JOÃO PAULO LORDELO

CONSTITUCIONALISMO DIGITAL E DEVIDO PROCESSO LEGAL

Prefácio: Luiz Fux

2022

EDITORA JusPODIVM
www.editorajuspodivm.com.br

EDITORA *Jus*PODIVM
www.editorajuspodivm.com.br

Rua Canuto Saraiva, 131 – Mooca – CEP: 03113-010 – São Paulo – São Paulo
Tel: (11) 3582.5757
• Contato: https://www.editoraJuspodivm.com.br/sac

Copyright: Edições *Jus*podivm

Diagramação: Equipe *Jus*podivm

Capa: Ana Caquetti

C758 Constitucionalismo digital e devido processo legal / João Paulo Lordelo – São Paulo: Editora Juspodivm, 2022.
352 p. (Ensaios)

Bibliografia.
ISBN 978-85-442-3679-6.

1. Direito Digital. 2. LGPD. 3. Novas Tecnologias. I. Lordelo, João Paulo. II. Título.

CDD 340.004.678

"Roy Batty: I've done... questionable things.
Dr. Eldon Tyrell: Also extraordinary things; revel in your time.
Roy Batty: Nothing the God of biomechanics wouldn't let you into heaven for."
(Blade Runner, 1982)

4. ESBOÇO DE UM DEVIDO PROCESSO DIGITAL: ALCANCE E CONTEÚDO

4.1. Introdução: tecnoautoritarismo *vs.* humanismo digital

Ao longo dos capítulos anteriores, duas importantes premissas foram estabelecidas. A primeira consiste na compreensão do devido processo legal como uma garantia adaptativa do *rule of law*, que há de ser responsavelmente ampliada para novos contextos fora da relação indivíduo-Estado. A segunda é percepção da 4ª revolução industrial como um fenômeno que trouxe novos desafios jurídicos à humanidade, sobretudo no campo da proteção dos direitos fundamentais. Enquanto o constitucionalismo tem sido tradicionalmente desenvolvido para limitar os poderes governamentais, novas forças privadas surgiram ameaçando a proteção dos direitos fundamentais[1].

Entre as características do atual estágio do exercício de poderes por agentes tecnológicos, destaca-se a escalabilidade praticamente infinita das ferramentas que lidam com informações igualmente

1. DE GREGORIO, Giovanni. From constitutional freedoms to the power of the platforms: protecting fundamental rights online in the algorithmic society. *European Journal of Legal Studies*, vol. 11, n. 2, 2019, p. 102.

infinitas nos espaços digitais. Conquanto seja claro o relevante papel da tecnologia na evolução dos atores privados no ambiente *online*, não se pode negar que, por muito tempo, os atores públicos têm facilitado o surgimento de novas formas de exercícios de poderes por plataformas digitais[2].

Na realidade ora experimentada, não apenas atores privados têm exercido, de forma discricionária, poderes capazes de afetar diretamente o gozo de direitos fundamentais pelas pessoas em geral, como também os estados têm utilizado ferramentas algorítmicas em variados campos, sem as garantias adequadas. Em ambos os casos, é possível identificar uma elevada concentração de poder, em detrimento da autonomia dos indivíduos – sejam eles consumidores, trabalhadores, jurisdicionados etc.

Firmadas essas bases, a proposta do presente capítulo consiste em estabelecer os contornos do que pode ser denominado "devido processo digital", "devido processo tecnológico"[3] ou "devido processo 4.0" em suas dimensões procedimental e substantiva. Tal instituto jurídico há de ser compreendido como o elemento-chave capaz de impedir a escalada do tecnoautoritarismo, firmando um marco civilizatório mínimo do humanismo digital.

4.2. O microssistema brasileiro de tutela de direitos cibernéticos

Não é difícil reconhecer a existência, no Brasil, de um microssistema de proteção a direitos cibernéticos, assim compreendidos os direitos particularmente identificados nos contextos em que empregadas novas tecnologias digitais.

O núcleo desse microssistema é composto basicamente de três importantes diplomas: a) o Código de Defesa do Consumidor –

2. DE GREGORIO, Giovanni. From constitutional freedoms to the power of the platforms: protecting fundamental rights online in the algorithmic society. *European Journal of Legal Studies*, vol. 11, n. 2, 2019, p. 101.

3. A expressão é utilizada por Citron, Danielle Keats; Pasquale, Frank. The Scored Society: Due Process for Automated Predictions. *Washington Law Review*, vol. 89, 2014, p. 19.

CDC (Lei nº 8.078/1990); b) o Marco Civil da Internet – MCI (Lei nº 12.965/2014); e c) a Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018). Como em qualquer outro microssistema, outros atos normativos satelitários também são relevantes, a exemplo da Lei do Processo Administrativo Federal (Lei nº 9.784/1999), da Lei de Acesso à Informação (Lei nº 12.527/2011) e da Resolução CNJ nº 332/2020.

Embora, em uma primeira análise, possa parecer estranha a inserção do CDC no núcleo desse microssistema, sobretudo por se tratar de um diploma editado na longínqua década de 1990, não se pode perder de vista que o diploma representa uma importante garantia protetiva contra qualquer agente que atue no mercado de consumo. Mesmo nas situações em que ausente uma prévia relação contratual, a regra do art. 17 do CDC estabelece um conceito ampliado de consumidor ("bystander"), que abrange as vítimas de produtos ou serviços defeituosos[4].

Como destacado na jurisprudência do Superior Tribunal de Justiça, "toda e qualquer vítima de acidente de consumo equipara-se ao consumidor para efeito da proteção conferida pelo CDC", o que abrange "os chamados bystanders, na terminologia da *common law*, que são os terceiros que, embora não estejam diretamente envolvidos na relação de consumo, são atingidos pelo aparecimento de um defeito no produto ou no serviço"[5].

Em razão da regra do art. 17 do CDC, a disciplina protetiva do diploma – que tem por premissa a vulnerabilidade das pessoas frente a outros agentes econômicos – é aplicada em favor de qualquer pessoa atingida pela atividade empresarial, sem que configure o consumidor final de serviços e sem qualquer relação com o fornecedor. Assim, pode ser incluída, no rol das atividades disciplinadas, aquelas praticadas pelos provedores de aplicações,

4. Código de Defesa do Consumidor: "Art. 17. Para os efeitos desta Seção, equiparam-se aos consumidores todas as vítimas do evento".

5. REsp 1358513/RS, Quarta Turma, Relator: Ministro Luis Felipe Salomão, DJe 04/08/2020.

assim compreendidos os fornecedores de um "conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet"[6].

Entre as garantias processuais estabelecidas pelo CDC, destacam-se a facilidade na inversão do ônus da prova[7], a facilitação da desconsideração da personalidade jurídica[8] e as garantias no estabelecimento de bancos de dados e cadastros de consumidores[9]. Materialmente, merecem destaque o direito à informação, a proteção contra publicidade enganosa ou abusiva, a facilitação na modificação de cláusulas contratuais onerosas[10], o

6. Marco Civil da Internet: "Art. 5º Para os efeitos desta Lei, considera-se: [...] VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e [...]".

7. Código de Defesa do Consumidor: "Art. 6º São direitos básicos do consumidor: [...] VIII - a facilitação da defesa de seus direitos, inclusive com a inversão do ônus da prova, a seu favor, no processo civil, quando, a critério do juiz, for verossímil a alegação ou quando for ele hipossuficiente, segundo as regras ordinárias de experiências; [...]".

8. Código de Defesa do Consumidor: "Art. 28. O juiz poderá desconsiderar a personalidade jurídica da sociedade quando, em detrimento do consumidor, houver abuso de direito, excesso de poder, infração da lei, fato ou ato ilícito ou violação dos estatutos ou contrato social. A desconsideração também será efetivada quando houver falência, estado de insolvência, encerramento ou inatividade da pessoa jurídica provocados por má administração".

9. Código de Defesa do Consumidor: "Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes [...] § 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele; § 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas; § 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público [...]".

10. Código de Defesa do Consumidor: "Art. 6º São direitos básicos do consumidor: [...] III - a informação adequada e clara sobre os diferentes produtos e serviços,

regime de responsabilidade objetiva[11], a proteção contra práticas jurídicas específicas (como a recusa ao serviço)[12], a inaplicabi-

com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como sobre os riscos que apresentem; IV - a proteção contra a publicidade enganosa e abusiva, métodos comerciais coercitivos ou desleais, bem como contra práticas e cláusulas abusivas ou impostas no fornecimento de produtos e serviços; V - a modificação das cláusulas contratuais que estabeleçam prestações desproporcionais ou sua revisão em razão de fatos supervenientes que as tornem excessivamente onerosas; [...]".

11. Código de Defesa do Consumidor: "Art. 12. O fabricante, o produtor, o construtor, nacional ou estrangeiro, e o importador respondem, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos decorrentes de projeto, fabricação, construção, montagem, fórmulas, manipulação, apresentação ou acondicionamento de seus produtos, bem como por informações insuficientes ou inadequadas sobre sua utilização e riscos [...] Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos".
12. Código de Defesa do Consumidor: "Art. 39. É vedado ao fornecedor de produtos ou serviços, dentre outras práticas abusivas: [...] II - recusar atendimento às demandas dos consumidores, na exata medida de suas disponibilidades de estoque, e, ainda, de conformidade com os usos e costumes; [...] IV - prevalecer-se da fraqueza ou ignorância do consumidor, tendo em vista sua idade, saúde, conhecimento ou condição social, para impingir-lhe seus produtos ou serviços; [...] VII - repassar informação depreciativa, referente a ato praticado pelo consumidor no exercício de seus direitos; VIII - colocar, no mercado de consumo, qualquer produto ou serviço em desacordo com as normas expedidas pelos órgãos oficiais competentes ou, se normas específicas não existirem, pela Associação Brasileira de Normas Técnicas ou outra entidade credenciada pelo Conselho Nacional de Metrologia, Normalização e Qualidade Industrial (Conmetro); IX - recusar a venda de bens ou a prestação de serviços, diretamente a quem se disponha a adquiri-los mediante pronto pagamento, ressalvados os casos de intermediação regulados em leis especiais; [...] XII - deixar de estipular prazo para o cumprimento de sua obrigação ou deixar a fixação de seu termo inicial a seu exclusivo critério [...]".

lidade de cláusulas contratuais obscuras[13] (como em termos de serviços de plataformas digitais) etc.

A disciplina geral do CDC, todavia, há de ser conformada pelas normas do MCI, que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil, a exemplo do seu art. 19, que cria um distinto regime de responsabilidade por danos decorrentes de conteúdo gerado por terceiros[14].

Finalmente, soma-se a este núcleo a LGPD, que 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.

Embora o art. 4º, III, da LGPD excepcione expressamente a sua aplicação nos campos da segurança pública, atividades de investigação e repressão de infrações penais, o seu § 1º informa que, em tais campos, o tratamento de dados pessoais será regido por legislação específica, "que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei". Em razão do

13. Código de Defesa do Consumidor: "Art. 46. Os contratos que regulam as relações de consumo não obrigarão os consumidores, se não lhes for dada a oportunidade de tomar conhecimento prévio de seu conteúdo, ou se os respectivos instrumentos forem redigidos de modo a dificultar a compreensão de seu sentido e alcance".
14. Marco Civil da Internet: "Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros; Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário".

que dispõe o texto legal, ainda que inexistente uma LGPD penal, é possível aplicar, desde já, os princípios gerais e os direitos do titular da LGPD geral, bem como a cláusula do devido processo legal, observadas algumas relevantes balizas.

Entre os direitos do titular previstos no seu art. 18 particularmente aplicáveis às autoridades públicas, destacam-se a confirmação da existência de tratamento de dados; o acesso aos dados; a correção de dados incompletos, inexatos ou desatualizados; a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei e a informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.

4.3. A incidência da cláusula do devido processo nas relações verticais entre indivíduo e Estado

A incidência da cláusula do devido processo legal nas relações envolvendo indivíduos e o Estado é tema menos problemático. Afinal, como já exaustivamente demonstrado, desde as suas mais remotas influências históricas, a cláusula opera como uma espécie de metonímia do Estado de Direito, prevenindo os indivíduos contra ações estatais arbitrárias.

As dificuldades aqui podem surgir em duas situações. Primeiramente, como já exposto, existem casos em que o emprego de tecnologias digitais, em prejuízo ao exercício de direitos fundamentais, não vem acompanhado de uma disciplina legislativa que forneça às pessoas afetadas garantias procedimentais mínimas. É o que ocorre no emprego das chamadas *no-fly lists*, das ferramentas de reconhecimento facial ou nas demais formas de uso de *data matching* e *data mining* no campo da prevenção criminal.

De igual modo, pode ocorrer de até, num determinado contexto, existirem garantias legais, mas originariamente desenhadas para as tradicionais relações *off-line* entre indivíduos e Estado, previstas em códigos judiciais ou administrativos.

Seja como for, na ausência das garantias mínimas para um ecossistema digital, detalhadas nos tópicos seguintes, compreendemos pela possibilidade de intervenção judicial preventiva (*ex post*) ou repressiva (*ex ante*), em forma de tutela individual ou coletiva. Particularmente quanto às garantias relativas ao exercício do contraditório e da ampla defesa, elas variarão de acordo com a gravidade da privação ao direito, conforme reconhecido pela SCOTUS em *Mathews v. Eldridge*[15]. Em outras palavras, as garantias, se não previamente estabelecidas em lei, deverão ser extraídas das características de um assunto em particular, a exemplo da severidade da privação e do interesse público existente[16].

4.4. O problema da incidência da cláusula do devido processo legal no setor privado: em busca de uma solução no Estado de Direito

Um dos mais preocupantes problemas derivados da 4ª revolução industrial é certamente o acúmulo de poder privado pelas *big techs* e suas plataformas digitais (Google, Apple, Amazon, Twitter, Facebook etc.). Como reconhecem muitos autores, a concentração de poder nas mãos de companhias tem o potencial de restringir liberdades pessoais, a exemplo da liberdade de informação, liberdade de expressão e o direito à proteção de dados[17].

Mas há algo além da proteção de direitos individuais. O regime de quase monopólio, a questionável manipulação de dados privados e a massiva tendência expansiva sobre outros campos desafia não apenas o exercício de direitos fundamentais, mas

15. SUPREMA CORTE DOS ESTADOS UNIDOS. *Mathews v. Eldridge,* 424 U.S. 319, 1976.

16. FRIENDLY, Henry. Some kind of hearing. U. Pa. L. Rev., vol. 123, n. 1267, 1975. Disponível em: https://scholarship.law.upenn.edu/penn_law_review/vol123/iss6/2. Acesso em: 4 nov. 2021.

17. WOLFF, Daniel. Fundamental rights in the digital era: horizontal effect and the distinction between State and society in German and European constitutional theory. *Frontiers of Law in China*, vol. 13, n. 3, p. 441-455, 2018, p. 444.

também a institucionalização da esfera pública digital[18]. Afinal, como destaca Teubner, o monopólio informacional torna-se um problema para a constituição das novas mídias, o que não se reduz a questões econômicas. Cuida-se de um contexto que questiona a própria constituição da internet global, marcada por relações assimétricas de poder. A falta de transparência em suas estruturas de governança levanta questões constitucionais de democracia e de controle público. Essa abordagem parte do pressuposto de que os direitos constitucionais servem não apenas à proteção de direitos individuais, mas também de instituições sociais vulneráveis, como a arte ou a ciência, afastando-as de tendências totalizantes que operam na sociedade[19].

Disso decorre que a permeabilidade da cláusula do devido processo legal, como metonímia do Estado de Direito, às relações assimétricas travadas no contexto das tecnologias digitais conduzidas agentes privados, serve, a um só tempo, à tutela de direitos individuais e à conformação da esfera pública digital. Nesta segunda relevante missão, o devido processo serve como uma forma de promoção da liberdade de uma instituição social por meio da sua organização. E mais: tratando-se de uma cláusula geral, ele possibilita a existência de um dinâmico processo sociojurídico de normatização sujeito a mudanças constantes[20].

Sob uma perspectiva sociológica, atualmente não há dúvidas de que as esferas estatal e social, em verdade, fazem parte de uma mesma realidade. Como destaca Wolff, o Estado não se encontra ao lado ou acima da sociedade, havendo de ser compreendido

18. TEUBNER, Gunther. Horizontal Effects of Constitutional Rights in the Internet: A Legal Case on the Digital Constitution. *Italian Law Journal*, v. 3, n. 2, p. 485–510, 2017, p. 196 e 201.
19. TEUBNER, Gunther. Horizontal Effects of Constitutional Rights in the Internet: A Legal Case on the Digital Constitution. *Italian Law Journal*, v. 3, n. 2, p. 485–510, 2017, p. 197.
20. TEUBNER, Gunther. Horizontal Effects of Constitutional Rights in the Internet: A Legal Case on the Digital Constitution. *Italian Law Journal*, v. 3, n. 2, p. 485–510, 2017, p. 199.

como um subsistema dela[21]. Além disso, também parece claro que a promoção das liberdades constitucionais, empiricamente, depende não apenas do Estado, mas também da conduta de outros agentes sociais. Consequentemente, ao não considerar a relevância da estrutura interna da sociedade – e, portanto, não distinguir as formas assimétricas de exercício de poder –, a doutrina liberal do *state action* falha consideravelmente[22].

Essas premissas sobrelevam o papel da eficácia direta da cláusula do devido processo legal como uma resposta à altura dos desafios trazidos pela era informacional vivenciada. Essa aplicação, contudo, apresenta ao menos duas importantes objeções, além de alguns problemas práticos.

A primeira objeção é levantada por aqueles que acreditam que a eficácia horizontal direta seria desnecessária, em razão da possibilidade de incidência indireta, mediante a interpretação da legislação infraconstitucional à luz dos direitos fundamentais[23]. De acordo com essa corrente, a eficácia horizontal indireta teria a vantagem de mover a responsabilidade protetiva ao legislador infraconstitucional e, assim, evitar a instabilidade que deriva da interpretação judicial caso a caso[24]. Como aponta Wolff, a objeção não prospera por alguns motivos. Primeiramente, a doutrina da eficácia horizontal indireta falha em razão do seu baixo nível de proteção. Isso porque é possível que o legislador deixe de cumprir o seu dever diante de violações evidentes de direitos fundamentais.

21. WOLFF, Daniel. Fundamental rights in the digital era: horizontal effect and the distinction between State and society in German and European constitutional theory. *Frontiers of Law in China*, vol. 13, n. 3, p. 441-455, 2018, p. 441.
22. WOLFF, Daniel. Fundamental rights in the digital era: horizontal effect and the distinction between State and society in German and European constitutional theory. *Frontiers of Law in China*, vol. 13, n. 3, p. 441-455, 2018, p. 450-451.
23. GRIMM, Dieter. Der Datenschutz vor einer Neuorientierung. *JuristenZeitung*, vol. 68, n. 2, 2013.
24. WOLFF, Daniel. Fundamental rights in the digital era: horizontal effect and the distinction between State and society in German and European constitutional theory. *Frontiers of Law in China*, vol. 13, n. 3, p. 441-455, 2018, p. 452.

Além disso, as próprias entidades privadas também são titulares de direitos fundamentais, o que torna mais difícil o controle de suas atividades pela via legislativa. Finalmente, a dinâmica das transformações tecnológicas torna difícil ao legislador prever todos os aspectos protetivos relevantes, mediante uma regulamentação detalhada e atualizada[25].

A segunda objeção consiste no risco à segurança jurídica que pode derivar da aplicação indiscriminada dos direitos fundamentais horizontalmente, com excessivo empoderamento de tribunais e fragilização da autonomia privada. Essa preocupação ganha especial destaque se considerarmos a sua aplicação *ex post* pelos tribunais[26].

A preocupação é relevante, na medida em que, em muitos casos, será difícil decidir com precisão sobre a existência de uma assimétrica relação de poder entre pessoas privadas. De fato, a mera assimetria de poder, isoladamente considerada, não é suficiente para justificar uma intervenção estatal, desde que presente um ambiente de justa competição[27]. Em outras palavras, como

25. WOLFF, Daniel. Fundamental rights in the digital era: horizontal effect and the distinction between State and society in German and European constitutional theory. *Frontiers of Law in China*, vol. 13, n. 3, p. 441-455, 2018, p. 452.

26. No original: "Applying extensively this doctrine could lead to negative effects for legal certainty. Indeed, every private conflict can virtually be represented as a clash between different fundamental rights. The result could lead to the extension of constitutional obligations to every private relationship, thus hindering any possibility to foresee the consequences of a specific action or omission. Fundamental rights can be applied horizontally only ex post by courts through the balancing of the rights in question. This process could increase the degree of uncertainty as well as judicial activism, with evident consequences for the separation of powers and the rule of law" (DE GREGORIO, Giovanni. From constitutional freedoms to the power of the platforms: protecting fundamental rights online in the algorithmic society. *European Journal of Legal Studies*, vol. 11, n. 2, 2019, p. 100).

27. CANARIS, Claus-Wilhelm. Grundrechte und Privatrecht. *Archiv für die Civilistische Praxis*, vol 184, n. 3, 1984, p. 206-207.

destaca Wolff, o mero exercício de poder econômico não é, por si só, algo ilegítimo[28].

Conquanto relevante a objeção, ela ser minorada por duas razões.

A primeira delas consiste no evidente reconhecimento de que é e sempre será possível o estabelecimento de um marco regulatório pelo legislador infraconstitucional. Como descrito anteriormente, o constitucionalismo digital encontra-se em um estágio relativamente avançado na Europa e em países como o Brasil. Nesse contexto, a mera preocupação quanto ao desenvolvimento de um ambiente de instabilidade jurídica, decorrente da atividade jurisdicional, pode servir como incentivo para o desenvolvimento de uma legislação adequada, a exemplo do anteprojeto de "Carta de Direitos Fundamentais Digitais da União Europeia"[29]. Quanto mais adequada e abrangente a atividade legislativa produzida, menor será o exercício da revisão judicial *ex post facto* e, portanto, menor o risco de insegurança jurídica.

Além disso, é importante reforçar que a aplicação horizontal da cláusula do devido processo legal, em suas dimensões procedimental e substantiva, não deve ocorrer de forma desregrada. Ao revés, o teste proposto no capítulo introdutório buscou estabelecer alguns balizes relevantes, levando em consideração "propósitos públicos"[30].

A primeira baliza parte da distinção entre a horizontalização do devido processo legal procedimental e a aplicação horizontal do

28. WOLFF, Daniel. Fundamental rights in the digital era: horizontal effect and the distinction between State and society in German and European constitutional theory. *Frontiers of Law in China*, vol. 13, n. 3, p. 441-455, 2018, p. 453.

29. WOLFF, Daniel. Fundamental rights in the digital era: horizontal effect and the distinction between State and society in German and European constitutional theory. *Frontiers of Law in China*, vol. 13, n. 3, p. 441-455, 2018, p. 443.

30. WOLFF, Daniel. Fundamental rights in the digital era: horizontal effect and the distinction between State and society in German and European constitutional theory. *Frontiers of Law in China*, vol. 13, n. 3, p. 441-455, 2018, p. 454.

devido processo legal em sua dimensão substantiva. Ela objetiva a adequada preservação daquilo que a doutrina verticalista objetiva proteger: o exercício da autonomia privada. Por essa razão – e também pelas preocupações já explicitadas quanto ao excessivo empoderamento de tribunais, fragilizando-se os processos políticos –, compreendemos adequado o reconhecimento da eficácia horizontal do devido processo legal, em sua dimensão substantiva, apenas de forma *indireta*. Evita-se, com isso, a recorrente invocação da aplicação do princípio da proporcionalidade no campo das relações entre particulares.

Consequentemente, um ato jurídico praticado no âmbito privado, se considerado arbitrário por um interessado, pode vir a ser invalidado *ex post* se o tribunal identificar a ausência de razoabilidade no emprego da legislação infraconstitucional.

Por outro lado, no que diz respeito ao devido processo legal procedimental, garantias mínimas – a exemplo do direito de notificação e defesa – podem e devem ser reconhecidas tanto *direta* quanto *indiretamente,* notadamente na arquitetura codificada do ciberespaço. Como apontam Karavas e Teubner, no ambiente digital, o "código" consiste na matéria prima da ordem normativa, em lugar das normas legais[31]. Nesse contexto, a eficácia horizontal *direta* deve ser reconhecida sempre que identificado um contexto de considerável relação assimétrica de poder que afete o livre exercício de um direito fundamental. Ausente essa relação, a eficácia horizontal haverá de ser reconhecida apenas *indiretamente*.

No exercício de tal tarefa, é relevante a identificação do grau de concentração de poderes nas mãos de agentes privados. Isso porque, como já referido, a digitalização contribui para a reunião dos poderes de elaboração de normas, aplicação e execução em um

31. KARAVAS, Vagias; TEUBNER, Gunther. Www.CompanyNameSucks.Com: The Horizontal Effect of Fundamental Rights on "Private Parties" Within Autonomous Internet Law. *Constellations*, vol. 12, p. 262–282, 2005, p. 268-269.

único agente interessado. A ausência de uma divisão de poderes – a exemplo do controle de conduta, construção de expectativas e solução de conflitos – é um importante parâmetro para o reconhecimento da incidência da cláusula do devido processo[32].

Além disso, toma-se emprestado o teste estabelecido pela Corte Constitucional da África do Sul, no caso *Daniels v. Scribante and Another*[33], com o enfrentamento das seguintes questões: a) qual é a natureza do direito fundamental afetado? b) qual é a história por trás do direito? c) o que o direito busca alcançar? e) qual é a melhor forma de conseguir isso? e) qual é o potencial de invasão desse direito por outras pessoas que não o Estado ou órgãos do Estado? f) deixar pessoas privadas fora da incidência constitucional negaria o conteúdo essencial do direito?

4.5. Devido processo formal: garantias mínimas para um ecossistema digital

As premissas firmadas nos tópicos anteriores servem de fundamento para o reconhecimento da incidência da cláusula do devido processo legal nas relações jurídicas travadas entre agentes privados (eficácia horizontal). Ultrapassado esse ponto, é importante saber quais garantias mínimas devem ser reconhecidas àqueles sujeitos à variadas formas de automação decisória.

Nesse sentido, o objetivo dos tópicos seguintes é o de elencar desdobramentos concretos do devido processo digital, evitando-se a mera enumeração de princípios abstratos, desprovidos de conteúdo.

32. KARAVAS, Vagias; TEUBNER, Gunther. Www.CompanyNameSucks.Com: The Horizontal Effect of Fundamental Rights on "Private Parties" Within Autonomous Internet Law. *Constellations*, vol. 12, p. 262–282, 2005, p. 269.

33. CORTE CONSTITUCIONAL DA ÁFRICA DO SUL, *Daniels v. Scribante and Another*, CCT50/16, 2017.

4.5.1. Contraditório e ampla defesa: notificação adequada, participação e julgamento imparcial com reversibilidade de papéis

Como já referido nas premissas estabelecidas no primeiro capítulo, as garantias procedimentais relativas ao exercício do contraditório e à ampla defesa, quando não expressamente reguladas, variarão de acordo com a gravidade da privação ao direito. Cuida-se de resultado do precedente fixado pela SCOTUS em *Mathews v. Eldridge* e do trabalho seminal de Henry Friendly (1971), em que destacou a ausência de um *check-list* procedimental rígido.

Em síntese, as garantias, se não já previamente e adequadamente estabelecidas em lei, deverão ser extraídas das características de um caso em particular, como a severidade da privação e do interesse público ou privado contraposto. Em seu trabalho seminal, Friendly destacou 7 (sete) garantias defensivas capazes de assegurar um processo justo. Nem todas são necessárias, ele afirma, mas todas devem ser avaliadas, de acordo com as circunstâncias do caso. São elas[34]:

a) direito a um julgamento imparcial;
b) direito à notificação sobre a ação proposta e os seus fundamentos;
c) direito de apresentar argumentos pelos quais um resultado não deve ser atingido;
d) direito de produzir provas;
e) direito de conhecer as provas em seu desfavor;
f) direito a uma decisão fundamentada apenas nas evidências do caso;
g) direito a um advogado;
h) direito de registro dos atos processuais;

34. FRIENDLY, Henry. Some kind of hearing. U. Pa. L. Rev., vol. 123, n. 1267, 1975. Disponível em: https://scholarship.law.upenn.edu/penn_law_review/vol123/iss6/2. Acesso em: 4 nov. 2021.

i) direito de acesso às razões decisórias;
j) publicidade;
k) direito de recorrer da decisão tomada.

É importante destacar, porém, que embora a existência de uma margem de flexibilidade seja necessária, ela há de ser observada somente após o estabelecimento de um conjunto mínimo de garantias e valores, evitando-se uma abordagem excessivamente abstrata[35]. Como destacado por Redish e Marshall, o devido processo deve ser flexível, principalmente, em termos de procedimentos específicos a serem exigidos. Por outro lado, os valores centrais que a cláusula representa e impõe devem estar sempre presentes, a exemplo da previsibilidade, da transparência e da racionalidade[36]. Tais valores resultam no reconhecimento de ao menos três garantias fundamentais: notificação, participação e julgamento imparcial. Elas compõem o tripé da "racionalidade procedimental".

Um parâmetro inicial na fixação das garantias procedimentais defensivas decorre da diferenciação entre (a) *tomada de uma ação* e (b) *o ato de negar um pedido.* De uma forma geral, a tomada de uma ação contra um determinado indivíduo – demissão, impedimento de ingressar em transportes públicos, suspensão de benefícios assistenciais, suspensão de licença profissional, banimento de redes sociais, expulsão de associações ou outros grupamentos etc. – costuma ser algo bem mais sério que a denegação de um pedido[37]. Consequentemente, mais garantias podem ser exigidas.

35. REDISH, Martin H.; MARSHALL, Lawrence C. Adjudicatory Independence and the Values of Procedural Due Process. *Yale Law Journal*, vol. 95, n. 3, 1986, p. 456.
36. REDISH, Martin H.; MARSHALL, Lawrence C. Adjudicatory Independence and the Values of Procedural Due Process. *Yale Law Journal*, vol. 95, n. 3, 1986, p. 474.
37. CRAWFORD, Kate; SCHULTZ, Jason. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review*, vol 55, 2014, p. 110.

Um segundo parâmetro consiste na identificação do direito fundamental afetado, bem como do grau de ingerência. A título de exemplo, ferramentas decisórias automatizadas que afetem a liberdade de locomoção (a exemplo das ferramentas de monitoramento criminal) ou o acesso ao emprego devem ofertar garantias adequadas, como os direitos de notificação, defesa e retificação.

Finalmente, um terceiro parâmetro consiste na identificação da compatibilidade da garantia com um devido processo digital.

O direito de produzir prova testemunhal, por exemplo, seria algo aparentemente incompatível, tendo em vista o modo como os sistemas de *big data* processam as suas métricas. Por outro lado, o direito a um julgamento imparcial com reversibilidade de papéis, ao conhecimento das provas que pesam em desfavor de alguém e a uma decisão fundamentada são garantias mínimas de um *data due process.*

Do mesmo modo, o direito à notificação, embora comumente levantado como de difícil realização, costuma ser previsto na legislação de proteção aos dados, sendo razoável a sua realização prévia à tomada de uma decisão que afete sensivelmente a esfera de liberdade ou propriedade de alguém. Sua principal função consiste em oferecer àqueles que podem sofrer danos à liberdade, privacidade ou propriedade a oportunidade de intervir no processo preditivo[38]. Exatamente por isso, o devido processo tecnológico demanda que os sistemas automatizados incluam trilhas de auditoria imutáveis para garantir que os indivíduos recebam notificação sobre os fundamentos das decisões proferidas contra eles[39].

Exemplo de caso em que o direito à notificação é exigido é apresentado por Crawford e Schultz: se uma companhia empregadora pretende utilizar dados de buscadores como o *Google* ou *Bing* para decidir quais candidatos são mais adequados a uma oferta de trabalho, será necessário notificar os interessados sobre o uso dessas ferramentas para análise preditiva. De igual modo, se imobiliárias limitarem a oferta de imóveis para aquisição por meio de um aplicativo de *big data,* essa informação deverá ser individual ou coletivamente disponibilizada[40].

38. CRAWFORD, Kate; SCHULTZ, Jason. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review,* vol 55, 2014, p. 116-125.

39. CITRON, Danielle Keats; PASQUALE, Frank. The Scored Society: Due Process for Automated Predictions. *Washington Law Review*, vol. 89, 2014, p. 28.

Como apontam Danielle Keats Citron e Frank Pasquale, as garantias de notificação e transparência são particularmente relevantes quando empregados sistemas automatizados de pontuação de indivíduos (*scoring systems*), que podem se revelar estigmatizantes[41]. Tais sistemas podem ser empregados com múltiplas finalidades: concessão de empréstimos a consumidores, avaliação de profissionais, contratação de trabalhadores, avaliação de risco por seguradoras ou até mesmo concessão de benefícios na execução penal[42]. Em todos esses casos, ferramentas são responsáveis por classificar indivíduos, transformados em objetos de pontuação[43].

Particularmente em relação às redes sociais, que exercem um papel considerável na moderação do debate público nos dias atuais, com relevante afetação da liberdade de expressão, uma garantia se destaca. Trata-se do direito a um julgador imparcial. Exemplo disso é o *Facebook Oversight Board,* anunciado por Mark Zuckerberg, CEO e fundador da rede social, em novem-

40. CRAWFORD, Kate; SCHULTZ, Jason. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review,* vol 55, 2014, p. 126.

41. CITRON, Danielle Keats; PASQUALE, Frank. The Scored Society: Due Process for Automated Predictions. *Washington Law Review*, vol. 89, 2014.

42. CITRON, Danielle Keats. Data Mining for Juvenile Offenders. *Concurring Opinions*, 2010. Disponível em: http://www.concurringopinions.com/archives/2010/04/data-mining-for-juvenileoffenders.html. Acesso em: 30 nov. 2021.

43. RITCHEL, Matt. I Was Discovered by an Algorithm. *N. Y. Times*, 28 de abril de 2013. Disponível em: http://archive.indianexpress.com/news/i-was-discovered-by-an-algorithm/1111552/. Acesso em: 30 nov. 2021.

bro de 2018[44]. O órgão entrou em funcionamento no ano de 2020, com funções autocompositivas e capacidade de suplantar decisões da empresa[45]. Apesar da relevância da criação do órgão, é importante notar que a fundamentação das suas decisões leva em consideração o "conjunto de valores" e políticas desenhado pela própria empresa.

Mesmo no âmbito da segurança pública e da inteligência, campos não raramente marcados pela atuação sigilosa do Estado, é possível assegurar garantias procedimentais mínimas. É o caso do tratamento de dados realizado para fins de inclusão de indivíduos considerados suspeitos de atividades terroristas nas *no-fly lists*, impedindo-os de ingressarem em aeronaves. O mecanismo atualmente existente nos Estados Unidos poderia incorporar três garantias relevantes: a realização de audiências sumárias antes da privação do direito de acesso a transportes aéreos; a abertura de oportunidades de correção após uma primeira consequência derivada da aplicação de técnicas de *data matching* ou *data mining*; e a possibilidade de responsabilização por resultados do tipo "falso-positivo", indenizando-se as vítimas de constrangimentos indevidos. Nenhuma dessas garantias é atualmente assegurada naquele país[46].

Por seu turno, no âmbito da prestação de serviços públicos, é relevante a garantia da oportunidade de ser ouvido, mesmo que sob o risco do viés de automação dos agentes públicos, que pode ser diminuído com o treinamento adequado[47]. Além disso, a possibilidade de intervenção de especialistas, ainda que em um caso

44. KLONICK, Kate. The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression. *The Yale Law Jou*rnal, vol. 129, n. 8, p. 2418-499, 2020.

45. Cf. https://oversightboard.com/governance/. Acesso em: 30 nov. 2021.

46. CITRON, Danielle Keats. Technological Due Process. *Washington University Law Review*, vol. 85, n. 1249, 2008, p. 1.282.

47. SKITKA, Linda J. et al. Automation Bias and Errors: Are Crews Better Than Individuals? The *International Journal of Aviation Psychology*, vol. 10(1), p. 85-97, 2000.

isolado, pode contribuir para o aperfeiçoamento dos sistemas, em benefício de toda a coletividade. Como defende Citron, o teste que a SCOTUS estabeleceu no julgamento de *Mathews*, ao levar em consideração os custos adicionais das garantias processuais, deve passar a considerar o efeito sistêmico do aprimoramento tecnológico, evitando-se erros em incontáveis casos futuros[48].

Finalmente, uma importante garantia processual merece especial atenção, no contexto da a automação decisória. Como destacam Brennan-Marquez e Henderson, em uma democracia liberal, o autogoverno impõe um aspecto de "reversibilidade de papéis" no processo decisório[49]. Isso significa que aqueles que exercem o julgamento devem ser vulneráveis, reciprocamente, aos seus processos. O problema com os juízes robôs ou IA é que não podem experimentar a responsabilização da forma como um ser humano o faria. A reversibilidade de papéis é necessária para que decisores sejam compelidos a levar o processo decisório a sério, respeitando a gravidade da tomada de decisões do ponto de vista das partes afetadas[50]. Particularmente no âmbito estatal, essa garantia parece ser absolutamente imprescindível em qualquer atividade, evitando-se o processo decisório inteiramente automatizado.

48. CITRON, Danielle Keats. Technological Due Process. *Washington University Law Review*, vol. 85, n. 1249, 2008, p. 1.282-1.285.

49. BRENNAN-MARQUEZ, Kiel; HENDERSON, Stephen E. Artificial Intelligence and Role-Reversible Judgment. Journal of Criminal Law and Criminology, vol. 109, 2019, p. 137.

50. PASQUALE, Frank. Inalienable Due Process in an Age of AI: Limiting the Contractual Creep toward Automated Adjudication. In MICKLITZ, H.; POLLICINO, O.; REICHMAN; A.; SIMONCINI, A.; SARTOR, G.; DE GREGORIO, G. (Eds.), Constitutional Challenges in the Algorithmic Society (p. 42-56). Cambridge: Cambridge University Press, 2021, p. 46.

4.5.2. Princípio da auditabilidade

Entende-se por auditabilidade a capacidade de preservação de todo o conjunto de informações utilizadas na cadeia de funcionamento de uma determinada ferramenta. As auditorias envolvem a coleta de dados sobre o comportamento de um algoritmo em um determinado contexto, possibilitando avaliar se o comportamento está impactando negativamente alguns interesses (ou direitos) das pessoas afetadas[51].

Sem auditabilidade, qualquer ferramenta se transformará em uma caixa-preta, impossibilitando tanto o conhecimento da sua funcionalidade quanto a transparência[52].

Uma auditoria adequada pode ser empregada com ao menos três finalidades gerais. Primeiramente, ela pode ser usada por reguladores para avaliar se algum algoritmo atende normas legais ou políticas internas. É o caso da sua realização sobre algoritmos de empréstimo de um banco, de modo a saber se atendem à disciplina do BACEN. Em segundo lugar, uma auditoria de algoritmo pode ser usada por fornecedores e compradores de algoritmos para mitigar ou controlar riscos éticos e de reputação, bem como para identificar maneiras de remediar esses riscos. Finalmente, as partes interessadas podem estar interessadas em uma avaliação ética geral de um algoritmo, a fim de fazer escolhas informadas sobre votação, investimento, envolvimento com certas empresas etc. Como informam Brown *et al.,* a estrutura de auditoria deve

51. BROWN, Shea; DAVIDOVIC, Jovana; HASAN, Ali. The algorithm audit: Scoring the algorithms that score us. Big Data & Society, vol. 8, no. 1, 2021.

52. Conferir: BATHAEE, Yavar. Artificial Intelligence Black Box and the Failure of Intent and Causation. *Harvard Law Review,* v. 31, n. 2, p. 889-938, 2018; YANISKY-RAVID, Shlomit; HALLISEY, Sean. Equality and Privacy by Designa: a New Model of Artificial Intelligence Data Transparency via Auditing, Certification, and Safe Harbor Regimes. *Fordham Urban Law Journal,* v. 46, n. 2, p. 428-486, 2019.

produzir uma gama de detalhes de avaliação, abrangendo essas três categorias (regulamentação, gestão de risco e avaliação ética geral)[53].

Em se tratando de algoritmos de automação decisória, essas informações compreendem ao menos três categorias[54].

A primeira categoria consiste no registro de todos os dados abstratos que são levados em consideração pelo algoritmo (*inputs* e dados estatísticos abstratamente utilizados). É importante saber a natureza dos dados de entrada, como eles são colhidos e como são colocados em ação. A título exemplificativo, em uma ferramenta voltada à classificação de usuários de serviços públicos em ordem prioritária, é necessário saber quais dados são levados em consideração (estatísticas relativas à idade, enfermidade, renda etc.). De igual modo, em se tratando de ferramenta voltada à análise da periculosidade de investigados ou réus em processos criminais, para fins de prisão preventiva, é importante saber que tipo de dado é utilizado (estatísticas relativas a reincidência, circunstâncias do crime etc.).

A segunda categoria consiste nas informações específicas utilizadas numa decisão concreta (*inputs* concretamente utilizados). No segundo exemplo utilizado acima, seria o caso de ser utilizado o histórico prisional de um determinado réu.

A terceira categoria consiste na regra do algoritmo. É necessário ter, em registro, toda a cadeia lógica e matemática utilizada para, mediante processamento dos dados de entrada (*inputs*) ser produzido o resultado (*output*). Essa terceira categoria informacional é particularmente potencializada no âmbito público, por decorrência do princípio do devido processo legal. Uma forma de "armazenar" um algoritmo consiste no registro da cadeia completa de códigos utilizada para a sua implementação. Embora normalmente seja bastante difícil para alguém compreender as

53. BROWN, Shea; DAVIDOVIC, Jovana; HASAN, Ali. The algorithm audit: Scoring the algorithms that score us. Big Data & Society, vol. 8, no. 1, 2021.

54. VILLASENOR, John; FOGGO, Virginia. Artificial Intelligence, Due Process and Criminal Sentencing. *Michigan State Law Review,* v. 295, 2020, p. 339-340.

linhas de programação, esse registro possibilita o controle por agências independentes. Além, disso, é possível a utilização de *pseudocode,* comumente utilizado no campo da ciência da computação[55], de modo a registrar o os algoritmos de uma forma mais compreensível, mediante técnicas representativas[56].

Uma particular observação diz respeito aos estágios evolutivos dos algoritmos de *machine learnig*. Levando-se em consideração a sua capacidade de aprendizado e "mutação", uma forma segura de registro das informações consiste numa espécie de "captura de imagem" (*snapshot*) cada vez que o algoritmo é acionado, permitindo a sua testagem futura.

Além disso, não se desconhecem as dificuldades decorrentes da identificação das três categorias de informações mencionadas em determinados algoritmos de *machine learning,* especialmente quando empregadas técnicas de aprendizado não supervisionado[57]. Cada vez mais, os desenvolvedores de algoritmos de inteligência artificial são confrontados com a necessidade de compreender o que os seus modelos têm aprendido[58]. Em alguns campos, sobretudo quando utilizados modelos mais genéricos de *machine learning*, soluções eficientes têm sido apresentadas a exemplo do modelo

55. BBC BITESIZE. *Representing an algorithm: Pseudocode.* Disponível em: https://www.bbc.co.uk/bitesize/guides/zpp49j6/revision/2#:~:text=Writing%20in%20pseudocode%20is%20similar,pseudocode%2C%20INPUT%20asks%20a%20question. Acesso em: 24 out. 2020.

56. VILLASENOR, John; FOGGO, Virginia. Artificial Intelligence, Due Process and Criminal Sentencing. *Michigan State Law Review*, v. 295, 2020, p. 341.

57. Cf. Roldán, José Mena; Vila, Oriol Pujol; Marca, Jordi Vitrià. Dirichlet uncertainty wrappers for actionable algorithm accuracy accountability and auditability. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 2020, p. 581.

58. BÜCKER, Michael; SZEPANNEK, Gero; GOSIEWSKAC, Alicja; BIECEK, Przemyslaw. Transparency, auditability, and explainability of machine learning models in credit scoring. *Journal of the Operational Research Society,* p. 1-21, 2021. Disponível em: https://www.tandfonline.com/doi/full/10.1080/01605682.2021.1922098. Acesso em: 10 dez. 2021.

de *Transparency, Auditability and eXplainability for Credit Scoring* (TAX4CS)[59]. Em muitos outros, porém, tanto a auditabilidade quanto a transparência consistem em algo de difícil implementação. Em tais situações, a melhor solução parece ser a adoção dos princípios da precaução e da prevenção, evitando-se o uso de ferramentas demasiadamente opacas, pelo setor público ou privado, em áreas sensíveis ao exercício dos direitos fundamentais (ambientes de "alto risco").

Feitas essas considerações, resta o seguinte questionamento: quem deve guardar essas informações?

Uma primeira opção consiste em atribuir essa obrigação às empresas, órgãos ou instituições responsáveis pelo desenvolvimento da ferramenta. A vantagem está no reconhecimento de que aquele que desenvolveu o algoritmo é, presumidamente, quem detém maior conhecimento sobre o seu funcionamento. Consequentemente, também detém uma capacidade mais elevada de monitoramento e correção. Por outro lado, é possível que os dados a serem armazenados sensíveis, envolvendo a privacidade de muitas pessoas. Além disso, o desenvolvedor do produto é, presumidamente, o menos interessado em revelar eventuais falhas encontradas.

Uma segunda opção consiste em atribuir a responsabilidade pelo armazenamento de informações às pessoas ou órgãos responsáveis pela sua aplicação. Essa parece ser uma forma mais segura de preservar a segurança e a privacidade dos dados, permitindo-se ao desenvolvedor o seu acesso parcial apenas em situações específicas, mediante tráfego criptografado, para fins de auditabilidade.

59. BÜCKER, Michael; SZEPANNEK, Gero; GOSIEWSKAC, Alicja; BIECEK, Przemyslaw. Transparency, auditability, and explainability of machine learning models in credit scoring. Journal of the Operational Research Society, p. 1-21, 2021, p. 13. Sobre a auditabilidade de sistemas de armazenamento na nuvem, conferir: Tian, Hui; Chen, Zhaoyi; Chang, Chin-Chen; Kuribayashi, Minoru; Huang, Yongfeng; Cai, Yiqiao; Chen, Yonghong; Wang, Tian. Enabling Public Auditability for Operation Behaviors in Cloud Storage. *Soft Computing,* vol. 21, n. 8, p. 2175-2187, 2016.

4.5.3. Princípio da transparência e direito a explicações contrafactuais

Enquanto a auditabilidade diz respeito ao registro de informações, o princípio da transparência impõe que essas informações possam ser adequadamente acessadas e explicadas. Da transparência, extraem-se duas obrigações: acesso (publicidade) e explicação.

Exemplo de garantia de acesso é estabelecido no art. 43 do Código de Defesa do Consumidor, ao dispor que o consumidor "terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes". O seu § 2° acrescenta que "a abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele".

Atenta às garantias de acesso e transparência, dispõe a Lei Geral de Proteção de Dados brasileira (LGPD), em seu art. 6°, que as atividades de *tratamento* de dados pessoais deverão observar, entre outros, os seguintes princípios:

a) livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais (inciso IV);

b) 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 (inciso VI).

A atividade de tratamento é amplamente definida como

> [...] 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; [...]

Ainda quanto ao acesso, uma objeção comum consiste no argumento voltado à proteção do segredo industrial.

De acordo com desenvolvedores, o acesso amplo e ilimitado a algoritmos desenvolvidos por empresas pode colocá-las em situação de desvantagem econômica em relação aos seus competidores no mercado comum.

Por outro lado, a negativa de acesso em aos interessados pode representar uma grave violação ao princípio do devido processo legal. Basta imaginar o emprego de ferramentas de avaliação de risco utilizadas em processos criminais[60]. Desde a data de 1963, no célebre caso *Brady v. Maryland*, a Suprema Corte dos Estados Unidos fixou o entendimento no sentido de que um promotor não pode reter evidências "favoráveis a um acusado", sob pena de violação da cláusula do devido processo legal, previstas na 5ª e 14ª emendas[61]. A chamada doutrina *Brady*, portanto, impõe aos promotores o dever de tomar conhecimento e divulgar ao réu qualquer informação em sua posse que seja "favorável" e "relevante para a culpa ou punição, independentemente da boa ou má fé da acusação"[62].

De fato, como aponta Deborah Won, conquanto relevantes os interesses empresariais, os riscos para os réus criminais são muito grandes para priorizar as questões de propriedade intelectual em detrimento das proteções constitucionais[63]. Disso decorre a

60. VILLASENOR, John; FOGGO, Virginia. Artificial Intelligence, Due Process and Criminal Sentencing. *Michigan State Law Review*, v. 295, 2020, p. 343.
61. SUPREMA CORTE DOS ESTADOS UNIDOS. *Brady v. Maryland, 373 U.S. 83*, 1963.
62. WON, Deborah. The Missing Algorithm: Safeguarding The Missing Algorithm: Safeguarding Brady Against the Rise of Against the Rise of Trade Secrecy in Policing. *Michigan Law Review*, vol. 120, 157, 2021.
63. WON, Deborah. The Missing Algorithm: Safeguarding The Missing Algorithm: Safeguarding Brady Against the Rise of Against the Rise of Trade Secrecy in Policing. *Michigan Law Review*, vol. 120, 157, 2021.

preferência pela aquisição de sistemas de código aberto, como indicado no art. 24 da Resolução CNJ nº 332/2020[64].

Além disso, como forma de preservar minimamente o segredo industrial, algumas providências podem ser tomadas. Uma delas consiste no emprego de *protective orders,* bastante comuns em processos civis em que discutidas supostas violações de patentes. Em casos assim, assistentes técnicos dos autores podem ter acesso ao código-fonte de aplicações, bem como a outros dados secretos, mediante o emprego de técnicas protetivas e obrigações específicas. Um exemplo consiste na disponibilização do código em um único terminal informático sem acesso à internet, em uma sala dedicada e na presença de representantes do desenvolvedor[65].

Uma outra forma consiste na disponibilização de dados apenas a instituições de checagem certificadas e a órgãos e instituições públicas, impondo-se o dever de manutenção da confidencialidade.

Para além do acesso (publicidade), a segunda dimensão da transparência consiste no direito à explicação. Cuida-se de um desdobramento do *right to explanation*, registrado no considerando nº 71 do Regulamento (UE) 2016/679 (*General Data Protection Regulation*)[66]. Por se tratar de um considerando, o texto não pode ser considerado vinculante.

64. Resolução CNJ nº 332/2020: "Art. 24. Os modelos de Inteligência Artificial utilizarão preferencialmente software de código aberto que: I – facilite sua integração ou interoperabilidade entre os sistemas utilizados pelos órgãos do Poder Judiciário; II – possibilite um ambiente de desenvolvimento colaborativo; III – permita maior transparência; IV – proporcione cooperação entre outros segmentos e áreas do setor público e a sociedade civil".

65. VILLASENOR, John; FOGGO, Virginia. Artificial Intelligence, Due Process and Criminal Sentencing. *Michigan State Law Review*, v. 295, 2020, p. 344.

66. "(71) O titular dos dados deverá ter o direito de não ficar sujeito a uma decisão, que poderá incluir uma medida, que avalie aspetos pessoais que lhe digam respeito, que se baseie exclusivamente no tratamento automatizado e que produza efeitos jurídicos que lhe digam respeito ou o afetem significativamente de modo similar, como a recusa automática de um pedido de crédito por via eletrónica ou práticas de recrutamento eletrónico sem qualquer intervenção humana. [...] *Em qualquer dos casos, tal tratamento deverá ser acompanhado das garantias adequadas, que deverão incluir a informação específica ao titular dos dados e o direito de obter a intervenção humana, de manifestar o seu ponto de vista, de obter uma explicação sobre a decisão tomada na sequência dessa avaliação e de contestar a decisão. Essa medida não deverá dizer respeito a uma criança*" (PARLAMENTO EUROPEU E CONSELHO DA UNIÃO EUROPEIA. *Regulamento (UE) 2016/679*. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso: 18 out. 2020, grifos aditados).

É importante notar que, conquanto o art. 22 do GDPR, ao disciplinar as decisões individuais tomadas "exclusivamente com base no tratamento automatizado", não tenha mencionado o direito à explicação, o seu art. 15 assegura ao titular de dados, em caso de decisões automatizadas, o direito de *acesso* a "informações úteis relativas à lógica subjacente, bem como a importância e as consequências previstas de tal tratamento para o titular dos dados".

Existe, portanto, bastante controvérsia quanto ao alcance do direito à explicação, especialmente no âmbito das relações privadas. Mesmo o considerando nº 71 do GDPR, única parte do documento que menciona explicitamente a necessidade de explicações, não é claro quanto aos escopos e conteúdo das explicações. Para alguns autores, ao que tudo indica, a lógica do GDPR é a de que "as explicações podem ser voluntariamente apresentadas após a tomada das decisões, e não são consideradas condição para a impugnação decisória"[67].

Influenciada pela legislação europeia, o art. 20 da LGPD brasileira, com redação dada pela Lei nº 13.853/2019, dispõe que o titular dos dados tem direito a solicitar a revisão de decisões tomadas "unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade".

67. WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology*, vol. 31, p. 841-888, 2018, p. 880.

O seu § 1º esclarece que o controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. Em caso de não oferecimento de informações de que trata o § 1º baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais (§ 2º).

Assim como o Regulamento (UE) 2016/679 (GDPR), a legislação brasileira peca ao reconhecer o direito apenas nas hipóteses de decisões tomadas "unicamente com base em tratamento automatizado". O texto legal parece excluir, forma injustificada, o direito de explicação para os casos em que a decisão é tomada parcialmente com base em tratamento automatizado de dados.

Também não há clareza quanto à forma de prestação das informações, valendo-se o legislador de expressões genéricas ("informações claras e adequadas").

Por fim, nem a legislação brasileira nem a europeia parecem fazer uma conexão entre o direito de impugnação e os mecanismos de transparência, notificação e direito de acesso.

Firmadas essas premissas, compreendemos que a concretização do direito à explicação demanda duas especiais observações, extraídas da cláusula do devido processo legal.

Inicialmente, o cumprimento do dever não deve ser confundido com a mera disponibilização do código-fonte. Como registram Kroll *et al.*, uma solução ingênua para a verificação da regularidade procedimental consiste em demandar transparência do código-fonte, bem como dos *inputs* e *outputs* para relevantes decisões[68]. A publicidade, por si só, não é suficiente para promover

68. KROLL, Joshua A.; HUEY, Joanna; BAROCAS, Solon; FELTEN, Edward W.; REIDENBERG, Joel R.; ROBINSON, David G.; YU, Harlan. Accountable algorithms. *University of Pennsylvania Law Review*, v. 165, n. 3, p. 633-706, 2017, p. 657.

accountability, sobretudo porque não explica o porquê de uma determinada decisão ter sido tomada. Para que se atinja esse benefício, a instituição ou órgão que utiliza determinado algoritmo deve fornecer uma explicação mínima sobre o seu funcionamento numa determinada situação concreta, em extensão suficiente a permitir o exercício do direito de defesa.

A segunda, e talvez mais importante observação, diz respeito à forma de concretização. Não é incomum a apresentação de objeções à explicabilidade de um sistema decisório, com fundamento na impossibilidade técnica, elevado custo ou sigilo industrial[69].

Um ponto que parece negligenciado, porém, é que a pessoa que busca explicações dificilmente estará interessada em compreender e forma como um sistema de algoritmos funciona. É possível satisfazer esse princípio sem que se abra a "caixa-preta", partindo-se do pressuposto de que as explicações devem ser concebidas como um meio que permita ao indivíduo a possibilidade *de agir*, mais do que de *entender*[70].

Resumidamente, as explicações servem a três grandes propósitos: a) informar e ajudar as pessoas a compreenderem o porquê de uma decisão ter sido tomada; b) prover elementos que permitam a impugnação da decisão; c) permitir ao destinatário da decisão que compreenda o que deve ser mudado para que a decisão seja proferida da forma desejada. Embora nem a LGPD brasileira nem a GDPR europeia disciplinem o tema de forma a

69. WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology*, vol. 31, p. 841-888, 2018.

70. Essa importantíssima abordagem foi apresentada, de forma pioneira por Wachter, Mittelstadt e Russel: "Looking at explanations as a means to help a data subject act rather than merely understand, one could gauge the scope and content of explanations according to the specific goal or action they are intended to support." (WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology*, vol. 31, p. 841-888, 2018, p. 843).

permitir que se atinjam adequadamente esses objetivos, a garantia em questão há de ser extraída do princípio do devido processo legal e do direito de impugnação.

Essa garantia pode ser compreendida como o *direito a explicações contrafactuais,* que poderá ser exercido diante de decisões positivas ou negativas, parcialmente ou totalmente automatizadas. Essa abordagem é capaz de, a um só tempo, realizar o devido processo legal e estabelecer um ponto de encontro entre os interesses dos titulares dos dados pessoais e dos controladores de dados[71].

Conforme o Stanford Encyclopedia of Philosophy, *contrafactuais* são formas de discursos modais que dizem respeito às maneiras alternativas pelas quais as coisas poderiam ter sido. Trata-se de afirmar o que não é verdade, mas poderia ter sido se algo tivesse sido feito. No campo da filosofia, sentenças dessa natureza podem ser apresentadas da seguinte maneira: "se as potências coloniais não tivessem invadido, as Américas seriam muito diferentes"[72].

Aplicando-se ao campo das decisões automatizadas, imagine-se uma situação em que foi negado um pedido de concessão de empréstimo a uma determinada pessoa, com fundamento em seus dados pessoais. Uma explicação contrafactual poderia ser apresentada da seguinte forma: "você não conseguiu o empréstimo porque sua renda anual é de R$ 90.000,00 ao ano. Se você tivesse uma renda anual de R$100.000,00, teria conseguido o empréstimo".

Explicações contrafactuais podem prover: a) as razões pelas quais a decisão em particular foi proferida (ex.: baixo nível de

71. WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology*, vol. 31, p. 841-888, 2018, p. 844.

72. STANFORD ENCYCLOPEDIA OF PHILOSOPHY. *Counterfactuals*. Disponível em: https://plato.stanford.edu/entries/counterfactuals/#WhatCoun. Acesso em: 21 out. 2021.

renda); b) razões para permitir a impugnação da decisão (se, por exemplo, o sistema utilizou dados imprecisos a respeito da renda do interessado); e c) informações sobre como obter uma futura decisão favorável (ex.: um aumento de R$ 10.000,00/ano resultaria uma decisão favorável)[73]. Elas não objetivam esclarecer a lógica interna da caixa-preta de um algoritmo. Elas não buscam saber como uma decisão é produzida internamente, mas sim expor quais fatos externos deveriam ser diferentes para que a decisão desejada fosse proferida. Disso resulta uma forma simples de balancear transparência, explicabilidade e *accountability* com outros interesses, a exemplo do sigilo industrial. Além, explicações dessa natureza podem fornecer evidências de que um determinado algoritmo utiliza uma variável que pode ser considerada discriminatória (ex.: raça ou gênero).

Finalmente, explicações contrafactuais são tecnicamente mais facilmente empregadas em sistemas computacionais, especialmente em redes neurais. A transitoriedade dos modelos de tomada de decisão sugere que os algoritmos contrafactuais precisam ser computados automaticamente no momento em que uma decisão é tomada ou computados posteriormente com base em um arquivo cópia do modelo[74].

Na medida em que não se ocupam em relevar o código fonte do algoritmo, as explicações contrafactuais, porquanto necessárias ao exercício do direito de defesa, podem ser compreendidas como uma garantia explicatória mínima, extraída da cláusula geral do devido processo legal.

73. O exemplo é uma adaptação de Wachter, Mittelstadt e Russel. Cf. WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology*, vol. 31, p. 841-888, 2018, p. 882.

74. WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology*, vol. 31, p. 841-888, 2018, p. 881.

4.5.4. Princípio da consistência ou regularidade procedimental

Pelo princípio da consistência ou regularidade procedimental, é necessário assegurar que a cada destinatário ou usuário de uma determinada ferramenta construída a partir de algoritmos seja aplicado o mesmo *procedimento*, bem como que esse procedimento não tenha sido desenvolvido de forma que cause desvantagens a alguém em particular[75].

Cuida-se de uma decorrência não apenas do devido processo legal, mas também do princípio da isonomia. Além disso, para que seja realizado, o princípio da consistência depende da prévia auditabilidade do sistema. O mais importante aqui é o exame dos *inputs* e *outputs,* o que afasta as preocupações relativas à proteção de segredos industriais, próprias do princípio da transparência. Embora exista uma relação próxima com a "justiça" do algoritmo, o escopo da consistência é mais restrito.

A regularidade procedimental deve conduzir à consistência dos *outputs,* evitando que *inputs* similares produzam resultados discrepantes. Um exemplo é fornecido por Villasenor e Foggo: considerem-se dois diferentes réus com perfis idênticos quanto aos *inputs* específicos submetidos a um mesmo algoritmo de avaliação de risco. O primeiro é avaliado em março, o segundo em outubro. Embora seja possível a apresentação de resultados diversos em razão de melhoras na acurácia do algoritmo de inteligência artificial, aos réus que, numa visão retrospectiva, foram avaliados de forma mais severa, deve ser dada a possibilidade de conhecimento e de busca de correção[76].

Em uma ferramenta desprovida de algoritmos de inteligência artificial, *inputs* idênticos ou similares implicariam sempre o mesmo

75. KROLL, Joshua A.; HUEY, Joanna; BAROCAS, Solon; FELTEN, Edward W.; REIDENBERG, Joel R.; ROBINSON, David G.; YU, Harlan. Accountable algorithms. *University of Pennsylvania Law Review*, v. 165, n. 3, p. 633-706, 2017, p. 656.

76. VILLASENOR, John; FOGGO, Virginia. Artificial Intelligence, Due Process and Criminal Sentencing. *Michigan State Law Review*, v. 295, 2020, p. 343.

resultado. Com inteligência artificial, por outro lado, as técnicas de *machine learning* podem ensejar a "evolução" do algoritmo. Isso não significa que, em qualquer mudança algorítmica, todos os casos anteriores tenham que ser individualmente verificados, na medida em que essa forma de proceder poderia resultar na impraticabilidade do emprego da ferramenta. Em verdade, essa checagem pode ser feita também de forma automatizada – igualmente por meio de algoritmos auditáveis – e em casos de mudanças sensíveis proporcionadas pela inteligência artificial.

A consistência algorítmica é algo que pode ser avaliado por algoritmos de checagens. Ao invés de um ser humano realizar a checagem procedimental de cada caso, é possível que sistemas sejam desenvolvida para isso, reforçando a segurança de forma automatizada. Kroll *et al.* registram que o atual estágio tecnológico da ciência da computação contempla ferramentas capazes de avaliar a regularidade procedimental, incorporando-se no desenho dos sistemas. De forma específica, essas ferramentas podem assegurar que: a) a mesma disciplina foi utilizada na construção de cada decisão; b) a disciplina foi integralmente especificada antes de os sujeitos envolvidos serem conhecidos, reduzindo-se a possibilidade de desenvolvimento de um procedimento em desfavor de alguém em particular; c) cada decisão é o produto das regras e dos *inputs* aplicados; d) se a decisão requer *inputs* randômicos, a sua escolha ocorreu para além do interesse de qualquer pessoa[77].

4.5.5. Princípio do controle social

O uso de tecnologias de automação decisória pelo Estado demanda algo além das garantias de transparência e auditabilidade. Trata-se do controle social, que permite a participação da sociedade

77. KROLL, Joshua A.; HUEY, Joanna; BAROCAS, Solon; FELTEN, Edward W.; REIDENBERG, Joel R.; ROBINSON, David G.; YU, Harlan. Accountable algorithms. *University of Pennsylvania Law Review*, v. 165, n. 3, p. 633-706, 2017, p. 657.

não apenas na fiscalização da aplicação dos recursos públicos, mas também na formulação, acompanhamento da implementação e testagens de políticas. Um controle social adequado contribui para o legítimo exercício do poder estatal[78].

No campo da automação tecnológica, uma importante medida de implementação do controle social consiste na divulgação do código-fonte dos *softwares* utilizados ao público[79]. Uma opção a ser avaliada consiste na utilização de sistemas de código aberto[80], com exceção daqueles cuja transparência possa comprometer a segurança pública (a exemplo dos sistemas de *no-fly*). Essas medidas revelam uma dimensão procedimental do devido processo digital capaz de facilitar a correção de erros em ferramentas decisórias.

Para além disso, uma medida a ser considerada é o estabelecimento de uma rígida rotina de testagem de *softwares* antes da sua implantação, com participação da sociedade civil. Cuida-se de prática já realizada pelo Tribunal Superior Eleitoral brasileiro, cuja Resolução nº 23.444/2015 dispõe sobre a realização periódica do Teste Público de Segurança (TPS) nos sistemas eleitorais[81]. Os testes públicos disciplinados no referido ato normativo decorrem do comando do art. 66, *caput,* da Lei nº 9.504/1997, ao estabelecer que os partidos e coligações poderão fiscalizar todas as fases

78. Sobre o tema, conferir: BARCELLOS, Ana Paula de. Um debate para o neoconstitucionalismo. Papeis do Direito Constitucional no fomento do controle social democrático: algumas propostas sobre o tema da informação. *Revista de Direito do Estado*, Rio de Janeiro, n. 12, 2008.

79. CITRON, Danielle Keats. Technological Due Process. *Washington University Law Review*, vol. 85, n. 1249, 2008, p. 1.308.

80. Lee, Jyh-An. New Perspectives on Public Goods Production: Policy Implications of Open Source Software. *Vanderbilt Journal of Entertainment and Technology Law*, vol. 9, n. 1, 2006. Conferir também: KARAVAS, Vagias; TEUBNER, Gunther. Www.CompanyNameSucks.Com: The Horizontal Effect of Fundamental Rights on "Private Parties" Within Autonomous Internet Law. *Constellations*, vol. 12, p. 262–282, 2005, p. 270.

81. Cf. https://www.justicaeleitoral.jus.br/tps/. Acesso em: 30 nov. 2021.

do processo de votação e apuração das eleições e o processamento eletrônico da totalização dos resultados.

O art. 3º da Resolução TSE nº 23.444/2015 estabelece que o TPS "tem por objetivo fortalecer a confiabilidade, a transparência e a segurança da captação e da apuração dos votos e propiciar melhorias no processo eleitoral". Por seu turno, o seu parágrafo único dispõe que o teste "contempla ações controladas com o objetivo de identificar vulnerabilidades e falhas relacionadas à violação da integridade ou do anonimato dos votos de uma eleição".

A testagem de softwares utilizados na implementação de políticas públicas, funções jurisdicionais e outras atividades preditivas exige uma rígida e obrigatória rotina. Como sugere Citron, as agências estatais devem manter suítes de teste que executem cenários hipotéticos esperados e inesperados projetados por especialistas em políticas independentes por meio de sistemas de decisão para expor políticas distorcidas. Além disso, protocolos de teste devem ser executados antes do lançamento de um sistema, durante a implementação e sempre que as políticas forem alteradas. Os regulamentos de contratações públicas podem exigir que os contratos especifiquem que os sistemas de decisão sejam aprovados nos conjuntos de testes antes que os estados possam aceitar os sistemas dos fornecedores[82].

Finalmente, um importante modelo de controle social é aquele comumente estabelecido em alguns países, por meio de comitês de reformas integrados por representantes da sociedade civil[83], inclusive com poderes decisórios. No Brasil, um exemplo de órgão consultivo e deliberativo misto é o Conselho Nacional do Meio Ambiente – CONAMA, instituído pela Lei nº 6.938/1981, que dispõe sobre a Política Nacional do Meio Ambiente. Órgãos

82. CITRON, Danielle Keats. Technological Due Process. *Washington University Law Review*, vol. 85, n. 1249, 2008, p. 1.311.

83. DILLER, Matthew. The Revolution in Welfare Administration: Rules, Discretion, and Entrepreneurial Government. *New York University Law Review*, vol. 75, 2000, p. 1213.

semelhantes poderiam ser criados com o objetivo específico de supervisionar a estratégia de automação decisória implementada em cada ente federativo.

4.5.6. Princípio da precaução

As práticas discriminatórias que podem resultar das tecnologias de automação, algumas expostas nos tópicos anteriores, proporcionam novos e grandes desafios. Isso porque, diferentemente das formas discriminatórias tradicionais, as discriminações por ferramentas de automação decisória costumam ser mais contraintuitivas e silenciosas. Consequentemente, como apontam Wachter *et. al*, são mais difíceis de serem detectadas, na medida em que, em muitos casos, as vítimas sequer sabem que foram ou estão sendo abusivamente discriminadas[84]. É o caso das ferramentas de direcionamento publicitário *online*, em que as vítimas dificilmente serão capazes de identificar a existência de um preço "personalizado" discriminatório ou até mesmo a omissão na exibição de um produto ou serviço[85]. Do mesmo modo, os vieses existentes em ferramentas de contratação são raramente identificados por candidatos aos postos de trabalho, que sequer conhecem o funcionamento dos algoritmos decisórios.

Essas características podem conduzir a um cenário distópico, em que, por um lado, as "sensações" quanto à existência de práticas discriminatórias tendem a diminuir, ao passo em que tais práticas crescem exponencialmente.

84. WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Why Fairness Cannot be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI. *Computer Law and Security Review,* vol. 41, 2021, p. 2.

85. WACHTER, Sandra. Affinity Profiling and Discrimination by Association in Online Behavioural Advertising. Berkeley Technology Law Journal, vol. 35, 2020 Disponível em: https://pa-pers.ssrn.com/abstract=3388639. Acesso em: 8 dez. 2021.

4.5.6.1. O Direito da antidiscriminação e a discriminação indireta proporcionada por ferramentas de automação

O Direito da Antidiscriminação pode ser concebido como a área do conhecimento e da prática jurídica que tem por objetivo o estudo e a aplicação das "normas, institutos, conceitos e princípios relativos ao direito de igualdade como mandamento proibitivo de discriminação, aí incluídos os instrumentos normativos, nacionais e internacionais"[86].

A partir da leitura dos instrumentos internacionais de proteção dos direitos humanos, sobretudo a Convenção Internacional da ONU sobre a Eliminação de todas as Formas de Discriminação Racial (1965), a Convenção da ONU sobre a Eliminação de todas as Formas de Discriminação contra a Mulher (1979) e a Convenção da ONU sobre os Direitos das Pessoas com Deficiência (2006), diplomas incorporados ao ordenamento jurídico brasileiro, podemos compreender a discriminação como "qualquer distinção, exclusão, restrição ou preferência que tenha o propósito ou o feito de anular ou prejudicar o reconhecimento, gozo ou exercício em pé de igualdade de direitos humanos e liberdades fundamentais nos campos econômico, social, cultural ou em qualquer campo da vida pública"[87].

Esse conceito geral pode ser agregado às manifestações específicas de discriminação, tais como: religião, raça e etnia, gênero, orientação sexual, deficiência e idade. Disso decorrem as discriminações religiosa, racial, sexual etc., que têm origem em fenômenos ou ideologias mais profundas, como o racismo, a intolerância religiosa, o sexismo e a LGBTQIA+fobia. Exemplo

86. RIOS, Roger Raupp; SILVA, Rodrigo da. Discriminação múltipla e discriminação interseccional. *Revista Brasileira de Ciência Política*, vol. 16, p. 11-37, 2015.

87. RIOS, Roger Raupp; SILVA, Rodrigo da. Discriminação múltipla e discriminação interseccional: aportes do feminismo negro e do direito da antidiscriminação. Dossiê Feminismo e Antirracismo. *Revista Brasileira de Ciência Política*, v. 16, 2015.

de um dispositivo que proíbe amplamente múltiplas formas de discriminação é a Carta dos Direitos Fundamentais da União Europeia, cujo art. 21 dispõe:

> Artigo 21.º – Não discriminação
>
> 1. É proibida a discriminação em razão, designadamente, do sexo, raça, cor ou origem étnica ou social, características genéticas, língua, religião ou convicções, opiniões políticas ou outras, pertença a uma minoria nacional, riqueza, nascimento, deficiência, idade ou orientação sexual.
>
> 2. No âmbito de aplicação dos Tratados e sem prejuízo das suas disposições específicas, é proibida toda a discriminação em razão da nacionalidade.

Os conceitos de discriminação direta e indireta encontram sólida fundamentação doutrinária e normativa. O tema é expressamente disciplinado na Diretiva nº 2000/43/CE do Conselho da União Europeia, de 29 de junho de 2000. A Diretiva tem por objetivo estabelecer um quadro jurídico para o combate à discriminação baseada em motivos de origem racial ou étnica, objetivando colocar em prática nos Estados-Membros o princípio da igualdade de tratamento.

Tomando por empréstimo o seu texto, podemos fazer a seguinte classificação:

a) considera-se que existe discriminação direta sempre que, em razão de fatores discriminatórios de qualquer origem (racial ou étnica, gênero, idade, opção sexual etc.), uma pessoa seja objeto de tratamento menos favorável que aquele que é, tenha sido ou possa vir a ser dado a outra pessoa em situação comparável;

b) considera-se que existe discriminação indireta sempre que uma disposição, critério ou prática aparentemente neutra coloque pessoas numa situação de desvantagem comparativamente com outras pessoas, a não ser que essa disposição, critério ou prática seja objetivamente justificada por um critério legítimo e que os meios utilizados para o alcançar sejam adequados e necessários.

A discriminação indireta, reconhecida pela jurisprudência do Tribunal de Justiça da União Europeia quanto pelo Supremo Tribunal Federal brasileiro, tem origem na chamada teoria do impacto desproporcional, denominada disparate impact pela jurisprudência da Suprema Corte dos Estados Unidos.

No caso Griggs v. Duke Powers Co, a Corte fixou precedente no sentido de que, "mesmo que não haja intenção discriminatória, um empregador não pode usar um requisito de trabalho que exclui funcionalmente membros de uma determinada raça, se não tiver relação com a medição do desempenho das funções do trabalho. Os procedimentos de teste ou medição não podem ser determinantes nas decisões de emprego, a menos que tenham alguma conexão com o trabalho"[88].

O caso dizia respeito a um requisito imposto por um empregador, ao exigir que os interessados a postos de trabalho tivessem um diploma escolar ou passassem em um teste de aptidão ("intelligence test"). Esses testes não eram relacionados à aptidão para um posto de trabalho específico (ou seja, não tinham nenhuma relação com as funções a serem desempenhadas), mas eram permitidos pelo Civil Rights Act, "desde que não utilizados com o propósito de discriminação".

De acordo com a Suprema Corte dos Estados Unidos, a exigência laboral impediu um número elevado de afro-americanos de serem contratados, em razão da sua vulnerabilidade social. Registrou ainda que os testes de aptidão não tinham correlação com uma função específica desempenhada na empresa. Assim, concluiu que ações aparentemente neutras – como os testes, direcionados a toda e qualquer pessoa, independentemente da etnia – podem gerar impactos desproporcionais (disparate impact). Este caso mostrou que a discriminação pode ser encontrada não apenas em condutas com um propósito abertamente discriminatório,

88. SUPREMA CORTE DOS ESTADOS UNIDOS, *Griggs v. Duke Power Co.*, 401 U.S. 424, 1971.

mas também em condutas aparentemente neutras que causam impactos desproporcionais sobre determinados grupos de pessoas.

Esse tipo de discriminação (indireta) pode decorrer não apenas de processos irracionais inconscientes[89], mas também por intermédio de tecnologias de automação, a exemplo do uso de inteligência artificial na contratação de trabalhadores, no monitoramento policial por data mining, data matching ou reconhecimento facial, na concessão de benefícios assistenciais, no direcionamento publicitário e na moderação de conteúdo em redes sociais.

Daí decorrem duas importantes questões. A primeira delas consiste em saber como é possível evitar práticas discriminatórias abusivas causadas por novas tecnologias, a exemplo dos algoritmos de machine learning. A segunda consiste em saber se é possível a automatização do processo decisório para fins de identificação de práticas discriminatórias.

4.5.6.2. A impossibilidade de delegação do processo decisório e a necessidade de utilização de procedimentos consistentes na identificação de práticas abusivas

No julgamento da ADI 1.946 – DF, o STF apreciou importante caso relativo a possível prática discriminatória indireta. A questão principal dizia respeito à constitucionalidade da regra do art. 14 da EC nº 20/98, que limitava os valores pagos pela Previdência a título de licença-maternidade a R$ 1.200,00, por mês, ficando o restante a cargo do empregador. Conforme voto proferido pelo Ministro Sydney Sanches, a regra estimularia a opção pelo trabalhador masculino, em lugar da mulher trabalhadora. O Tribunal, por unanimidade, julgou parcialmente procedente o pedido formulado na inicial da ação para dar ao artigo 14 da EC nº 20/98, sem redução de texto, interpretação conforme a Constituição Federal, para excluir sua aplicação ao salário da licença à gestante a que se refere o artigo 7º, inciso XVIII.

89. JAKUTIS, Paulo. *Manual de estudo da discriminação no trabalho*. São Paulo: LTr, 2006, p. 33.

Casos como esse permitem aos tribunais uma análise detalhada de todas as circunstâncias envolvidas, de modo a decidir sobre a existência de uma prática discriminatória. Trata-se da possibilidade que o Poder Judiciário tem de "decompor esses grandes sistemas em componentes isolados", e então "avaliar se cada política satisfaz a legislação antidiscriminação"[90]. Essa atividade se torna bastante complexa em ferramentas algorítmicas, em razão das dificuldades de obtenção de dados estatísticos necessários para uma decisão justa[91], o que reforça a importância das garantias procedimentais de auditabilidade e transparência.

Na jurisprudência da CJUE, a análise de uma suposta prática discriminatória, a fim de se decidir acerca da sua abusividade, depende da identificação de um grupo negativamente afetado pela medida, um grupo comparativo e a evidência de uma desvantagem particularmente sofrida[92]. Para tanto, destaca-se o papel das evidências estatísticas[93].

Além disso, o reconhecimento de práticas discriminatórias por órgãos jurisdicionais parte de uma análise de um campo normativo bastante contextual e flexível que é o direito da antidiscriminação. Apenas uma análise caso a caso permite a identificação de uma prática discriminatória abusiva, sobretudo

90. WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Why Fairness Cannot be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI. *Computer Law and Security Review*, vol. 41, 2021, p. 6.

91. MAKKONEN, Timo. *Measuring Discrimination*: Data collection and EU Equality Law: Thematic Report of the Group of Independent Experts. Brussels: European Commission, 2007.

92. MAKKONEN, Timo. *Measuring Discrimination*: Data collection and EU Equality Law: Thematic Report of the Group of Independent Experts. Brussels: European Commission, 2007, p. 36.

93. TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. *Regina v Secretary of State for Employment, ex parte Nicole Sey-mour-Smith and Laura Perez, Case C-167/97*, 1999 E.C.R. I–60.

em contextos mais sutis e de pouca visibilidade, notadamente em zonas de tensão entre direitos fundamentais[94].

Em verdade, como apontam Wachter *et al.*, a legislação e a jurisprudência dos tribunais concebem as noções de justiça e discriminação como conceitos fundamentalmente contextuais[95]. Consequentemente, com o objetivo de evitar a inadequada solução de questões essenciais no contexto do direito da antidiscriminação, o processo decisório não pode ser automatizado. No atual contexto jurídico e tecnológico, não apenas o Poder Judiciário e os reguladores detêm a *capacidade* de responder a essas questões normativas de "igualdade contextual"[96], como também são os únicos legitimados a fazê-lo[97]. Cuida-se não apenas de decorrência do princípio da precaução, que tem por objetivo evitar práticas danosas em ambientes de incerteza quanto ao resultado danoso,

94. Cf. BICKEL, P. J.; HAMMEL, E. A.; O'CONNELL, J. W. Sex Bias in Graduate Admissions: Data from Berkeley. *Science*, vol. 187, p. 398-404, 1975.

95. WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Why Fairness Cannot be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI. *Computer Law and Security Review*, vol. 41, 2021, p. 28.

96. O tema é objeto de considerando da Resolução nº 405 – P9_TA(2021)0405, do Parlamento da União Europeia: "B. Considerando que, não obstante os progressos contínuos a nível da velocidade de processamento e da capacidade de memória, não existem ainda programas capazes de igualar a flexibilidade humana no que se refere a domínios mais amplos ou a tarefas que exijam a compreensão do contexto ou uma análise crítica; considerando que algumas aplicações de IA alcançaram, na execução de determinadas tarefas específicas (por exemplo, tecnologias jurídicas), níveis de desempenho semelhantes aos de peritos e profissionais humanos, sendo capazes de gerar resultados a uma velocidade excecionalmente elevada e a uma escala muito mais vasta [...]" (Cf. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_PT.html. Acesso em: 18 nov. 2021).

97. WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Why Fairness Cannot be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI. *Computer Law and Security Review*, vol. 41, 2021, p. 256. Conferir também: Rosenfeld, Michel. The rule of law and the legitimacy of constitutional democracy. *Southern California law review*, vol. 74, n. 5, p. 1307-1351, 2001.

mas também do pressuposto liberal da capacidade de responsabilização dos julgadores[98].

Essa conclusão não implica a exclusão a participação da comunidade tecnológica do processo decisório. Pelo contrário, ela tem uma importante tarefa de fornecer as evidências estatísticas necessárias ao processo decisório, além do desenvolvimento de ferramentas consistentes que sejam capazes de auxiliar na detecção e mensuração de vieses, ainda que incapazes de decidir ao seu respeito. Partindo-se da premissa de que a discriminação algorítmica é mais facilmente detectada a partir de evidências estatísticas, em lugar de conceber a noção de "justiça" como algo a ser alcançado pelas máquinas, a comunidade tecnológica há de se concentrar na importante tarefa colaborativa no campo probatório. Embora sistemas não devam ser desenvolvidos para avaliar e corrigir, de forma automática e independente, práticas discriminatórias, eles podem ser desenhados com a missão de assegurar a produção das evidências necessárias para uma decisão bem informada, a cargo do legislador e do Poder Judiciário, preferencialmente de forma preventiva[99]. Exemplo disso é o desenvolvimento de ferramentas

98. PASQUALE, Frank. Inalienable Due Process in an Age of AI: Limiting the Contractual Creep toward Automated Adjudication. In MICKLITZ, H.; POLLICINO, O.; REICHMAN; A.; SIMONCINI, A.; SARTOR, G.; DE GREGORIO, G. (Eds.), Constitutional Challenges in the Algorithmic Society (p. 42-56). Cambridge: Cambridge University Press, 2021, p. 46.

99. A conclusão é extraída de Wachter et al.: "Rather than viewing fairness as a problem to be solved through automation or technical fixes alone, the technical community should embrace the challenge as a starting point for collaborative investigation. Systems cannot and should not be designed to automatically detect, evaluate, and correct for discriminatory decision-making independent of local guidance and interpretation from the judiciary. Rather, what is required is an 'early warning system' for auto-mated discrimination. This can be achieved by designing systems to automatically or consistently produce the types of statistical evidence necessary for the judiciary to make well-informed normative decisions, and for system controllers to systematically detect potential discrimination before it occurs" (Wachter, Sandra; Mittelstadt, Brent; Russell, Chris. Why Fairness Cannot be Automated: Bridging the Gap Between EU

capazes de identificar a chamada "disparidade condicional demográfica" ("conditional demographic disparity" – CDD)[100] como um padrão mínimo para estatísticas em casos de não discriminação que abordam sistemas automatizados[101].

Ainda sob o princípio da precaução, uma outra importante medida pode ser exigida. Trata-se da vedação ao setor público de *delegar à automação*, ainda que parcialmente, políticas que não tenham sido submetidas a procedimentos formais ou informais de elaboração de regras, tais como regras interpretativas. Como aponta Citron, os programadores que codificam regras interpretativas e declarações de políticas públicas encontram-se afastados do processo democrático para justificar o risco significativo de distorção de política que a automatização implica[102]. Ainda que se trate de uma atividade exercida diretamente pelo Estado, a automação, ao exigir de um terceiro (programadores) a codificação de políticas estatais, acaba por equivaler (ou mesmo superar) uma delegação total da atividade a particulares.

4.6. A dimensão substantiva do devido processo legal digital

A dimensão substantiva do devido processo legal tem por objetivo proteger os indivíduos contra decisões arbitrárias, desproporcionais ou desarrazoadas nos ambientes marcados por uma relevante assimetria de poder.

Non-Discrimination Law and AI. *Computer Law and Security Review*, vol. 41, 2021, p. 21).

100. KAMIRAN, Faisal; ŽLIOBAITĖ, Indrė; CALDERS, Toon. Quantifying explainable discrimination and removing illegal discrimination in automated decision making. *Knowledge and Information Systems*, vol. 35, p. 613–644, 2013.

101. WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Why Fairness Cannot be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI. *Computer Law and Security Review*, vol. 41, 2021, p. 24.

102. CITRON, Danielle Keats. Technological Due Process. *Washington University Law Review*, vol. 85, n. 1249, 2008, p. 1.313-1.312.

Particularmente no contexto tecnológico, essa dimensão tem especial aplicação na tutela do direito à liberdade, cujo escopo foi ampliado pela tradição constitucional americana, para abranger direitos dele derivados. Exemplo disso é a preocupação da Suprema Corte dos Estados Unidos na proteção do direito à privacidade, concebido como a liberdade para alguém ser "deixado só" (*right to be let alone*)[103].

No caso *Griswold v. Connecticut* (1965), o *justice* Harlan, aderindo à maioria da corte, registrou que a cláusula do devido processo legal também protege o direito à privacidade contra interferências arbitrárias. Por seu turno, no caso *United States v. Jones* (2012), o *justice* Alito, ao integrar a maioria no resultado, deixou clara a necessidade de aplicação da Quarta Emenda a buscas e apreensões operadas através de novas tecnologias (à época, o GPS). Segundo seu voto, "ironicamente, o Tribunal decidiu decidir este caso com base em premissas jurídicas do século XVIII", havendo de ser adaptada a garantia do devido processo legal à nova realidade tecnológica[104].

Desse raciocínio histórico, pode ser extraída a tese de aplicação da cláusula do devido processo legal, em sua dimensão substantiva, não apenas em situações nas quais haja uma arbitrária ingerência do Estado sobre a privacidade das pessoas em geral. Como defendemos no presente trabalho, algumas garantias, ainda

103. "The protection guaranteed by the (Fourth and Fifth) amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the signifi cance of man's spiritual nature, of his feelings and of his intellect. Th ey knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men" (SUPREMA CORTE DOS ESTADOS UNIDOS. Olmstead v. United States, 277 U.S. 438, 1928).

104. SUPREMA CORTE DOS ESTADOS UNIDOS. *United States v. Jones*, 565 U.S. 400, 2012.

que mínimas, devem ser asseguradas também nas relações entre agentes particulares, observada a premissa da incidência indireta do *due process*. Essa incidência indireta permitirá a adequada interpretação das garantias do microssistema brasileiro de proteção de direitos cibernéticos, cujo núcleo é composto basicamente de três importantes diplomas: a) o Código de Defesa do Consumidor – CDC (Lei nº 8.078/1990); b) o Marco Civil da Internet – MCI (Lei nº 12.965/2014); e c) a Lei Geral de Proteção de Dados – LGPD (Lei nº 13.709/2018).

Nos tópicos seguintes, apresentaremos três garantias que merecem especial destaque.

4.6.1. Princípio da privacidade diferencial sobre dados e inferências

Como já referido, não apenas a coleta de dados sensíveis, mas também a aplicação e o compartilhamento de *inferências* sensíveis podem desencadear práticas lesivas à privacidade, bem como discriminatórias[105].

Uma característica comum dos sistemas de proteção a direitos cibernéticos consiste na preocupação com a tutela da privacidade. Seja na GDPR europeia, na LGPD ou no MCI brasileiros, a disciplina da proteção de dados pessoais tem, entre seus fundamentos, tanto o respeito à privacidade e a inviolabilidade da intimidade, da honra e da imagem quanto o desenvolvimento econômico e tecnológico e a inovação. A harmonização entre esses dois importantes valores (privacidade e desenvolvimento tecnológico) exige, no processo de interpretação das garantias legais, o emprego concreto de técnicas conciliatórias.

Um interessante evento, apresentado por Kearns e Roth, explica as dificuldades em lidar com os problemas relativos à

105. CRAWFORD, Kate; SCHULTZ, Jason. Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms. *Boston College Law Review*, vol 55, 2014, p. 98.

privacidade no campo do uso de dados pessoais. Na década de 1990, uma agência governamental no Estado de Massachussetts, nos Estados Unidos, decidiu ajudar pesquisadores acadêmicos, fornecendo uma série de informações relativas a pacientes hospitalares. Para evitar a divulgação de dados privados, foram excluídas informações que pudessem identificar diretamente os pacientes, a exemplo dos nomes, endereços, número de identidade etc. Por outro lado, foram fornecidas as datas de aniversário, o sexo e o CEP de cada um deles, em razão da utilidade na pesquisa estatística empregada. Embora o Governador do Estado, William Weld, tivesse assegurado aos seus eleitores que a exclusão de elementos identificadores explícitos dos pacientes seria suficiente para a proteção da privacidade, Latanya Sweeney, uma estudante de doutorado do MIT à época, provou o contrário. Sweeney foi capaz de revelar os registros médicos do próprio Governador, a partir do cruzamento dos dados fornecidos com bancos de dados de eleitores. Isso porque apenas seis pessoas compartilhavam a mesma data de aniversário do Governador, três dos quais eram homens. Apenas um deles vivia na área do CEP do Governador. Consequentemente, a combinação "anonimizada" dos dados de aniversário, sexo e CEP de William Weld eram únicas. Em verdade, como Sweeney comprovou, cerca de 87% da população dos Estados Unidos pode ser unicamente identificada a partir desses três elementos[106].

O "experimento" de Massaschussetts revelou algo preocupante: a identificabilidade das pessoas a partir de dados aparentemente anônimos. Esses dados incluem elementos aparentemente insignificantes, como "curtidas" em redes sociais e listas de filmes assistidos em plataformas de *streaming*.

Uma importante forma de mitigar violações à privacidade consiste no emprego do conceito de "privacidade diferencial", consistente numa técnica que tem como objetivo "anonimizar

106. KEARNS, Michael; ROTH, Aaron. *The ethical algorithm*. Oxford: Oxford Press, 2020, p. 22-23.

dados pessoais ao adicionar ruídos no conjunto de dados de modo que se possam gerar informações úteis com o conjunto ao mesmo tempo em que inibe a identificação do titular do dado"[107]. Esses ruídos são gerados por algoritmos de randomização, capazes de inserir informações estatisticamente pouco irrelevantes, de modo a impedir a engenharia reversa de identificação das pessoas cujos dados são analisados.

Algoritmos de randomização podem ser particularmente úteis na coleta e tratamento de dados sensíveis. Basta imaginar uma pesquisa que tente saber o percentual de uma determinada população que é infiel ao seu cônjuge. Naturalmente, as pessoas não se sentirão encorajadas a fornecer essa resposta sem alguma segurança. Uma alternativa consiste no emprego da seguinte técnica algorítmica: pedir a cada participante que, inicialmente, jogue uma moeda, sem dizer ao entrevistador qual foi a face voltada para cima. Se a face for "cara", o(a) candidato(a) deve dizer, honestamente, se já traiu o seu cônjuge. Se for "coroa", a resposta deve ser aleatória. Em seguida, a mesma pessoa deve jogar novamente a moeda e dizer "sim" se caiu "cara" e "não", se "coroa". Como resultado escalado, em três quartos dos casos, as pessoas terão dito a verdade, na medida em que, na metade do tempo, o protocolo exige que se diga a verdade e, na eventual resposta aleatória, a chance de ser verdadeira a resposta é de 50%. Afinal, existe 50% de chance de o entrevistado dizer a verdade (se a face inicial for "cara"), somada a um quarto de chance de dizer a verdade (se a face for "coroa")[108]. Nesse caso, ainda que as respostas sejam gravadas, não é possível afirmar se uma pessoa em particular traiu ou não seu cônjuge.

A "privacidade diferencial" pode ser também concebida como a tradução matemática da ideia de que é preciso comparar o que

107. GOMES, Marison. *Privacidade diferencial e anonimização*. Disponível em: https://privacytech.com.br/artigos/privacidade-diferencial-e-anonimizacao,319897.jhtml. Acesso em: 6 dez. 2021.

108. KEARNS, Michael; ROTH, Aaron. *The ethical algorithm*. Oxford: Oxford Press, 2020, p. 40-41.

se pode aprender de uma análise se um dado de uma determinada pessoa foi incluído no banco de dados com o que é possível aprender se esse dado não tivesse sido inserido[109]. O conceito foi desenvolvido por Dwork, McSherry, Nissim e Smith na década de 2000, o que lhes rendeu o prêmio Gödel[110]. Ele exige que a adição ou remoção de um registro de dado de um indivíduo não altere significativamente a probabilidade de um resultado. Kearns e Roth explicam:

> Como uma forma final de interpretar essa mesma garantia de privacidade, suponha que um observador externo esteja tentando advinhar se uma pessoa específica – digamos, Rebecca – está no banco de dados de interesse ou não (ou se o registro dela especifica alguma doença em particular, como câncer de pulmão, ou não). Ao observador é permitido usar uma regra arbitrária para fazer a sua suposição, baseado no resultado da computação de privacidade diferencial. Se ao observador é exibido um resultado computacional com os dados de Rebecca ou o mesmo resultado computacional sem os seus dados, ele não será capaz de advinhar qual resultado foi exibido a ele de forma mais acurada que advinhando aleatoriamente[111].

O seu uso objetiva a proteção dos indivíduos contra danos arbitrários à privacidade. Em termos mais simples, a técnica promete que a probabilidade de alguém receber ligações de telemarketing abusivas não aumente sensivelmente se esta pessoa permitir o uso de seus dados em um estudo; ou então que a probabilidade de o prêmio pago a uma seguradora não aumente em razão disso. Para conseguir esses objetivos, ela tenta impedir

109. KEARNS, Michael; ROTH, Aaron. *The ethical algorithm*. Oxford: Oxford Press, 2020, p. 36.

110. DWORK, Cynthia; MCSHERRY, Frank; NISSIM, Kobbi; SMITH, Adam. Calibrating Noise to Sensitivity in Private Data Analysis. *The Journal of Privacy and Confidentiality*, vol. 7, n. 3, 2006.

111. KEARNS, Michael; ROTH, Aaron. *The ethical algorithm*. Oxford: Oxford Press, 2020, p. 39.

a "reidentificação" do titular dos dados, como realizado por Sweeney em Massaschussetts[112].

Atualmente, a privacidade diferencial é concebida como uma das mais fortes ferramentas de segurança capazes de ajudar o desenvolvimento de pesquisas estatísticas, evitando o seu completo banimento ou alguma forma de limitação considerável. Cuida-se, portanto, de uma espécie de ponto de equilíbrio, uma garantia que deve estar presente, somando-se a outras, de modo a prevenir abusos nas atividades de tratamento de dados e realização de inferências. O seu uso deve ser não apenas incentivado, mas sobretudo *exigido*, como forma de tutela preventiva do direito à privacidade, evitando-se o uso desproporcional e desarrazoado de tecnologias de mineração de dados.

Em alguns casos, porém, ela pode não oferecer a segurança necessária[113], sobretudo se o algoritmo responsável pela randomização das informações – ou acréscimo de ruídos – se encontra centralizado nas mãos do operador dos dados, em lugar das mãos do titular. A preferência pelo método centralizado decorre da maior precisão dos dados, mas vem com o custo da insegurança. A título exemplificativo, tanto o Google[114] quanto a Apple[115] informam publicamente que têm empregado técnicas de privacidade diferencial no tratamento de dados de seus usuários. Apesar disso, se o método de desidentificação for do tipo centralizado, o esforço pode contribuir pouco no caso de compartilhamento de dados por ordem de autoridades estatais. Segundo o relatório de transparência do Google, somente no

112. KEARNS, Michael; ROTH, Aaron. *The ethical algorithm*. Oxford: Oxford Press, 2020, p. 38.

113. Conferir: CHAUDHURI, Kamalika; HSU, Daniel. Sample Complexity Bounds for Differentially Private Learning. *JMLR: Workshop and Conference Proceedings*, vol. 19, p. 155-56. 2011.

114. Cf. https://developers.googleblog.com/2021/01/how-were-helping-developers-with-differential-privacy.html. Acesso em: 6 dez. 2021.

115. Cf. https://machinelearning.apple.com/research/learning-with-privacy-at-scale. Acesso em: 6 dez. 2021.

ano de 2020, as autoridades públicas apresentaram mais de 113 mil requisições de dados relativos a mais de 261 mil usuários[116].

4.6.2. Direito a inferências razoáveis: existiria um direito a como ser visto?

A essa altura, não há dúvidas quanto à importância da legislação de proteção de dados pessoais, algo que tem sido objeto das atenções em muitos países em todo o mundo. A premissa maior subjacente à GDPR europeia ou à LGPD brasileira, por exemplo, é certamente a necessidade de proteção da privacidade e da autodeterminação dos usuários no ambiente digital.

Além disso, nos últimos anos, diversos trabalhos foram publicados com o objetivo de abordar temas como a auditabilidade e a explicabilidade das decisões automatizadas[117]. Embora tais assuntos, assim como a proteção dos usuários quanto à *co-*

116. Cf. https://transparencyreport.google.com/user-data/overview?hl=en Acesso em: 6 dez. 2021.

117. Conferir: PASQUALE, Frank. *The Black Box Society*: The Secret Algorithms That Control Money and Information. Cambridge, MA: Harvard University Press, 2015; VELIZ, C.; PRUNKL, C.; PHILLIPS-BROWN, M.; LECHTERMAN, T. M. We might be afraid of black-box algorithms. *Journal of Medical Ethics*, vol. 47, n. 5, p. 339-340, 2021; BATHAEE, Yavar. Artificial Intelligence Black Box and the Failure of Intent and Causation. *Harvard Law Review*, v. 31, n. 2, p. 889-938, 2018; YANISKY-RAVID, Shlomit; HALLISEY, Sean. Equality and Privacy by Designa: a New Model of Artificial Intelligence Data Transparency via Auditing, Certification, and Safe Harbor Regimes. *Fordham Urban Law Journal*, v. 46, n. 2, p. 428-486, 2019; Laat, Paul B. Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability? *Philosophy & Technology*, vol. 31, iss. 4, 2018; WON, Deborah. The Missing Algorithm: Safeguarding The Missing Algorithm: Safeguarding Brady Against the Rise of Against the Rise of Trade Secrecy in Policing. *Michigan Law Review*, vol. 120, 157, 2021; WACHTER, Sandra; MITTELSTADT, Brent; RUSSELL, Chris. Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR. *Harvard Journal of Law & Technology*, vol. 31, p. 841-888, 2018, p. 880.

leta e *transmissão* dos dados pessoais, sejam algo bastante sólido na doutrina e em variados atos legislativos, pouco se discute a respeito das *inferências* que podem ser realizadas a partir do uso destes dados[118].

De forma sintética, tais inferências consistem nas previsões que os algoritmos de inteligência artificial podem fazer a respeito de determinada pessoa. Não se trata de algo que um usuário informa diretamente a uma plataforma digital, mas sim de uma conclusão que a plataforma faz a partir de elementos objetivos fornecidos pelo usuário.

Muitos são os exemplos de inferências que são realizadas. Um dos mais famosos consiste na capacidade que o Netflix, plataforma de *streaming,* desenvolveu de inferir a raça dos seus usuários, em razão dos seus hábitos no uso do aplicativo[119]. O Facebook, por sua vez, é capaz de inferir a orientação sexual dos seus usuários, o que levou a plataforma apresentar anúncios de "cura gay" para alguns dos seus usuários[120]. Em estudo publicado em 2018, White, Doraiswamy e Horvitz descreveram até mesmo a existência de algoritmos capazes de inferir se determinados usuários eram portadores das doenças de Alzheimer ou Parkinson,

118. O tema é enfrentado por WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, v. 2019, n. 2, p. 494-620, 2019.

119. ARNOLD, Ben. Netflix user anger over 'racial targeting' of movie posters. *Yahoo Movies*, 2018. Disponível em: https://uk.movies.yahoo.com/netflix--users-anger-racial-targeting-movie-posters-104325948.html. Acesso em: 26 dez. 2021.

120. STEWART, Rebecca. Facebook removes ads promoting 'gay cure' to young LGBT users. *The Drum,* 2018. Disponível em: https://www.thedrum.com/news/2018/08/27/facebook-removes-ads-promoting-gay-cure-young-lgbt--users. Acesso em: 26 nov. 2021. Cf. CABAÑAS, José González; CUEVAS, Ángel; CUEVAS, Rubén. Facebook Use of Sensitive Data for Advertising in Europe. *27th USENIX Security Symposium*, p. 479-495, 2018. Disponível em: https://arxiv.org/abs/1802.05030. Acesso em: 26 nov. 2021.

a partir dos seus hábitos de pesquisa[121]. Por fim, a nova patente do Alexa, assistente pessoal da Amazon, é capaz de identificar enfermidades a partir da voz do usuário, sugerindo o uso de determinados medicamentos[122].

Em alguns casos, essas inferências podem resultar na negativa de acesso de uma determinada pessoa a um produto ou serviço. É o caso das inferências realizadas por instituições financeiras e seguradoras, que fazem constantes previsões sobre a confiabilidade dos seus consumidores, a partir não apenas dos seus dados, mas também do seu círculo de amigos[123]. Com o avanço dos sistemas automatizados de pontuação de indivíduos (*scoring systems*), cada vez mais o acesso a serviços e produtos é concretizado mediante prévia classificação e pontuação dos interessados[124]. Disso podem resultar falhas grosseiras, como revelado em estudo publicado em 2006. Após a análise de cerca de 500.000 arquivos, o estudo identificou que aproximadamente 29% (vinte e nove por cento) dos consumidores tinham *credit scores* que divergiam em ao menos 50 (cinquenta) pontos entre três agências de crédito[125].

Como expõem Wachter e Mittelstadt, além de invasivas e imprevisíveis, essas inferências podem ser inexplicáveis e con-

121. WHITE, Ryen W.; DORAISWAMY, P. Murali; HORVITZ, Eric. Detecting neurodegenerative disorders from web search signals. *NPJ digital medicine*, vol. 1, n. 1, p. 8, 2018.

122. SPANU, Anca. Amazon's new Alexa will know someone is sick by listening to their voice. *Healthcare Weekly*, 2018. Disponível em: https://healthcareweekly.com/amazon-alexa/. Acesso em: 26 nov. 2021.

123. TAYLOR, Astra; SADOWSKI, Jathan. How Companies Turn Your Facebook Activity into a Credit Score. *The Nation,* 2015. Disponível em: https://www.thenation.com/article/how-companies-turn-your-facebookactivity-credit--score/. Acesso em: 26 nov. 2021.

124. RITCHEL, Matt. I Was Discovered by an Algorithm. *N. Y. Times*, 28 de abril de 2013. Disponível em: http://archive.indianexpress.com/news/i-was-discovered--by-an-algorithm/1111552/. Acesso em: 30 nov. 2021.

125. CARTER, Carolyn; RENUART, Elizabeth; SAUNDERS, Margot; WU, Chi Chi. *North Carolina Banking Institute*, vol. 10, iss. 1, 2006.

traintuitivas, colocando em risco a privacidade, a identidade, a proteção de dados, a reputação e a autodeterminação informativa. Os autores questionam, a partir do reconhecimento do direito a ser *esquecido* pelo Tribunal de Justiça da União Europeia, se não seria possível reconhecer também um direito sobre *como as pessoas são vistas.* Trata-se do direito a inferências razoáveis[126].

Para enfrentar o assunto, o primeiro passo consiste em identificar a natureza jurídica das inferências. Seriam elas equiparadas a dados pessoais ou teriam outra natureza? Não há dúvidas de que as informações utilizadas pelo Netflix, ao inferir a raça ou gênero de um determinado usuário, são dados pessoais. É o caso dos dados cadastrais preenchidos pelo próprio consumidor, da lista de filmes assistidos ou do horário em que os filmes ou documentários são assistidos etc. As inferências, por seu turno, consistem no resultado do tratamento desses dados, a partir da aplicação de métodos estatísticos.

Na hipótese de as inferências serem consideradas dados pessoais, então dúvidas não há quanto à aplicação de toda a disciplina protetiva estabelecida pelas leis de proteção de dados pessoais, a exemplo dos direitos de acesso e retificação. Além disso, abre-se caminho para a aplicação da cláusula do devido processo legal em sua dimensão substantiva, evitando inferências desarrazoadas.

Na Europa, de acordo com o art. 4º do GDPR, dados pessoais, consistem em qualquer informação relativa a uma pessoa singular identificada ou identificável. O diploma considera identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular. De

126. WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, v. 2019, n. 2, p. 494-620, 2019, p. 502.

forma semelhante, a LGPD brasileira considera dado pessoal a "informação relacionada a pessoa natural identificada ou identificável" (art. 5º, I). Além disso, ambos os diplomas asseguram o direito à "correção de dados" incompletos, inexatos ou desatualizados (art. 18, III da LGPD e art. 16 da GDPR).

Uma análise literal desses dispositivos parece indicar que as inferências também podem ser consideradas dados pessoais, na medida em que se enquadram na noção geral de "qualquer informação", seja ela um dado objetivo ou o produto de uma análise de probabilidade. Consequentemente, também haveria de ser reconhecido o direito à retificação das inferências.

O tema já foi objeto de análise pelo Tribunal de Justiça da União Europeia (CJEU), cuja jurisprudência ainda é inconsistente. Em 2014, no julgamento do caso *YS. and M. and S,* quando ainda vigente a *Directive 95/46/EC,* a corte compreendeu que apenas os dados "verificáveis" (a exemplo dos "fatos" relativos a alguém, como o gênero e a idade) podem ser considerados dados pessoais. Em contrapartida, as análises e opiniões alcançadas a partir deles não poderiam ser assim consideradas[127].

Posteriormente, no caso *Nowak*[128], julgado em 2017, a corte entendeu que não apenas as respostas escritas encaminhadas por um candidato num exame profissional, mas também os comentários feitos pelo examinador relativos a essas respostas constituem dados pessoais. Em *Nowak,* a CJEU registrou que a expressão "qualquer informação", utilizada na definição de dados pessoais, impõe o reconhecimento de um conceito amplo, a abranger não apenas elementos objetivos, mas também subjetivos, a exemplo de opiniões e avaliações relativas ao titular dos dados. Apesar do nítido avanço apresentado em *Nowak* quanto à definição de dados pessoais, a corte deixou claro que o direito de retificação não permitiria a correção da avaliação feita pelo examinador.

127. TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. *C-141/12 and C-372/12,* 2014.

128. TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. *C-434/16,* 2017.

Consequentemente, à luz do mencionado precedente, os direitos relativos às inferências seriam limitados ao acesso[129].

Em síntese, é possível dizer que a jurisprudência do Tribunal de Justiça da União Europeia considera que a legislação de proteção aos dados não garante aos usuários o direito a um processo decisório justo, mediante a retificação de inferências desarrazoadas.

Embora, por um lado, possa parecer razoável reservar ao controlador de dados uma margem de liberdade na análise de dados pessoais, a postura do Tribunal parece ignorar a real possibilidade de serem realizadas inferências manifestamente equivocadas e lesivas aos usuários, sobretudo nos casos de alto risco. É o caso da negativa de concessão de empréstimo ou outro serviço ou produto a um consumidor com fundamento em inferências sem respaldo lógico. Além disso, o reconhecimento da dimensão substantiva da cláusula do devido processo legal em múltiplas jurisdições tem por objetivo impedir uma "ingerência desarrazoada, desnecessária e arbitrária no direito e na liberdade do indivíduo"[130].

Dessa forma, é possível reconhecer não apenas as inferências como dados pessoais – em razão da amplitude do conceito legal –, mas também a incidência horizontal indireta da cláusula do devido processo legal, pela via da interpretação do direito de retificação e das cláusulas gerais que indicam a necessidade de propósito legítimo do tratamento de dados. Essa tese, ao tempo em que preserva a liberdade na análise dos dados, proíbe a tomada de decisões com base em inferências desarrazoadas, porquanto discriminatórias, ilógicas, sem mínimo respaldo científico ou abusivas.

Para a sua concretização, o direito a inferências razoáveis demanda dos controladores de dados, a adoção de uma conduta

129. WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, v. 2019, n. 2, p. 494-620, 2019, p. 502.

130. SUPREMA CORTE DOS ESTADOS UNIDOS. *Lochner v. New York*, 198 U.S. 45, 1905.

preventiva, sendo capazes de explicar (a) o porquê de determinados dados serem aceitos para a realização de inferências, (b) o porquê de essas inferências serem normalmente aceitáveis e relevantes para a análise automatizada proposta e (c) se os dados e métodos utilizados para a realização das inferências são confiáveis e precisos[131].

Além disso, é razoável restringir o reconhecimento do direito às inferências de alto risco, assim consideradas aquelas que (a) são invasivas à privacidade ou capazes de causar danos à reputação de alguém no momento atual ou no futuro; ou (b) têm baixa verificabilidade, embora aplicadas para a tomada de decisões relevantes[132]. É o caso do emprego de sistemas automatizados de pontuação de indivíduos (*scoring systems*), que podem se revelar estigmatizantes[133]. A classificação de alguém como uma "má contratação" é capaz de aumentar a probabilidade de desemprego ou insolvência, contribuindo para a concretização da realidade que os programadores afirmam meramente prever. Essa capacidade de "condução" da realidade, em lugar da "descrição"[134], levanta preocupações quanto à justificação para a prática dos atos decisórios[135].

131. WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, v. 2019, n. 2, p. 494-620, 2019, p. 581.

132. WACHTER, Sandra; MITTELSTADT, Brent. A right to reasonable inferences: re-thinking data protection law in the age of big data and AI. *Columbia Business Law Review*, v. 2019, n. 2, p. 494-620, 2019, p. 581-583.

133. CITRON, Danielle Keats; PASQUALE, Frank. The Scored Society: Due Process for Automated Predictions. *Washington Law Review*, vol. 89, 2014.

134. Cf. MACKENZIE, Donald. *An Engine, Not a Camera*: How Financial Models Shape Markets. Cambridge, MA: MIT Press, 2008.

135. CITRON, Danielle Keats; PASQUALE, Frank. The Scored Society: Due Process for Automated Predictions. *Washington Law Review*, vol. 89, 2014.

4.6.3. Vedações decorrentes do princípio da prevenção da automação discriminatória

Tal como ocorre no campo do direito ambiental, em que o princípio da prevenção tem por objetivo a adoção de estratégias visando a evitar consequências sabidamente danosas ao meio ambiente[136], algumas tecnologias de automação devem ser objeto de uma especial atenção no campo legislativo. Trata-se das ferramentas cujo uso já foi apontado em estudos como capaz de resultar em práticas discriminatórias abusivas. Se, por um lado, o mero desconhecimento quanto ao potencial lesivo de um processo de automação deve ser objeto de testagem e monitoramento, certamente aquelas ferramentas já apontadas pela comunidade científica como causadoras de danos devem ser objeto de um regime diferenciado.

Esse regime diferenciado pode variar sensivelmente, a depender da potencialidade da causação de danos, bem como da sensibilidade do ambiente em que utilizada a ferramenta. A título de exemplo, uma ferramenta de monitoramento para fins de segurança pública, porquanto aplicada em ambiente evidentemente sensível, há de observar um regime mais restritivo. Por outro lado, a automação de etapas de processos administrativos ou judiciais cíveis há de observar um regime de menor restrição. Tomando emprestada a obrigação geral de prevenir dos Estados, estabelecida pela Corte Interamericana de Direitos Humanos, é possível destacar algumas medidas a serem implantadas não apenas pelos agentes responsáveis pela implementação automação tecnológica, mas também pelos órgãos encarregados da função legislativa. Na hipótese de eventual inação dos agentes responsáveis, será possível a intervenção judicial, de forma a concretizar o princípio da prevenção.

136. Cf.: MINASSA, Pedro Sampaio; VINCENZI, Brunela. A incógnita ambiental do princípio da precaução. *Revista Direito Ambiental e Sociedade*, vol. 8, n. 1, p. 148-189, 2018; Ribeiro, Cristina Figueiredo Terezo; Alves, Raysa Antonia Alves; Lima, Tamires da Silva A jurisprudência da Corte Interamericana de Direitos Humanos e o princípio da precaução. *Revista Direito Ambiental e Sociedade*, vol. 9, n. 1, p. 149-174, 2019.

As medidas em questão podem ser aplicadas isolada ou cumulativamente, compreendendo as seguintes providências: a) regulação; b) monitoramento; c) realização de estudos de impactos; d) vedação da implementação tecnológica de forma temporária ou definitiva[137].

Nesse sentido, em 6 de outubro de 2021, o Parlamento da União Europeia aprovou a Resolução nº 405 – P9_TA(2021)0405, que tem por objeto "a inteligência artificial no direito penal e a sua utilização pelas autoridades policiais e judiciárias em casos penais"[138]. Embora o ato tenha caráter não vinculante, cuida-se de importante marco inicial, a informar a relevância do princípio da prevenção no âmbito da regulação tecnológica e influenciar a legislação interna de cada país.

A Resolução inicia, em seu primeiro considerando, reconhecendo que que as tecnologias digitais, em geral, e a proliferação do tratamento e da análise de dados possibilitados pela inteligência artificial, em particular, são promissoras, embora acarretem riscos. Destaca que, nos últimos anos, foram verificados grandes avanços no desenvolvimento da IA, fazendo dela uma das tecnologias estratégicas do século XXI, com potencial para gerar benefícios substanciais em termos de eficiência, precisão e comodidade, trazendo, assim, uma mudança positiva para a sociedade, mas também sérios riscos para os direitos fundamentais e para as democracias alicerçadas no Estado de direito.

Particularmente no campo do policiamento preditivo e persecução penal, a Resolução apresenta as seguintes considerações

137. RIBEIRO, Cristina Figueiredo Terezo; ALVES, Raysa Antonia Alves; LIMA, Tamires da Silva A jurisprudência da Corte Interamericana de Direitos Humanos e o princípio da precaução. *Revista Direito Ambiental e Sociedade*, vol. 9, n. 1, p. 149-174, 2019, p. 169.

138. Cf. https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_PT.html. Acesso em: 18 nov. 2021.

introdutórias, que explicam o presente contexto tecnológico e as preocupações com a ocorrência de "alertas falsos":

> M. Considerando que a IA é utilizada pelas autoridades policiais em programas informáticos como as tecnologias de reconhecimento facial, nomeadamente para procurar suspeitos em bases de dados e identificar vítimas de tráfico de seres humanos ou de exploração sexual e abuso de menores, no reconhecimento automático de matrículas, na identificação de pessoas pela voz, no reconhecimento da fala, na leitura labial, nas escutas (ou seja, algoritmos de deteção de disparos), na investigação e na análise autónomas de bases de dados identificadas, nas previsões (previsão policial e análise de locais de criminalidade), nas ferramentas de deteção de comportamentos, as ferramentas avançadas de autópsia virtual, para ajudar a determinar a causa da morte, nos instrumentos autónomos para detetar fraudes financeiras e o financiamento do terrorismo, na monitorização das redes sociais (extração e recolha de dados para a identificação de ligações) e nos sistemas de vigilância automatizada que integram diferentes possibilidades de deteção (como a deteção de batimentos cardíacos e as câmaras térmicas); considerando que as aplicações atrás referidas, a par de potenciais ou futuras aplicações da tecnologia de IA no âmbito da aplicação da lei, podem ter graus de fiabilidade e precisão muito variados e um impacto na proteção dos direitos fundamentais e na dinâmica dos sistemas de justiça criminal; considerando que muitas dessas ferramentas são utilizadas em países terceiros, mas seriam ilegais nos termos do quadro legislativo e da jurisprudência da União em matéria de proteção de dados; considerando que a utilização rotineira de algoritmos, ainda que com uma taxa reduzida de falsos positivos, pode conduzir a que o número de alertas falsos ultrapasse, de longe, o de alertas corretos.

Ainda em tal campo, o Parlamento Europeu insiste que os Estados-Membros, em conformidade com a legislação aplicável, devem garantir que as pessoas sejam informadas se forem sujeitas à utilização de aplicações de IA pelas autoridades policiais ou judiciais. Além disso, destaca a relevância de se evitar o chamado *machine bias,* caracterizado pela confiança excessiva nos resultados fornecidos pelos sistemas de IA[139]. Nesse sentido, salienta a necessidade de as autoridades reforçarem a confiança e os conhecimentos necessários para desafiar ou anular uma recomendação algorítmica, considerando importante nutrir expectativas realistas sobre tais soluções tecnológicas.

No que diz respeito às ferramentas que, em razão de estudos que sinalizam a ocorrência de discriminações abusivas, devem ser evitadas, destacam-se as seguintes considerações da Resolução:

a) em contextos judiciais e policiais, toda e qualquer decisão judicial ou similar deve ser sempre tomada por um ser humano, que pode ser responsabilizado pelas decisões tomadas. As autoridades que utilizam sistemas de IA devem assegurar a intervenção humana, especialmente na análise dos dados provenientes desses sistemas, razão pela qual deve ser mantido o poder soberano dos juízes e a tomada de decisões numa base a cada caso, proibindo-se o uso de IA e das tecnologias relacionadas para propor decisões judiciais;

b) embora o policiamento preditivo possa analisar os conjuntos de dados fornecidos para a identificação de padrões e correlações, não pode dar resposta ao problema da causalidade e não pode fazer previsões fiáveis sobre o comportamento individual, pelo que não pode constituir a única base para uma intervenção. Opõe-se, por conseguinte, à utilização da IA pelas autoridades policiais para fazer previsões comportamentais sobre indivíduos ou grupos com base em dados históricos e comportamentos passados, pertença a grupos, localização ou quaisquer

139. Cf. McDERMOTT, Yvonne; KOENIG, Alexa; MURRAY, Daragh. Open Source Information's Blind Spot: Human and Machine Bias in International Criminal Investigations. *Journal of International Criminal Justice*, vol. 19, n. 1, p. 85-105, 2021. Disponível em: https://doi.org/10.1093/jicj/mqab006. Acesso em: 8 dez. 2021.

outras características semelhantes, tentando, assim, identificar pessoas suscetíveis de cometer um crime;

c) a implantação de sistemas de reconhecimento facial pelas autoridades policiais deve ser limitada a fins claramente justificados, no pleno respeito dos princípios da proporcionalidade e da necessidade, bem como da lei aplicável; reitera que a utilização de tecnologia de reconhecimento facial tem, no mínimo, de cumprir os requisitos de minimização dos dados, exatidão dos dados, limitação do armazenamento, segurança dos dados e responsabilização, devendo também ser lícita, equitativa e transparente e prosseguir uma finalidade específica, explícita e legítima que seja claramente identificada no direito da União ou dos Estados-Membros; entende que os sistemas de verificação e autenticação só podem continuar a ser implantados e utilizados com êxito se os seus efeitos adversos puderem ser atenuados e se os critérios acima referidos forem cumpridos;

d) apela à proibição permanente do recurso a análises automatizadas e/ou do reconhecimento em espaços acessíveis ao público de outras características humanas, tais como o andar, as impressões digitais, o DNA, a voz e outros sinais biométricos e comportamentais;

e) sugere, porém, uma moratória à implantação de sistemas de reconhecimento facial para fins de aplicação da lei destinados à identificação, a menos que sejam estritamente utilizados para efeitos de identificação de vítimas de crime, até que as normas técnicas possam ser consideradas plenamente conformes com os direitos fundamentais;

f) manifesta profunda preocupação com o recurso, pelas autoridades policiais e pelos serviços de informação, a bases de dados privadas de reconhecimento facial como a Clearview AI, com mais de rês mil milhões de imagens, que foram recolhidas ilegalmente de redes sociais e outras partes da internet. Insta a Comissão a proibir a utilização

de bases de dados privadas de reconhecimento facial no domínio da aplicação da lei;

g) considera que o recolhimento e a utilização de quaisquer dados biométricos para fins de identificação à distância, por exemplo, através de reconhecimento facial em espaços públicos, bem como em cancelas de controlo automatizado de fronteiras utilizadas em aeroportos, podem acarretar riscos específicos para os direitos fundamentais, cujas implicações podem variar consideravelmente em função da finalidade, do contexto e do âmbito da utilização. Entende que o uso da identificação biométrica nos contextos policial e judicial deve ser sempre considerada de "alto risco" e, por conseguinte, sujeita a requisitos adicionais, de acordo com as recomendações do Grupo de Peritos de Alto Nível sobre IA da Comissão;

h) manifesta profunda preocupação com projetos de investigação financiados pelo Horizonte 2020 que implantam inteligência artificial nas fronteiras externas, como o projeto iBorderCtrl, um "sistema inteligente de detecção de mentiras" que traça o perfil dos viajantes com base numa entrevista automatizada por computador realizada, antes da viagem, com recurso à câmara Web do viajante, bem como uma análise de 38 pequenos gestos, baseada em inteligência artificial e testada na Hungria, na Letónia e na Grécia. Exorta a Comissão a aplicar, através de medidas legislativas e não legislativas, e, recorrendo, se necessário, a processos por infração, uma proibição de todo e qualquer tratamento biométrico, inclusive o reconhecimento facial, para efeitos de aplicação da lei, que resulte numa vigilância em larga escala nos espaços acessíveis ao público.

4.7. Devido processo e a disciplina das evidências digitais no Brasil

A cada dia, cresce o uso de evidências digitais no Brasil. O que antes parecia se limitar aos processos penais – especialmente

para fins de comprovação de crimes como o de divulgação de pornografia infantil pela internet, previsto no art. 241-A da Lei nº 8.069/1990 – passou a fazer parte também de processos cíveis.

Isso se deve, especialmente, ao crescente acesso à internet pela população brasileira, bem como à popularização das redes sociais, ferramentas que acabaram produzindo efeitos relevantes em campos como o da responsabilidade civil e do processo eleitoral. Lamentavelmente, diferentemente do que se observa na experiência estrangeira, a doutrina brasileira parece não atentar ao tema, sendo raros os trabalhos voltados a uma descrição mínima do estado da arte no país[140].

4.7.1. Conceitos fundamentais

Para que se possa conhecer a disciplina da produção de provas digitais, é necessária a prévia compreensão a respeito de alguns conceitos fundamentais, relativos ao funcionamento das tecnologias de conexão à internet e acesso às aplicações disponíveis. O objetivo dos tópicos seguintes é o de, pressupondo-se o alheamento dos juristas em geral em relação a tais temas, desenvolvê-los de forma acessível e objetiva, focando-se em seus aspectos mais relevantes para fins probatórios.

4.7.1.1. Endereço de protocolo de internet *(endereço IP),* domain names *e DNS*

O conceito de endereço de protocolo de internet (endereço IP) é certamente o elemento nuclear para a compreensão do funcionamento da internet. Isso porque ela consiste num sistema global de redes de computadores conectados a partir de protocolos de comunicação padronizados que utilizam tais endereços como "caminhos" ou "rotas" de interconectividade[141].

140. Cf. TAVARES, João Paulo Lordelo Guimarães. O regime jurídico das provas digitais no direito brasileiro. Revista de Processo, vol. 316, p. 373-387, 2021.

141. HARGREAVES, Stuart; LOKMAN, Tsui. IP Addresses as Personal Data Under Hong Kong's Privacy Law: An Introduction to the Access My Info HK Project. *Journal of Law, Information & Science*, vol. 25, vol. 25, p. 68-83, 2017; Borgesius, Frederik Zuiderveen. The Breyer Case of the Court of Justice of the European Union: IP Addresses and the Personal Data Definition. *European Data Protection Law Review (EDPL)*, vol. 3, p. 130-137, 2017.

Toda pessoa conectada à internet o faz sob um endereço IP numérico. Esse número não é infinito. Cada endereço é distribuído pela *Internet Assigned Numbers Authority* (IANA), organização mundial sediada na Califórnia[142], encarregada de supervisionar e atribuir IPs aos provedores de conexão de internet, possibilitando a atribuição aos seus usuários. Desde 1998, a IANA consiste em um departamento da *Internet Corporation for Assigned Names and Numbers* (ICANN)[143], entidade sem fins lucrativos responsável pelo desenvolvimento de políticas voltadas ao funcionamento e expansão da internet em todo o mundo.

Atualmente, as versões dos endereços de protocolo de internet utilizados são duas. A mais comum ainda é o IPv4, que utiliza endereços de 32 bits, limitando a sua atribuição para até 4.294.967.296 (2^{32}) endereços. O IPv4 utiliza quatro campos para definir o endereço IP (ex.: 225.109.4.98). A acelerada expansão da internet conduziu à necessidade de aumento dos números de protocolo de internet existentes, o que resultou na criação do IPv6, versão mais atual e com capacidade consideravelmente superior.

Cada vez que alguém se conecta à internet, o provedor de conexão atribui a ela um determinado endereço de IP. Normalmente, a cada conexão é atribuído um número de endereço distinto (endereço de IP dinâmico[144]), muito embora seja permitido aos

142. McGILLIVRAY, Kevin. Give it away now? Renewal of the IANA functions contract and its role in internet governance. *International Journal of Law & Information Technology*, vol. 22, p. 3-26, 2014. Cf. http://www.iana.org. Acesso em: 9 dez. 2021.

143. SALIBA, Aziz Tuffi; BAHIA, Amael Notini Moreira. A jurisdição da ICANN: desafios atuais e prospectivas futuras. *Revista de Direito Internacional*; 2019, Vol. 16, p. 335-345. Cf. http://icann.org.

144. EL KHOURY, Alessandro. Dynamic IP Addresses Can be Personal Data, Sometimes. A Story of Binary Relations and Schrödinger's Cat. *European Journal*

provedores de internet atribuir endereços fixos aos seus usuários. Além disso, o normal é que cada endereço seja designado para apenas uma pessoa, permitindo o registro individualizado da sua atuação na internet.

Apesar de a designação de endereços IPs pela IANA ser individual para cada servidor, é possível que um determinado usuário se utilize de uma ferramenta chamada *Network Address Translation* (NAT), conhecida também como *masquerading*, em sua rede privada[145]. A título de exemplo, se alguém utiliza um roteador *wireless* em casa, muito embora esse roteador utilize um único endereço IP para se conectar à internet, ele distribui, para cada usuário doméstico, um número interno, conhecido como "IP privado" (ex.: 192.168.0.0/16). Esses números internos não são roteados na internet (e por isso, podem coincidir em casas diversas), mas apenas o número do endereço IP do roteador. Isso faz com que todos os usuários, ao final, se conectem à internet por um mesmo endereço IP público, embora por meio de portas lógicas distintas.

Situações assim dificultam a individualização de determinada conduta praticada na internet, para fins probatórios. Imagine-se um indivíduo que se conecta à rede *wireless* de um bar e pratica um delito por meio do seu celular. Como identificá-lo? Essa tarefa exige uma verificação mais acurada, a partir da análise dos registros de conexão que permanecem dentro do roteador (*logs*).

Por fim, é preciso esclarecer o conceito de nome de domínio (*domain name*). Cuida-se de uma forma de se conferir uma aparência mais compreensiva a um endereço IP. Toda vez que um usuário de internet digita, em um navegador de internet (*internet browser*), um determinado endereço de registro (ex.: www.joaolordelo.com), esse endereço consiste num *domain name* que uma empresa de registros – chamada *Registrar* – alienou a

of Risk Regulation, vol. 8, p. 191-197, 2017.

145. WING, Dan. Network Address Translation. *IEEE Internet Computing*, vol. 14, p. 66-70, 2010.

alguém – chamado *Registrant*. Esses nomes de domínio facilitam a navegação pela internet e também se sujeitam ao controle da IANA. Cada vez que alguém adentra um *website*, o Sistema de Nomes de Domínio (*Domain Name System* – DNS) faz a associação entre o domínio e o respectivo endereço IP a ele atribuído, permitindo a conexão. Cada equipamento que hospeda um determinado *website* possui o seu endereço IP, que é alcançado pelo protocolo de conexão por meio do *domain name*.

4.7.1.2. Provedores de conexão à internet

Conforme disposto no art. 5º, V, do Marco Civil da Internet (Lei nº 12.965/2014), entende-se por conexão à internet "a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP". Os provedores de conexão, como o próprio nome sugere, são pessoas que prestam o serviço de habilitar os seus usuários ao acesso à internet. Quando algum consumidor paga uma determinada quantia para uma companhia habilitar o seu *smartphone*, possibilitando sua conexão à internet, essa companhia é um provedor de conexão.

Na forma do art. 13 da Lei nº 12.965/2014, na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. Essa responsabilidade não poderá ser transferida a terceiros (§ 1º).

Os registros de conexão conservam dados como o endereço IP atribuído ao usuário, a data e o horário da conexão, a duração da designação do e o número da conta do usuário. O descumprimento das regras relativas à conservação desses dados poderá sujeitar o provedor a sanções que variam desde a advertência até a proibição de exercício de atividades (art. 12, I a IV).

É importante notar que, em respeito à intimidade e à privacidade dos usuários, aos provedores de conexão é vedado guardar os registros de acesso a aplicações de internet – a exemplo

do acesso a um determinado *website* ou rede social –, devendo se limitar aos dados de conexão (art. 14). Em outras palavras, os provedores de conexão não podem monitorar, muito menos registrar informações relativas aos *websites* e aplicativos acessados pelos seus usuários.

4.7.1.3. Provedores de aplicações de internet

A Lei nº 12.965/2014 conceitua as aplicações de internet de forma ampla, compreendidas como "o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet" (art. 5º, VII). Após uma determinada pessoa se conectar à internet, o caminho natural consiste no acesso a determinadas aplicações, a exemplo de *websites*, redes sociais (*Twitter, Instagram, Facebook* etc.), ferramentas de comunicação instantânea (*WhatsApp, Telegram, Skype, Hangouts* etc.), caixas de mensagens de e-mail (*Hotmail, Gmail, Yahoo* etc.), buscadores (*Google, Yahoo, Bing* etc.), entre outras. Todas essas aplicações são mantidas por provedores específicos (ex.: o Google é o provedor da aplicação Gmail), que se ocupam de ofertar funcionalidades ao acesso à internet.

Vê-se, assim, que os provedores de aplicação, ao contrário dos provedores de conexão, não se ocupam do serviço de habilitação de um usuário para o acesso à internet, mas sim de ofertar funcionalidades variadas, gratuitas ou onerosas, que imprimem maior utilidade à rede mundial de computadores.

Na forma do art. 15 da Lei nº 12.965/2014, o provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento. Em termos mais simples, se alguém acessa o seu e-mail particular mantido pelo provedor Google (Gmail) em um determinado dia, num determinado horário, esse provedor possui a obrigação de guardar os dados desse acesso (endereço IP, data, horário e dados cadastrais) por pelo menos 6 (seis) meses. Igualmente, se alguém publica algo na rede social *Twitter*, os dados relativos a essa publicação devem permanecer guardados.

4.7.1.4 Servidores proxy, *VPN e rede TOR*

O uso de *proxies* e VPNs tem sido cada vez mais frequente por pessoas que buscam maior privacidade na internet mediante a ocultação do endereço IP. Até mesmo usuários comuns têm utilizado tais ferramentas, cuja compreensão é também necessária para fins de coleta de evidências digitais[146].

Um *proxy* consiste em um servidor que atua como intermediário – um verdadeiro "representante" – de um determinado usuário de internet, emprestando-lhe o seu endereço IP. A título de exemplo, um usuário brasileiro conectado à internet por meio do endereço IP 200.200.200.1 pode se utilizar de um servidor de *proxy* chinês com endereço IP diverso para acessar variadas aplicações na internet. Em tal caso, ao solicitar o acesso a um provedor de aplicação como uma rede social (*Twitter, Facebook, Instagram* etc.), o usuário enviará esse pedido ao servidor *proxy*, conectando-se a ele. O *proxy*, por seu turno, fará a conexão com a rede social. Consequentemente, o tráfego de dados com o endereço IP da rede social será feito por um IP diverso (o endereço distribuído a um servidor *proxy* chinês), que encaminhará esses dados ao usuário brasileiro.

Em razão disso, no exemplo citado, os dados de conexão armazenados pelo provedor de aplicação não serão aqueles do usuário brasileiro, mas sim do servidor *proxy*. Assim, a identificação do usuário dependerá de uma prévia investigação a respeito do serviço de *proxy* oferecido, o pode ser feito por meio do banco de dados existente em locais como a empresa *Domains by proxy*[147],

146. MORRIS, Antonio. How to surf privately (& watch 0/S TV). *APC (Bauer Media Group)*, vol. 30, p. 84-84, 2010.

147. Cf. https://www.domainsbyproxy.com/AboutUs.aspx. Acesso em: 9 dez. 2021.

ou por medidas de cooperação internacional voltadas à coleta dos dados de conexão do servidor *proxy* estrangeiro.

De forma similar, uma *virtual private network* (VPN) também permite a ocultação do endereço IP de um determinado usuário, mas com algumas diferenças relevantes. De início, as VPNs conseguem redirecionar todo o tráfego de um terminal[148] – um computador, um *smartphone* etc. Um *proxy*, por outro lado, é utilizado em um aplicativo que permita conexão com a internet, a exemplo de um navegador ou mesmo um jogo, não sendo possível configurar todas as conexões de um computador ou roteador. Além disso, as VPNs submetem o tráfego de dados a um processo de criptografia, que pode ser traduzido como uma espécie de "envelopamento das informações e seu tráfego por um túnel totalmente seguro que interliga seu computador a uma rede remota"[149]. Por consequência desse procedimento, as VPNs costumam reduzir bastante a velocidade da navegação do usuário[150].

Por fim, o *The Onion Router* (TOR) consiste em uma aplicação de internet que oculta a identidade do seu usuário, através não apenas da criptografia dos dados de tráfego, mas também pelo seu direcionamento por variados servidores operados por voluntários. Há aqui uma sobreposição de servidores que repassam os dados, o que gera uma espécie de "criptografia multicamadas".

Apesar da complexidade dessas ferramentas, é possível a obtenção de dados de conexão de usuários que se utilizam de *proxy*, VPN ou TOR[151], o que demanda atuações de órgãos especializados em combate a crimes cibernéticos (FBI, Ministério Público, Polícia Federal etc.).

148. BRANDT, Andrew. Easy VPNs Secure Wi-Fi at Home and on the Road. *PCWorld*, vol. 23, 2005, P. 40.

149. Cf. https://canaltech.com.br/seguranca/afinal-de-contas-qual-a-diferenca-entre-proxy-e-vpn-62225/. Acesso em: 9 dez. 2021.

150. BANDLER, John. Network Cybersecurity in Your Home and Office. GPSolo, Mar/abr, vol. 35, p. 52-55, 2018.

151. CHAKRAVARTY, Sambuddho; PORTOKALIDIS, Georgios; POLYCHRONAKIS, Michalis; KEROMYTIS, Angelos. Detection and analysis of eavesdropping in anonymous communication networks. *International Journal of Information Security*, Jun. 2015, Vol. 14, p. 205-220.

4.7.2. O regime processual estabelecido pelo Marco Civil da Internet (Lei nº 12.965/2014)

Como expressamente anunciado em seu art. 1º, o Marco Civil da Internet (Lei nº 12.965/2014) tem por objetivo estabelecer princípios, garantias, direitos e deveres para o uso da internet no Brasil, além de determinar as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Entre os princípios elencados no art. 3º do diploma legal, destacam-se, para fins probatórios, a "proteção da privacidade" (inciso II) e a "proteção dos dados pessoais" (inciso III). Em decorrência desses dois princípios, o art. 7º estabelece, entre outros direitos dos usuários, a "inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei" (inciso II), a "inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial" (inciso III), bem como o "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;" (inciso VII).

Em reforço à disciplina estabelecida em seus dispositivos inaugurais, o art. 22 assegura genericamente à "parte interessada", com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, a possibilidade de requerer ao juiz que ordene ao responsável pela

guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet[152].

Para tanto, o seu parágrafo único estabelece três requisitos, sob pena de inadmissibilidade do requerimento: a) fundados indícios da ocorrência do ilícito; b) justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e c) período ao qual se referem os registros.

É importante atentar, porém, a duas sutilezas.

A primeira delas consiste na compreensão de que o requerimento a que alude o art. 22 da Lei nº 12.965/2014 pode assumir duas naturezas bastantes distintas.

De um lado, é possível que ele se resuma a um pedido de quebra de dados informáticos ou telemáticos já armazenados em provedores de conexão, a exemplo um requerimento voltado ao conhecimento do endereço IP, dia e hora que um determinado usuário acessou a internet ou usou determinado aplicativo.

De outro lado, é possível que o pedido consista na interceptação do fluxo de dados, mediante o monitoramento do fluxo de dados de conexão ou de acesso de um determinado usuário, caso em que são atraídos os requisitos adicionais relativos à interceptação de comunicações telefônicas, por força do que dispõe o art. 1º, parágrafo único, da Lei nº 9.296/1996, que regulamenta o inciso XII, parte final, do art. 5º da Constituição da República. Conforme estabelece o aludido diploma, essa medida somente pode ser determinada para fins de investigação de infração de natureza criminal punida com reclusão.

Uma outra diferença, conforme precedente do Superior Tribunal de Justiça, reside no requisito da indicação, no requerimento, do "período ao qual se referem os registros" (art. 22, parágrafo único, III). No julgamento do RHC n. 117.680/PR, o tribunal compreendeu que essa exigência somente se faz para a interceptação de fluxos de dados requisitados a provedores de aplicações de internet[153]. Isso se deve ao acentuado caráter interventivo, na medida em que a interceptação do fluxo de dados – a exemplo do acesso contínuo à caixa de e-mail ou das conversas em um determinado aplicativo de *chat* – não diz respeito a dados estáticos, interferindo diretamente na liberdade de comunicação em si, a merecer limitação temporal.

No particular, entende-se que o aludido precedente, embora com a melhor das intenções, chegou a uma conclusão equivocada. Em realidade, a partir das premissas elencadas, o resultado deveria ser o inverso: a necessidade de indicação de um lapso temporal preciso para o acesso a dados estáticos, algo que, para a interceptação do fluxo de dados, parece ilógico, na medida em que o objetivo da interceptação consiste na obtenção de informações *futuras* relativas a ilícitos penais.

De um lado, não é razoável permitir-se o acesso ilimitado a todos os dados telemáticos ou informáticos estáticos relativos a um determinado usuário, sob pena de exposição de dados temporalmente muito distantes dos fatos cuja comprovação se busca. De outro lado, na interceptação do fluxo de dados, é suficiente o estabelecimento de um lapso temporal para fins de análise da necessidade de prorrogações, tal como ocorre na disciplina que a Lei nº 9.296/1996 estabeleceu para a interceptação telefônica.

Há ainda uma segunda sutileza.

Embora o Marco Civil da Internet discipline a guarda e a exibição de dados de conexão – no caso dos provedores de conexão (art. 13, § 5º) – e de acesso – no caso dos provedores de aplicações de internet (art. 15, § 1º) –, existem outros dados igualmente relevantes, que podem ser fornecidos especialmente pelos provedores de aplicações de internet. Cuida-se de dados

152. Nesse sentido, já decidiu o Superior Tribunal de Justiça: "O Marco Civil da Internet afirma a obrigatoriedade de ordem judicial para que os provedores de acesso e de aplicação apresentem dados considerados pessoais e sigilosos a interessados. Trata-se de a proteção necessária e esperada à privacidade e à intimidade dos usuários de aplicações da internet" (REsp 1782212/SP, Terceira Turma, Relatora: Min. Nancy Andrighi, DJe 7.11.2019).

153. RHC 11780/PR, Sexta Turma, Relator: Min. Nefi Cordeiro, DJe 14.2.2020.

que, embora também possam ser compreendidos, genericamente, como dados telemáticos – no caso de aplicação para *smartphone* – ou informáticos – se utilizado outro tipo de terminal –, não dizem respeito apenas à conexão à internet ou acesso a uma determinada aplicação.

Curiosamente, o Marco Civil da Internet não parece se preocupar com essas informações, concentrando-se a Lei nº 12.965/2014 em disciplinar dados pessoais relativos à conexão à internet – a exemplo do endereço IP, data e hora do acesso, além da porta lógica, no caso do uso de ferramenta NAT[154] – e de acesso às aplicações – notadamente endereço IP, data, hora e duração do acesso. O que dizer de dados como as informações cadastrais em uma determinada rede social ou até mesmo o conteúdo de mensagens privadas de *chat* ou de e-mail? Certamente, não se trata de dados de conexão ou de acesso, mas são igualmente relevantes para fins probatórios.

No que diz respeito aos dados cadastrais, a lei confere uma proteção menor ao seu acesso, sendo permitida, por exemplo, a requisição direta por membros do Ministério Público ou por autoridades policiais, desde que limitados a informações referentes à qualificação pessoal, filiação e o endereço do usuário (art. 10-A, § 1º, II, c/c arts. 15 a 17 da Lei nº 12.850/2013). No caso de particulares ou outros órgãos públicos, a requisição desses dados dependerá de prévia autorização judicial.

154. Segundo precedente do Superior Tribunal de Justiça, "Pelo cotejamento dos diversos dispositivos do Marco Civil da Internet mencionados acima, em especial o art. 10, *caput* e § 1º, percebe-se que é inegável a existência do dever de guarda e fornecimento das informações relacionadas à porta lógica de origem. 9. Apenas com a porta lógica de origem é possível fazer restabelecer a univocidade dos números IP na internet e, assim, é dado essencial para o correto funcionamento da rede e de seus agentes operando sobre ela. Portanto, sua guarda é fundamental para a preservação de possíveis interesses legítimos a serem protegidos em lides judiciais ou em investigações criminais" (REsp 1777769/SP, Terceira Turma, Relatora: Min. Nancy Andrighi, Dje 8.11.2019).

Por seu turno, o acesso ao conteúdo de documentos e conversas armazenados em aplicativos – a exemplo de mensagens de e-mail, mensagens de aplicativos de comunicação instantânea, documentos e conteúdos armazenados na nuvem, dados de localização, dados relativos à utilização de aplicações de serviços de transporte (*Uber*, 99POP etc.), entre outros – deve sempre ser objeto de requerimento judicial prévio, da mesma forma que ocorre com documentos físicos ou correspondências obtidos por meio de busca e apreensão. É o que dispõe o art. 7º do MCI, ao assegurar aos usuários da internet o direito à inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei (inciso II). Na hipótese de interceptação do fluxo desses dados, ou seja, quando o que se deseja é o acesso simultâneo aos dados produzidos, será aplicado o regime das interceptações telefônicas (art. 1º, parágrafo único, da Lei nº 9.296/1996).

4.7.3. Metodologia básica para a produção da prova digital

Um questionamento comum, frequentemente formulado por profissionais não especializados em evidências digitais, consiste em saber a forma de identificação de usuários a partir de um acesso a uma aplicação. Imagine-se que um determinado usuário anônimo de uma rede social publique uma mensagem ofensiva a alguém. Para além da comprovação da existência da mensagem, como identificar esse usuário? De igual modo, como proceder no caso de a prova de um determinado fato consistir em uma mensagem de e-mail enviada por um usuário?

Firmadas as premissas anteriores, é importante saber, em termos pragmáticos, a forma de postulação de acesso ao dados pessoais e documentos eletrônicos.

Em processos cíveis, o procedimento adotado será o da produção antecipada de provas, que, na disciplina do novo Código de Processo Civil, poderá ser proposta mesmo sem razões cautelares, bastando que o "prévio conhecimento dos fatos possa justificar ou evitar o ajuizamento de ação" (art. 381, III, do CPC).

Se o que se objetiva é a *identificação* de usuários responsáveis por determinada conduta praticada por intermédio de provedores de aplicações de internet – a exemplo do envio de mensagem de e-mail, publicações de imagens, mensagens em redes sociais, áudios, páginas etc. –, o primeiro passo consiste em saber o endereço IP que foi utilizado para a concretização dessa conduta. Isso porque, como já referido, o tráfego de dados entre um determinado usuário e um provedor de aplicações ocorre por intermédio de um endereço IP que lhe foi distribuído por um provedor de conexão à internet.

Assim, nesse caso, a postulação deve seguir o seguinte roteiro: a) requerimento de quebra do sigilo de dados informáticos, de modo que o provedor de aplicações (*Twitter, Facebook, Google* etc.) exiba o endereço IP utilizado para a publicação de determinada mensagem, informando-se as suas circunstâncias (usuário, dia e hora); b) requerimento de quebra de sigilo de dados pessoais, para que esse mesmo provedor de aplicações informe as informações utilizadas pelo usuário para abrir a sua conta. No caso de mensagens de e-mail, o destinatário da mensagem, ao recebê-la, já é informado também sobre o endereço IP do usuário que a enviou, tornando-se desnecessário o primeiro requerimento.

Com frequência, os dados pessoais informados por ocasião do cadastro (nome, endereço etc.) são falsos. Nesse caso, será necessário passar para um segundo passo, consistente na identificação do provedor de conexão a partir do endereço IP informado pelo provedor de aplicações. Essa identificação não é difícil, na medida em que cada endereço é distribuído pela *Internet Assigned Numbers Authority* (IANA). Para tanto, basta inserir o número do endereço IP em uma ferramenta *Whois*, o que pode ser feito pelo próprio requerente.

Existem diversos *websites* que permitem o acesso gratuito ao *Whois*, a exemplo daqueles que podem ser acessados pelos endereços http://registro.br (para endereços nacionais) e http://www.whois.net. Outros são pagos, ofertando informações mais detalhadas. O *Whois* informa, entre outros, os seguintes dados, que são relevantes para a identificação do usuário: a) o local do

endereço IP (país, geralmente); b) *Host name*; c) *Whois server* (mantenedor do IP); d) *IP range* (bloco de números IP que o provedor de conexão possui); etc. Identificado o provedor de conexão (Claro, Vivo, Velox, NET etc.), o terceiro passo consistirá no requerimento de quebra de sigilo de dados, possibilitando-se o acesso às informações cadastrais do usuário junto a essas empresas. Esse último passo dispensará a mediação judicial, na hipótese de o requerente ser o Ministério Público ou autoridade policial, por força do que dispõe a Lei nº 12.850/2013 (art. 10-A, § 1º, II, c/c arts. 15 a 17). Ainda que essas informações sejam falsas, é possível identifica-lo por metodologias empregadas a partir dos dados relativos à forma de pagamento do serviço.

Por outro lado, se o que se quer é a *obtenção de um documento virtual* – a exemplo do acesso à caixa de e-mail de um determinado usuário em um período específico, o acesso aos documentos armazenados em uma conta na "nuvem", o histórico de buscas de um determinado buscador, o histórico de localização ou de uso de aplicações de transporte, entre outros –, o prévio conhecimento do endereço IP do usuário pode ser desnecessário. Para tanto, será suficiente a indicação de informações como o endereço de e-mail, nome ou número de identificação do perfil nas redes sociais.

4.7.4. Busca e apreensão virtual x interceptação de fluxo de dados: distinções necessárias

No clássico precedente formado por ocasião do julgamento do RE 418416/SC, o Supremo Tribunal Federal consolidou o entendimento no sentido de que "a proteção a que se refere o art. 5º, XII, da Constituição, "é da comunicação 'de dados' e não dos 'dados em si mesmos', ainda quando armazenados em computador"[155]. Naquela oportunidade, foi feita uma clara

155. RE 418416/SC, Tribunal Pleno, Relator: Min. Sepúlveda Pertence, j. 10.5.2006. cf. voto no MS 21.729, Pleno, 5.10.95, red. Néri da Silveira - RTJ 179/225, 270.

distinção entre a comunicação ("fluxo") de dados e a obtenção de dados informáticos "estáticos" – ex.: mensagens de e-mail e documentos armazenados em um dispositivo.

Essa distinção é também realizada pelo Marco Civil da Internet, cujo art. 7º assegura aos usuários da internet dois direitos distintos: a inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei (inciso II); a inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial (inciso III).

No primeiro caso, temos a interceptação de fluxos de dados, medida que, por força do art. 5º, XII, da Constituição da República, regulamentado pelo art. 1º, parágrafo único, da Lei nº 9.296/1996, somente pode ser judicialmente deferida para fins de investigação criminal ou instrução processual relativa a crime punido com reclusão. Assim, não é possível formular, em processos de natureza cível, pedidos de interceptação de mensagens em aplicativos de *chat* ou de e-mail, nem mesmo o acesso à senha do usuário em aplicativos dessa natureza, o que permitiria o monitoramento da comunicação. É permito, porém, o empréstimo de prova produzida por meio de interceptação do fluxo de dados, em processo ou investigação criminal, para processos cíveis e até mesmo processos administrativos, conforme a jurisprudência do Supremo Tribunal Federal[156] e do Superior Tribunal de Justiça[157].

No segundo caso, todavia, os dados já existem e estão armazenados em algum local, que pode ser um terminal do usuário (*smartphone,* computador etc.) ou um servidor (caixa de e-mail, *iCloud, Google Drive* etc.). O que temos aqui são dados estáticos que podem ser objeto de um pedido judicial de busca e apreensão

156. RMS 36434 AgR/DF, Primeira Turma, Relator: Min. Alexandre de Moraes, DJe 11.10.2019; RMS 30295 AgR/DF, Primeira Turma, Relatora: Min. Rosa Weber, Dje 12.2.2019.

157. MS 24031/DF, Primeira Seção, Relatora: Ministra Regina Helena da Costa, DJe 16.10.2019.

"física" – no caso de celulares, computadores etc. – ou busca e apreensão "virtual" (quebra de sigilo telemático/informático). É o que ocorre na formulação de pedido de apreensão de mensagens de e-mail de um determinado período, que se encontrem armazenadas na caixa de um determinado usuário de um serviço de correio eletrônico (Gmail, Hotmail etc.). Nesta hipótese, inexiste a necessidade de fundamentação do uso dos dados para fins de investigação criminal ou instrução processual relativa a crime punido com reclusão. Tampouco existe a garantia da subsidiariedade prevista no art. 2º, II, da Lei nº 9.296/1996, que impede o deferimento do pedido de interceptação de fluxo de dados se "a prova puder ser feita por outros meios disponíveis".

4.7.5. Busca e apreensão de dispositivos informáticos ou telemáticos, cadeia de custódia da prova, perícia e hashing

Em processos cíveis ou criminais, é comum a formulação de pedidos de busca e apreensão de dispositivos informáticos (computadores, *laptops* etc.) ou telemáticos (*smartphones*) para fins de obtenção de provas.

Questão relevante consiste em saber se, apreendido o dispositivo, seria necessária a formulação de novo pedido, voltado à extração do conteúdo já armazenado. Quanto a isso, a jurisprudência do Superior Tribunal de Justiça é sólida no sentido de que, se ocorreu a busca e apreensão da base física dos aparelhos de telefone celular, ante a relevância para as investigações, "não há óbice para se adentrar ao seu conteúdo já armazenado, porquanto necessário ao deslinde do feito, sendo prescindível nova autorização judicial para análise e utilização dos dados neles armazenados"[158].

158. HC 372.762/MG, Quinta Turma, Relator: Ministro Felix Fischer, DJe 16.10.2017.

Por outro lado, o STJ considera ilícito o acesso aos dados do celular extraídos do aparelho celular apreendido em flagrante delito, "quando ausente de ordem judicial para tanto, ao entendimento de que, no acesso aos dados do aparelho, se tem a devassa de dados particulares, com violação à intimidade do agente"[159].

Apreendido o dispositivo mediante ordem judicial, a atividade pericial exige cuidados relativos à *cadeia de custódia* da prova, assim compreendido "o conjunto de todos os procedimentos utilizados para manter e documentar a história cronológica do vestígio coletado em locais ou em vítimas de crimes, para rastrear sua posse e manuseio a partir de seu reconhecimento até o descarte" (art. 158-A do CPP).

Um método valioso para a sua preservação consiste no uso de ferramentas de *hashing*. Cuida-se de operação realizada por meio de aplicativo que cria um código único (*hash*) para quaisquer dados que sejam nele inseridos, tornando-se extremamente relevante para fins de preservação da integridade de uma evidência digital coletada. A título de exemplo, ao se utilizar o aplicativo de *hashing* no conteúdo de um disco rígido (HD) externo ou no conteúdo armazenado por um aparelho celular, será gerado um número de *hash* único. Se um único arquivo daquela base de dados for modificado, o número *hash* será diverso. Assim, qualquer alteração no conteúdo poderá ser identificada pela comparação entre o número *hash* inicial e o número após a suposta alteração, tornando-se inservível a prova[160].

159. AgRg no HC 542940/SP, Sexta Turma, Relator: Nefi Cordeiro, DJe 10.3.2020.

160. Truong, Tri. Hashing in the Cloud: The Private Search Defense Is Active and Potent. *MU Law Review*, vol. 72, p. 343-350, 2019; Branham, Rebekah. Hash it out: fourth amendment protection of electronically stored child exploitation. *Akron Law Review*, vol. 53, p. 217-244, 2019.

4.7.6. Pedidos de preservação de conteúdo

O Marco Civil da Internet (Lei nº 12.965/2014) também disciplina um instrumento bastante utilizado na experiência estrangeira, consistente nas requisições de preservação de conteúdo. A sua relevância decorre não apenas da limitação temporal que a legislação estabelece para a guarda dos dados de conexão e acesso, mas sobretudo da facilidade com que os usuários de aplicações de internet podem excluir o registro de dados, especialmente após a edição da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

Na forma do art. 13, § 2º, e art. 15, § 2º, do Marco Civil da Internet, a autoridade policial ou administrativa ou o Ministério Público poderão "requerer" cautelarmente que os registros de conexão ou os registros de acesso a aplicações de internet sejam guardados por prazo superior ao previsto na lei (um ano, para os registros de conexão; seis meses, para os de acesso a aplicações).

Apesar da literalidade do texto legal, compreendemos que a regra em questão não trata propriamente de um *requerimento*, mas sim de uma verdadeira *requisição*, com conteúdo de ordem direta aos provedores de conexão e de aplicação, como a experiência estrangeira ensina. Isso porque, à luz do que dispõem o art. 13, § 3º, e o art. 15, § 2º, a autoridade "requerente" terá o prazo de 60 (sessenta) dias, contados a partir do "requerimento", para ingressar com o pedido de autorização judicial de acesso aos registros previstos no *caput*. Se acaso fosse necessária a prévia autorização judicial para a mera preservação de dados, essa ferramenta careceria de utilidade, na medida em que o lapso temporal entre o requerimento e o deferimento judicial a tornaria inócua. Além disso, bastaria o requerimento judicial de acesso imediato aos dados, não havendo utilidade em primeiramente se pedir judicialmente a sua preservação.

Em atenção à disciplina legal, diversos provedores de aplicações de internet já estabeleceram ferramentas automatizadas de preservação de conteúdo, acessíveis em *websites* específicos. É o caso do *Facebook*, rede social que desenvolveu uma plataforma

específica, denominada *Facebook Records* (https://www.facebook.com/records/login/), destinada a "solicitações online para autoridades de aplicação da lei".

Embora a *preservação* do conteúdo seja alcançada extrajudicialmente, o seu *acesso* depende de prévia autorização judicial. Excepcionalmente, a experiência revela que os provedores de aplicações de internet disponibilizam diretamente dados de acesso e até mesmo conteúdos privados, em hipóteses como as de flagrantes de crimes ou de indícios de planejamento de suicídios de usuários.

4.7.7. A coleta de evidências criminais por requisição judicial direta ou acordos de cooperação mútua (MLAT)

A natureza "além das fronteiras" dos provedores de aplicações de internet tem gerado um importante debate sobre "se, e em que extensão, os tribunais podem expedir mandados obrigando os provedores de acesso à internet e fornecer esses dados em cumprimento a ordens judiciais"[161]. O tema desafia os limites territoriais do exercício da jurisdição, na medida em que tais provedores (a exemplo do Google ou do Facebook) prestam serviços em múltiplos países e possuem servidores em múltiplos outros.

Nos últimos anos, diversos países aprovaram leis locais, estabelecendo obrigações de guarda de registros de acesso a aplicações de internet[162], a exemplo do art. 15 do MCI[163], o que tem gerado críticas quanto à fragmentação da disciplina da internet[164].

Um caso emblemático consiste no julgamento do caso *United States v. Microsoft Corporation*[165], em que a Suprema Corte dos Estados Unidos foi chamada a decidir a respeito da validade de uma requisição judicial direta, realizada por um juiz da primeira instância. Por meio dessa decisão, juízo autorizou o governo dos EUA a acessarem dados armazenados pela Microsoft na Irlanda, com o objetivo de colher elementos de informação relativos a uma investigação pelo delito de tráfico de drogas nos EUA. A autorização judicial fundamentou-se no *Stored Communications Act*. Por outro lado, a Microsoft argumentava que a "apreensão" dos dados armazenados na Irlanda configuraria uma busca e apreensão extraterritorial[166], em desrespeito aos limites da jurisdição dos EUA. Para a companhia, seria necessário um pedido de cooperação internacional à Irlanda, em lugar da requisição direta. Antes que o tema pudesse ser enfrentado pela Suprema Corte, a

161. MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. *Revista Brasileira de Direito*, vol. 16, n. 1, p. 1-33, 2020, p. 22-28.

162. DASKAL, Jennifer. Privacy and Security Across Borders. *Yale Law Journal Forum*, v. 1029, p. 1-16, 2019.

163. Lei nº 12.965/2014: "Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento".

164. LAMBACH, Daniel. The Territorialization of Cyberspace. *International Studies Review*, vol. 2, n. 3, p. 482-506, 2020.

165. ESTADOS UNIDOS DA AMÉRICA. *United States v. Microsoft Corporation*. On writ of Certiorari To The United States Court of Appeals for The Secound Circuit, 584 U. S. ____ 2018.

166. MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. *Revista Brasileira de Direito*, vol. 16, n. 1, p. 1-33, 2020, p. 22-28. Cf. também: Vargas-León, Patricia A. Microsoft Corp. v. United States and the 'Hot Pursuit': A Case Study Against the Application of the Law of the Sea into the Cyberspace. *Zeitschrift Für Ausländisches öffentliches Recht Und Völkerrecht*, vol. 81, n. 3, p. 755-780, 2021.

causa perdeu o objeto, em razão da aprovação do *CLOUD Act*, que passou a disciplinar o tema de forma diversa.

Atualmente, como explicam Mendes e Fernandes, não apenas o *CLOUD Act* americano, como também as propostas de negociações do *e-Evidence Regulation* na União Europeia caminham para uma situação intermediária, em que essas "jurisdições não abririam mão do poder de requisição direta dos dados, mas compartilhariam com os países estrangeiros regras de cooperação jurisdicional claras para a proteção da privacidade e de outros direitos"[167]. Nesse sentido, dispõe o *CLOUD Act* que, como regra, os provedores de internet devem cumprir os mandados judiciais de requisição de dados ainda que estes estejam armazenados fora dos EUA. O ato, todavia, estabelece duas exceções, nas quais a requisição direta não é possível: a) quando o usuário do serviço cujos dados devem ser fornecidos não for um cidadão norte-americano ou não residir nos EUA; b) quando a coleta dos dados puder ensejar uma violação das leis do país estrangeiro[168].

No Brasil, o tema é tratado no *caput* do art. 11 do MCI, ao dispor que, como regra, em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

O seu § 1º acrescenta que essa regra é aplicável aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil. Por seu turno, o § 2º acrescenta que a obrigação geral do *caput* é aplicável mesmo que as atividades sejam realizadas

167. MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. *Revista Brasileira de Direito*, vol. 16, n. 1, p. 1-33, 2020, p. 27.

168. Cf. https://www.justice.gov/dag/cloudact. Acesso em: 9 dez. 2021.

por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

Isso significa que, como firmado pelo Superior Tribunal de Justiça, "por estar instituída e em atuação no País, a pessoa jurídica multinacional submete-se, necessariamente, às leis brasileiras, motivo pelo qual se afigura desnecessária a cooperação internacional para a obtenção dos dados requisitados pelo juízo"[169]. Em outras palavras, prestado o serviço no Brasil, torna-se desnecessário o uso dos acordos de assistência mútua (MLAT), que são naturalmente mais morosos (e frequentemente não cumpridos), por demandarem que o Estado requerente faça uma solicitação pelas vias diplomáticas e aguarde a resposta do Estado que detém o controle sobre as provas requeridas.

O regime do MCI é objeto de debate na Ação Direta de Inconstitucionalidade (ADC) nº 51, ainda pendente de julgamento pelo STF, ajuizada pela Federação das Associações das Empresas de Tecnologia da Informação – ASSESPRO NACIONAL, com o objetivo de ver declarada a constitucionalidade do Decreto Executivo Federal nº 3.810, de 2 de maio de 2001, que promulgou o Acordo de Assistência Judiciário-penal entre o Governo da República Federativa do Brasil e o Governo dos Estados Unidos da América (Mutual Legal Assistance Treaty – MLAT), do artigo 237, inciso II, do CPC, e dos artigos 780 e 783, do CPP. O objetivo é que as autoridades de persecução penal brasileiras utilizem o MLAT sempre que precisem de autorização judicial para acesso a dados que se encontrem em servidores fora do Brasil.

De um lado, colocando de lado os interesses das *big techs* quanto ao funcionamento global dos seus modelos de negócio, não há dúvidas quanto à relevância da preocupação com a violação

169. RMS 55.109/PR, Relator: Ministro Reynaldo Soares da Fonseca, Quinta Turma, julgado em 7/11/2017, DJe 17.11.2017.

das leis de proteção de dados vigentes no local das suas sedes[170]. Basta imaginar um órgão de persecução penal em um país sem apreço aos direitos fundamentais requisitando o encaminhamento indiscriminado de dados de usuários brasileiros.

Por outro lado, a obrigatoriedade da adoção do MLAT traria resultados bastante negativos à persecução nacional. Segundo levantamento divulgado em audiência pública conduzida pelo STF, 74% dos pedidos feitos pelo Brasil aos EUA por meio do MLAT não tiveram resposta positiva. Apenas 26% tiveram cumprimento total ou parcial, de acordo com levantamento feito pelo Ministério da Justiça entre 2016 e 2019. Além disso, a média de demora é de 10 (dez) meses[171].

Como se não bastasse, o caráter descentralizado do armazenamento de dados (muitas vezes em fracionados em múltiplos servidores "na nuvem") acaba gerando o fenômeno da ubiquidade digital. Em algumas situações, a coleta de dados de uma única pessoa, a exemplo de um suspeito de atividade terrorista, poderia resultar em dezenas de pedidos de cooperação internacional, na medida em que seus dados podem estar pulverizados em servidores localizados em diversos países. E mais: periodicamente, esses dados podem ser automaticamente remanejados a outros servidores, em razão de ferramentas automatizadas de realocação por eficiência. Isso pode gerar a constante perda de objeto dos pedidos de cooperação, decorrente da migração de dados. Em algumas situações, nem mesmo o representante do provedor de aplicações pode saber, com facilidade, em que país se encontra

170. MENDES, Gilmar Ferreira; FERNANDES, Victor Oliveira. Constitucionalismo digital e jurisdição constitucional: uma agenda de pesquisa para o caso brasileiro. *Revista Brasileira de Direito*, vol. 16, n. 1, p. 1-33, 2020, p. 24.

171. Cf. PORTAL JOTA. O alcance do MLAT em investigações criminais em debate no STF: Audiência pública reuniu autoridades brasileiras, pesquisadores, representantes de empresas e dos EUA. Disponível em: https://www.jota.info/coberturas-especiais/liberdade-de-expressao/mlat-stf-audiencia-11022020. Acesso em: 9 dez. 2021.

o servidor de alocação, em razão da existência de algoritmos automatizados que cuidam dessa tarefa.

Como resolver o impasse?

A melhor solução parece ser aquela já prevista no *caput* do art. 11 do MCI, ao estabelecer a aplicação da lei brasileira sempre que ao menos uma das operações indicadas (coleta, armazenamento, guarda ou tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet) ocorra em território nacional. Eis o lastro de territorialidade a fundamentar o exercício da jurisdição.

Uma segunda opção consistiria na adoção, como solução intermediária, daquilo que estabelece *CLOUD Act* americano. Assim, como regra, os provedores de aplicações de internet deveriam cumprir os mandados judiciais de requisição de dados, ainda que estejam armazenados fora Brasil; excepcionalmente, a requisição direta poderia ser afastada quando a coleta dos dados puder ensejar uma violação das leis do país estrangeiro[172]. Prestigia-se o regime mais protetivo aos direitos fundamentais. Essa solução, porém, pode se tornar de difícil aplicação na hipótese de atividades desenvolvidas, ao mesmo tempo, em múltiplos países (como na ubiquidade digital). Além disso, pode resultar, a longo prazo, em um estímulo aos provedores de aplicações, de modo a estabelecerem suas sedes em locais estratégicos, com o objetivo de se furtar ao cumprimento das obrigações.

172. Cf. https://www.justice.gov/dag/cloudact. Acesso em: 9 dez. 2021.

5. CONCLUSÃO

Ao final do exposto, apresentam-se as seguintes conclusões, sem prejuízo de outras ilações realizadas ao longo do texto.

Ao longo dos três primeiros capítulos, duas importantes premissas foram estabelecidas. A primeira consiste na compreensão do devido processo legal como uma garantia adaptativa do *rule of law,* que há de ser responsavelmente ampliada para novos contextos fora da relação indivíduo-Estado. A segunda é percepção da 4ª revolução industrial como um fenômeno que trouxe novos desafios jurídicos à humanidade, sobretudo no campo da proteção dos direitos fundamentais. Enquanto o constitucionalismo tem sido tradicionalmente desenvolvido para limitar os poderes governamentais, novas forças privadas surgiram ameaçando a proteção dos direitos fundamentais.

Na realidade ora experimentada, não apenas atores privados têm exercido, de forma discricionária, poderes capazes de afetar diretamente o gozo de direitos fundamentais pelas pessoas em geral, como também o Poder Público tem utilizado ferramentas algorítmicas em variados campos, sem as garantias adequadas. Em ambos os casos, é possível identificar uma elevada concentração de poder, em detrimento da autonomia dos indivíduos.

Esse contexto permite estabelecer os contornos do que pode ser denominado "devido processo digital", "devido processo tecnológico" ou "devido processo 4.0" em suas dimensões procedimental e substantiva. Tal instituto jurídico há de ser compreendido como o elemento-chave capaz de impedir a escalada

do tecnoautoritarismo, firmando um marco civilizatório mínimo do humanismo digital.

A incidência da cláusula do devido processo legal nas relações envolvendo indivíduos e o Estado é tema menos problemático. Afinal, desde as suas mais remotas influências históricas, a cláusula opera como uma espécie de metonímia do Estado de Direito, prevenindo os indivíduos contra ações estatais arbitrárias.

Na ausência das garantias mínimas para um ecossistema digital, será possível a intervenção judicial preventiva (*ex post*) ou repressiva (*ex ante*), em forma de tutela individual ou coletiva. Particularmente quanto às garantias relativas ao exercício do contraditório e da ampla defesa, elas variarão de acordo com a gravidade da privação ao direito, conforme reconhecido pela SCOTUS em *Mathews v. Eldridge*. Em outras palavras, as garantias, se não previamente estabelecidas em lei, deverão ser extraídas das características de um assunto em particular, a exemplo da severidade da privação e do interesse público existente.

Mas há algo além das relações entre indivíduos e Estado. O regime de quase monopólio, a questionável manipulação de dados privados e a massiva tendência expansiva sobre outros campos desafia não apenas o exercício de direitos fundamentais, mas também a institucionalização da esfera pública digital. Afinal, o monopólio informacional torna-se um problema para a constituição das novas mídias, o que não se reduz a questões econômicas. Cuida-se de um contexto que questiona a própria constituição da internet global, marcada por relações assimétricas de poder. A falta de transparência em suas estruturas de governança levanta questões constitucionais de democracia e de controle público. Essa abordagem parte do pressuposto de que os direitos constitucionais servem não apenas à proteção de direitos individuais, mas também de instituições sociais vulneráveis, como a arte ou a ciência, afastando-as de tendências totalizantes que operam na sociedade.

Disso decorre que a permeabilidade da cláusula do devido processo legal, como metonímia do Estado de Direito, às relações assimétricas travadas no contexto das tecnologias digitais