

Discriminação algorítmica: para que fins e como devem ser julgadas as pessoas?

A necessária discussão sobre o que é inaceitável e o que é aceitável desde que
com as devidas salvaguardas

Parte IX

Ana Frazão

Advogada. Professora de Direito Civil e Comercial da UnB. Ex-Conselheira do
CADE.

Como se observou ao longo da presente série, a solução do problema da discriminação algorítmica requer o endereçamento de muitas questões prévias, dentre as quais a de saber que dados pessoais podem ser tratados e para que fins.

Vale ressaltar que tal análise igualmente exige a reflexão sobre a congruência entre a finalidade legítima e os dados tratados para atingi-la, a fim de evitar discriminações indevidas. Um dos exemplos de distorção consta da obra de Cathy O’Neil, retratada no artigo anterior¹, ao salientar que algoritmos utilizados por companhias de seguros de carro privilegiam motoristas ricos, mesmo com mau histórico de direção, em detrimento dos motoristas pobres, mesmo com bom histórico de direção.

Todos esses problemas potencializam-se diante do fenômeno da datificação, em que toda experiência humana é transformada em dados. Consequentemente, diante da extensão do que pode ser considerado dado pessoal, a sua mera coleta já apresenta riscos significativos, como os

¹ <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/discriminacao-algoritmica-por-que-algoritmos-preocupam-quando-acertam-e-erram-04082021>

relacionados à cibersegurança. Afinal, quanto mais dados pessoais são coletados, maiores os riscos de incidentes de segurança, como vazamentos, bem como de utilizações indevidas e discriminatórias².

Sob essa perspectiva, não há como se separar a temática da discriminação algorítmica de discussões mais amplas sobre a licitude do tratamento de dados e sobre os procedimentos de segurança, já que um dos maiores riscos de incidentes é a utilização dos dados para fins outros que não os que justificaram originariamente o tratamento, incluindo fins ilícitos ou discriminatórios.

Sobre o tema, vale lembrar a recente polêmica envolvendo o Pegasus, sistema desenhado para auxiliar governos na luta contra o crime e o terrorismo, mas que acabou sendo utilizado para rastrear jornalistas, advogados e ativistas, o que mostra os riscos de perseguições e discriminações por motivos políticos e o seu potencial de reforçar tendências autoritárias de governos³.

Além dos riscos de segurança, é necessário que se reflita igualmente sobre os limites de julgamentos e perfilizações de indivíduos. No seu livro *Privacy is power. Why and how you should take back control of your data*⁴, Carissa Véliz faz uma interessante contextualização da discussão, ao ressaltar alguns dos perfis que têm sido utilizados para os mais diversos fins, incluindo os comerciais: pessoas que foram vítimas de estupro, incesto ou outros abusos sexuais, pacientes de AIDS ou de doenças sexualmente transmissíveis, homens com impotência sexual, dentre outros. Daí a constatação da autora de que os interessados nesse tipo de categorização agem como verdadeiros predadores, que sentem o “cheiro de sangue”, para o fim de encontrar e explorar as vulnerabilidades das pessoas.

Aliás, a autora chama a atenção também para a perigosa utilização política da exploração de perfis e características sensíveis das pessoas, afirmando que Palantir, Amazon e Microsoft proveram ferramentas que

² Ver FRAZÃO, Ana; MULHOLLAND, Caitlin. Vazamento de Dados. *Podcast Direito Digital*. <http://www.podcastdiretodigital.com.br/>

³ BBC. Pegasus: o que é o sistema que espionou jornalistas, ativistas e advogados. <https://www.bbc.com/portuguese/internacional-57885795>.

⁴ VÉLIZ, Carissa. *Privacy is power. Why and how you should take back control of your data*. Bantam Press, 2021.

ajudaram a administração Trump a identificar, monitorar e deportar imigrantes, mesmo no contexto de políticas altamente questionáveis, como as que separavam as crianças de seus pais⁵.

Uma das conclusões de Carissa Véliz é que alguns julgamentos simplesmente não poderiam ser feitos, tais como os decorrentes de inferências sensíveis sub-reptícias, dentre os quais se incluem diagnósticos que são feitos a partir de gestos ou comportamentos corriqueiros das pessoas – a forma como usam seus smartphones, como digitam ou como movimentam seus olhos – mas que permitem a identificação de habilidades cognitivas, de problemas de saúde, como perda de memória, dislexia, depressão e de informações sensíveis, como orientação sexual, etnia, visões políticas e religiosas, traços de personalidade, inteligência, felicidade, uso de substâncias viciantes, circunstâncias familiares (como a separação dos pais), dentre inúmeras outras⁶.

Diante desse contexto, verifica-se que uma das raízes do problema da discriminação algorítmica encontra-se na premissa equivocada de que todos os julgamentos sobre seres humanos são possíveis. Logo, é imprescindível diferenciar, com urgência, que tipos de perfis, julgamentos e diagnósticos, por qualquer que seja o meio utilizado – incluindo as inferências – devem ser considerados inadmissíveis e, conseqüentemente, proibidos.

Aliás, a proposta da União Europeia para a regulação da inteligência artificial trata dos chamados riscos inaceitáveis, assim considerados aqueles que representam clara ameaça à segurança, à vida e aos direitos das pessoas, o que inclui sistemas ou aplicações que manipulam comportamentos humanos a fim de limitar o livre-arbítrio ou sistemas que permitem o *social scoring* por parte de governos⁷. Em casos assim, a solução não é o controle de resultado das análises algorítmicas, mas sim o próprio banimento do tratamento de dados para tal fim.

Não é sem razão que a proposta de regulação da União Europeia sobre inteligência artificial está lastreada na preocupação de se evitar qualquer tipo de discriminação indevida, razão pela qual se baseia em diversas vedações,

5 Op.cit.

6 Op.cit.

7 https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682

dentre as quais a utilização de sistemas que, por meio de técnicas subliminares e que vão além da consciência das pessoas, têm por fim distorcer o seu comportamento, de maneira que seja possível causar dano físico ou psicológico à própria pessoa ou a outrem⁸.

De toda sorte, o trabalho da Comissão Europeia também mapeou, ao lado dos riscos inaceitáveis, aqueles que devem ser considerados como altos riscos, tais como (i) acesso a infraestruturas críticas, de que é exemplo transporte, na medida em que podem submeter a vida e a saúde dos cidadãos a riscos, (ii) as aplicações educacionais ou de treinamento, que podem determinar o acesso a educação ou cursos profissionais, (iii) componentes de segurança dos produtos, como é o caso dos robôs que auxiliam em cirurgias, (iv) procedimentos para acesso a empregos e gerenciamento de trabalhos, o que inclui sistemas de recrutamento, (v) serviços essenciais privados ou públicos, o que inclui o *credit scoring*, em razão do seu potencial de impedir o acesso de cidadãos a empréstimos, (vi) *enforcement* jurídico, que se refere a sistemas que podem interferir em direitos fundamentais das pessoas, como os que avaliam a confiabilidade das provas, (vii) questões afetas a migração, asilo e administração de controle de fronteiras e (viii) questões afetas à administração da justiça e de processos democráticos⁹.

É importante verificar que vários dos exemplos considerados de alto risco assim o são precisamente em razão do seu alto potencial de discriminações indevidas, o que pode acontecer tanto quando o algoritmo erra, como também quando o algoritmo acerta¹⁰.

Havendo alto risco, a proposta da União Europeia é de que os sistemas correspondentes estejam submetidos a diversas obrigações antes de serem colocados no mercado, tais como (i) adequada avaliação de riscos e sistemas de mitigação de danos, (ii) alta qualidade das bases de dados que alimentam os sistemas e minimizam riscos de resultados discriminatórios, (iii) registro e rastreabilidade da atividade, (iv) documentação detalhada para prover todas as informações necessárias do sistema e seus propósitos, inclusive para o

8 https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0001.02/DOC_1&format=PDF

9 https://ec.europa.eu/commission/presscorner/detail/en/IP_21_1682

10 A Parte VIII da presente série trata precisamente da problemática dos algoritmos tanto quando erram como também quando acertam.

fim de que autoridades possam avaliar o seu *compliance*, (v) clara e adequada informação para o usuário, (vi) adequada supervisão humana para minimizar os riscos e (vii) alto nível de robustez, segurança e acuidade.

Observa-se, portanto, que os problemas de resultados ilícitos ou discriminatórios apenas podem ser evitados de forma eficiente se a programação dos sistemas algorítmicos for orientada pelo respeito aos direitos daqueles que serão impactados por esses direitos. Trata-se de etapa fundamental para se analisar não somente a qualidade e a licitude dos dados, como também a congruência entre esses dados e as finalidades pretendidas pelo tratamento.

Todas essas questões rompem com a naturalização dos julgamentos algorítmicos que tanto vem caracterizando os nossos tempos, em que partimos da premissa de que todos os dados podem ser utilizados para todos e quaisquer tipos de julgamentos. Mais do que isso, rompem também com a ideia de que todos os dados podem ser utilizados para todos os julgamentos, ainda que a ausência de congruência possa ser um fator de agravamento de discriminações indevidas.

Se é lícito e razoável que agentes econômicos possam fazer suas avaliações de risco e investimento, a grande questão é saber quais são os limites para suas análises, que dados não podem ser considerados para tal objetivo e que dados, diante do seu potencial discriminatório, devem ser tratados com cuidado adicional ou contrabalançados com outros dados, a fim de assegurar resultados que não restrinjam indevidamente os direitos das pessoas sob julgamento.

Uma coisa é certa: nem todos os dados podem ser utilizados para fins comerciais ou políticos e, mesmo aqueles que podem, devem ser utilizados para finalidades lícitas e congruentes, sempre se respeitando os direitos dos usuários. A grande questão é responder, a partir dos necessários parâmetros éticos e jurídicos, a pergunta que consta do título da presente coluna: para que fins, como e mediante que salvaguardas podem ser julgadas as pessoas?

Com isso, evidencia-se a importância de que o problema da discriminação algorítmica seja atacado desde a origem, na programação,

realçando a importância do fator estrutural e preventivo. Afinal, o mero controle de resultados de sistemas algorítmicos – tarefa que é sabidamente complexa - pode ser insuficiente, ainda mais quando o ecossistema de programação pode gerar incentivos para discriminações.

Entretanto, mesmo observado o *check list* ora apresentado- dados de qualidade e adequados, finalidade lícita e congruência entre esses dois fatores -, é fundamental entender que o formalismo e a matematização que são inerentes aos sistemas algorítmicos apresentam outras frentes de desafios, que serão explorados na próxima coluna.

Publicado em 11/08/2021

Link:<https://www.jota.info/opiniao-e-analise/artigos/discriminacao-algoritmica-para-que-fins-e-como-devem-ser-julgadas-as-pessoas-11082021>