
Data
Privacy
BR

DATA PRIVACY BRASIL

A Data Privacy Brasil tem como objetivo promover a produção de conhecimento, conscientização e educação sobre privacidade e proteção de dados pessoais. Seus profissionais estão diretamente envolvidos nas principais casos e discussões sobre leis de proteção de dados, nacionais e internacionais, com aplicação no Brasil, principalmente os que envolvem a Lei Geral de Proteção de Dados do Brasil. Essa característica permite uma abordagem pragmática e teórica baseada em situações reais e interpretações conforme a vontade do legislador e das autoridades responsáveis por supervisionar a aplicação das normas. Desta forma, é possível conferir o nível de conhecimento necessário para enfrentar os principais desafios de uma sociedade e economia cada vez mais movida por dados.

MINISTÉRIO PÚBLICO DO DISTRITO FEDERAL E TERRITÓRIOS
UNIDADE ESPECIAL DE PROTEÇÃO DE DADOS E INTELIGÊNCIA ARTIFICIAL - ESPEC

Ref. Inquérito Civil Público n. 08190.052289/18-94

Audiência Pública: uso de ferramentas de reconhecimento facial por parte de empresas e governos

Fundadores
Bruno Ricardo Bioni
Renato Leite Monteiro

Autore(a)s
Bruno Ricardo Bioni, Fundador-Professor
Mariana Rielli, Pesquisadora

Data Privacy Brasil

I - Apresentação e objetivos da intervenção

Diante do avanço das tecnologias de reconhecimento facial e a difusão do seu uso por parte dos setores privado e público, o Ministério Público do Distrito Federal e Territórios (MPDFT), por sua Comissão de Proteção dos Dados Pessoais. instaurou o Inquérito Civil Público nº 08190.052289/18-94, com o fim de '' investigar a criação e o uso de bancos de dados biométricos (Reconhecimento Facial) para fins comerciais, bem como o funcionamento dos algoritmos'' (Portaria nº 10, de 15 de agosto de 2018).

No âmbito deste ICP, em 12 de março de 2019, foi convocada Audiência Pública ''para debater o uso das ferramentas de reconhecimento facial'', para qual foram convidados membros de entidades da sociedade civil, da academia, do setor empresarial e de instituições públicas.

O objetivo da intervenção é, em linhas gerais, apresentar o estado da arte da discussão sobre o tema, do ponto de vista teórico e jurídico, bem como pincelar as tendências regulatórias que podem ser extraídas dos debates internacionais e de algumas propostas de regulação em andamento em diferentes localidades e esferas. Com isso, pretende-se apontar quais são os riscos e benefícios do emprego das tecnologias de reconhecimento facial, cuja equação tem tonificado não só o debate necessidade de regulação, mas, também e principalmente, qual o seria o seu perfil necessário.

II - Introdução - delimitação do objeto do debate regulatório

Reconhecimento facial parece ser o estopim de uma demanda regulatória represada em torno de inteligência artificial[1] de uma maneira geral.[2] Evidências sobre os altos índices de falso positivos[3] e, principalmente, revelações em torno do reforço de práticas discriminatórias[4] 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.[5] 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:[6]

---

[1] 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*.

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

[3] 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

[4] O estudo ''The Perpetual Line Up'', do Centro Para a Privacidade e Tecnologia, da Universidade de Georgetown, chega a esta conclusão e pode ser acessado em sua versão interativa em: https://www.perpetuallineup.org/

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

[6] Em geral, esse é o mote das perguntas que encabeçam o convite para participação da audiência pública1) Quais os benefícios advindos do uso de ferramentas de reconhecimento facial pelas empresas? 2) Quais os benefícios advindos do uso de ferramentas de reconhecimento facial pelo Poder Público? 3) O uso do reconhecimento facial gera risco real à privacidade do cidadão? 4) Onde estamos e para onde vamos em relação ao reconhecimento facial no Brasil e no mundo. 5) A Lei Geral de Proteção de Dados Pessoais brasileira já é suficiente para proteger as informações biométricas dos titulares dos dados pessoais?

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;[7]

c) ao centro desse movimento pendular, encontra-se uma estratégia que visa desenhar uma arquitetura precaucionária de danos, de modo que o emprego de 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[8] acerca da segurança de tais tecnologias,[9] 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.[10]

Com isso, formata-se uma discussão regulatória de três feixes distintos, nos quais se exige mais ou menos por parte dos desenvolvedores das tecnologias de reconhecimento facial antes do seu lançamento no mercado consumidor. Trata-se de uma arquitetura precaucionária diante das incertezas quantos aos benefícios e riscos decorrentes da adoção de tais tecnologias, a qual pode ser resumida da seguinte forma com base na literatura teórica sobre o princípio do campo do direito ambiental:

Princípio da precaução e estratégias regulatórias para tecnologias de reconhecimento facial[11]		
Fraca: o fato de haver incerteza quanto ao risco gerado pela atividade de tratamento de dados não pode justificar inércia por parte do controlador, nem a atribuição de deveres que desencadeariam ações para controlar o risco em si e gerar evidências a esse respeito;	**Moderada**: incerteza na avaliação do risco justifica ação, mas há a atribuição de deveres para controlar o risco e gerar evidências a esse respeito. Ao final, há discricionariedade por parte do agente econômico em prosseguir ou não com a atividade;	**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.;

[7] MEDIUM. Facial recognition is the perfect tool for oppression. Disponível em: https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66

[8] CRAWFORD, Kate et al. AI now report 2018. p. 05. Disponível em: https://ainowinstitute.org/AI_Now_2018_Report.pdf

[9] 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

[10] Essa é a conclusão de: 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). Available at: https://ir.lawnet.fordham.edu/iplj/vol29/iss2/6

[11] BIONI, Bruno Ricardo. LUCIANO, Maria. Princípio da precaução como vetor de regulação de Inteligências Artificial: seriam as leis de proteção de dados pessoais o seu portal de entrada? In Inteligências Artificial (Organizadores Caitlin Sampaio et al). Rio de Janeiro, 2019.

III - Reconhecimento facial e propostas regulatórias

No debate geral sobre proteção de dados, que possui distintos graus de maturidade a depender da região e de temáticas específicas, vem sendo observada uma mudança de um paradigma focado na autodeterminação informacional do indivíduo para um modelo voltado para prevenção e gerenciamento de riscos criados pelas atividades de tratamento de dados.[12]

O emprego de inteligência artificial para a coleta e tratamento de dados pessoais considerados sensíveis, como os dados biométricos, amolda-se a esta perspectiva na medida em que, se é consenso tratar-se de atividade que envolve altos riscos a direitos e liberdades de cidadãos, também é verdade que estes riscos são de difícil mensuração, especialmente pela maior parte da população, que não detém a tecnologia nem o conhecimento para reconhecer a extensão do impacto sobre os seus dados pessoais. Essa combinação de fatores - riscos substanciais e assimetria informacional e de poder - aponta para a necessidade de implantação de processos detalhados de avaliação e mitigação dos riscos, sob responsabilidade de quem controla o uso destas tecnologias de coleta e tratamento de dado, além de prestação de contas e abertura para a participação nesse processo regulatório.

Tal lógica já vem sendo incorporada ao debate e à regulação propriamente dita da proteção de dados pessoais. Nesse sentido, a exigência de relatórios de impacto à proteção de dados pessoais/RIPDP é um exemplo importante que vem ganhando destaque nas legislações, como a normativa europeia, a própria recém aprovada Lei Geral de Dados Pessoais e também projetos de lei em âmbito internacional, com destaque para os Estados Unidos. Entretanto, a depender das especificidades na regulação destes relatórios - se obrigatórios ou uma discricionariedade, se avaliados por um órgão independente ou não, por exemplo - varia o ônus sobre os detentores da tecnologia de reconhecimento facial que buscam tratar dados biométricos e, por consequência, varia a ‘’força’’ da aplicação do princípio da precaução frente aos riscos da atividade.

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, concluiu-se, pelas seguintes razões, que a lei geral brasileira de proteção de dados/LGPD apresenta um modelo fraco e janelas 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 com 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;
- **a.3)** não há um processo de tomada de decisão que extrapole as figuras do controlador e do órgão regulador, diferentemente de outras propostas em que 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*);

[12] 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

b) 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, pode vir a 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[13];

c) 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 está parcialmente excepcionado 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;[14]

III.A – Quadro comparativo de tendências regulatórias: um olhar para a experiência internacional

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.		
Estratégias de Regulação		
Regulação específica para dados biométricos-reconhecimento facial		
Lei-norma	**Descrição**	**Grau de força da aplicação do Princípio da Precaução**
1. Biometric Information Privacy Act, Illinois[15], EUA	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	**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

[13] 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>.

[14] BIONI, 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.

	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.	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.
2. HB 1493, Washington[16], 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	**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.

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

[16] 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

	para cumprir obrigações legais, proteger os dados de possíveis fraudes e outros ilícitos ou preencher o objetivo para o qual os dados foram coletados.	
3. Texas Business and Commerce Code - BUS & COM § 503.001. Capture or Use of Biometric Identifier, Texas[17], 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 Code - Acquisition of Surveillance Technology, San Francisco, EUA[18]	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 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.	**Alto grau de força do princípio da precaução:** a proposta em tramitação na cidade de São Francisco parte do 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 a administração pública empregar tal tecnologia, é necessário a execução de RIV que deve ser revisado pelo procurador

[17] A lei pode ser consultada na íntegra, em inglês, no seguinte link: https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm
[18] 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

		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[19]	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[20]	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[21]	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; **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	**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).

[19] O projeto pode ser consultado na íntegra, em inglês, no seguinte link: https://malegislature.gov/Bills/191/SD671
[20] O projeto pode ser consultado na íntegra, em inglês, no seguinte link: https://malegislature.gov/Bills/191/H287
[21] O projeto pode ser consultado na íntegra, em inglês, no seguinte link: https://pt.scribd.com/document/401931553/The-Commercial-Facial-Recognition-Privacy-Act

	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.	
Regulação geral contida em leis de proteção de dados ou de governança algorítmica		
Lei-norma	**Descrição**	**Grau de força da aplicação do Princípio da Precaução**
8. Regulamento Geral sobre a Proteção de Dados (UE)	No caso da GDPR (RGPD, na sigla em português), embora não se trate de uma regulação específica sobre dados biométricos ou reconhecimento facial, há previsão dos chamados relatórios de impacto à proteção de dados pessoais,[22] que se estendem aos dados biométricos e devem ser **obrigatoriamente** executados pelo controlador - quem tem poder de tomada decisão na cadeia de tratamento de dados - quando houver um *alto risco em jogo*. Além de trazer uma lista exemplificativa dessas situações, a normativa exige que os órgãos fiscalizadores sejam comunicados apenas quando o próprio agente econômico não encontrar meios de mitigar os prováveis malefícios da sua respectiva atividade, devendo nesse caso aguardar "luz verde" da autoridade para seguir em frente. Levando-se em consideração que tecnologias de reconhecimento facial envolvem técnicas de profiling e/ou monitoramento de áreas públicas, enquadra-se como uma das situações de alto risco pelo RGPD.	**Alto grau de força do princípio da precaução:** ao se deparar com uma situação de alto risco que não pode ser mitigado por meio de medidas adequados 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. Portanto, além da procedimentalização de deveres de informação, publicização e de bases legais para o tratamento de dados pessoais próprios de uma lei geral de proteção de dados, há a atribuição de um dever de cuidado por parte de quem é o proponente de tal tecnologia, cujo circuito decisório pode envolver outros interessados.
9. Algorithmic Accountability Act, EUA[23]	Este projeto, proposto recentemente pelos Senadores Cory Booker e Ron Wyder, trata de hipóteses de emprego de algoritmo em processos automatizados de tomada de decisão. Nesses casos, o projeto estabelece a obrigação de elaboração de relatórios de impacto à proteção de dados pessoais (quando houver tratamento). Entretanto, nesse caso não se prevê o envolvimento do órgão regulador no processo.	**Moderado grau de força do princípio da precaução:** apesar de obrigar a elaboração de RIPDP em situações de alto risco, o projeto é silente quanto à eventual paralisação de uma atividade quando houver ameaça de dano e ausência de medidas para preveni-lo. Dessa forma, a incerteza quanto aos malefícios de uma atividade pode justificar ação, mas ela não deixa de ser uma discricionariedade do próprio proponente da atividade.

[22] WRIGHT, David; DE HERT, Paul (Orgs.), *Privacy Impact Assessment*, Dordrecht: Springer Netherlands, 2012.
[23] O projeto pode ser consultado na íntegra, em inglês, no seguinte link: https://www.wyden.senate.gov/imo/media/doc/Algorithmic%20Accountability%20Act%20of%202019%20Bill%20Text.pdf

10. Lei Geral de Proteção de Dados Pessoais (Brasil)	A LGPD, a exemplo do regulamento europeu, também adotou o instrumento de avaliação de impacto. O chamado "relatório de impacto à proteção de dados" é definido como "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (art. 5º, XVII). No entanto, ele não é obrigatório para atividades de alto risco, como definido na legislação europeia, sendo apenas mencionado como algo exigível por parte da Autoridade Nacional de Proteção de Dados Pessoais. Além de não prever a obrigatoriedade dos relatórios, a LGPD também não especifica quais seriam os casos considerados de ''alto risco''.	**Baixo grau de força do princípio da precaução** ao não procedimentalizar minimamente em que situações os RIPDP são obrigatórios, muito menos quais devem ser os elementos a compor tal documentação. Assim, ao mesmo tempo em que parece estar presente a ideia de que a incerteza quanto aos malefícios de uma atividade não justifica inação, daí a previsão de relatórios de impacto, seu desenho não é suficientemente robusto para se enquadrar em outros níveis de aplicação do princípio. No entanto, destaca-se que uma regulação posterior por parte da ANPD ou de outros órgãos reguladores pode alterar o *status* de força de aplicação do princípio da precaução em questão.