Luminate
Construindo sociedades mais fortes

A ilusão dos dados: proteger dados individuais não é suficiente quando o dano é coletivo

Autor: Martin Tisné, Diretor Administrativo, Luminate

Editor: Marietje Schaake, Diretora de Política Internacional, Centro de Política Cibernética da Universidade de Stanford

Julho de 2020

A ameaça de discriminação digital

Em 17 de março de 2018, questões sobre privacidade de dados explodiram com o escândalo da anteriormente desconhecida empresa de consultoria Cambridge Analytica. Legisladores ainda estão lutando para atualizar as leis para conter os danos do 'big data' e da Inteligência Artificial - IA.

Na primavera de 2020, a pandemia da COVID-19 trouxe de volta ao debate público questões sobre proteções legais suficientes, com alertas urgentes sobre as implicações de privacidade dos aplicativos de rastreamento de contatos.[1] Mas as consequências da vigilância dos efeitos da pandemia são muito maiores do que qualquer aplicativo: transporte, educação, sistemas de saúde e escritórios têm sido transformados em vastas redes de vigilância.

Os dados são o novo CO_2

Tal como acontece com o CO_2, a privacidade dos dados vai muito além do indivíduo. Somos prisioneiros do consentimento de outras pessoas. Se você comparar o impacto dos danos causados por dados aos do CO_2, ficará claro como os impactos são sociais, não individuais. As emissões do carro do meu vizinho, a fumaça das fábricas de outro continente, me afetam mais do que a minha própria pequena pegada de carbono jamais o fará. Essa ameaça coletiva da mudança climática está bem refletida na legislação ambiental e sustenta a lógica (política) das reduções de emissões e o acordo de Paris.[3]

"A natureza coletiva do 'big data' significa que as pessoas são mais afetadas pelos dados de outras pessoas do que pelos dados sobre elas próprias. Assim como em relação à mudança climática, a ameaça é social e pessoal."

Se considerarmos apenas as compensações individuais entre sacrifícios de privacidade e supostos benefícios à saúde, perderemos o ponto. A natureza coletiva do 'big data' significa que as pessoas são mais afetadas pelos dados de outras pessoas do que pelos dados sobre elas próprias. Assim como em relação à mudança climática, a ameaça é social e pessoal.

Na era do 'big data' e da IA, as pessoas podem sofrer por causa da forma como a soma dos dados individuais é analisada e classificada em grupos de algoritmos. Como resultado, novas formas de danos coletivos baseados em dados estão aparecendo: anúncios online de habitação, emprego e crédito discriminando com base em raça e gênero, mulheres excluídas de empregos com base em gênero e atores estrangeiros que visam grupos de centro-direita, puxando-os para a extrema direita.[2] Nosso debate público, governos e leis estão mal equipados para lidar com esses danos coletivos, em oposição aos individuais.

Os indivíduos podem desfrutar de benefícios de curto prazo que prejudicarão o coletivo no longo prazo. Pensando com otimismo, a crise do Coronavírus pode abrir o caminho para leis que lidam com danos coletivos causados por dados. Provavelmente, o conflito entre os medos imediatos e compreensíveis da sociedade em relação à saúde será confrontado com as proteções à privacidade. Por exemplo, o ministro da saúde do Reino Unido disse que "ninguém deve restringir o trabalho de resposta ao coronavírus devido às leis de proteção de dados".[4] Até mesmo a Estratégia de Dados da Comissão Europeia se concentra principalmente em capacitar os indivíduos em relação aos "seus" dados.[5] A necessidade de direitos coletivos de dados continua a ser ignorada.

Dos direitos coletivos aos individuais, e vice-versa

Os direitos dos dados não eram historicamente tão individualizados como são hoje. A legislação de direitos humanos no final da Segunda Guerra Mundial concentrava-se principalmente na proteção de grupos. O regime nazista oprimiu e massacrou judeus, ciganos e outros povos perseguidos por pertencerem a um grupo minoritário. O dano coletivo causado por um estado pernicioso foi articulado com o conceito de genocídio: um novo conceito para descrever crimes cometidos "com a intenção de destruir, no todo ou em parte, um grupo nacional, étnico, racial ou religioso". O objetivo era então proteger os grupos de futuros crimes genocidas.[6]

A ironia da história é que, à medida que governos e leis passavam da proteção de grupos para a proteção de indivíduos, as empresas de tecnologia iam na outra direção, da análise do comportamento individual para o dos grupos. A era do 'machine learning' efetivamente torna a negação individual do consentimento sem sentido. Mesmo se eu me recusar a usar o Facebook, Twitter ou Amazon, o fato de que todos ao meu redor aderiram significa que há muitos pontos de dados sobre mim para atingir.

À medida que engenheiros e empresas começaram a implantar algoritmos cada vez mais complexos, juntamente com dados coletados em escala, o mercado evoluiu além da transação de dados individuais, em direção à extração de valor de dados coletivos. O fato

"A era do 'machine learning' efetivamente torna a negação individual do consentimento sem sentido."

Na década de 1970, o pêndulo começou a oscilar na direção da privacidade individual, com a ascensão da computação. A Organização para o Desenvolvimento Econômico e Cooperação (OCDE) desenvolveu um conjunto de diretrizes de privacidade em 1980. Essas diretrizes popularizaram a noção de que os indivíduos devem dar consentimento informado para qualquer informação usada para eles e sobre eles.[7] Durante o mesmo período, a lei francesa de proteção de dados de 1978 consagrou a noção de que os dados pessoais das pessoas devem ser coletados e processados de forma justa e legal para fins específicos, explícitos e legítimos, e com o consentimento da própria pessoa (chamada "titular dos dados").[8] A lei francesa, por sua vez, inspirou a Diretiva de 1995 da União Europeia sobre proteção de dados pessoais, que inspirou o Regulamento Geral de Proteção de Dados (RGPD) de 2018, muitas vezes chamado de "padrão ouro" das leis de proteção de dados. Hoje, os direitos de dados são vistos como "direitos individuais" e a individualização dos direitos de dados tornou-se a pedra angular das leis de proteção de dados em todo o mundo.[9]

das leis permanecerem focadas no indivíduo coloca-o fora em contato com a realidade que se desenvolve rapidamente e que a tecnologia e a inteligência artificial criam. Nossas sociedades precisam de direitos de dados em nível coletivo e individual, de forma semelhante à lei de não discriminação que abrange indivíduos e grupos.[10]

Por que a falácia individualista se adapta à Big Tech

Quando o professor de design de mídia David Carroll tentou recuperar dados sobre ele da Cambridge Analytica, ele entrou com uma ação judicial sob a lei de proteção de dados do Reino Unido. O Prof. Carroll então contestou a liquidação da empresa, citando o interesse público na prestação de contas e na supervisão independente. Documentos judiciais mostram que ele acreditava que aprender mais sobre como seus dados individuais estavam sendo coletados e usados lançaria luz sobre o

impacto do big data e da IA no coletivo e na democracia. Seu recurso foi rejeitado.[11] O caso mostra como é difícil para os indivíduos buscar soluções para danos coletivos, em oposição a invasões de privacidade pessoal.

O valor dos dados de um indivíduo para o Google ou Facebook é marginal. Para as empresas, o valor está nas inferências tiradas de sua interação com outras pessoas.[12] Em 2018, o Facebook gerou uma renda de US$ 10/ano por usuário diário ativo.[13] Os danos que o indivíduo pode demonstrar são, portanto, mínimos. Misturar indivíduos em uma classe e monitorar como essa classe responde a diferentes estímulos significa que o Google não pode dizer como os dados sobre você foram usados. Mas o valor do processamento de dados coletivos é enorme. Desses US$ 10 por pessoa por ano, o Facebook gerou uma receita líquida anual de US$ 22 bilhões em 2018, enquanto a Alphabet gerou US$ 30 bilhões. A PwC descobriu que empresas com recursos de análise de dados têm valores de mercado de ações mais elevados do que seus pares no mesmo setor.[14]

a injustiça foi cometida de forma invisível, por um modelo de computador (embora projetado por humanos).[16] A ação coletiva é, portanto, também menos provável de ocorrer.[17] A tarefa em mãos é entender a natureza dos novos danos e tornar o invisível visível.

Tornando o invisível visível: danos coletivos baseados em dados

Quanto mais coletivo o dano, menos as pessoas são protegidas e menos visível ele é. Quanto mais o dano é individual, mais visíveis são seus impactos e mais pessoas são legalmente protegidas. Se uma pessoa for discriminada por causa de características protegidas, como idade, gênero ou etnia, isso será visível para ela e, com sorte, ela estará em posição de buscar reparação. Quando uma pessoa é discriminada devido a uma decisão algorítmica, é provável que seja menos visível e, atualmente, difícil de buscar reparação.[18]

> “Mesmo se eu me recusar a usar o Facebook, Twitter ou Amazon, o fato de que todos ao meu redor aderiram significa que há muitos pontos de dados sobre mim para atingir.”

As leis e o pensamento desenvolvidos na década de 1970 não são mais adequados para lidar com a realidade de hoje. A questão aqui é um descompasso fundamental entre a lógica do mercado e a lógica do direito.[15] Os mercados de tecnologia contemporâneos extraem valor de dados coletivos. Nossas leis respondem a danos individuais e não foram alteradas para refletir as mudanças na tecnologia. Os governos devem mudar os regimes jurídicos para corresponder à lógica do mercado. Talvez não haja urgência até agora porque a natureza dos danos coletivos - assim como a poluição por CO_2 - é invisível para a pessoa comum. Os algoritmos são ocultados, seus efeitos são onipresentes, mas invisíveis. A noção de injustiça, que pode levar à conscientização e reivindicações legais, é evanescente quando

As pessoas tendem a sofrer danos causados por dados de três maneiras principais. Em primeiro lugar, existem danos puramente individuais. Por exemplo, um indivíduo é visto como impróprio para o emprego devido a dados diretamente relacionados a eles (por exemplo, sua idade). As proteções contra esses tipos de danos estão bem estabelecidas por lei.

Em segundo lugar, existem danos inferidos. É aqui que se infere que o indivíduo faz parte de um grupo ou categoria de pessoas, mas a pessoa cujos dados são usados não é prejudicada. Considere as pessoas que carregam fotos públicas de si mesmas em um popular site de namoro americano, cujas fotos foram usadas, de modo discutível, por pesquisadores que desenvolveram algoritmos

para determinar a sexualidade das pessoas com base em suas características faciais. [19] Os indivíduos cujas fotos são usadas não são os únicos necessariamente prejudicados. Pessoas cuja sexualidade é "identificada" (ainda que de maneira espúria) por meio dessas técnicas são prejudicadas por inferências feitas como resultado de dados coletados e processados.[20]

Terceiro, existem danos otimizados. Esses são danos sofridos como resultado de modo pelo qual os sistemas de 'machine learning' são otimizados. O algoritmo do YouTube concluiu que as pessoas são atraídas por um conteúdo mais extremo do que o que estão vendo atualmente e as leva a um caminho que, como escreveu o acadêmico e ativista Zeynep Tufekci, pode ser inofensivo (de correr a ultramaratonas) ou prejudicial (de comícios políticos a teorias da conspiração).[21] As pessoas são inadvertidamente definidas pelo algoritmo. Como acontece com todos os sistemas de otimização, o algoritmo do YouTube é totalmente focado em seus usuários e não enfoca suas externalidades em não usuários, minorias e qualquer pessoa que não esteja no sistema (ou seja, a sociedade em geral).

Os sistemas jurídicos e arsenais de políticas públicas de nossos países estão mal equipados para responder aos dois últimos danos causados por dados. A proteção de dados, como atualmente estruturada, tem como premissa um relacionamento entre os controladores de dados e os titulares dos dados. Conforme a tecnologia se torna cada vez mais sofisticada, a conexão entre controladores de dados e titulares de dados vacila. Nem sempre está claro quem é o controlador, nem qual sujeito foi prejudicado. Um vazio legal surgirá - e possivelmente já existe - e a responsabilidade desaparecerá.[22]

À medida que o mundo se move mais online devido ao Coronavírus, as empresas e os governos obterão muito mais informações sobre as pessoas por meio da coleta de dados. Isso provavelmente aumentará o uso de decisões automatizadas, por exemplo, sobre como alocar recursos. E com mais automação, haverá implicações de patrimônio ainda maiores. O processamento de dados pode decidir quem tem acesso à educação, assistência social ou ao sistema judicial. Pesquisas nos últimos cinco anos mostraram como os impactos negativos da tomada de decisão automatizada sobre as pessoas recaem desproporcionalmente sobre aqueles já marginalizados na sociedade, como a população negra, mulheres e imigrantes.[23]

A pegadinha do século 21 para o problema da privacidade e discriminação de dados é que os membros do público não sabem mais de qual grupo eles fazem parte ou não, apenas o algoritmo sabe. Muitas pessoas nem saberão que estão sendo classificadas ou discriminadas.[24] A conversa precisa ser reformulada em torno de automação e poder, e de quais grupos serão afetados negativamente.

> "Nossas sociedades precisam de direitos de dados em nível coletivo e individual, de forma semelhante à lei de não discriminação que abrange indivíduos e grupos."

As soluções consistem em responsabilidade rígida, forte supervisão regulatória da tomada de decisão baseada em dados e a capacidade de auditar e inspecionar as decisões e os impactos dos algoritmos na sociedade.

Regulamentar a automação é regular o poder: o caso para responsabilidade rígida

Em vez de regulamentar como as pessoas consentem que seus dados sejam usados para proteger sua privacidade, os formuladores de políticas devem regular a automação, começando com algoritmos de caixa preta

que coletam, ordenam e classificam os dados. Isso exigirá um método totalmente novo de regulamentação. Os cidadãos precisam de informações, escrutínio público e responsabilização pelos os impactos díspares das enormes quantidades de automação que são apontadas para eles a cada segundo do dia.

Na União Europeia, o RGPD é fraco em automação e danos coletivos.[25] A responsabilidade dos sistemas de decisão algorítmicos é principalmente coberta pelos artigos 13-15 e 22, mas estes são limitados a decisões que são totalmente automatizadas, que usam dados pessoais e que são consideradas "decisões significativas", evitando assim muitos dos danos menores detalhados anteriormente - que cumulativamente representam danos coletivos significativos.[26] O RGPD individualiza ainda mais os danos causados por dados, exigindo que a pessoa que sofreu o dano esteja no centro de qualquer reclamação resultante dele. Isso seria como exigir que um caso sobre as emissões de CO_2 de um país inteiro dependesse de seus impactos prováveis sobre uma pessoa.[27]

Três elementos são necessários para garantir a responsabilidade total: (1) transparência clara sobre onde e quando as decisões automatizadas ocorrem[28] e seu impacto nas pessoas e grupos, (2) o direito de dar contribuições públicas significativas e chamar aqueles com autoridade para justificar suas decisões, e (3) a capacidade de aplicar sanções.[29] Uma lei de dados de interesse público deve englobar esses três pontos.

Transparência clara

O foco deve ser o escrutínio público da tomada de decisão automatizada e os tipos de transparência que levam à responsabilização.[30] Isso inclui revelar os dados existentes, de propósito e de treinamento por trás dos algoritmos, bem como seus impactos - se eles levaram a resultados díspares e em quais grupos. A transparência clara e direcionada lança luz sobre os algoritmos e as instituições que os implantam. Ela revela, por exemplo, informações sobre o desempenho institucional, (como o obtido a partir do uso de câmeras de reconhecimento facial pela polícia e seu impacto), e torna os algoritmos explícitos sobre o que é medido, por quem e como. A transparência continua sendo uma condição necessária, porém não suficiente para a responsabilização.[31] Para tal, são necessárias contribuições significativas do público e a possibilidade de aplicar sanções.

> **"As soluções consistem em responsabilidade rígida, forte supervisão regulatória da tomada de decisão baseada em dados e a capacidade de auditar e inspecionar as decisões e os impactos dos algoritmos na sociedade."**

Participação pública

O público tem o direito fundamental de convocar os detentores do poder a justificar suas decisões. Este direito de exigir respostas não deve ser limitado à participação consultiva, onde as pessoas são solicitadas a dar sua opinião e os agentes públicos seguem em frente. Deve incluir participação capacitada na qual a opinião pública é obrigatória antes da implementação de um algoritmo na sociedade. Por exemplo, as avaliações de impacto algorítmicas devem fornecer aos cidadãos a possibilidade de dar contribuições significativas para o uso da tomada de decisão automatizada, expandindo essas avaliações como uma ferramenta para a tomada de decisões conduzida pela comunidade.

Sanções

Finalmente, o poder de punição é fundamental para que essas reformas tenham sucesso e para que a responsabilização seja alcançada. O RGPD foi prejudicado pela falta de financiamento e capacidade dos comissários de proteção de dados em toda a Europa.

“Semelhante à natureza coletiva da ameaça da mudança climática, nossos governos e formuladores de políticas públicas devem mudar a maneira como pensam sobre a resposta regulatória.”

Apesar do poder do RGPD de impor multas de até 4% do faturamento anual de uma empresa, poucas dessas multas foram aplicadas e metade dos reguladores de proteção de dados da Europa têm apenas cinco ou menos especialistas técnicos.[32] Mas a proteção de dados ou as comissões de informação não podem ser as únicas responsáveis pela ‘accountability’ dos algoritmos, pois nossas sociedades são transformadas pela inteligência artificial. Empresas e governos precisam de leis que restrinjam o uso e a automação de dados, acima e além das implicações para os dados pessoais de cada indivíduo. Para isso, as sociedades também precisarão da modernização das legislações setoriais, como a legislação trabalhista, penal, genética, ambiental e de combate à discriminação.[33] Por exemplo, as leis que regulam a administração pública já poderiam ser aplicadas aqui. A lei administrativa poderia ser usada para exigir maior responsabilidade da tomada de decisão automatizada usada pelo setor público.[34] As leis trabalhistas poderiam ser adaptadas para considerar o papel da tecnologia na gestão das relações empregador/empregado.[35]

Precedente

Existem exemplos de projetos de lei que procuraram preencher essa lacuna. Nos Estados Unidos, foi realizado um esforço em 2019 para promulgar uma Lei de Responsabilidade Algorítmica, que posteriormente foi paralisado no Congresso, com o objetivo de determinar se algoritmos do setor privado resultaram em discriminação ou não. A lei teria exigido que as empresas realizassem avaliações de impacto algorítmico em certas situações, para verificar se há preconceito ou discriminação.[36] Na França, a Lei da República Digital (Loi Pour Une République Numérique) hoje se aplica a decisões administrativas tomadas por sistemas algorítmicos do setor público, mas poderia fornecer um modelo para leis futuras. Ela joga luz à importância que a automação teve para a decisão final, permitindo o acesso aos dados utilizados e suas fontes, bem como a quaisquer parâmetros de tratamento e ponderações utilizados nas decisões que afetaram as pessoas. Além disso, ela fornece informações sobre o resultado do processo automatizado. Em contrapartida, o RGPD impõe restrições, mas apenas ao uso de dados pessoais em decisões totalmente automatizadas.[37]

Conclusão

As preocupações com a privacidade em torno da COVID-19 trouxeram à tona uma série de incompatibilidades sistêmicas entre a lei de privacidade individual e o valor do processamento coletivo de dados. A pandemia acelera substancialmente o risco de desigualdade e novos danos à medida em que a vigilância e a coleta de dados são aceleradas em nome do fim da crise de saúde. Muitos daqueles que sofrem já estão marginalizados e vulneráveis em nossas sociedades. Semelhante à natureza coletiva da ameaça da mudança climática, nossos governos e formuladores de políticas públicas devem mudar a maneira como pensam sobre a resposta regulatória. Eles precisam considerar o impacto coletivo e individual dos dados.

Uma lei de dados de interesse público

Transparência clara

Exigir que empresas e governos abram os dados e o código-fonte por trás de algoritmos de alto risco, e definam quais são considerados de "alto risco" em relação às evidências sobre os impactos díspares desses algoritmos na população (por exemplo, se eles afetam de modo desproporcional comunidades marginalizadas).

Exigir que empresas e governos publiquem avaliações de impacto algorítmico medindo os resultados do tratamento algorítmico em grupos, bem como quaisquer danos coletivos baseados em dados. Garantir que os resultados de tais avaliações sejam publicados abertamente. Garantir que isso anteceda a execução de implantações de IA de alto risco e renove-as regularmente.[38]

Garantir total transparência e responsabilidade da automação:

- Ajustes em algoritmos que podem parecer pequenos ou insignificantes quando considerados isoladamente, mas podem resultar em um impacto coletivo substancial quando considerados em conjunto. Isso não deve ser limitado a decisões tomadas por um algoritmo nem às decisões que precisam ser "significativas", como é o caso atualmente com o artigo 22[39] do RGPD.
- Aplicar tanto a decisões totalmente quanto parcialmente automatizadas.[40]
- Exigir transparência e responsabilidade em relação a como uma decisão foi tomada com base em um modelo de computador, não simplesmente explicando o modelo em abstrato (o grau e o modo de contribuição do processamento algorítmico para a decisão tomada.)[41]
- Cobrir decisões para além daquelas que usam dados pessoais. Por exemplo, isso cobriria carros automatizados ou dados que já foram pessoais e, então, supostamente tornados anônimos. As pessoas são afetadas por dados que não são pessoais e por dados pessoais que não dizem respeito a elas.

Participação pública

Oferecer aos cidadãos a possibilidade de fornecer informações significativas sobre o uso da tomada de decisão automatizada (incluindo informações em avaliações de impacto algorítmico, mas não se limitando a elas).

Garantir que a participação pública tenha poder e não seja apenas consultiva.

Sanções

Garantir a capacidade de aplicar sanções por descumprimento.

Organismos de prestação de contas de recursos e fundos de forma adequada, incluindo órgãos de supervisão para leis setoriais, como direito do trabalho, direito penal, direito genético, direito ambiental e combate à discriminação, além dos órgãos de proteção de dados.

Relevância para grupos e também para indivíduos.

Permitir que pessoas e organizações apresentem solicitações.[42]

Fornecer acesso aos parâmetros de tratamento e, quando apropriado, sua ponderação, aplicada à situação da(s) pessoa(s) ou dos grupos em questão.

Sobre o autor

Martin Tisné é diretor da Luminate, uma organização filantrópica global. Ele é responsável pela área de Direitos Digitais e de Dados da Luminate, , coordenando o trabalho de políticas públicas e as atividades da Fundação na Europa. Em conjunto com a Casa Branca de Obama, Martin fundou a Open Government Partnership e a ajudou a se tornar uma iniciativa de mais de 70 países. Ele também foi um dos resonsáveis pela Carta Internacional de Dados Abertos, pela Carta de Dados Abertos do G8 e pelo compromisso do G20 com os princípios de dados abertos. Martin é o cofundador da Publish What You Fund, uma campanha global pela transparência da ajuda externa, e da Integrity Watch Afghanistan, a principal ONG anticorrupção do país. Twitter: @martintisne

Sobre o editor

Marietje Schaake é diretora de política internacional do Centro de Política Cibernética da Universidade de Stanford e pesquisadora de política internacional do Instituto de Inteligência Artificial Centrada no Homem de Stanford. Ela foi nomeada presidente do Cyber Peace Institute.

Entre 2009 e 2019, Marietje serviu como membro do Parlamento Europeu para o partido liberal democrático holandês, onde se concentrou em comércio, relações exteriores e políticas de tecnologia. Marietje é afiliada a várias organizações sem fins lucrativos, incluindo o Conselho Europeu de Relações Exteriores e a Observer Research Foundation na Índia, e escreve uma coluna mensal para o Financial Times e uma coluna bimestral para o jornal holandês NRC.

Agradecimentos do autor

Sou extremamente grato a Salmana Ahmed, Madeleine Clare Elish, Kate Crawford, Polly Curtis, Jonathan Fox, Janet Haven, Swee Leng Harris, Gus Hosein, Karen Levy, Jim Peacock, Ravi Naik, David Robinson, Marietje Schaake, Ben Scott e Sandra Wachter por revisar este documento em forma de rascunho e por seus comentários extremamente úteis.

Eu também gostaria de fazer um agradecimento especial a Adrien Abecassis, Julia Angwin, Azeem Azhar, Solon Barocas, Ailidh Callander, Simon Chignard, Sylvie Delacroix, Alix Dunn, Alex Goodman, Seda Gürses, Kieron O'Hara, Gry Hasselbalch, Carly Kind, Neil Lawrence, Sean Macdonald, Aiha Nguyen, Tanya O'Carrol, Reema Patel, Seeta Peña Gangadharan, Imogen Parker, Phil Sheldrake, Martha Spurrier, Katarzyna Szymielewicz, Linnet Taylor, Jeni Tennison, Zeynep Tufekci, Michael Veale, Henri Verdier, Stefaan Verhulst, Adrian Weller, Glen Weyl, Meredith Whittaker e Caroline Wilson Palow por seus conselhos. Sou muito grato pela ajuda deles.

Luminate

Luminate é uma organização filantrópica global focada em fortalecer pessoas e instituições para trabalharem juntas para construir sociedades justas e equitativas. Apoiamos organizações e empreendedores inovadores e corajosos em todo o mundo e defendemos as políticas e ações que impulsionarão a mudança em quatro áreas de impacto: Empoderamento Cívico, Direitos Digitais e de Dados, Transparência Financeira e Mídia Independente. Trabalhamos com nossos parceiros para garantir que todos tenham a oportunidade de participar e moldar as questões que afetam suas sociedades e para tornar aqueles em posições de poder mais responsivos e responsáveis. A Luminate foi fundada em 2018 pelos filantropos Pierre e Pam Omidyar. A organização foi fundada pelo Grupo Omidyar. www.luminategroup.com

Stanford | Cyber Policy Center
Freeman Spogli Institute

O Cyber Policy Center do Freeman Spogli Institute for International Studies é o principal centro da Universidade de Stanford para o estudo interdisciplinar de questões relacionadas à tecnologia, governança e políticas públicas. Por meio de pesquisa, engajamento de políticas e ensino, o Cyber Policy Center trabalha para trazer soluções de ponta para governos nacionais, instituições internacionais e indústria.

Notas Finais

1. Veja John Thornhill; Naomi Klein
2. Ali, Sapiezynski, Bogen, Korolova, Mislove e Rieke, "Discrimination through optimization: How Facebook's ad delivery can lead to skewed outcomes", 2019 https://arxiv.org/abs/1904.02095
3. Mais recentemente, na Holanda, o Caso Climático Urgenda contra o governo holandês estabeleceu que o governo tem o dever legal de prevenir a mudança climática de efeito perigoso e deve reduzir significativamente as emissões para proteger os direitos humanos.
4. https://twitter.com/MattHancock/status/1240189379676712960?s=20
5. https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy
6. Samantha Power, "A Problem From Hell", 2002.
7. https://www.oecd.org/sti/ieconomy/privacy-guidelines.htm
8. https://www.cnil.fr/sites/default/files/typo/document/Act78-17VA.pdf
9. Vão desde o direito a ser informado, o direito de acessar os dados, a retificá-los, apagá-los, restringir o seu processamento. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/ https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT De acordo com a Carta dos Direitos Fundamentais da União Europeia: "todas as pessoas têm direito à proteção dos dados pessoais que lhes digam respeito."
10. Agradeço a Prof. Sandra Wachter por este comentário. Consulte Perfil de afinidade e discriminação por associação em publicidade comportamental on-line https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3388639
11. O juiz da liquidação observa que "os 'interesses' relevantes são os interesses do Prof. Carroll como credor, não seus interesses como acadêmico curioso ou como alguém que lidera uma campanha para estabelecer um princípio sobre o uso de dados ou como alguém que está inseguro com o que pode ter acontecido com seus dados no passado. https://www.judiciary.uk/judgments/vincent-john-green-mark-newman-v-cambridge-analytica-uk-limited-others/
12. A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829
13. https://investor.fb.com/investor-news/press-release-details/2019/Facebook-Reports-Fourth-Quarter-and-Full-Year-2018-Results/default.aspx
14. https://www.bennettinstitute.cam.ac.uk/publications/value-data-summary-report/ ; pwc.co.uk/issues/data-analytics/insights/putting-value-on-data.html
15. Consulte Julie Cohen, "Between Truth and Power", 2019
16. Um estudo recente do uso de IA em contratações no Reino Unido determinou que as ferramentas de auditoria usadas para garantir a conformidade não eram capazes de determinar com precisão o viés em um sistema de IA. Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547922
17. Agradeço ao Prof. Wachter por essa percepção.
18. Trabalhos pioneiros nessa área incluem "Group Privacy: The Right to Huddle" de E. Bloustein https://heinonline.org/HOL/LandingPage?handle=hein.journals/rutlj8&div=24&id=&page=; Taylor, Floridi e van der Sloot (editores) de "Group Privacy: New Challenges of Data Technologies" https://www.springer.com/gp/book/9783319466064; Mittelstadt "From Individual to Group Privacy in Big Data Analytics" https://link.springer.com/article/10.1007/s13347-017-0253-7
19. https://www.economist.com/science-and-technology/2017/09/09/advances-in-ai-are-used-to-spot-signs-of-sexuality
20. Consulte a Dra. Sandra Wachter "A right to reasonable inferences: re-thinking data protection law in the age of big data and AI" https://www.law.ox.ac.uk/business-law-blog/blog/2018/10/right-reasonable-inferences-re-thinking-data-protection-law-age-big
21. https://www.nytimes.com/2018/03/10/opinion/sunday/youtube-politics-radical.html
22. Consulte Ravi Naik, 2020 https://jolt.law.harvard.edu/digest/the-gentle-civilizer-of-technology
23. https://www.theguardian.com/technology/series/automating-poverty
24. Why Fairness Cannot Be Automated: Bridging the Gap Between EU Non-Discrimination Law and AI https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3547922
25. https://gdpr-info.eu/
26. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" Wachter, Floridi, Mittelstadt 2017 https://academic.oup.com/idpl/article/7/2/76/3860948; "Enslaving the algorithm: from a right to an explanation to a right to better decisions" Edwards e Veale 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3052831;
27. A lei permite que as ONGs aceitem reclamações sem serem ordenadas por uma pessoa específica (o "titular dos dados"), mas, novamente após intenso lobby, essa seção da lei tornou-se opcional e apenas três dos vinte e oito países europeus decidiram decretá-ao. Quando as ONGs podem fazer reivindicações sistêmicas em nome do público sem a necessidade de autorização de um indivíduo, é possível se proteger coletivamente de danos baseados em dados da mesma forma que de danos ambientais. Seção 80 do RGPD. (2) O principal remédio do RGPD para combater os danos coletivos baseados em dados é quando a violação dos direitos individuais de uma pessoa é sintomática da mesma violação sofrida por todos ou quando uma ação coletiva pode ser preparada. Existem poucos casos assim. Essa seção aparentemente obscura da lei aponta para uma tendência futura potencialmente interessante. Sou grato à equipe da Privacy International pelo tempo dedicado a explicar esse ponto.
28. Às vezes chamada de "Lei do Blade Runner", exigindo que um sistema automatizado ou bot se declare como tal e não se camufle como humano.
29. Veja a distinção do Prof. Jonathan Fox entre responsabilidade física e social aqui https://www.tandfonline.com/doi/full/10.1080/09614520701469955
30. https://luminategroup.com/posts/report/public-scrutiny-of-automated-decisions-early-lessons-and-emerging-methods
31. Jonathan Fox, "The uncertain relationship between transparency and accountability", 2007, https://www.tandfonline.com/doi/full/10.1080/09614520701469955; Fung, Graham, Weil "Full Disclosure: The Perils and Promise of Transparency", 2007
32. "GDPR accused of being toothless because of lack of resources", Financial Times, 20 de abril de 2020, https://www.ft.com/content/a915ae62-034e-4b13-b787-4b0ac2aaff7e
33. Para obter uma atualização do RGPD para cobrir essas questões, consulte a conclusão de "A right to reasonable inferences: re-thinking data protection law in the age of Big Data and AI" https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829
34. Jennifer Cobbe, "Administrative Law and The Machines of Government", 2018 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3226913
35. Em relação à otimização usada com os trabalhadores da Amazon, a melhor resposta pode ser os direitos e proteções dos trabalhadores, em vez de leis especificamente voltadas para a tecnologia usada.
36. https://www.congress.gov/bill/116th-congress/house-bill/2231/all-info. O projeto foi um começo promissor, mas também criticado por contar com o poder de aplicação relativamente fraco da Comissão Federal de Comércio, por não oferecer uma oportunidade para contribuições públicas significativas, como no caso das avaliações de impacto ambiental, e por não exigir um nível claro de transparência pública para os resultados das avaliações de impacto algorítmico.
37. A Lei da República Digital Francesa (Loi Pour Une République Numérique) é pouco pesquisada devido ao foco excessivo do campo do aprendizado de máquina em exemplos e estudos de caso anglo-saxões. A lei hoje se aplica a decisões administrativas tomadas por sistemas algorítmicos do setor público, mas fornece um modelo para leis futuras. Ele fornece acesso à importância que a automação teve para a decisão final. Ela também abre o acesso aos dados usados e à sua fonte, bem como quaisquer parâmetros de tratamento e ponderações se usados em decisões que afetaram as pessoas. Ele também fornece informações sobre o resultado do processo automatizado. Por exemplo, uma pessoa pode ter acesso aos dados e ao código-fonte usado em um algoritmo que decide se concede a ela uma vaga em uma universidade pública ou não, e como essa decisão foi tomada e ponderada (por exemplo, suas notas foram mais importantes do que onde eles vivem?). Por outro lado, o RGPD impõe restrições, mas apenas ao uso de dados pessoais em decisões totalmente automatizadas. Consulte também Edwards e Veale, 2018
38. https://ainowinstitute.org/aiareport2018.html
39. Como diz o Dr. Michael Veale, "decisões que parecem "insignificantes" no nível individual podem, na verdade, ser muito impactantes no nível do grupo".
40. As disposições do RGPD para explicação e responsabilidade de algoritmos são restritas a decisões que são 100% automatizadas. Na realidade, a maioria das decisões automatizadas envolve um humano em algum ponto, mesmo que seu envolvimento seja superficial ou substancialmente influenciado pelo veredicto do algoritmo.
41. https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000031366350&idArticle=LEGIARTI000034195881
42. Veja nota de rodapé 27