e ressignificados, requalificou o debate. Mais recentemente, muitos autores e instituições internacionais passaram a adotar a expressão "política públicas informadas por evidências" (evidence-informed policy") (Head, 2016).

Ademais, as incertezas e limitações do conhecimento científico acabam dificultando esse tipo de abordagem, impondo novos desafios a práticas regulatórias. O conceito de "incerteza" é mais complexo do que aparenta. Para além da falta de dados ou inadequação de modelos de avaliação de risco, ele também abarca a "indeterminação" (quando não se conhece todas as relações causais), a "ambiguidade" e a "ignorância" (*unknow unkowns*) (Science for Environment Policy, 2017). Os métodos tradicionais de regulação de risco (*risk assessment*, *risk managment* e análises de custo-benefício), que pressupõem algum conhecimento e estimativas de probabilidade na antecipação de riscos, parecem não dar conta do desconhecido.

É nesse cenário que surge o princípio da precaução. Originado na década de 1970 a partir de iniciativas de proteção ambiental, o princípio passa a fazer parte, na década de 1980, do direito alemão (*Vorsorgeprinzip*) (Majone, 2002; Stirling, 2016). Seu significado, contudo, permanece em disputa até os dias atuais. Tem-se notícia de 11 (onze) significados diferentes atribuídos a ele nos debates sobre políticas públicas (Resnik, 2003). Destacamos os três mais importantes.

Uma das primeiras formulações, e a mais aceita por diferentes jurisdições (Stirling, 2016), é a da Declaração do Rio sobre Meio Ambiente e Desenvolvimento de 1992 (Rio 92), segundo a qual uma abordagem precaucionária deveria ser amplamente aplicada pelos Estados, de acordo com suas capacidades, para a proteção do meio ambiente.[4] A falta de "completa"

[4] "Art. 15: In order to protect the environment, the precautionary approach shall be widely applied by States according to their capabilities. Where there are threats of serious or irreversible damage, lack of full scientific certainty shall not be used as a reason for postponing cost-effective measures to prevent environmental degradation."

certeza científica quanto a ameaças de dano "sério" ou "irreversível" não poderia, assim, ser usada como desculpa para não se empregar medidas para evitar danos ambientais.

Em 1998, em uma conferência de cientistas, filósofos, advogados e ativistas ambientais em Wisconsin nos EUA, a Declaração de Wingspread (Wingspread Statement, 1998) determinou que medidas precaucionárias deverão ser tomadas em casos de ameaça de dano à saúde humana ou ao meio ambiente, ainda que relações causais entre a atividade e os possíveis danos não sejam estabelecidas cientificamente. Nesses casos, haveria ainda uma inversão do ônus da prova, cabendo então ao proponente da atividade demonstrar a segurança do seu exercício.[5]

Finalmente, em 2000, um Comunicado da Comissão Europeia (CE) buscou esclarecer pontos a respeito da aplicação do princípio que vinham sendo disputados em tribunais ao redor da União Europeia. Segundo o documento, o recurso à aplicação do princípio pressupõe efeitos potencialmente perigosos ocasionados por um fenômeno, produto ou processo, e cuja avaliação científica não fornece grau suficiente de certeza. Nesse caso, diversas seriam as medidas possíveis a serem adotadas, de contratos e acordos legalmente definidos a projetos de pesquisa e recomendações. Em alguns casos, inclusive, a medida correta seria não fazer nada.[6]

Nenhuma das formulações conceitua o que seja o princípio da precaução. Elas apenas indicam situações em que a abordagem e lógica da precaução deve ser adotada. Essas situações podem ser mais ou menos restritivas, o que tem levado alguns autores a diferenciar graus de aplicação desse princípio de acordo com essas formulações históricas. Nesse sentido, Garnett e Parsons (2017), por exemplo, ao analisarem a jurisprudência europeia sobre o tema, observaram "ambiguidades inerentes" à determinação do nível de incerteza e o tipo de dano que justifiquem a invocação do princípio. Para esses autores, a Declaração Rio 92 representaria uma aplicação fraca do princípio da precaução, enquanto o Comunicado da CE e a Declaração de Wingspread teriam, respectivamente, uma aplicação moderada e forte.

---

[5] "When an activity raises threats of harm to human health or the environment, precautionary measures should be taken even if some cause and effect relationships are not established scientifically. In this context the proponent of the activity, rather than the public, should bear the burden of proof."

[6] "Recourse to the precautionary principle presupposes that potentially dangerous effects deriving from a phenomenon, product or process have been identified, and that scientific evaluation does not allow the risk to be determined with sufficient certainty. In some cases, the right answer may be not to act or at least not to introduce a binding legal measure. A wide range of initiatives is available in the case of action, going from a legally binding measure to a research project or a recommendation."

Grau de força da aplicação do Princício da precaução	**Fraca**: incerteza não justifica inação	**Moderada**: incerteza na avaliação do risco justifica ação	**Forte**: quando houver ameaça de dano, medidas de precaução devem ser tomadas; diante da incerteza, inverte-se o ônus da prova
Gravidade dos danos potenciais que demandariam ações de precaução	A **Declaração do Rio de 92** sugere que medidas podem ser tomadas para evitar "*danos sérios e irreversíveis*"	A **Comunicação da Comissão Europeia** sugere o uso de regulação proporcional ao nível de risco dos "*efeitos perigosos potenciais*", com avaliação científica objetiva preliminar	A **Declaração de Wingspread** determina que a responsabilidade de provar que uma atividade é segura recai sobre o proponente dessa atividade, mesmo que a relação causa e efeito não possa ser cientificamente determinada para evitar "*a ameaça de dano*"
Grau de incerteza ou qualidade das evidências que demandariam ações de precaução	É **permitida regulação na ausência de certeza científica**; medidas de precaução podem ser invocadas diante da incerteza	Pesquisas serão necessárias para reduzir incertezas; até lá, a a**ções de precaução incluem o estabelecimento de padrões regulatórios** com grandes margens de segurança	A **incerteza demanda a proibição da atividade potencialmente arriscada** até que o seu proponente demonstre que ela não oferece risco ou oferece risco aceitável
Natureza das ações de precaução	Pressuposto de **gerenciamento de risco**	Pressuposto de gerenciamento de risco implícito; **medidas sujeitas a revisão quando novas informações ou evidências científicas surgirem**	Pressuposto de se **evitar o risco**
Indicação dos atores envolvidos na avaliação dos riscos ou na definição das medidas a serem adotadas	A melhor maneira de tratar as questões ambientais é **assegurar a participação de todos os cidadãos interessados**; cada indivíduo terá **acesso adequado às informações** relativas ao meio ambiente, **inclusive informações acerca de materiais e atividades perigosas em suas comunidades**, bem como a oportunidade de participar dos processos decisórios	Julgar quais níveis de risco são "aceitáveis" é tarefa eminentemente *política*; os **processos de tomada de decisão devem ser transparentes e envolver o máximo de atores possíveis**	Corporações, entidades governamentais, organizações, comunidades, cientistas e outros indivíduos devem adotar uma abordagem de precaução para todos os empreendimentos humanos; o processo de **aplicação do princípio da precaução deve ser aberto, informado e democrático** e deve **incluir as partes potencialmente afetadas**

Tabela 1: Quadro comparativo das definições e aplicações do Princípio da Precaução
Fonte: Elaborada pelos autores com base em Garnett & Parsons D. J. (2017)

Entretanto, alguns pontos parecem comuns às formulações apresentadas. Primeiramente, não se trata de um recurso a ser invocado de maneira indiscriminada, havendo exigências de potencial dano.

Outro ponto importante é que, ao não definir expressões como "dano", "irreversível", "risco", "sério", as formulações parecem deixar a tarefa de fazê-lo às experiências participativas e deliberativas que procuram promover (Tabela 1). Essas expressões parecem conter uma presunção normativa em favor de certos valores ou qualidades que, em um regime democrático, caberia à toda a sociedade definir. Ademais, os valores a serem protegidos com a aplicação do princípio, como saúde, meio-ambiente e privacidade, quando confrontados com outros valores, demandam algum tipo de *trade-off* (Persson, 2016). Nesse sentido, o princípio da precaução reconheceria as assimetrias de poder e de informação dos processos de avaliação regulatória e ajudaria a remodelar os diferentes conhecimentos dos diversos atores envolvidos e afetados por esses processos (Stirling, 2016, p. 649). Trata-se, assim, de assumir compromissos com a deliberação e a *accountability*, assegurando justificações explícitas e cuidadosas sobre as escolhas regulatórias feitas diante de um "conhecimento incompleto" - algo que, inclusive, fomentaria e criaria obrigações para com a pesquisa e o conhecimento científico, com vistas a obtenção de informações sobre os riscos desconhecidos (Hartmann, 2012).

Compreender o princípio da precaução como um tipo de racionalidade a ser empregada durante a escolha das medidas regulatórias endereça as principais críticas feitas à sua aplicação. A primeira delas aponta a indeterminação de alguns dos conceitos utilizados nas formulações (*ill-defined*) (Majone, 2012; Sunstein, 2005). Essa crítica pressupõe tratar-se de uma regra procedimental e autossuficiente, o que o distanciaria da própria ideia de princípio. O Comunicado da CE endereça esse questionamento ao indicar o princípio da precaução como um *framework* para se pensar medidas regulatórias, dentre as quais contratos, sanções, acordos legalmente definidos, financiamento a projetos de pesquisa e recomendações. É justamente essa tarefa de determinação que abre espaços para a discussão de valores a serem protegidos ou preteridos, convidando diferentes stakeholders a discutir padrões de segurança. Schomberg (2012) aponta essa abertura de padrões de atuação como uma característica positiva de regimes regulatórios em sociedades democráticas.

A segunda crítica caracteriza o princípio como "irracional" e "não científico" (Sunstein, 2005; Resnik, 2003) por seu suposto caráter normativo. Esses autores parecem atribuir uma confiança demasiada à crença do conhecimento *científico neutro*, presumindo que procedimentos regulatórios convencionais cientificamente orientados (e menos aberto à

participação de diversos stakeholders, vale dizer) seriam capaz de transpor essa normatividade e indeterminação. Apenas os "experts" teriam competência para, "ao menos tentar", estimar e valorar os custos em uma análise de custo-benefício, enquanto "cidadãos comuns" imprimiriam seus medos irracionais às decisões regulatórias (Sunstein, 2005, p. 86). Além disso, essa crítica ignora que os métodos tradicionais de avaliação e gestão de riscos também demandam julgamentos avaliativos. Nesse sentido, o princípio da precaução seria tão "intrinsicamente imune" a manipulações como qualquer outro método (Stirling, 2016).

Finalmente, a terceira crítica à aplicação do princípio seria sua rejeição a novas tecnologias por seu caráter "paralisante", priorizando medidas que ponham fim ou dificultem o desenvolvimento tecnológico com determinações de "não-fazer" (Sunstein, 2005). Como já apontamos, a decisão por não tomar qualquer medida é apenas uma das possibilidades dentro do *framework* da precaução. O princípio tem por foco as razões para se tomar determinadas decisões regulatórias, e não as decisões em si (Stirling, 2016), bem como verificar qual é o nível de engajamento e participação pública nesses processos de tomada de decisão.

III. Leis de proteção de dados pessoais: o portal de entrada para a aplicação do Princípio da Precaução em Decisões Automatizadas e regulação de IA?

Uma vez realizada a radiografia do princípio da precaução, pretende-se verificar qual é o seu nível de aproximação frente aos objetivos regulatórios e o formato atual das leis de proteção de dados pessoais/LDPD. O princípio da *accountability* e os relatórios de impacto à proteção de dados pessoais, elementos centrais das LPDPs, revelam-se como possíveis feixes de entrada para a aplicação do princípio da precaução à IA, ainda mais quando se tem em vista que boa parte do emprego dessa tecnologia envolverá o processamento de dados pessoais.

III. A. Regulação da proteção de dados enquanto regulação de risco e o princípio da *accountability:* primeiro possível feixe de entrada do princípio da precaução[7]

Houve e está havendo uma virada "Copernicana" (Kuner, 2012) no campo da proteção de dados, representada por um "ponto de virada" em sua "moldura teórica". Se antes o sistema girava todo em torno da perspectiva da autodeterminação informacional, a sua rotação se dá

[7] Parte dos achados dessa subsecção derivam de outro trabalho: BIONI, Bruno Ricardo. Abrindo a caixa de ferramentas da LGPD para dar vida ao conceito de privacy by design (no prelo). In Direito & Internet IV: Lei Geral de Proteção de Dados Pessoais (Organizadores Newton de Lucca et al.,) Quartier Latin, 2019.

cada vez mais ao redor de processos de gerenciamento dos riscos das atividades de tratamento de dados.[8]

Como bem alerta Rafael Zanatta (2018), não se trata de "um processo de colisão jurídica ou de substituição normativa", mas de uma nova tipologia a respeito da emergência de mecanismos mais centrados na identificação e mitigação das incertezas e das probabilidades dos malefícios decorrentes da manipulação das informações pessoais dos indivíduos. Nadezhda Purtova, professora de Tilburg, resume bem: há uma guinada de "*informational self-determination*" na direção de "*information-induced-harms"* (Purtova, 2018). Em poucas palavras, o *saldo normativo* das novas leis de proteção de dados pessoais é resultado cada vez mais de uma *arquitetura precaucionária* de danos.

O fio condutor de todo esse processo é o acirramento da assimetria de informação[9], o qual, apesar de ser um elemento histórico da própria formação de leis de proteção de dados[10], atingiu um patamar ainda mais elevado diante dos avanços da tecnologia e pela consolidação de uma economia movida e orientada por dados. A nova onda de tecnologias de informação e comunicação (TICs) tornou ainda mais exponencial os possíveis efeitos adversos de uma atividade de tratamento de dados pessoais. Juntas, Internet das Coisas, *Big Data* e Inteligência Artificial permitem a coleta massiva de informações pessoais e, principalmente, inferências mais intrusivas a respeito dos cidadãos (Spina, 2014). Com isso, torna-se mais complexo o processo de cognição, avaliação e gerenciamento dos riscos de uma economia de dados. Os agentes de tratamento de dados – controladores e operadores – passaram a deter uma superioridade informacional ainda maior frente aos demais atores – cidadãos e órgãos fiscalizadores – desse ecossistema.

Esse é o pano de fundo que está por trás de uma estratégia que desloca mais "competências decisórias" (Quelle, 2017, p. 96) para quem está com a "mão na massa" dos

---

[8] Veja o debates e os desafios teóricas dessa "risquificação" do campo de proteção de dados pessoais por: QUELLE, Claudia. *The 'Risk Revolution' in EU Data Protection Law: We Can't Have Our Cake and Eat It, Too*. Rochester, NY: Social Science Research Network, 2017.

[9] Com maior ou menor intensidade o debate regulatório de proteção de dados pessoais sempre envolveu o gerenciamento de risco, mas o que nos parece mais sintomático é a complexificação no processo de reunião de informação para tomadas de ações ou inações para a modificação de comportamentos, o que impacta o próprio conceito e empreitada de regulatória desse campo. Veja, nesse sentido: GELLERT, Raphaël, We Have Always Managed Risks in Data Protection Law. *European Data Protection Law Review*, v. 2, n. 4, pp. 481–492, 2016.

[10] Veja, por exemplo, a própria decisão da Corte Constitucional Alemã que, ao cunhar o termo autodeterminação informacional, traz ínsita a ideia de reduzir a assimetria de informação perante o cidadão para que o cidadão tenha controle sobre seus dados. SCHWABE, Jürgen; MARTINS, Leonardo; WOISCHNIK, Jan. *Cinqüenta anos de jurisprudência do Tribunal Constitucional Federal Alemão.* Montevideo: Fundación Konrad-Adenauer, 2005. p. 233.

dados. A introjeção ou o reforço[11] de ferramentas como relatórios de impacto à proteção de dados indicam o tamanho da fé que está sendo depositada em tais agentes da cadeia de tratamento de dados. A partir dessa e outras ferramentas (Bennett e Raab, 2006), espera-se que a empreitada regulatória seja cada vez mais colaborativa com quem está no "chão da fábrica" e, sobretudo, que contas sejam prestadas - princípio da *accountability* - acerca das ações tomadas para avaliar e gerir os riscos em jogo.

Nesse cenário, o princípio da *accountability* apresenta-se como um vetor determinante para a *abertura* dos processos de tomadas de decisão acerca do que será considerado como um *risco tolerável* nas atividades de tratamento de dados. Isto porque a participação e o engajamento público em tais circuitos decisórios serão diretamente proporcionais ao quão elástico será o conteúdo de tal obrigação de prestação de contas por parte dos agentes econômicos. Com isso, permite-se, ao mesmo tempo, que a discussão seja porosa à valores eventualmente preteridos, uma vez experimentada a participação de atores com um outro olhar e motivados por interesses até mesmo antagônicos por parte de quem tem o dever de reportar.

Esse é o ponto de chegada proposto pelo jurista italiano Alessandro Mantelero, ao defender um arranjo institucional multissetorial em tais processos de tomadas de decisão (Mantelero, 2016). Tal olhar plural seria o gatilho inclusive para considerações de ordem ética, social e de direitos humanos, muitas vezes negligenciados por análises tecnocráticas, com o objetivo de conter riscos sistêmicos e de ordem coletiva (Mantelero, 2018).

Na medida em que boa parte dos processos de decisões automatizadas com o emprego de IA envolverá o processamento de dados pessoais, leis gerais de proteção de dados, talhadas com base em uma mentalidade de regulação de risco e no princípio da *accountability*, são vetores de democratização do próprio processo de regulação de tal tecnologia. Tais leis apresentam-se como um feixe de entrada para a aplicação do princípio da precaução, em sua conotação de deliberação pública, acerca da adoção ou não de IA em vista da definição do tipo de riscos que lhes são subjacentes.

III.B. Relatórios de Impacto: o grau de força de aplicação do princípio da precaução

Os relatórios de impacto à proteção de dados pessoais (RIPDP) têm ganhado um protagonismo cada vez maior nas leis de proteção de dados pessoais (Wright e De Hert, 2012). Em linhas gerais, tais relatórios seriam a documentação pela qual o controlador - quem tem

[11] Com exceção de *privacy by design*, todo os outros mecanismos já estavam positivados leis de proteção de dados ainda que com um grau mais normativo apagado. Por isso, fala-se em reforço e não apenas introjeção.

poder de tomada decisão na cadeia de tratamento de dados – registraria seus processos de tratamento de dados e as respectivas medidas adotadas para mitigar riscos gerados aos direitos dos titulares dos dados.

No cenário europeu, o controlador é obrigado a executar um RIPDP sempre que houver um *alto risco em jogo*. Há uma lista exemplificativa das hipóteses em que o tratamento de dados seria de alto risco, destacando-se a situação de perfilhamento[12] como ponto de apoio para tomada de decisões. Através dessa definição, o emprego de IA para automatização de processos de concessão à crédito, precificação de planos e seguro de saúde, seleção e ou recrutamento de candidatos, elegibilidade à programas de assistências social, dentre uma outra série de situações do nosso cotidiano, deveriam ser antecedidos pela elaboração de um RIPDP. Além disso, quando o controlador não encontrar meios para mitigar os prováveis malefícios da sua respectiva atividade, deve, nesse caso, aguardar "luz verde" do regulador para seguir em frente.

No cenário brasileiro, a lei geral de proteção de dados pessoais não procedimentalizou minimamente o RIPDP. Muito embora haja algumas menções a tal instrumento, não há um capítulo próprio para tratar da matéria. Dessa forma, o RIPDP estaria condicionada à regulação posterior por parte de órgãos reguladores que precisariam quando seria obrigatório, bem como quais elementos e o tipo de análise que se espera encontrar em tal documentação.

No cenário americano, há, igualmente, um projeto de lei,[13] de autoria dos Senadores Cory Booker e Ron Wyden, que obriga a elaboração de relatórios de impacto à proteção de dados, bem como de um relatório de impacto mais genérico, nas hipóteses em que não há o tratamento de dados pessoais, toda vez que houver o emprego de IA para automatização de processos de tomadas decisão. Intitulado como *Algorithmic Accountability*, diferentemente da racionalidade regulatória europeia, não há a previsão da necessidade de iniciar uma conversa com o regulador quando se deparar com uma situação de alto risco e na qual não se encontrou medidas para controlá-lo.

Do norte ao sul global e dos dois lados do atlântico, nota-se a emergência de uma racionalidade regulatória bastante próxima ao conteúdo normativo do princípio da precaução. Cabe ao proponente da atividade demonstrar a segurança da sua atividade, especialmente as

---

[12] De acordo com a definição adotada no RGPD: "'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;"

[13] Disponível em: <https://www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202019%20Bill%20Text.pdf>

medidas adotadas para gerenciar os seus respectivos riscos. Diferem, no entanto, com relação ao grau de força do princípio da precaução:

Grau de força da aplicação do Princípio da precaução	**Fraca**: incerteza não justifica inação	**Moderada**: incerteza na avaliação do risco justifica ação	**Forte**: quando houver ameaça de dano, medidas de precaução devem ser tomadas; diante da incerteza, inverte-se o ônus da prova
RGPD (EU)	**Forte**: ao se deparar com uma situação de alto risco que não pode ser mitigado por meio de medidas adequadas em acordo com a tecnologia disponível e os custos de implementação,o controlador não deve seguir em frente com o tratamento de dados e, ainda, deve consultar antes a autoridade de proteção de dados (*prior notification*).		
Accountability Algorithm (USA)	**Moderado:** apesar de obrigar a elaboração de RIPDP em situações de alto risco, é silente quanto a eventual paralisação de uma atividade quando houver ameaça de dano e medidas de prevenção. Dessa forma, a incerteza quanto aos malefícios de uma atividade pode justificar ação, sendo uma discricionariedade do próprio proponente da atividade		
LGPD (BR)	**Fraca:** ao não procedimentalizar minimamente em que situações os RIPDP são obrigatórios, muito menos quais devem ser os elementos a compor tal documentação, a incerteza quanto aos malefícios de uma atividade não justifica inação. No entanto, regulação posterior, por parte dos órgãos reguladores (e.g., ANPD), podem alterar o *status* de força de aplicação do princípio da precaução em questão.		

Tabela 2: Quadro comparativo da aplicação do princípio da precaução quanto ao desdobramento e exigências de relatórios de impacto à proteção de dados pessoais
Fonte: elaboração pelo(a)s autore(a)s

Em conclusão, um outro possível vetor de entrada para a aplicação do princípio da precaução na regulação IA são os RIPDPs previstos em leis de proteção de dados pessoais. No entanto, varia o grau de força com que ele é cristalizado a partir de tal ferramenta, especialmente se a avaliação do risco resultará em ação ou inação por proponente da tecnologia em lançá-la ao meio ambiente.

III. C. Direito à revisão de decisões automatizadas: princípio da precaução como racionalidade para o direito à explicação

O direito à explicação decorre do princípio da transparência[14], previsto na maioria das leis de proteção de dados do mundo (Monteiro, 2018). A RGPD, por exemplo, prevê o direito à informação *qualificada* (*meaningful*) sobre a lógica dos processos de decisões automatizadas

[14] LGPD, art. 6º, "VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;". RGPD, art. 5. "Personal data shall be: 1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')".

(Selbst e Powles, 2017). Já a LGPD, em seu art. 20, garante o direito de revisão de decisões tomadas unicamente por tratamento automatizado. A lógica do direito à explicação e do direito à revisão de decisões automatizadas que impacta o titular dos dados, contudo, já havia sido inaugurada, no Brasil, no artigo 5º da Lei de Cadastro Positivo (Lei 12.414/2011).[15] Ao não dispor de uma proibição geral à perfilização, o dispositivo parece objetivar a garantia do direito à não discriminação[16] e fornecer instrumento para a identificação de potenciais violações de direitos (Zanatta, 2019).[17]

A explicação surge, assim, como uma ferramenta à *accountability* de IA ao expor a lógica da decisão, devendo permitir ao observador determinar a extensão em que um *input* particular foi determinante ou influenciou um resultado (Doshi-Velez e Kortz, 2017). Entretanto, os segredos comercial e industrial constituem objeções à transparência.

A abordagem da precaução parece ser útil na definição dos contornos desse debate. De um lado, ela colabora na construção de espaços de deliberação para se discutir o que seria "informação qualificada" ou como mitigar os problemas em decisões futuras. De outro, ela possibilita endereçar questionamentos a respeito dos segredos comercial e industrial. Ao exigir informações sobre a racionalidade de uma decisão específica, o direito à explicação não se confunde com a transparência pura e simples. Variações nos dados de raça, por exemplo, já poderiam fornecer o impacto e a maneira como esse tipo de dado impacta uma decisão, sem, contudo, demandar a revelação de todo o sistema automatizado envolvido naquela decisão (Doshi-Velez e Kortz, 2017). Ademais, espaços deliberativos com a participação de diversos atores podem ajudar a mitigar os custos envolvidos em sistemas de explicação - que, de outra forma, poderia afetar desproporcionalmente empresas menores - bem como os desafios tecnológicos de se pensar esse tipo de sistema.

---

[15] Art. 5º São direitos do cadastrado: IV - conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial; V - ser informado previamente sobre o armazenamento, a identidade do gestor do banco de dados, o objetivo do tratamento dos dados pessoais e os destinatários dos dados em caso de compartilhamento; VI - solicitar ao consulente a revisão de decisão realizada exclusivamente por meios automatizados.

[16] Art. 8º São obrigações das fontes: VI - fornecer informações sobre o cadastrado, em bases não discriminatórias, a todos os gestores de bancos de dados que as solicitarem, no mesmo formato e contendo as mesmas informações fornecidas a outros bancos de dados.

[17] Lógica semelhante à do Código de Defesa do Consumidor (Lei No. 8.078/90), que prevê a transparência e a boa-fé como princípios norteadores (artigos 4º, 6º e 43).

III. D. Tecnologias de reconhecimento: um caso de fronteira à aplicação do princípio da precaução

Reconhecimento facial parece ser o estopim de uma demanda regulatória represada em torno de inteligência artificial[18] de uma maneira geral (AI Now, 2016).[19] Evidências sobre os altos índices de falso positivos[20] e, principalmente, revelações em torno do reforço de práticas discriminatórias (Garvie, 2016) a partir do seu emprego para fins de policiamento preditivo, fizeram com que vários atores do campo de políticas públicas se movimentassem recentemente.

No setor privado, ao clamar por uma regulação estatal, o presidente da Microsoft, Brand Smith, mostrou ceticismo caso se apostasse em uma autorregulação do setor que forçaria as empresas a escolherem entre responsabilidade social e sucesso no mercado.[21] Por parte do terceiro setor, a American Civil Liberties Union (ACLU) ganhou adesão dos próprios funcionários da *Amazon* ao peticionar que a empresa suspendesse a venda de tecnologias de reconhecimento facial para autoridades de repressão penal.

As incertezas quanto aos benefícios e os riscos pelo emprego de tecnologias de reconhecimento facial formaram uma arena regulatória efervescente, a qual está formatada em três eixos. O que lhes permite comparar é justamente carga de atribuição de obrigações precaucionárias diante das incertezas quantos aos benefícios e riscos em jogo decorrentes do emprego de tecnologias de reconhecimento facial:

a) de um lado, ainda há parte do setor privado que acredita na suficiência de diretrizes éticas e autorregulação enquanto uma estratégia regulatória que não colocaria entraves ao desenvolvimento da tecnologia em questão;

b) no outro extremo, há vozes que clamam pelo banimento da tecnologia por vislumbrar no seu *design* riscos exacerbados para fins de opressão (Hartzog, 2019);

c) ao centro desse movimento pendular, encontra-se uma estratégia que visa desenhar uma arquitetura precaucionária de danos, de modo que o emprego de

---

[18] É a partir do emprego de algoritmos supervisionados ou de autoaprendizados que se torna possível treinar uma máquina (machine-learning) a reconhecer padrões em imagens e, com isso, identificar não só os donos de seus rostos, mas, até mesmo, o seu respectivo estado emocional. Essa última técnica ficou conhecida como *affect recognition*.

[19] Veja, a título de ilustração, as primeiras discussões do AI Now 2017: https://ainowinstitute.org/AI_Now_2016_Report.pdf

[20] Em maio de 2018, a BBC divulgou estudo do grupo Big Brother Watch, que, baseado em pedidos de informação encaminhados a todas as forças de segurança do Reino Unido, identificou números desproporcionalmente elevados de falsos positivos em Londres e no País de Gales. Matéria disponível em: https://www.bbc.com/news/technology-44089161

[21] O posicionamento completo pode ser acessado em: https://blogs.microsoft.com/on-the-issues/2018/12/06/facial-recognition-its-time-for-action/

> tecnologias de reconhecimento facial deveria ser antecedido de ações por parte do seu próprio proponente que mitigassem seus eventuais malefícios. A produção de possíveis evidências científicas (AI Now, 2018) acerca da segurança de tais tecnologias (Calo, 2017), sobretudo de ordem dos próprios agentes econômicos poderia desencadear um sistema de corregulação que evitaria a *ossificação* de uma regulação baseada em comando e controle somente por parte do Estado (WRIGHT, 2019).

Como será detalhado na tabela a seguir, diante da experiência estrangeira e do que foi mapeado em termos de modelos regulatórios de tecnologias de reconhecimento facial, a lei geral brasileira de proteção de dados/LGPD apresenta um *modelo fraco* e janelas muito incipientes para a estruturação de um modelo de governança:

a) há baixa atribuição de deveres para os desenvolvedores de tais tecnologias, bem como por parte de quem será seu consumidor final e dele fará uso seja o setor público ou privado; **a.1)** ao não procedimentalizar minimamente em que situações os RIPDP são obrigatórios, muito menos quais devem ser os elementos a compor tal documentação, a LGPD abre espaço para a adoção de tais tecnologias sem que haja correspondentes ações para mitigar seus possíveis malefícios; **a.2)** em especial não há a previsão do controlador iniciar conversas regulatórias quando se deparar em uma situação de um risco não controlável, hipótese na qual notificaria os órgãos reguladores antes de lançar uso da tecnologia a exemplo do que se encontra no RGPD;

b) não há um processo de tomada de decisão que extrapole as figuras do controlador e do órgão regulador, diferentemente de outras propostas aonde se busca um debate público informado com a inclusão de representantes dos interesses dos cidadãos nos circuitos decisórios (e.g., *Code - Acquisition of Surveillance Technology, San Francisco, EUA*);

c) ainda assim, futura regulamentação *a posteriori* da Autoridade Nacional de Proteção de Dados Pessoais/ANPD concernente a relatórios de impacto à proteção de dados pessoais, bem como na validação de códigos de boa conduta ou mesmo de entidades certificadoras podem formatar uma regulação mais catalisadora dos benefícios em contraposição aos riscos do emprego da IA para fins de reconhecimento facial no âmbito do setor privado. Há, portanto, espaço para uma

regulação experimental que é, no entanto, condicionada pela efetiva operação da ANPD e da definição do seu próprio perfil institucional ainda indefinido (Bioni, 2019);

d) no âmbito do setor público, o emprego de tecnologias de reconhecimento facial para fins de segurança pública, segurança nacional, defesa do Estado e investigações de natureza penal estão parcialmente excepcionados do escopo de aplicação da LGPD. Ainda que sejam aplicáveis os princípios de proteção de dados pessoais e do devido processo legal, bem como a observação do interesse público, a nova redação dada ao artigo 4º, § 3º, retira da ANPD o poder emitir opiniões técnicas, recomendações e de solicitar RIPDPs (Bioni & Rielli, 2019);

<table>
<tr><th colspan="3">Princípio da precaução e estratégias regulatórias para tecnologias de reconhecimento facial

Legenda:
Baixo: o fato de haver incerteza quanto ao risco gerado pela atividade de tratamento de dados não pode justificar inércia por parte do controlador;
Moderado: incerteza na avaliação do risco justifica ação, mas há algum grau de discricionariedade;
Forte: quando houver ameaça de dano, medidas de precaução devem obrigatoriamente ser tomadas; diante da incerteza, inverte-se o ônus da prova, que passa a ser do controlador para o emprego da tecnologia em questão e com arranjos de deliberação pública.</th></tr>
<tr><th colspan="3">Estratégias de Regulação</th></tr>
<tr><th colspan="3">Regulação específica para dados biométricos-reconhecimento facial</th></tr>
<tr><th>Lei-norma</th><th>Descrição</th><th>Grau de força da aplicação do Princípio da Precaução</th></tr>
<tr><td>1. Biometric Information Privacy Act, Illinois[22], EUA</td><td>A Lei, que foi a primeira a regular a coleta e tratamento de dados biométricos nos Estados Unidos, requer que empresas que operem no estado de Illinois cumpram alguns requisitos:
1. informem o titular dos dados sobre a coleta e armazenamento do dado, bem como a finalidade do tratamento e o tempo de armazenamento;
2. obtenham consentimento expresso e escrito para tal;
Os mesmos requisitos se aplicam para a disseminação de dados biométricos.
Além disso, a Lei também proíbe que as empresas efetuem transações com dados biométricos de indivíduos e exige que as empresas elaborem e publicizem uma política com cronograma de retenção de dados e princípios para destruição de identificadores de biometria (cujo prazo máximo é de 3 anos, contando da última interação entre empresa e indivíduo).
Por fim, a Lei exige que as empresas armazenem e protejam os dados biométricos, mantendo um padrão que seja no mínimo o mesmo adotado pela empresa para outras informações sensíveis e que seja razoável dentro da indústria em que se encontra.</td><td>Baixo grau de força do princípio da precaução quanto à adoção de produção de evidências para controlar os eventuais malefícios. Ênfase na procedimentalização de deveres de informação, publicização e de bases legais para o tratamento de dados pessoais (e.g., consentimento) e, por fim, quanto ao período de armazenamento.
O processo de tomada de decisão quanto ao emprego da tecnologia concentra-se nas mãos do próprio proponente.</td></tr>
</table>

[22] A lei pode ser consultada na íntegra, em inglês, no seguinte link: http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57

2. HB 1493, Washington[23], EUA	A Lei, aprovada em 2018, aplica-se a utilização de dados biométricos para fins comerciais, excluindo expressamente seu uso com finalidade de segurança. Veda a inclusão de dados biométricos em bases de dados para fins comerciais caso não haja uma de três opções: (i) um aviso, que é definido como ‘’uma notificação dada por meio de um procedimento desenhado para estar prontamente disponível para indivíduos afetados’’; (ii) consentimento expresso (que deve ser renovado a cada novo uso comercial) ou (iii) provisão de um mecanismo para prevenir o uso posterior de identificadores biométricos para fins comerciais. A não ser que tenha sido obtido o consentimento expresso, a lei veda a venda, arrendamento ou outro uso comercial, a não ser que o objetivo seja o cumprimento de obrigações legais, o perfazimento de transações comerciais ou financeiras autorizadas pelo titular ou a transferência a um terceiro contratualmente obrigado a não repassar novamente os dados ou dar a eles finalidade inconsistente com a Lei. Aquele que detém dados biométricos utilizados para fins comerciais deve manter cuidados razoáveis contra acessos não autorizados e armazenar os referidos dados por não mais do que o razoavelmente necessário para cumprir obrigações legais, proteger os dados de possíveis fraudes e outros ilícitos ou preencher o objetivo para o qual os dados foram coletados.	**Baixo grau de força do princípio da precaução** quanto à adoção de produção de evidências para controlar os eventuais malefícios. Ênfase na procedimentalização de deveres de informação, publicização e de bases legais para o tratamento de dados pessoais (e.g., consentimento) e sem que haja um controle social em torno da decisão do emprego da tecnologia e, por fim, quanto ao período de armazenamento. O processo de tomada de decisão quanto ao emprego da tecnologia concentra-se nas mãos do próprio proponente.
3. Texas Business and Commerce Code - BUS & COM § 503.001. Capture or Use of Biometric Identifier, Texas[24], EUA	A Lei exige a informação prévia sobre a coleta de dados biométricos para fins comerciais, seguida do consentimento do indivíduo. A venda, arrendamento ou divulgação de dados biométricos que foram capturados para fins comerciais é vedada, exceto nas hipóteses de autorização por lei federal, cumprimento de obrigações legais, perfazimento de transações financeiras autorizadas pelo titular ou autorização pelo titular de divulgação para fins de investigação em caso de desaparecimento ou morte. Os controladores dos dados biométricos devem armazená-los e protegê-los, mantendo um padrão que seja no mínimo o mesmo adotado pela empresa para outras informações sensíveis e que seja razoável dentro da indústria em que se encontra. Por fim, devem destruir estes dados dentro de um tempo razoável, que, em regra, não pode passar de 1 ano da data em que a finalidade para a coleta original expirar.	**Baixo grau de força do princípio da precaução** quanto à adoção de produção de evidências para controlar os eventuais malefícios. Ênfase na procedimentalização de deveres de informação, publicização e de bases legais para o tratamento de dados pessoais (e.g., consentimento) e, por fim, quanto ao período de armazenamento. O processo de tomada de decisão quanto ao emprego da tecnologia concentra-se nas mãos do próprio proponente.
Regulação específica para reconhecimento facial		
Lei-norma	**Descrição**	**Grau de força da aplicação do Princípio da Precaução**
4. Ordinance amending the Administrative	O projeto, de autoria do conselheiro Aaron Peskin, condiciona o uso de tecnologia de vigilância à aprovação, pelo Conselho de Supervisores da cidade, de uma Política de Tecnologia para	**Alto grau de força do princípio da precaução:** a proposta em tramitação na cidade de São Francisco parte do

[23] A lei pode ser consultada na íntegra, em inglês, no seguinte link: http://lawfilesext.leg.wa.gov/biennium/2017-18/Pdf/Bills/House%20Passed%20Legislature/1493-S.PL.pdf

[24] A lei pode ser consultada na íntegra, em inglês, no seguinte link: https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm

Code - Acquisition of Surveillance Technology, San Francisco, EUA[25]	Vigilância. Além da política, a proposta também determina que o solicitante de aprovação para emprego destas tecnologias publique, no site do órgão e com ao menos 30 dias de antecedência em relação à reunião em que o pedido será avaliado, um Relatório de Impacto à Vigilância. O critério para aprovação de um pedido é a avaliação de que os impactos positivos da implantação da tecnologia de vigilância superam os efeitos negativos. Em caso de aprovação, os órgãos ficam obrigados a submeter relatórios anuais de vigilância.	pressuposto de que os riscos apresentados por tecnologias de vigilância, que incluem reconhecimento facial, superam seus eventuais benefícios. Assim, em regra, veda sua aplicação, relegando ao proponente do emprego da tecnologia demonstrar que, no caso concreto, sua proposta não se encaixa nesta regra. Antes de administração pública empregar tal tecnologia, é necessário a execução de RIV que deve ser revisar pelo procurador do município e, em seguida, ser enviado ao Conselho Supervisor para sua aprovação. Tal relatório deve identificar os riscos para direitos liberdades fundamentais do cidadãos e os benefícios para a sociedade
5. Bill S.1385, Massachusetts, EUA[26]	O projeto, de autoria da Senadora estadual Cynthia Creem, pretende condicionar a ‘’aquisição, posse, acesso ou uso’’ de qualquer sistema de vigilância com biometria ou qualquer informação obtida por meio do uso desse tipo de tecnologia a uma autorização estatutária. A autorização, conforme o projeto, deve conter, dentre outras informações: **1.** quais entidades podem usar os sistemas de vigilância com biometria, as finalidades para estes usos e usos proibidos; **2.** padrões para o uso e manejo de informação obtida por estes meios, inclusive quanto à retenção de dados, compartilhamento, acesso e trilhas de auditoria; **3.** proteções rigorosas ao devido processo legal, à privacidade, liberdade de expressão e associação e equidade racial, religiosa e de gênero; **4.** mecanismos para garantia de *compliance*.	**Moderado grau de força do princípio da precaução:** ao reconhecer os riscos em jogo com o emprego de tecnologias de reconhecimento facial, proíbe-se a sdua adoção até que seja estabelecidos padrões de segurança e regras de auditoria sobre tais sistemas.
6. Bill H.287, Massachusetts, EUA[27]	Essa proposta, do Senador Ronald Mariano, inclui dados biométricos nas categorias protegidas da lei estadual de segurança de dados. Dessa forma, entidades que tratam esse tipo de dado deverão revelar aos titulares caso as informações sejam hackeadas, perdidas ou roubadas.	**Baixo grau de força do princípio da precaução** quanto à adoção de produção de evidências para controlar os eventuais malefícios. Ênfase na procedimentalização do dever de informação.
7. Commercial Facial Recognition Privacy Act of 2019, EUA[28]	O projeto de lei, introduzido pelos Senadores Brian Schatz e Roy Blunt, pretende regular os usos comerciais de tecnologias de reconhecimento facial. O projeto condiciona o uso de tecnologia de reconhecimento facial a: **1.** consentimento expresso do titular;	**Baixo grau de força do princípio da precaução** quanto à adoção de produção de evidências para controlar os eventuais malefícios. Ênfase na procedimentalização de deveres de informação, publicização

[25] O projeto pode ser consultado na íntegra, em inglês, no seguinte link: https://cdn.vox-cdn.com/uploads/chorus_asset/file/13723917/ORD__Acquisition_of_Surveillance_Technology.pdf

[26] O projeto pode ser consultado na íntegra, em inglês, no seguinte link: https://malegislature.gov/Bills/191/SD671

[27] O projeto pode ser consultado na íntegra, em inglês, no seguinte link: https://malegislature.gov/Bills/191/H287

[28] O projeto pode ser consultado na íntegra, em inglês, no seguinte link: https://pt.scribd.com/document/401931553/The-Commercial-Facial-Recognition-Privacy-Act

	2. quando possível, a apresentação de um aviso sobre o uso da tecnologia e onde encontrar mais informações e informações gerais e acessíveis sobre as características da tecnologia. O projeto também veda o uso dessa tecnologia com fins discriminatórios e com fins distintos àqueles apresentados ao titular. Por fim, proíbe o compartilhamento destes dados com terceiros, a não ser que haja consentimento específico para isso.	e de bases legais para o tratamento de dados pessoais (e.g., consentimento).

Tabela 3: Quadro comparativo do aplicação do princípio da precaução nas estratégias regulatórias para tecnologias de reconhecimento facial
Fonte: Bioni & Rielli (2019)

No campo da regulação de tecnologia de reconhecimento facial experimenta-se um grau de maturidade peculiar, havendo variações fraca, moderada e forte do princípio da precaução. O apetite dessa regulação setorial deságua não só no reforço de deveres de cuidado e segurança por quem pretende lançar mão da tecnologia em específico, mas, também e principalmente, na constituição de arranjos de deliberação pública a seu respeito (e.g., *Code - Acquisition of Surveillance Technology, San Francisco, EUA*)

IV. CONSIDERAÇÕES FINAIS

O princípio da precaução fornece um substrato importante para se pensar medidas e estratégias de regulação de IA, notadamente como lidar com situações de riscos de danos ou de desconhecimento dos potenciais malefícios e benefícios desse tipo de tecnologia. A automatização de processos de tomadas de decisão, a partir do emprego de IA, não deve se constituir como um argumento ingênuo em defesa de sua objetividade e neutralidade. Tais circuitos decisórios carregam escolhas das entidades e pessoas envolvidas na sua construção, sendo modulado pela agenda política e aspectos socioeconômico, de forma implícita ou explícita, que lhes são subjacentes (Data & Society, 2018).

Diante disso, o princípio da precaução apresenta dois vetores de regulação que merecem atenção: **a)** a abertura do debate regulatório a todos os atores envolvidos na implementação dessa tecnologia (e nas escolhas que ela impõe), de desenvolvedores àqueles que sofrerão seus possíveis efeitos, o que é um requisito obrigatório de um sistema democrático com históricas dinâmicas de assimetria de poder e informação; **b)** a atribuição de obrigações que reduzam as incertezas quantos aos benefícios e riscos em questão, de sorte a determinar a adoção ou não de IA.

Nesse sentido, leis gerais de proteção de dados pessoais, leis setoriais de dados biométricos e de reconhecimento facial apresentam um ferramental precaucionário a ser analisado. A sua calibração variará a escala em baixa, moderada e alta quanto ao nível de

prudência acerca do emprego de IA. Ao contrário de paralisia ou inação, a execução de relatórios de impacto à proteção de dados pessoais, de mecanismos de auditoria e conversas com os órgãos reguladores e outros atores afetados são ações que podem servir de força motriz consciente e responsável para o lançamento dessa tecnologia no meio ambiente (Abramovay, 2016).

V. REFERÊNCIAS BIBLIOGRÁFICAS

AI Now, AI Now Report 2018, dec.2018. Disponível em: https://ainowinstitute.org/AI_Now_2018_Report.pdf

AI Now, AI Now Report 2016, dec.2016. Disponível em: https://ainowinstitute.org/AI_Now_2016_Report.pdf

ABRAMOVAY, Ricardo. A A heurística do medo, muito além da precaução. In Revista de Estudos Avançados da Universidade de São Paulo. São Paulo: USP, p. 167-179.

ANANNY, Mike; CRAWFORD, Kate. Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability. New media & society, Vol. 20 (3), 2018, pp. 973-989.

BENNETT, Colin J.; RAAB, Charles D., The governance of privacy: policy instruments in global perspective, 2nd and updated ed. Cambridge, Mass: MIT Press, 2006.

BIONI, Bruno Ricardo. Agenda da privacidade de proteção de dados em 2019. Portal Jota, março de 2019. Disponível em: < https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/privacidade-e-protecao-de-dados-pessoais-em-2019-28012019>.

_____, Bruno Ricardo. Abrindo a caixa de ferramentas da LGPD para dar vida ao conceito de privacy by design (no prelo). In Direito & Internet IV: Lei Geral de Proteção de Dados Pessoais (Organizadores Newton de Lucca et al.,) Quartier Latin, 2019.

_____, Bruno; LEITE MONTEIRO, Renato; OLIVEIRA, Maria Cecília. GDPR Matchup: Brazil's General Data Protection LAW, IAPP, 2018.

_____, Bruno Ricardo. RIELLI, Mariana. Contribuição do Data Privacy Brasil a MPV 869/2018: tratamento de dados no âmbito do setor público. São Paulo: abril, 2019.

_____, Bruno Ricardo. RIELLI, Mariana. Contribuição do Data Privacy Brasil à audiência publica de tecnologias de reconhecimento facial (Organizador Ministério Público do Distrito Federal e Territórios/MPDFT). Brasília: abril, 2019

Calo, Ryan, Artificial Intelligence Policy: A Primer and Roadmap (August 8, 2017). Disponível em SSRN: https://ssrn.com/abstract=3015350 ou http://dx.doi.org/10.2139/ssrn.3015350

Comissão Europeia. Comunicação da Comissão relativa ao Princípio da Precaução, 2000. Conferência das Nações Unidas sobre o Meio Ambiente. Declaração do Rio sobre Meio Ambiente e Desenvolvimento, 1992.

Data & Society. Algorithmic Accountability: A Primer, 2018.

Declaração de Wingspread sobre o Princípio da Precaução. Eugene, OR: Science & Environmental Health, 1998.

DOSHI-VELEZ, Finale; KORTZ, Mason. Accountability of AI Under the Law: The Role of Explanation, 2017.

GARNETT, Kenisha; PARSONS, David J. Multi-Case Review of the Application of the Precautionary Principle in European Union Law and Case Law. Risk Analysis, Vol. 37, No. 3, 2017.

GARVIE, Clary et al . The Perpetual Line-up Unregulated Police Face Recognition in America: Georgetwon Univerisity, 2016.

GILLESPIE, Tarleton. “The relevance of algorithms”. In (Ed.), Media Technologies: Essays

on Communication, Materiality, and Society. Cambridge: The MIT Press, 2014.

HARTMANN, Ivar Alberto Martins. O princípio da precaução e sua aplicação no direito do consumidor: dever de informação. Direito & Justiça, v. 38, n. 2, jul./dez., 2012, pp. 156-182.

HARTZOG, Woodrow. SELINGER, Evan. Facial recognition is the perfect tool for oppression. Disponível em: https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66

HEAD, Brian W. Toward More "Evidence-Informed" Policy Making? Public Administration Review, Vol. 76, no. 3, 2015, pp. 472-484.

KUNER, Christopher. The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law. *Bloomberg BNA Privacy and Security Law Report*, v. 6, n. 11, p. 1–15, 2012.

MAJONE, Giandomenico. What Price Safety? The Precautionary Principle and its Policy Implications. Journal of Common Market Studies, 40. 2002, pp. 89-110.

MANTELERO, Alessandro, AI and Big Data: A blueprint for a human rights, social and ethical impact assessment, Computer Law & Security Review, v. 34, n. 4, p. 754–772, 2018
MANTELERO, Alessandro, Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection, Computer Law & Security Review, v. 32, n. 2, p. 238–255, 2016.

MONTEIRO, Renato Leite. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil? Artigo Estratégico 39, Instituto Igarapé, 2018.

PERSSON, Erik. What are the core ideas behind the Precautionary Principle? Science of the Total Environment, 557–558, 2016, pp. 134–141.

PURTOVA, Nadezhda. The law of everything. Broad concept of personal data and future of EU data protection law. *Law, Innovation and Technology*, v. 10, n. 1, pp. 40–81, 2018.

QUELLE, Claudia, Privacy, Proceduralism and Self-Regulation in Data Protection Law, Rochester, NY: Social Science Research Network, 2017. p. 96.

RESNIK, David B. Is the Precautionary Principle Unscientific? Studies in the History and Philosophy of Biological and Biomedical Sciences, 34(2), 2003, pp. 329-344.

SELBST, Andrew D.; POWLES, Julia. Meaningful information and the right to explanation. International Data privacy Law, 2017, Vol. 7, No. 4, pp. 233-242.

SCHOMBERG, René von. The Precautionary Principle: Its Use Within Hard and Soft Law. European Journal of Risk Regulation, No. 2, 2012, pp. 147-156.

Science for Environment Policy, The Precautionary Principle: decision making under uncertainty. Future Brief 18. Produced for the European Commission DG Environment by the Science Communication Unit, UWE, Bristol, 2017. Disponível em < http://ec.europa.eu/science-environment-policy >.

SPINA, Alessandro, Risk regulation of big data: has the time arrived for a paradigm shift in EU data protection, European Journal of Risk Regulation, v. 2, p. 248–252, 2014.

STIRLING, Andrew. Precaution in the Governance of Technology. Working Paper. SPRU - Science Policy Research Unit, Brighton, 2016.

SUNSTEIN, Cass R. Laws of Fear: beyond the Precautionary Principle. Cambridge: Cambridge University Press, 2005.

WRIGHT, David; DE HERT, Paul (Orgs.), Privacy Impact Assessment, Dordrecht: Springer Netherlands, 2012.

WRIGHT, Elias. The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector. In Fordham Intell. Prop. Media & Ent. L.J. 611 (2019). Disponível em: https://ir.lawnet.fordham.edu/iplj/vol29/iss2/6

ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação do risco: uma nova moldura teórica? *in*: *I Encontro da Rede de Pesquisa em Governança da Internet*. Rio de Janeiro: Rede de Pesquisa em Governança da Internet, 2018, pp. 175–193.

ZANATTA, Rafael A. F. Perfilização, Discriminação e Direitos: do Código de Defesa do Consumidor à Lei Geral de Proteção de Dados Pessoais, 2019.