e92408
https://doi.org/10.5007/2177-7055.2024.e92408

ARTIGO ORIGINAL

Esboço de um devido processo digital: garantias mínimas para uma persecução penal em rede

Outline of a digital due process: minimum guarantees for a networked criminal prosecution

João Paulo Lordelo Guimarães Tavares[1]
[1]Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa, Brasília, Brasil.

Resumo: O artigo pretende responder ao seguinte problema de pesquisa: quais garantias podem ser extraídas de uma compreensão evolutiva da cláusula do devido processo legal, no contexto do emprego das novas tecnologias digitais para fins de persecução penal? A hipótese – confirmada a título de conclusão – é a de que o uso de recursos tecnológicos digitais pelo Poder Público, inclusive com o emprego de algoritmos de inteligência artificial, é algo irrefreável, sendo capaz de agregar utilidades, notadamente no âmbito decisório. Por outro lado, o seu emprego, especialmente no campo da persecução penal, implica o reconhecimento de novas garantias e deveres acentuados de transparência e *accountability*, havendo suporte normativo e meios tecnológicos de promovê-los de forma satisfatória e sem prejuízo à propriedade industrial. Em conclusão, tais garantias comporiam uma dimensão procedimental contemporânea da cláusula do devido processo legal. Os suportes fáticos e teóricos do trabalho são fornecidos por uma análise comparatista, com destaque para relatórios, a disciplina normativa e a jurisprudência dos Estados Unidos e da Comunidade Europeia. O método de abordagem empregado é o hipotético-dedutivo.

Palavras-chave: Devido processo legal. Tecnologias digitais. Algoritmos. Transparência.

Abstract: The article aims to answer the following research problem: what guarantees can be extracted from an evolving understanding of the due process clause, in the context of the use of new digital technologies for the purposes of criminal prosecution? The hypothesis – confirmed as a conclusion – is that the use of digital

technological resources by the Public Power, including the use of artificial intelligence algorithms, is something unstoppable, being able to add utilities, notably in the decision making field. However, its use, especially in the field of criminal prosecution, implies the recognition of new guarantees and enhanced duties of transparency and accountability, with normative support and technological means to promote them satisfactorily and without damage to industrial property. In conclusion, such guarantees would compose a contemporary procedural dimension of the due legal process clause. The factual and theoretical supports of the work are provided by a comparative analysis, with emphasis on reports, the normative discipline and the jurisprudence of the courts in the United States and the European Community. The method used is the hypothetical-deductive approach.

KEYWORDS: Due process of law. Digital technologies. Algorithms. Transparency.

1 INTRODUÇÃO

Em 2005, Antoine Jones foi preso com posse de drogas, após a polícia de Washington, D. C., ter anexado um rastreador GPS em seu carro, acompanhando o seu percurso por cerca de um mês. À época, a autoridade investigativa compreendeu ser desnecessária prévia autorização judicial para tanto, por se tratar de método de investigação similar ao acompanhamento do veículo por um agente policial à paisana, para o qual inexiste a exigência.

Em sede de recurso, a Suprema Corte dos Estados Unidos entendeu que a medida investigativa empregada deveria ser equiparada a uma busca e apreensão sujeita a prévia autorização judicial, em razão do que dispõe a 4ª emenda à Constituição. Consequentemente, a prova foi considerada ilícita.

Para a Corte, o importante foi a compreensão de que o Governo ocupou fisicamente propriedade privada com o objetivo de obter informações (*trespass*). O fundamento, contudo, desperta dúvidas. Afinal, o que diria a Corte se o monitoramento houvesse sido realizado por meio de um satélite de vigilância, sem contato físico? A questão de fundo parecia ser outra: a potencialização da capacidade de vigilância, inaugurada pelas recentes viradas tecnológicas, exige uma

interpretação evolutiva da cláusula do devido processo legal. Décadas atrás, o monitoramento tradicional, aplicado na extensão do caso, seria certamente uma providência de difícil realização, além de custosa. A tarefa que, hoje, um GPS realiza com facilidade demandaria um grande número de agentes, múltiplos veículos e até mesmo assistência aérea.

Essa importante premissa foi notada pelo *justice* Alito, que integrou a maioria no resultado, embora com fundamentos distintos. De fato, a questão fática relevante ao caso não parecia ser a "presença física" do Estado na propriedade de Jones, mas algo além: o uso de um aparato tecnológico (GPS) para fins de rastreamento de longo prazo.

Nos últimos anos, a humanidade assiste ao surgimento de novos dispositivos que permitem o monitoramento dos movimentos de uma pessoa em detalhes, não apenas pelo Estado, mas também por companhias privadas. Aparelhos celulares registram, com precisão, até mesmo dados biométricos dos seus usuários, como o tom de voz, impressões digitais e batimentos cardíacos. Cuida-se do produto da chamada "quarta revolução industrial" expressão que se popularizou com Klaus Schwab, no Forum Econômico Mundial de 2016, como referência às novas ondas tecnológicas. Essas tecnologias modernas compreendem variados campos, a exemplo da "internet das coisas" (*Internet of Things* – IOT), da inteligência artificial, big data e da computação na nuvem.

Essas rápidas e constantes inovações tecnológicas têm o potencial de promover uma ampla gama de benefícios. Mas os atributos que as fazem tão especiais – a exemplo da capacidade de aprendizado a partir de dados e, portanto, de evoluir no tempo sem um input humano explícito – também levantam preocupações. Isso ocorre em especial no que diz respeito aos desafios necessários à defesa dos direitos fundamentais, como o direito à vida, o direito ao devido processo legal, o direito à presunção de inocência e o direito à privacidade.

Bem observados os crescentes dilemas que se apresentam nesse contexto, parece haver uma questão jurídica central a uni-los. Todos eles estão, de alguma forma, ligados ao exercício de garantias procedimentais

e substantiva historicamente extraídas do princípio do devido processo legal. Seria então possível falar em um "novo" devido processo, a partir do que se tem denominado de constitucionalismo digital?

Firmadas tais premissas, o presente artigo pretende responder ao seguinte problema de pesquisa: quais garantias procedimentais e substantivas mínimas devem ser asseguradas, no campo da persecução penal, de forma a se promover adequadamente o devido processo legal no contexto da virada tecnológica?

A hipótese é a de que o uso de recursos tecnológicos de inteligência artificial pelo Poder Público é algo irrefreável, sendo capaz de proporcionar diversos benefícios, notadamente no âmbito decisório. A sua utilização, especialmente no campo da persecução penal, implica o reconhecimento de deveres acentuados de transparência e *accountability*, havendo meios tecnológicos de promovê-los de forma satisfatória e sem prejuízo à propriedade industrial.

Para tanto, será inicialmente exposto o alcance da cláusula do devido processo legal na jurisprudência norte-americana. Em seguida, serão expostos alguns riscos no uso de algoritmos no campo da persecução penal. Ao final, serão desenvolvidos alguns princípios mínimos que podem ser extraídos de uma interpretação evolutiva da cláusula do devido processo legal.

Os suportes fáticos e teóricos são fornecidos por uma análise comparatista, com destaque apara os relatórios e a disciplina normativa produzia no âmbito da Comunidade Europeia.

O método de abordagem empregado é o hipotético-dedutivo.

2 DEVIDO PROCESSO LEGAL: HISTÓRIA E CONTEÚDO NA JURISPRUDÊNCIA NORTE-AMERICANA

O conjunto de três palavras que forma a expressão "devido processo legal" é uma representação simples e fiel da fusão de uma complexa forma de pensar politicamente e juridicamente (Pasquale,

2021, p. 42-56). Tamanha a sua relevância, a cláusula do devido processo – numa visão que supera a sua dimensão exclusivamente "procedimental" – é usualmente confundida com a própria noção de Estado de Direito (Allan, 2003, p. 121).

Embora não mencione expressamente a expressão *rule of law,* a Constituição dos Estados Unidos de 1787 é certamente o resultado de muitos princípios do Estado de Direito desenvolvidos na Europa ao longo dos séculos. Isso não ocorreu por acaso. O pensamento político dos colonos foi fortemente influenciado por escritos da antiguidade clássica, pelos autores iluministas – entre eles John Loke –, pela *common law* inglesa e pelas teorias puritanas. Todas essas fontes influenciaram não apenas a Declaração de Independência, mas a Constituição e o posterior *Bill of Rights* americano, consistente nas dez primeiras emendas (Lutz, 1984, p. 189-197).

A sua redação original, todavia, não contemplava a cláusula do devido processo legal. A garantia foi inserida na 5ª e 14ª emendas, cujos textos têm evidente inspiração na Magna Carta.

O texto da cláusula do devido processo legal trazida pela 14ª emenda à Constituição dos Estados Unidos informa as categorias de direitos em que há de ser aplicada: vida, liberdade e propriedade. Cada uma delas integra o núcleo do exercício da cidadania em uma democracia. Além disso, esses direitos representam qualitativamente o nível de seriedade do ato de privação para justificar a invocação do devido processo, além de refletirem o tipo de dano que se quer prevenir (Crawford; Schultz, 2014, p. 110).

Nos dias atuais, é possível conceituar razoavelmente a dimensão procedimental do devido processo legal como a exigência constitucional de que qualquer privação da vida, liberdade ou propriedade de uma pessoa *empreendida pelo Estado* deve ser precedida de garantias mínimas. Essas garantias compreendem, em essência, o direito de ser notificado (contraditório), o direito de se defender (na tradição anglo-americana, o "direito de ser ouvido") e o direito a um julgador imparcial (Crawford; Schultz, 2014, p. 110).

Historicamente, o constitucionalismo norte-americano desenvolveu essa dimensão do *due process* a partir de dois casos julgados pela Suprema Corte: *Goldberg v. Kelly* (1970) *e Mathews v. Eldridge* (1976).

No primeiro, compreendeu o Tribunal, por maioria (5 a 3), que a dimensão procedimental do devido processo legal impõe que o Poder Público implemente audiências probatórias antes de encerrar benefícios assistenciais, ocasião em que os beneficiários podem ser ouvidos. Benefícios assistenciais foram compreendidos como elementos integrantes da propriedade dos beneficiários, e não como privilégios. Além disso, compreendeu a Corte que o Estado não precisaria oportunizar um procedimento completo, como aqueles de natureza judicial, sendo suficiente o respeito a quatro garantias procedimentais (Suprema Corte dos Estados Unidos, 1970): a) oportunidade de ser ouvido adequadamente; b) prévia e adequada notificação; c) oportunidade de apresentar testemunhas; d) oportunidade de apresentar argumentos e evidências.

Mais significativo foi o caso *Mathews v. Eldridge,* de 1976, em que a corte acabou mitigando o precedente anteriormente estabelecido em *Goldberg.* Embora os fatos do caso fossem bastante similares àqueles apresentados seis anos antes, o resultado foi diverso. Por maioria (6 a 2), a Corte compreendeu que o devido processo seria uma garantia flexível, a depender das circunstâncias do caso concreto (Redish; Marshall, 1986). Além disso, argumentou que, "em alguns casos, o benefício ou a garantia adicional para o indivíduo afetado pela ação administrativa e também para a sociedade, em termos de garantia de uma decisão justa, pode ser compensado pelos custos da garantia" (Suprema Corte dos Estados Unidos, 1976). A fim de balancear as garantias previamente estabelecidas em *Goldberg,* a Corte estabeleceu um teste voltado à análise da constitucionalidade da privação de liberdade ou propriedade por uma ação estatal.

Esse teste consiste no sopesamento de três elementos: a) primeiro, o interesse privado que será afetado por uma ação estatal; b) segundo, o risco de uma privação errônea de tal interesse por meio dos

procedimentos usados, e o valor provável, se houver, de salvaguardas processuais adicionais ou substitutas; c) terceiro, o interesse do Estado, incluindo a função envolvida e os encargos fiscais e administrativos que a exigência processual complementar ou substitutiva implicaria.

Em síntese, pelo precedente estabelecido em *Mathews v. Eldridge*, a Suprema Corte dos Estados Unidos fixou a orientação no sentido de que o devido processo legal, em sua dimensão procedimental, varia de acordo com a gravidade da privação e a magnitude do interesse estatal contraposto.

3 O IMPACTO DO GIRO TECNOLÓGICO NO CAMPO DA PERSECUÇÃO PENAL

Para além da quebra de sigilo de dados, procedimento normalmente utilizado mediante prévia autorização judicial e com o objetivo específico de desvendar um ilícito já ocorrido (dimensão *retrospectiva*), novas técnicas algorítmicas têm sido desenvolvidas para uso também no campo *preditivo,* ou seja, com o objetivo de prevenir ilícitos (dimensão *prospectiva*) ou conhecer delitos ainda desconhecidos (Castets-Renard, 2021, p. 42-56).

Dois conceitos são fundamentais para a compreensão dos algoritmos de prevenção criminal: correspondência de dados (*data matching*) e mineração de dados (*data mining*).

Entende-se por *data matching* o conjunto de técnicas de comparação automatizada de dois ou mais bancos de dados pessoais. Também conhecidas como *subject-based inquiries,* essas técnicas iniciam com um sujeito previamente identificado, na tentativa de construção de um perfil completo a partir das suas atividades, relação com outros indivíduos, locais ou eventos. No setor público, elas auxiliam na identificação de fraudes e abusos na obtenção de benefícios assistenciais (Steinbock, 2005, p. 10-11). Os resultados do *data matching* podem ser utilizados de forma *reativa*, de modo a revelar eventos passados – a

exemplo da comparação da análise dos dados profissionais, fiscais e patrimoniais de um determinado indivíduo, que podem indicar enriquecimentos ilícitos.

Diversamente, a mineração de dados (*data mining*) é um conjunto de técnicas que têm como foco padrões qualitativos e comportamentais utilizados em julgamentos *preditivos*. Essas técnicas utilizam análise estatística e modelagem, de forma a identificar padrões em dados que permitam inferir regras capazes de prever resultados futuros. O *data mining* é também conhecido como *dataveillance*, cuja origem remonta às práticas comerciais de individualização de marketing e definição de riscos na indústria dos seguros (Steinbock, 2005, p. 13).

Nos Estados Unidos, especialmente após o decreto do *Patriot Act,* assinado logo após o atentado de 11 de setembro de 2001, o uso de técnicas de *data matching* e *data mining* para fins *preventivos* – em contraste com as práticas reativas – cresceu sensivelmente. A título de exemplo, no ano de 2003, foi criado o *Terrorist Screening Center* (TSC), agência vinculada ao *Federal Bureau of Investigation* (FBI) responsável por consolidar uma *watchlist*, banco de dados contendo nome de suspeitos de participarem de atividades terroristas (*Terrorist Surveillance Program* – TSP). Esse banco de dados utiliza, entre outras técnicas não reveladas ao público, o cruzamento de informações extraídas de registros telefônicos e de e-mail de milhões de americanos (Citron, 2008, p. 1.257).

Sérias preocupações foram levantadas não apenas sobre a legalidade do TSP, mas também sobre a "crueldade" dos algoritmos que ele emprega e as informações imprecisas nas quais se baseia. Algoritmos não sofisticados e dados incorretos resultam em altas taxas de falsos positivos que podem servir como base para investigações criminais infundadas e estigmatizantes (Citron, 2008, p. 1.257).

Além disso, novos algoritmos têm sido utilizados não apenas para auxiliar investigações, mas também para fins *decisórios* – o que pode variar desde o impedimento de empréstimo de livros em bibliotecas públicas até a proibição de viagens aéreas a passageiros suspeitos – *passenger profiling* e *no-fly list* (O'Connor; Rumann, 2003). Há, portanto,

desde 2001, um sensível movimento na análise de dados: da reação à prevenção e da investigação à decisão.

Os modelos mais comuns costumam utilizar dados como datas, horários, tipos e locais de crimes recentemente cometidos com o objetivo de identificar "lugares quentes" que podem ser objeto de atuação policial mais intensa (Friend, 2013). Ocorre que a intensificação da supervisão policial, com o aumento de prisões, resultará em mais dados históricos para o local, reforçando ainda mais a atuação policial (Crawford; Schultz, 2014, p. 104).

Embora seja inegável o salto de eficiência proporcionado por algoritmos no campo da prevenção criminal, não são poucas as pesquisas acadêmicas que têm levantado preocupações, especialmente no que concerne à discriminação em desfavor de minorias.

Em artigo publicado em 2017, Danielle Kehl, Priscilla Guo e Samuel Kessler registram que, por um lado, os algoritmos preditivos podem trazer maior objetividade nos processos criminais, reduzindo o risco de erros humanos. Por outro, existe o risco de que, mal utilizados, possam reforçar vieses e prejudicar a aplicação da justiça, sobretudo se a raça, o gênero e a posição social de indivíduos forem considerados como variáveis preditivas (Kehl; Guo; Kessler, 2017).

Em trabalho publicado em 2019, Sandra Mayson defende que, no que diz respeito aos vieses raciais, o problema reside na própria natureza da *previsão*. Todos sistemas preditivos observam o passado para tentar adivinhar futuros eventos. Assim, em um mundo racialmente estratificado, qualquer método de predição projetará essas desigualdades do passado para o futuro (Mayson, 2019).

Exemplo preocupante foi exposto em 2007, pelo McClatchy-Tribune Information Services: nos Estados Unidos, a cada semana, cerca de 1.500 viajantes de avião são supostamente rotulados erroneamente como terroristas devido a erros no programa de comparação de dados – *no-fly list* (Gordon, 2007). Indivíduos inocentes enfrentam muitos questionamentos e perdem voos, sem nunca saber por que o sistema automatizado os destacou.

Para se ter uma noção da imprecisão do sistema, entre 2005 a 2008, o *no-fly* impediu dois senadores federais, um diplomata, um empregado de uma companhia aérea e uma criança de quatro anos de viajarem. Um piloto da American Airlines informou, perante depoimento a um comitê do Senado, que havia sido detido oitenta vezes em um ano, em razão do sistema (Citron, 2008, p. 1.274). Além disso, inexistem meios garantidos de limpar seus nomes, de modo que as mesmas pessoas podem ser constantemente detidas toda vez que tentarem embarcar em um avião (Citron, 2008, p. 1.251).

4 DEVIDO PROCESSO FORMAL: GARANTIAS MÍNIMAS PARA UM ECOSSISTEMA DIGITAL

Excluídos os princípios aplicáveis, de forma geral, às relações públicas (boa-fé, legalidade, transparência, não discriminação etc.), uma análise conjunta dos riscos do uso de algoritmos decisórios e das normas que já disciplinam o processamento de dados pessoais permite a definição de um esboço normativo próprio ao uso de algoritmos no ambiente estatal, o que inclui a persecução penal.

Isso porque as preocupações relativas à violação de direitos fundamentais pelo uso de algoritmos decorrem, em especial, de três achados: a opacidade dos algoritmos, o emprego de *inputs* viciados e a discriminação que pode ser gerada com o seu uso. Uma proposta de regime jurídico de mínima regulação algorítmica há de, ao menos, considerar esses três problemas, possibilitando a sua correção.

4.1 Contraditório e ampla defesa

Conforme racional extraído do precedente fixado pela SCOTUS em *Mathews v. Eldridge*, 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.

Essa margem de flexibilidade, contudo, há de ser observada somente após o estabelecimento de um conjunto mínimo de garantias e valores, evitando-se uma abordagem excessivamente abstrata (Redish; Marshall, 1986, p. 456). Isso porque os valores centrais que a cláusula representa e impõe devem estar sempre presentes, a exemplo da previsibilidade, da transparência e da racionalidade (Redish; Marshall, 1986, p. 474). 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 (Crawford; Schultz, 2014, p. 110). Consequentemente, mais garantias podem ser exigidas.

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 (Crawford; Schultz, 2014, p. 116-125). 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 (Citron; Pasquale, 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 (Citron; Pasquale, 2014). 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 (Citron, 2010). Em todos esses casos, ferramentas são responsáveis por classificar indivíduos, transformados em objetos de pontuação (Ritchel, 2013).

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 (Citron, 2008, p. 1.282).

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 (Brennan-Marquez; Henderson, 2019, p. 137). 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 (Pasquale, 2021, p. 46). Particularmente no âmbito estatal, essa garantia parece ser absolutamente imprescindível em qualquer atividade, evitando-se o processo decisório inteiramente automatizado.

4.2 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 (Brown; Davidovic, 2021).

Sem auditabilidade, qualquer ferramenta se transformará em uma caixa-preta, impossibilitando tanto o conhecimento da sua funcionalidade quanto a transparência (Bathaee, 2018).

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. 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 produzir uma gama de detalhes de avaliação, abrangendo essas três categorias – regulamentação, gestão de risco e avaliação ética geral (Brown; Davidovic, 2021). Em se tratando de algoritmos de automação decisória, essas informações compreendem ao menos três categorias (Villasenor; Foggo, 2020, p. 339-340).

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. 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*). 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 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 (BBC Bitesize, 2023), de modo a registrar o os algoritmos de uma forma mais compreensível, mediante técnicas representativas (Villasenor; Foggo, 2020, p. 341).

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.

Cada vez mais, os desenvolvedores de algoritmos de inteligência artificial são confrontados com a necessidade de compreender o que os seus modelos têm aprendido (Bücker et al., 2021, p. 1-21). Em alguns campos, sobretudo quando utilizados modelos mais genéricos de *machine learning*, soluções eficientes têm sido apresentadas a exemplo do modelo de *Transparency, Auditability and eXplainability for Credit Scoring* – TAX4CS (Bücker et al., 2021, p. 13). Em muitos outros, porém, tanto a auditabilidade quanto a transparência consistem em algo de difícil implementação (Tian et al., 2016, p. 2175-2187). 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").

4.3 Princípio da transparência e direito a explicacões 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.

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 (Villasenor; Foggo, 2020, p. 343). 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 (Suprema Corte dos Estados Unidos, 1963). 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" (Won, 2021).

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 (Won, 2021). Disso decorre a preferência pela aquisição de sistemas de código aberto, como indicado no art. 24 da Resolução CNJ nº 332/2020.

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 (Villasenor; Foggo, 2020, p. 344).

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*). Por se tratar de um considerando, o texto não pode ser considerado vinculante.

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" (Wachter; Mittelstadt; Russell, 2018, p. 880).

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".

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. 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 (Kroll et al., 2017, p. 657). A publicidade, por si só, não é suficiente para promover *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 (Wachter; Mittelstadt; Russell, 2018, p. 841-888, 2018).

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* (Wachter; Mittelstadt; Russell, 2018, p. 843).

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 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 (Wachter; Mittelstadt; Russell, 2018, p. 844).

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".

Aplicando-se ao campo das decisões automatizadas, imagine-se uma situação em que foi negado um benefício da execução penal a uma determinada pessoa, com fundamento em seus dados pessoais. Uma explicação contrafactual poderia ser apresentada da seguinte forma:

"você não conseguiu o benefício porque lhe faltam os pressupostos x, y e z. Se você reunisse tais pressupostos, teria conseguido o benefício".

Explicações contrafactuais podem prover: a) as razões pelas quais a decisão em particular foi proferida (ex.: ausência de residência fixa); b) razões para permitir a impugnação da decisão (se, por exemplo, o sistema utilizou dados imprecisos a respeito do interessado); e c) informações sobre como obter uma futura decisão favorável (Wachter; Mittelstadt; Russell, 2018, p. 882). 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).

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.

4.4 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 (Kroll et al., 2017, p. 656).

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.

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 (Villasenor; Foggo, 2020, p. 343).

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

4.5 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 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 (Barcellos, 2008).

No campo da automação tecnológica, uma importante medida de implementação do controle social consiste na divulgação do código-fonte dos *softwares* utilizados ao público (Citron, 2008, p. 1.308). Uma opção a ser avaliada consiste na utilização de sistemas de código aberto (LEE, 2006), 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, outra 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. 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 do processo de votação e apuração das eleições e o processamento eletrônico da totalização dos resultados.

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 (Citron, 2008, p. 1.311).

5 CONCLUSÃO

O uso de recursos tecnológicos de inteligência artificial pelo Poder Público é algo irrefreável, sendo capaz de proporcionar diversos benefícios, notadamente no âmbito decisório. Em razão da possibilidade de aprender pela experiência, os algoritmos de IA são capazes de adaptação e evolução. Consequentemente, os sistemas podem criar as próprias regras ou perguntas, sem a necessidade de que um programador preveja soluções específicas para as situações possíveis. Isso se deve, sobretudo, às técnicas de *machine learning*.

No âmbito público, os riscos do emprego de algoritmos de inteligência artificial envolvem atividades como a prevenção criminal. Novas técnicas têm sido desenvolvidas para uso também no campo *preditivo,* ou seja, com o objetivo de prevenir ilícitos (dimensão *prospectiva*) ou conhecer delitos ainda desconhecidos. É o caso do *data matching* e da mineração de dados (*data mining*). Não são poucas as pesquisas acadêmicas que têm levantado preocupações, especialmente no que concerne à discriminação em desfavor de minorias.

Em síntese, as preocupações relativas à violação de direitos fundamentais pelo uso de algoritmos decisórios decorrem, em especial, de três achados: a opacidade dos algoritmos, o emprego de *inputs* viciados e a discriminação que pode ser gerada com o seu uso. Em virtude disso, a sua utilização, especialmente no campo da persecução penal, implica o reconhecimento de deveres acentuados de transparência e *accountability*, havendo meios tecnológicos de promovê-los de forma satisfatória e sem prejuízo à propriedade industrial.

Excluídos os princípios aplicáveis, de forma geral, às relações públicas (boa-fé, legalidade, transparência, não discriminação etc.), uma análise conjunta dos riscos do uso de algoritmos decisórios e das normas que já disciplinam o processamento de dados pessoais permite a definição de um esboço normativo próprio ao uso de algoritmos na persecução penal. A proposta apresentada no presente trabalho contempla ao menos quatro princípios, capazes de contornar o déficit

procedimental atualmente experimentado: contraditório digital, auditabilidade, transparência, consistência ou regularidade procedimental e controle social. Tais garantias integram uma dimensão procedimental contemporânea da cláusula do devido processo legal.

REFERÊNCIAS

ALLAN, T. R. S. Constitutional Justice: **A Liberal Theory of the Rule of Law**. Oxford: Oxford University Press, 2003.

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.

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 Design: 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.

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. 2022.

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

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

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. 2022.

CASTETS-RENARD, C. Human Rights and Algorithmic Impact Assessment for Predictive Policing. In MICKLITZ, H.; POLLICINO, O.; REICHMAN; A.; SIMONCINI, A.; SARTOR, G.; DE GREGORIO, G. (Eds.), **Constitutional Challenges in the Algorithmic Society**. Cambridge: Cambridge University Press, 2021.

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. 2022.

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

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

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

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

FRIEND, Zach. Predictive Policing: Using Technology do Reduce Crime. **FBI L. Enforcement Bull**, 2013. Disponível em: https://leb.fbi.gov/articles/featured-articles/predictive-policing-using-technology-to-reduce-crime. Acesso em: 4 nov. 2022.

GORDON, Greg. `Data mining' may implicate innocent people in search for terrorists. **McClatchy-Tribune Information Services**. Disponível em: https://www.mcclatchydc.com/latest-news/article24460132.html. Acesso em: 08 nov. 2022.

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.

KEHL, Danielle; GUO, Priscilla; KESSLER, Samuel. Algorithms in the Criminal Justice System: Assessing the Use of Risk Assessments in Sentencing. **Responsive Communities Initiative, Berkman Klein Center for Internet & Society, Harvard Law School**, 2017. Disponível em:

https://dash.harvard.edu/bitstream/handle/1/33746041/2017-07_responsivecommunities_2.pdf. Acesso em 12 out. 2020.

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.

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.

LUTZ, Donald. The Relative Influence of European Writers on Late Eighteenth-Century American Political Thought. **The American Political Science Review**. Vol. 78, p. 189-197, 1984.

MAYSON, Sandra G. Bias In, Bias Out. **Yale Law Journal**, v. 128, 2019.

O'CONNOR, Michael P; RUMANN, Celia. Into the Fire: How to Avoid Getting Burned by the Same Mistakes Made Fighting Terrorism in Northern Ireland. **Cardozo Law Review**, v. 24, 2003.

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. 2022.

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**. Cambridge: Cambridge University Press, 2021.

REDISH, Martin H.; MARSHALL, Lawrence C. Adjudicatory Independence and the Values of Procedural Due Process. **Yale Law Journal**, vol. 95, n. 3, 1986.

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. 2022.

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.

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

STEINBOCK, Daniel J. Data Matching, Data Mining and Due Process. **Georgia Law Review**, v. 40, n. 1, 2005.

SUPREMA CORTE DOS ESTADOS UNIDOS, **Goldberg v. Kelly**, 397 U.S. 254, 1970.

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

SUPREMA CORTE DOS ESTADOS UNIDOS. **Brady v. Maryland**, 373 U.S. 83, 1963.

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.

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

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.

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.

JOÃO PAULO LORDELO GUIMARÃES TAVARES

Graduado em Direito pela Universidade Federal da Bahia. Especialista em Direito do Estado. Mestre em Direito Público pela Universidade Federal da Bahia. Mestre em Direito Constitucional pela Universidad de Sevilla. Doutor em Direito pela Universidade

Federal da Bahia. Realizou pesquisa de pós-doutoramento em Direitos Humanos pela Universidade de Coimbra e desenvolve segunda pesquisa de pós-doutoramento na Universidade do Estado do Rio de Janeiro (UERJ). Professor do programa de mestrado do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP). Professor da graduação em Direito da Universidade Presbiteriana Mackenzie. Pesquisador Visitante (Visiting Scholar) do Centre for Socio-Legal Studies da Universidade de Oxford (Oxford Faculty of Law). Professor visitante da Universidade Vytautas Magnus (Lituânia). Orientador pedagógico e professor da Escola Superior do Ministério Público da União (ESMPU). Membro da comissão avaliadora da Revista de Processo (REPRO), da Civil Procedure Review e da Seqüência Estudos Jurídicos e Políticos (UFSC - Q A.1). Membro do Conselho Consultivo sobre Internet e Eleições do Tribunal Superior Eleitoral (2018). Membro da comissão de juristas da Câmara dos Deputados de reforma da Lei de Lavagem de Capitais (2021). Coordenador da Assessoria Jurídica Criminal do Gabinete do Procurador-Geral da República junto ao Supremo Tribunal Federal (2020-2021). Coordenador do Grupo de Trabalho sobre Inovações no Processo Coletivo do Conselho Nacional do Ministério Público (CNMP). Ex-Defensor Público Federal (2010-2014), é membro do Ministério Público Federal (Procurador da República) em São Paulo.

Endereço profissional: SGAS II St. de Grandes Áreas Sul 607 Módulo 49 - Asa Sul, Brasília - DF, 70200-670, Brasil.

Orcid id: https://orcid.org/0000-0002-5190-2835

E-mail: joaolordelo@gmail.com

Recebido em: 04/01/2023
Aceito em: 05/09/2023