

# AS TRÊS LEIS DA ROBÓTICA NA ERA DO *BIG DATA*<sup>1</sup>

*THE THREE LAWS OF ROBOTICS IN THE AGE OF BIG DATA\**

**Jack M. Balkin<sup>2</sup>**

Yale Law School

## RESUMO

O trabalho examina os desafios das tecnologias emergentes, como robôs, inteligência artificial e algoritmos, na Sociedade Algorítmica. Contrasta-se o "Complexo de Frankenstein", que teme máquinas malévolas, com as Três Leis da Robótica de Isaac Asimov, ressaltando que, na prática, surgem questões legais e interpretativas que exigem regulamentações focadas nos seres humanos que desenvolvem e operam essas tecnologias. Argumenta-se que a governança deve priorizar a boa-fé, transparência e responsabilidade dos projetistas e operadores, em vez de se concentrar apenas nos dispositivos. A "falácia do homúnculo" é utilizada para criticar a falsa ideia de que existe uma entidade humana dentro dos programas de IA, destacando a necessidade de regular a programação e o uso dos dados. Além disso, discute-se o "efeito de substituição", onde IA e robôs substituem humanos, impactando as dinâmicas sociais. Por fim, propõem-se três princípios jurídicos fundamentais para orientar as interações na Sociedade Algorítmica: deveres fiduciários, obrigações públicas e a prevenção da externalização de custos, aplicando esses princípios tanto a empresas digitais quanto a governos.

**Palavras-chave:** algoritmos; *Big data*; inteligência artificial; Sociedade Algorítmica; Três Leis da Robótica.

## ABSTRACT

The work examines the challenges posed by emerging technologies, such as robots, artificial intelligence, and algorithms, within the Algorithmic Society. It contrasts the "Frankenstein Complex," which fears malevolent machines, with Isaac Asimov's Three Laws of Robotics, emphasizing that, in practice, legal and interpretative issues arise that necessitate regulations focused on the humans who develop and operate these technologies. The argument is made that governance should prioritize the good faith, transparency, and responsibility of designers and operators, rather than concentrating solely on the devices themselves. The "homunculus fallacy" is used to critique the mistaken belief that there is a human entity within AI programs, highlighting the need to regulate programming and data usage. Additionally, the "substitution effect," in which AI and robots replace humans, impacting social dynamics, is discussed. Finally, three fundamental legal principles are proposed to guide interactions within the Algorithmic Society: fiduciary duties, public obligations, and the prevention of cost externalization, applying these principles to both digital companies and governments.

**Keywords:** Algorithmic Society; algorithms; artificial intelligence; Big Data; Three Laws of Robotics.

<sup>1</sup> Tradução para o português brasileiro realizado por Joyce Finato Pires publicado originalmente em inglês na Ohio State Law Journal, Vol. 78, (2017), Forthcoming Yale Law School, Public Law Research Paper N.º 592 – Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=2890965f](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2890965f). A Equipe Editorial da Revista Direitos Fundamentais e Democracia agradece ao autor pela permissão da tradução do texto. Revisão Final: Elcio Domingues da Silva.

<sup>2</sup> Professor de Direito Constitucional e Primeira Emenda na *Yale Law School*. Fundador e diretor do *Information Society Project* de Yale, um centro interdisciplinar que estuda o direito e as novas tecnologias da informação. Ele também dirige o Instituto Abrams para a Liberdade de Expressão e o Programa Knight de Direito e Mídia em Yale.



## 1. CONSIDERAÇÕES INICIAIS

Em seus contos e romances, Isaac Asimov imaginou três leis da robótica programadas em cada robô. Em nosso mundo, as "leis da robótica" são os princípios legais e de políticas que devem governar como os seres humanos utilizam robôs, algoritmos e agentes de inteligência artificial. Este ensaio apresenta esses princípios legais básicos usando quatro ideias-chave: (1) a falácia do homúnculo; (2) o efeito de substituição; (3) o conceito de fiduciários de informação; e (4) a ideia de incômodo algorítmico.

A falácia do homúnculo é a atribuição de intenção e agência humana a robôs e algoritmos. Trata-se da crença equivocada de que há uma pequena pessoa dentro do robô ou programa que tem boas ou más intenções. O efeito de substituição refere-se aos múltiplos efeitos sobre o poder social e as relações sociais que surgem do fato de que robôs, agentes de IA e algoritmos substituem seres humanos e operam como pessoas de propósito específico. As questões mais importantes na lei da robótica exigem que compreendamos como os seres humanos exercem poder sobre outros seres humanos mediado por novas tecnologias. As "três leis da robótica" para nossa Sociedade Algorítmica, em outras palavras, devem ser leis direcionadas aos seres humanos e às organizações humanas, não aos robôs em si.

Por trás de robôs, agentes de inteligência artificial e algoritmos estão governos e empresas organizados e operados por seres humanos. Uma característica da Sociedade Algorítmica é que as novas tecnologias permitem que organizações públicas e privadas governem grandes populações. Além disso, a Sociedade Algorítmica também apresenta assimetrias significativas de informação, capacidade de monitoramento e poder computacional entre aqueles que governam outros com tecnologia e aqueles que são governados.

Com isso em mente, podemos estabelecer três "leis da robótica" básicas para a Sociedade Algorítmica: Primeiro, operadores de robôs, algoritmos e agentes de inteligência artificial são fiduciários de informação que têm deveres especiais de boa-fé e de negociação justa em relação a seus usuários finais, clientes e consumidores. Segundo, empresas privadas que não são fiduciárias de informação ainda assim têm deveres em relação ao público em geral.



Terceiro, o dever público central daqueles que utilizam robôs, algoritmos e agentes de inteligência artificial é não serem incômodos algorítmicos. Empresas e organizações não podem aproveitar as assimetrias de informação, capacidade de monitoramento e poder computacional para externalizar os custos de suas atividades para o público em geral. O termo "incômodo algorítmico" captura a ideia de que o melhor análogo para os danos da tomada de decisão algorítmica não é a discriminação intencional, mas a "poluição" socialmente injustificada - isto é, o uso do poder computacional para fazer com que outros arquem com os custos das atividades de uma organização.

Obrigações de transparência, devido processo e responsabilidade derivam desses três requisitos substantivos. Transparência – e suas variantes, responsabilidade e devido processo – aplicam-se de maneiras diferentes em relação a todos os três princípios. Transparência e/ou responsabilidade podem ser uma obrigação das relações fiduciárias, podem decorrer de deveres públicos, e podem ser uma medida profilática destinada a prevenir a externalização injustificada de danos ou para fornecer um remédio para o dano.

## 2.0 COMPLEXO DE FRANKENSTEIN

Quando eu era menino, li todas as histórias de Isaac Asimov sobre robótica. No mundo de Asimov, os robôs foram gradualmente integrados a todos os aspectos da sociedade. Eles tinham vários graus de semelhança com humanos, mas à medida que as histórias e romances progrediam, os robôs mais avançados tornavam-se cada vez mais semelhantes aos humanos em aparência e forma.

A característica mais famosa dessas histórias de robôs são as três leis da robótica de Asimov que deveriam ser incorporadas ao cérebro positrônico de cada robô. As três leis são:

*Primeira Lei:* “um robô não pode ferir um ser humano ou, por inação, permitir que um ser humano sofra algum mal”.<sup>3</sup>

*Segunda Lei:* “um robô deve obedecer às ordens dadas por seres humanos, exceto nos casos em que tais ordens entrem em conflito com a Primeira Lei.”<sup>4</sup>

<sup>3</sup> ASIMOV, Isaac. Runaround. In: **I Robot**. 1950, p. 37.

<sup>4</sup> *Idem*.



*Terceira Lei*: “um robô deve proteger sua própria existência, desde que tal proteção não entre em conflito com a Primeira ou Segunda Leis”.<sup>5</sup>

Essas três leis foram extremamente influentes e, até hoje, as pessoas ponderam sobre como seria – ou se seria possível – incorporá-las as tecnologias modernas, como aos carros autônomos<sup>6</sup>.

Como um artifício dramático, as leis da robótica substituíram uma convenção narrativa conhecida sobre robôs por uma alternativa muito mais interessante. A tradição anterior era a ideia do monstro de Frankenstein ou do robô assassino, que se torna malévolo ou enlouquece. Um exemplo desse tema literário na franquia de filmes *Exterminador do Futuro* é a rede neural *Skynet* se tornando autoconsciente e dominando o mundo<sup>7</sup>. Mas Asimov escreveu suas histórias de robôs para combater o que ele chamava de *Complexo de Frankenstein*, a ideia de que os robôs eram inerentemente ameaçadores ou malignos – e que os seres humanos inevitavelmente criariam seres mecânicos que se voltariam contra seus criadores.<sup>8</sup> Em muitas de suas histórias, de fato, as pessoas começam com preconceitos contra os robôs e depois passam a reconhecer seu valor. Por exemplo, o protagonista de várias de suas histórias, o detetive Elijah Bailey, que inicialmente é cético em relação aos robôs, eventualmente se torna melhor amigo de R. Daneel Olivaw, seu parceiro robótico.<sup>9</sup>

Ao criar as três leis, Asimov tornou as coisas muito mais interessantes. Em vez de apenas se preocupar se os robôs eventualmente se voltariam contra nós, ele levantou um problema adicional que é muito caro ao mundo do Direito – o problema da interpretação jurídica. O que nós – ou, em alguns casos, os próprios robôs – fazemos quando as leis não estão claras ou quando estão em conflito? Ao criar as três leis, Asimov transformou nossa visão sobre os robôs, de ameaças para objetos de interpretação e regulamentação, e assim

<sup>5</sup> ASIMOV, Isaac. Runaround. *In: I Robot*. 1950, p. 37.

<sup>6</sup> Verificar DENG, Boer. Machine ethics: the robot's dilemma. *Revista Nature*, v. 523, p. 24-26, jul. 2015. Disponível em: <http://www.nature.com/news/machine-ethics-the-robot-s-dilemma-1.17881>. Compare com: BARTHELMESS, Ulrike; FURBACH, Ulrich. Do we need Asimov's Laws? Cornell University Library, 2014, p. 11. Disponível em: <https://arxiv.org/ftp/arxiv/papers/1405/1405.0961.pdf>. Os autores argumentam que as leis refletem ansiedades culturais sobre robôs e que é desnecessário incorporá-las em robôs reais.

<sup>7</sup> **O exterminador do futuro**. Direção de James Cameron. Hermdale Film Corporation, Pacific Western Productions Cinema, 1984.

<sup>8</sup> ASIMOV, Isaac. The machine and the robot. *In: WARRICK, P. S.; GREENBERG, M. H.; OLANDER, J. D.* (Eds.). **Science Fiction: contemporary mythology**. 1978; MCCAULEY, Lee. The Frankenstein Complex and Asimov's Three Laws. *In: Association for the Advancement of Artificial Intelligence*. 2007, p. 09-14, p. 09. Disponível em: <https://perma.cc/AJ9F-FHTJ>.

<sup>9</sup> Por exemplo: ASIMOV, Isaac. **The caves of steel**. 1954; ASIMOV, Isaac. **The naked sun**. 1957; ASIMOV, Isaac. **Mirror image**. *In: Robot Visions*. 1990, p. 319; ASIMOV, Isaac. **The robots of dawn**. 1983.



também de ironia e conflito. É uma ideia muito sofisticada, e que ele desenvolve em muitas de suas histórias.

Hoje, não está claro se poderíamos realmente construir as três leis que Asimov postulou em robôs e agentes de inteligência artificial (IA). Afinal, as três leis de Asimov parecem bastante vagas e incompletas. Elas podem ter brechas. Claro, isso fazia parte do objetivo de Asimov. Uma convenção narrativa recorrente nas histórias de Asimov é que as leis eram obscuras, vagas ou poderiam entrar em conflito em certas circunstâncias; assim, a trama muitas vezes girava em torno de maneiras inteligentes de interpretá-las ou reinterpretá-las, ou como resolver conflitos entre elas, e assim por diante.

E em um romance posterior, Daneel Olivaw, um robô que começa como detetive, mas acaba sendo uma figura muito importante nos romances, torna-se tão avançado que cria sua própria lei zero – “um robô não pode ferir a humanidade, ou por inação, permitir que a humanidade sofra algum mal” – que precede todas as outras que ele recebeu em sua programação original.<sup>10</sup>

De qualquer forma, meu objetivo hoje é perguntar que uso podemos fazer da ideia original de Asimov das leis da robótica. Quando falo de robôs, no entanto, incluirei tanto robôs como objetos materiais que interagem com seu ambiente, agentes de inteligência artificial e algoritmos de aprendizado de máquina. Acredito que isso esteja perfeitamente alinhado com as preocupações de Asimov. Embora ele tenha escrito principalmente sobre robôs, também escreveu sobre computadores muito inteligentes<sup>11</sup>.

E o *Complexo de Frankenstein* que ele estava tentando combater poderia surgir do medo da IA ou de algoritmos tanto quanto do medo de robôs corpóreos. Hoje, as pessoas parecem temer não apenas robôs, mas também sistemas autômatos de IA e algoritmos, incluindo sistemas de aprendizado de máquina.<sup>12</sup> Os robôs parecem ser apenas um caso especial de um conjunto muito maior de preocupações.

---

<sup>10</sup> ANGELO, Joseph A. **Robotics**: a reference guide to the new technology. 2006, p. 103; ASIMOV, Isaac. **Robots and empire**. 1985, p. 291.

<sup>11</sup> ASIMOV, Isaac. The last question. *In*: **Robot dreams**. 1995, p. 204.

<sup>12</sup> Confira, por exemplo, CELLAN-JONES, Rory. Stephen Hawking warns artificial intelligence could end mankind. **BBC**, 2 dez. 2014. Disponível em: <http://www.bbc.com/news/technology-30290540>; GIBBS, Samuel. Elon Musk: artificial intelligence is our biggest existential threat. **The Guardian**, 27 out. 2014. Disponível em: <https://www.theguardian.com/technology/2014/oct/27/elon-musk-artificial-intelligence-ai-biggest-existential-threat>; “Com inteligência artificial, estamos convocando o demônio”. Roboticistas e pesquisadores em IA, por outro lado, podem apoiar formas específicas de regulamentação, mas tendem a ser menos assustados. Veja, por exemplo, LOIZOS, Connie. This famous roboticist doesn't think Elon Musk understands AI., 19 jul. 2017. Disponível em: <https://techcrunch.com/2017/07/19/this-famous-roboticist-doesnt-think-elon-musk-understands-ai/>. Rodney Brooks aponta que as pessoas famosas como Musk, que estão mais preocupadas



Na verdade, estamos rapidamente passando da era da internet para a Sociedade Algorítmica. Logo olharemos para trás na era digital como precursora dessa Sociedade. O que eu quero dizer com Sociedade Algorítmica? Refiro-me a uma sociedade organizada em torno da tomada de decisões sociais e econômicas por algoritmos, robôs e sistemas autômatos de IA; que não apenas tomam as decisões, mas também, em alguns casos, as executam. O uso de robôs e IA, portanto, é apenas um caso especial da Sociedade Algorítmica.

*Big Data*, também, é apenas uma característica da Sociedade Algorítmica. Na verdade, *Big Data* é apenas o outro lado de uma sociedade organizada em torno da tomada de decisões algorítmicas. Ela é o combustível que alimenta a Sociedade Algorítmica; também é o produto de suas operações. A coleta e o processamento de dados produzem cada vez mais dados, que, por sua vez podem ser usados para melhorar o desempenho dos algoritmos<sup>13</sup>. Para variar a famosa declaração de Kant, algoritmos sem dados são vazios; dados sem algoritmos são cegos.<sup>14</sup>

Nesta palestra, vou apresentar três novas leis da robótica (ou IA ou algoritmos de aprendizado de máquina) para a Sociedade Algorítmica, que, como acabei de explicar, também é o mundo do *Big Data* e da análise de *Big Data*. No processo, também introduzirei quatro ideias teóricas importantes que nos ajudarão a entender como devemos regular essas entidades. As quatro ideias são (1) a *falácia do homúnculo*; (2) o *efeito de substituição*; (3) o conceito de *fiduciários de informação*; e (4) a ideia de *incômodo algorítmico*. Vou explicar essas quatro ideias à medida que a palestra avança. Embora eu

---

com a inteligência artificial, “não trabalham com IA eles mesmos”, enquanto “a regulamentação dos Teslas autônomos é uma questão real”.

<sup>13</sup> Veja, por exemplo, **THE ECONOMIST**. Combustível do futuro: dados estão dando origem a uma nova economia. 6 maio 2017. Disponível em: <https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy>. “Dados serão a externalidade definitiva: nós os geraremos independentemente do que fizermos”; GANDOMI, Amir; HAIDER, Murtaza. Beyond the hype: Big data concepts, methods, and analytics. **International Journal of Information Management**, v. 35, n. 02, p. 137-144, 2015. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0268401214001066>. Descrevendo como as empresas usam algoritmos para transformar vastas quantidades de dados não estruturados em novas formas de dados que, por sua vez, podem ser usados para análise e tomada de decisões); SINTEF. Big Data, for better or worse: 90% of world's data generated over last two years. **Science Daily**, 22 maio 2013. Disponível em: <https://www.sciencedaily.com/releases/2013/05/130522085217.htm>. “Cada um de nós está constantemente produzindo e liberando dados sobre nós mesmos. Fazemos isso tanto ao nos movimentarmos passivamente – nosso comportamento sendo registrado por câmeras ou uso de cartões – quanto ao fazermos login em nossos PCs e navegarmos na internet”.

<sup>14</sup> KANT, Immanuel. **Critique of pure reason**. Editores e tradutores: Paul Guyer e Allen W. Wood. Cambridge: Cambridge University Press, 1998, p. 193-194. “Pensamentos sem conteúdo são vazios, intuições sem conceitos são cegas”.





seja inspirado pelas três leis da robótica de Asimov, descreverei a ideia de “leis da robótica” de forma muito diferente do que ele fez.

Em primeiro lugar, essas leis não se limitarão a robôs – elas se aplicarão a sistemas autômatos de IA e algoritmos, incluindo algoritmos de aprendizado de máquina. E quando eu quiser falar sobre todos os três juntos como um grupo, falarei sobre as leis dos algoritmos em geral.

Em segundo lugar, quando as pessoas pensam em robôs na ficção científica, geralmente pensam em entidades humanóides autônomas. Mas hoje sabemos que muitos robôs e sistemas autômatos de IA estão conectados à nuvem<sup>15</sup>. Isso certamente é verdade para a Internet das Coisas e robôs domésticos. Provavelmente também será verdade para carros autônomos. Portanto, as leis da robótica, sejam quais forem, também provavelmente serão as leis das inteligências em nuvem, geralmente conectadas à internet.

Em terceiro lugar, porque os robôs são robôs em nuvem, não devemos esquecer que uma das questões centrais em robôs e sistemas autômatos de IA é o manuseio de dados, e em particular, *Big Data*. Os robôs não são nada sem dados, e como muitos robôs serão robôs em nuvem, e muitos sistemas de IA estarão conectados à nuvem da internet, eles dependerão muito da análise de dados<sup>16</sup>. Poderíamos dizer que os dados são o combustível que alimenta os motores da inteligência artificial.

Então, quando falamos sobre robôs, sistemas autômatos de IA e algoritmos, geralmente também estamos falando sobre *Big Data* e conexão à internet, assim como quando falamos sobre *Big Data* também geralmente estamos falando sobre a regulamentação de robôs, algoritmos e sistemas autômatos de IA que o processam. Quando falamos sobre as leis da robótica, na verdade estamos falando sobre robótica, algoritmos e IA na era do *Big Data*. Daí o título desta palestra.

---

<sup>15</sup> Veja KEHOE, Ben *et al.* A survey of research on cloud robotics and automation. **Institute of Electrical and Electronics Engineers**, 2015. Disponível em: <http://goldberg.berkeley.edu/pubs/T-ASE-Cloud-RA-Survey-Paper-Final-2015.pdf>. “A nuvem pode fornecer aos robôs e sistemas de automação acesso a vastos recursos de dados que não são possíveis de manter na memória embarcada”.

<sup>16</sup> VIOLINO, Bob. Big data and robotics: a long history together. **ZDNet**, 12 ago. 2016. Disponível em: <http://www.zdnet.com/article/big-data-and-robotics-a-long-history-together/>. Observando que o conceito de big data “tem sido parte do mundo da robótica há muito tempo” e que “Robótica sempre foi sobre dados”; KEHOE, Ben; PATIL, Sachin; ABBEEL, Pieter; GOLDBERG, Ken. A survey of research on cloud robotics and automation. **IEEE Transactions on Automation Science and Engineering (T-ASE): Special Issue on Cloud Robotics and Automation**, v. 12, n. 02, abr. 2015. Disponível em: <http://goldberg.berkeley.edu/pubs/T-ASE-Cloud-RA-Survey-Paper-Final-2015.pdf>. Explica-se como o acesso a big data na nuvem melhora a capacidade dos robôs de realizar tarefas e interagir com seus ambientes.



Quarto, e talvez o mais importante, Asimov chamou suas leis de leis da robótica, não leis de usuários de robôs ou programadores de robôs ou operadores de robôs.<sup>17</sup> Suas leis eram direcionadas aos robôs.<sup>18</sup> Eram centradas nos robôs – isto é, eram instruções de programação inseridas no código dos próprios robôs. Eram leis que os robôs tinham que seguir – pois foram programados dessa forma – e não obrigações impostas aos usuários de robôs.<sup>19</sup> Podemos imaginar tais instruções também fazendo parte de sistemas autômatos de IA ou algoritmos como uma verificação do aprendizado de máquina do algoritmo. São uma espécie de restrição lateral de software, da mesma forma que os direitos são restrições laterais à ação.

É claro que os humanos eram obrigados a programar as leis em cada robô, mas as leis em si eram dirigidas aos robôs, não aos humanos.<sup>20</sup> Asimov não fala muito sobre as leis humanas que exigiam essa programação, mas presume-se que houve algum tipo de requisito governamental para que fossem inseridas no cérebro positrônico de cada robô.

Eu vou divergir de Asimov neste ponto. Em vez de me concentrar em leis dirigidas a robôs (ou algoritmos), me concentro em leis dirigidas às pessoas que programam e usam robôs, sistemas autômatos de IA e algoritmos. Isso ocorre porque o que precisamos na emergente Sociedade Algorítmica não são leis da robótica, mas leis dos operadores de robôs.

A pretensão da Sociedade Algorítmica é o aproveitamento de dados e algoritmos para governar a sociedade e torná-la melhor. A ambição da Sociedade Algorítmica é a da onisciência – saber tudo e prever tudo – uma ambição tão antiga quanto a humanidade, mas agora aparentemente cada vez mais próxima de estar ao nosso alcance.

Na Sociedade Algorítmica, o problema central da regulamentação não são os algoritmos, mas os seres humanos que os usam e permitem que sejam governados por eles. A governança algorítmica é a governança dos seres humanos por seres humanos usando uma tecnologia específica de análise e tomada de decisões.

Portanto, nossa necessidade não é de leis direcionadas a robôs, como as três leis da robótica de Asimov, mas de leis direcionadas àqueles que usam robôs para analisar, controlar e exercer poder sobre outros seres humanos.

<sup>17</sup> ASIMOV, Isaac. Runaround. In: *I Robot*. 1950, p. 37.

<sup>18</sup> *Idem*.

<sup>19</sup> *Idem*.

<sup>20</sup> *Idem*.





### 3.0 RABINO E O GOLEM

Deixe-me explicar essa ideia com uma história. Margot Kaminski e eu ensinamos o primeiro curso de direito e robótica na Faculdade de Direito de Yale na primavera de 2014. Ela elaborou uma lista de leitura que tenho usado nos anos seguintes. Para a primeira aula, ela escolheu uma seleção de exemplos literários famosos, incluindo um conto de Asimov que apresenta as três leis,<sup>21</sup> e a peça de 1921 de Karel Capek, *RUR*<sup>22</sup>, que é a origem da palavra “robô”. Ela também escolheu uma versão da lenda do Golem de Praga.<sup>23</sup>

Segundo a lenda, o Golem de Praga foi criado pelo Rabino Judah Loew ben Bezalel, o Maharal, um sábio do século XVI amplamente reverenciado por seu conhecimento e piedade<sup>24</sup>. O Maharal empregou o conhecimento secreto do misticismo judaico para moldar um ser vivo de argila, em paralelo à criação de Adão por Deus. Ao pronunciar o nome divino, ele concedeu vida ao Golem, que se assemelhava a um humano. Era muito forte, mas não podia falar, porque, segundo a lenda, o poder da fala foi dado apenas ao homem por Deus (da próxima vez que conversar com a Siri, considere como as coisas mudaram).<sup>25</sup>

De qualquer forma, o Maharal envia o Golem para lidar com ameaças à comunidade judaica. Na lenda, o Golem age como um detetive – assim como Daneel Olivaw de Asimov. Ele descobre quem está difamando os judeus e captura os malfeitores. Então, depois de cumprir seu propósito, ele retorna ao Rabino, que faz os mesmos encantamentos secretos ao contrário, e o Golem se transforma novamente em um monte de argila sem vida, onde é guardado no sótão da sinagoga<sup>26</sup>.

Qual é o ponto desta história? Bem, a coisa mais interessante nesta versão da história é o que não acontece. O Golem não enlouquece. Ele não pega a pessoa errada. A esposa do Rabino não descobre o Golem e o liberta acidentalmente; o genro do Rabino não usa o Golem para ganhar dinheiro; uma pessoa sem escrúpulos não reeduca o Golem

<sup>21</sup> ASIMOV, Isaac. Runaround. *In: I Robot*. 1950.

<sup>22</sup> KAREL, Capek. *RUR*. 1921.

<sup>23</sup> O GOLEM DE PRAGA. *In: AUSUBEL, Nathan (Ed.). A treasury of Jewish folklore*. 1948, p. 603.

<sup>24</sup> JESTICE, Phyllis G. *Holy people of the world: a cross-cultural encyclopedia*. Santa Barbara: ABC-CLIO, 2004, p. 450; COMAY, Joan; COHN-SHERBOK, Lavinia. *Who's who in Jewish history: after the period of the Old Testament*. 2. ed. Londres: Routledge, 2001, p. 221. Muito reverenciado por sua piedade e erudição.

<sup>25</sup> O GOLEM DE PRAGA. *In: AUSUBEL, Nathan (Ed.). A treasury of Jewish folklore*. 1948, p. 607-608.

<sup>26</sup> *Ibidem*, p. 609-611.



para fazer o mal, e assim por diante. Na verdade, nada de ruim acontece nesta história. O Golem faz exatamente o que deve fazer. E, de certa forma, esta versão da lenda é bastante entediante; existem outras versões da lenda do Golem em que as coisas dão errado e são muito mais interessantes dramaticamente<sup>27</sup>.

Mas a lição mais importante que podemos tirar dessa história é que o motivo de nada dar errado é que o Golem é programado e empregado pelo Maharal, um homem da maior piedade e conhecimento. Apenas um homem verdadeiramente justo, ou um santo, é capaz de usar o Golem apenas para o bem.

E isso, na minha opinião, é a verdadeira lição da história. Quando falamos sobre robôs, ou sistemas autômatos de IA, ou algoritmos, geralmente nos concentramos em se eles causam problemas ou ameaças. Mas na maioria dos casos, o problema não são os robôs. São os humanos.

Por que o problema são os humanos e não os robôs?

Primeiro, os humanos projetam os algoritmos, os programam, os conectam a bancos de dados e os liberam.

Segundo, os humanos decidem como usar os algoritmos, quando usá-los e para qual propósito.

Terceiro, os humanos programam os algoritmos com dados, cuja seleção, organização e conteúdo contêm o resíduo de discriminações e injustiças anteriores.

Quarto, embora as pessoas falem sobre o que os robôs fizeram ou o que os sistemas autômatos de IA fizeram, ou o que os algoritmos fizeram, falar dessa maneira deixa passar um ponto importante. Essas tecnologias mediam as relações sociais entre seres humanos e outros seres humanos. A tecnologia está incorporada às – e muitas vezes disfarça – relações sociais.

Quando os algoritmos discriminam ou fazem coisas ruins, portanto, sempre precisamos perguntar como os algoritmos estão envolvidos em reproduzir e dar efeito a relações sociais específicas entre seres humanos. São relações sociais que produzem e reproduzem justiça e injustiça, poder e impotência, status superior e subordinação. Os robôs, sistemas autômatos de IA e algoritmos são os dispositivos por meio dos quais essas

---

<sup>27</sup> Veja, por exemplo, LEIVICK, H. O Golem. *In: Golem: a new translation of the classic play and selected short stories*. Tradução de Joachim Neugroschel. 2006; veja também ELSWIT, Sharon Barcan. **The Jewish story finder: a guide to 668 tales listing subjects and sources**. 2012, p. 205. Lista-se a história básica e variações na literatura judaica.



relações sociais são produzidas, por meio dos quais formas particulares de poder são processadas e transformadas. É isso que quero dizer quando digo que o problema não são os robôs, são os humanos.

#### 4.A FALÁCIA DO HOMÚNCULO

Isso me leva à primeira das quatro ideias que prometi discutir nesta palestra. Eu criei uma frase – a falácia do homúnculo – para descrever a maneira como as pessoas tendem a pensar sobre robôs, sistemas autômatos de IA e algoritmos. A falácia do homúnculo é a crença de que há uma pequena pessoa dentro do programa que o faz funcionar – ela tem boas ou más intenções, e faz o programa realizar coisas boas ou ruins.

Mas na verdade não há uma pessoa dentro do algoritmo. Há programação – código – e há dados. E o programa usa os dados para funcionar, com efeitos bons ou ruins, alguns previsíveis, outros imprevisíveis.

Quando criticamos algoritmos, estamos realmente criticando a programação, ou os dados, ou a interação entre eles. Mas igualmente importante, estamos também criticando o uso que está sendo feito deles pelos humanos que programaram os algoritmos, coletaram os dados ou empregaram os algoritmos e os dados para realizar tarefas específicas. Estamos criticando o Rabino, não o Golem.

Então, que tipos de relações sociais essas tecnologias produzem e reproduzem? Para explicar isso, preciso introduzir a segunda das quatro ideias nesta palestra, uma ideia que discuti anteriormente. Este é o *efeito de substituição*.<sup>28</sup>

O efeito de substituição diz respeito aos efeitos sobre a sociedade produzidos pelo fato de que robôs, sistemas autômatos de IA e algoritmos substituem seres humanos. Eles operam como pessoas com propósitos especiais. A noção de robô ou algoritmo como substituto transmite quatro ideias diferentes: (1) o substituto é de alguma forma melhor que o original; (2) o substituto é de outras formas mais limitado que o original; (3) as pessoas tratam o substituto como se estivesse vivo – elas se envolvem em animismo ou antropomorfismo; e o substituto age como um fetiche ou desvio longe das bases sociais de poder entre seres humanos e grupos de seres humanos.<sup>29</sup>

<sup>28</sup> BALKIN, Jack M. The path of robotics law. *California Law Review Circuit*, v. 05, p. 45-60, 2015, p. 55-59.

<sup>29</sup> BALKIN, Jack M. The path of robotics law. *California Law Review Circuit*, v. 05, p. 45-60, 2015, p. 57-59.



Primeiro, a substituição significa superioridade: robôs, sistemas autômatos de IA e algoritmos são mais poderosos e rápidos que seres humanos e tomadores de decisão humanos.<sup>30</sup> Eles podem ver coisas, fazer coisas, analisar coisas e tomar decisões que seres humanos nunca poderiam fazer. Eles nunca se cansam de fazer isso, e não têm distrações emocionais ou escrúpulos emocionais sobre fazer isso.<sup>31</sup>

Segundo, a substituição também significa limitação ou deficiência. Robôs, sistemas autômatos de IA e algoritmos têm habilidades limitadas. Eles podem fazer apenas algumas coisas, mas não outras. Eles carecem de muitas das características do julgamento humano.<sup>32</sup>

Terceiro, a substituição envolve a projeção de vida, capacidade de agir e intenção em programas e máquinas.<sup>33</sup> Isso também encoraja a projeção de responsabilidade dos humanos que usam os algoritmos para os algoritmos em si – daí a falácia do homúnculo.

Quarto, a substituição envolve um *fetichismo* ou *desvio ideológico*. Marx falou famosamente do fetichismo das mercadorias<sup>34</sup>. Assim como as sociedades antigas acreditavam que totens, que eram objetos inanimados, eram imbuídos de poderes mágicos, Marx argumentou que as pessoas em uma sociedade de mercado tratam a mercadoria como se tivesse valor, quando na verdade o que lhe dá valor é o fato de estar embutida em um sistema de relações sociais.<sup>35</sup> Mercados são relações sociais que tanto capacitam as pessoas quanto permitem que elas exerçam poder sobre os outros.

O que é verdade das mercadorias nos mercados também é verdade do uso de substitutos tecnológicos na forma de robôs, sistemas autômatos de IA e algoritmos. Essas

---

<sup>30</sup> *Ibidem*, p. 59.

<sup>31</sup> *Ibidem*, p. 58-59.

<sup>32</sup> RASTOGI, Anupam. Artificial intelligence: human augmentation is what's here and now. **Medium**, 12 jan. 2017. Disponível em: <https://medium.com/reflections-by-ngp/artificial-intelligence-human-augmentation-is-whats-here-and-now-c5286978ace0>. Observando que “máquinas estão em sua infância relativa” no exercício de julgamentos de senso comum que são fáceis para os seres humanos, “apesar dos avanços rápidos no Processamento de Linguagem Natural usando aprendizado profundo”; HAVASI, Catherine. Who's common-sense reasoning and why it matters. **Techcrunch**, 9 ago. 2014. Disponível em: <https://techcrunch.com/2014/08/09/guide-to-common-sense-reasoning-whos-doing-it-and-why-it-matters/>. Observa-se que um desafio central da pesquisa em inteligência artificial é desenvolver capacidades para o raciocínio contextual e de senso comum.

<sup>33</sup> BALKIN, Jack M. The path of robotics law. **California Law Review Circuit**, v. 05, p. 45-60, 2015, p. 57.

<sup>34</sup> MARX, Karl. Capital: A critique of political economy. In: **The fetishism of commodities and the secret thereof**. ENGELS, Friedrich (Ed.). Tradução de Samuel Moore e Edward Aveling. Mineola: Dover Publications, Inc., 2011, p. 81.

<sup>35</sup> *Ibidem*, p. 83. “Uma mercadoria é, portanto, uma coisa misteriosa, simplesmente porque nela o caráter social do trabalho dos homens aparece a eles como um caráter objetivo estampado no produto desse trabalho”.



tecnologias se tornam parte das relações sociais de poder entre indivíduos e grupos. Não devemos confundir o Golem com o Rabino. Os efeitos da robótica são sempre sobre as relações de poder entre seres humanos ou grupos de seres humanos.

Recentemente, a mídia relatou uma história sobre um algoritmo para escolher concorrentes a concursos de beleza que preferia pessoas brancas.<sup>36</sup> Esse tipo de história encoraja a ideia de que algoritmos têm preconceitos psicológicos. Esta é a falácia do homúnculo – não há um pequeno juiz de concurso de beleza dentro do algoritmo que está empregando seus preconceitos. Há história de concursos de beleza anteriores, os pressupostos culturais sobre beleza que informam esses concursos, o modo como os dados são coletados, o código que o algoritmo emprega e o código para revisar o código, se o algoritmo emprega aprendizado de máquina. Há também as pessoas que lançam o algoritmo para uma tarefa específica. Devemos sempre lembrar que por trás do Golem está o Rabino (ou toda uma sociedade de Rabinos) que criam e usam o Golem.

## 5.AS LEIS DE UMA SOCIEDADE ALGORÍTMICA

Deixe-me resumir o argumento até agora. Comecei esta palestra com as três leis da robótica de Asimov. Apontei que essas leis eram direcionadas aos robôs e ao seu código. Em seguida, usando a história do Golem, apontei que o problema não são os robôs, mas sim os seres humanos. Se for assim, significa que, em vez das leis de robótica de Asimov, o que realmente precisamos são leis dos projetistas e operadores de robótica. As leis de robótica de que precisamos em nossa Sociedade Algorítmica são leis que controlam e direcionam os seres humanos que criam, projetam e empregam robôs, sistemas autômatos de IA e algoritmos. E como algoritmos sem dados são vazios, estas também são as leis que controlam a coleta, uso, distribuição e venda dos dados que fazem esses algoritmos funcionarem.

Em suma, as leis de robótica de que precisamos são leis dos seres humanos que fazem e usam robôs e os dados que os robôs usam. Que tipos de leis seriam essas? Volte ao meu ponto central – que por trás dos robôs, sistemas autômatos de IA e algoritmos estão

---

<sup>36</sup> LEVIN, Sam. A beauty contest was judged by AI and the robots didn't like dark skin. **The Guardian**, 8 set. 2016. Disponível em: <https://www.theguardian.com/technology/2016/sep/08/artificial-intelligence-beauty-contest-doesnt-like-black-people>. Uma empresa chamada Beauty.AI desenvolveu o algoritmo. Veja **BEAUTY.AI**. Welcome to the first international beauty contest judged by artificial intelligence. Disponível em: <http://beauty.ai/>.



relações sociais entre seres humanos e grupos de seres humanos. Portanto, as leis que precisamos são obrigações de boa-fé, não manipulação e não dominação entre aqueles que fazem e usam os algoritmos e aqueles que são governados por eles.

As pessoas usam algoritmos para classificar e governar populações de pessoas. Porque a relação é de governança, as obrigações são fiduciárias – de boa-fé, não manipulação e não dominação. Estes são os princípios que devem guiar a Sociedade Algorítmica. Ao contrário das três leis de Asimov, esses princípios não são automaticamente incorporados aos robôs. Temos que garantir que caracterizem as relações entre seres humanos. Devemos incorporá-los em nossa sociedade humana, devemos programá-los em nossas leis.

Quais são os deveres dos usuários de algoritmos para com a sociedade? Para responder a essa pergunta, considere a ambição da Sociedade Algorítmica. O sonho da Sociedade Algorítmica é o governo onisciente da sociedade. Das ambições vêm os danos: incluem, além da possibilidade de lesões físicas, violações de privacidade, exposição, danos à reputação, discriminação, conformação (ou normalização)<sup>37</sup> e manipulação.

A Sociedade Algorítmica é uma forma de governar populações. Por governança, quero dizer a maneira como as pessoas que controlam os algoritmos entendem, analisam, controlam, dirigem, ordenam e moldam as pessoas que são os sujeitos dos dados. As pessoas usam algoritmos para classificar, selecionar, compreender e tomar decisões sobre populações inteiras. Esta relação não é simplesmente uma relação de lucro de mercado. Também é uma relação de governança.

A Sociedade Algorítmica também envolve relações de poder informacional. A IA sabe muito sobre você; mas você não sabe muito sobre a IA. Além disso, você não pode monitorar muito bem o que o agente de IA ou algoritmo faz. Há uma assimetria de poder e uma assimetria de informação entre os operadores e aqueles que são afetados ou governados. Essa assimetria é uma característica central da Sociedade Algorítmica – é a assimetria de conhecimento e poder entre os governantes públicos e privados da Sociedade Algorítmica e aqueles que são governados por eles.

---

<sup>37</sup> Nota do tradutor: No texto original está a expressão "regimentation (or normalization)" que foi traduzida para o português brasileiro como "**conformação**" (ou **normalização**). Essas palavras capturam o sentido de ajuste comportamental ou conformidade às normas impostas, seja por meio de regras explícitas ou por influências implícitas, como a categorização por algoritmos. "Conformação" enfatiza a ideia de controle e organização estrita, enquanto "normalização" destaca o processo de tornar comportamentos ou características conformes a um padrão estabelecido.





Quais são as três leis – ou mais corretamente, os princípios jurídicos – da Sociedade Algorítmica? Eles são três princípios de governança justa.

(1) Em relação aos clientes, consumidores e usuários finais, os usuários de algoritmos são *fiduciários de informação*.

(2) Em relação àqueles que não são clientes, consumidores ou usuários finais, os usuários de algoritmos têm *deveres públicos*. Se forem governos, isso decorre de sua natureza como governos. Se são atores privados, seus negócios são afetados por um interesse público, como os constitucionalistas diriam durante a década de 1930.<sup>38</sup>

(3) O dever público central dos usuários de algoritmos é evitar a externalização dos custos (danos) de suas operações. A melhor analogia para os danos da tomada de decisões algorítmicas não é a discriminação intencional, mas a poluição socialmente injustificada.

Obrigações de transparência, compreensibilidade, devido processo e responsabilização decorrem desses três requisitos substantivos. Transparência – e suas derivações, devido processo, responsabilização e compreensibilidade – se aplicam de diferentes maneiras com relação a todos os três princípios.

Responsabilização, transparência e compreensibilidade podem ser uma obrigação de relações fiduciárias. Eles podem decorrer de deveres públicos. Eles podem ser uma medida profilática para evitar a externalização injustificada de danos, ou para fornecer um remédio para o dano. Permitam-me discutir cada um desses três princípios jurídicos.

## **6.PRIMEIRA LEI: OPERADORES ALGORÍTMICOS SÃO FIDUCIÁRIOS DE INFORMAÇÕES EM RELAÇÃO A SEUS CLIENTES E USUÁRIOS FINAIS**

Para discutir o primeiro princípio jurídico, introduzo mais uma das ideias-chave que prometi mencionar durante esta palestra. Esta é a ideia de *fiduciários de informação*, um conceito que desenvolvi em trabalhos anteriores<sup>39</sup>. Para entender o que é um fiduciário de informação, devemos primeiro perguntar, o que é um fiduciário? Exemplos de fiduciários são profissionais como médicos e advogados, e pessoas que administram patrimônios ou

<sup>38</sup> Veja *NEBBIA v. NEW YORK*, 291 U.S. p. 502-536, 1934. “A expressão ‘afetada pelo interesse público’ pode, pela própria natureza das coisas, significar nada mais do que uma indústria, por razão adequada, está sujeita a controle para o bem público”.

<sup>39</sup> BALKIN, Jack M. Information fiduciaries and the First Amendment. *U.C. Davis Law Review*, v. 49, p. 1183-1234, 2015, p. 1183.



propriedades de outras pessoas.<sup>40</sup> O que torna alguém um fiduciário é que as pessoas dependem deles para fornecer serviços, mas há uma assimetria significativa no conhecimento e na habilidade entre o fiduciário e o cliente, e o cliente não pode facilmente monitorar o que o fiduciário está fazendo em seu nome.<sup>41</sup> Como resultado, a lei exige que os fiduciários atuem de maneira confiável, de boa-fé, e evitem criar conflitos de interesse com o cliente ou paciente.<sup>42</sup> Fiduciários frequentemente coletam informações pessoais sensíveis sobre seus clientes, que poderiam usar em detrimento deles. Portanto, a lei exige que protejam a privacidade de seus clientes e não divulguem informações de maneiras que os prejudiquem.<sup>43</sup> Quando fiduciários coletam e processam informações sobre seus clientes, podemos dar-lhes um nome especial. Eles são fiduciários de informação.<sup>44</sup> A maioria dos profissionais também são fiduciários de informação.<sup>45</sup>

Os fiduciários têm dois deveres centrais. O primeiro é o dever de cuidado<sup>46</sup>. O segundo é o dever de lealdade.<sup>47</sup> O dever de cuidado significa que um fiduciário deve agir com cuidado razoável para evitar prejudicar o cliente ou paciente.<sup>48</sup> O dever de lealdade significa que o fiduciário deve evitar criar conflitos de interesse com seus clientes ou pacientes e deve zelar por seus interesses.<sup>49</sup> O grau de lealdade exigido depende da natureza do relacionamento entre o fiduciário e o cliente.

A era digital criou um conjunto de entidades que têm muitas características semelhantes às dos fiduciários tradicionais. Eles incluem grandes empresas online como Google, Facebook e Uber. Essas empresas coletam, compilam, analisam e usam informações sobre nós. Na verdade, elas coletam enormes quantidades de informações sobre nós, que teoricamente poderiam ser usadas em nosso prejuízo. Essas empresas se tornaram muito importantes, em alguns casos indispensáveis, para nossas vidas cotidianas. Também há uma assimetria de conhecimento entre as empresas e seus usuários finais e clientes. As empresas online sabem muito sobre nós; nós sabemos comparativamente

---

<sup>40</sup> BALKIN, Jack M. Information fiduciaries and the First Amendment. *U.C. Davis Law Review*, v. 49, p. 1183-1234, 2015, p. 1207.

<sup>41</sup> *Ibidem*, p. 1216-1217.

<sup>42</sup> *Ibidem*, p. 1207-1208.

<sup>43</sup> *Idem*.

<sup>44</sup> *Ibidem*, p. 1208.

<sup>45</sup> *Ibidem*, p. 1208-1209.

<sup>46</sup> *Ibidem*, p. 1207-1208.

<sup>47</sup> *Ibidem*, p. 1208.

<sup>48</sup> *Ibidem*, p. 1207-1208.

<sup>49</sup> *Ibidem*, p. 1208.



pouco sobre suas operações, e elas tratam seus processos internos como proprietários para evitar roubo por concorrentes. Ao mesmo tempo, essas empresas tentam tranquilizar seus usuários finais de que respeitarão sua privacidade e não trairão sua confiança. Porque são, nas palavras de Frank Pasquale, uma caixa preta,<sup>50</sup> a maioria das pessoas simplesmente tem que confiar nelas.

Eu argumento que empresas como essas têm muitas das características dos fiduciários tradicionais.<sup>51</sup> Elas coletam informações sobre nós; elas nos observam, mas nós não podemos facilmente observá-las, e temos que confiar nelas<sup>52</sup>. Tais relacionamentos tradicionalmente levaram ao status de fiduciário<sup>53</sup>. Portanto, argumento que essas empresas devem ter obrigações legais de serem confiáveis para seus usuários finais. Elas são as versões da era digital de fiduciários de informação<sup>54</sup>. No entanto, os deveres dos fiduciários de informação da era digital são diferentes dos médicos e advogados. Eles são mais limitados por causa do tipo de serviços que prestam e por causa dos tipos de confiança razoável que criam<sup>55</sup>.

Primeiro, ao contrário de médicos e advogados, a monetização de dados pessoais é central para muitas empresas de serviços online, porque lhes permite subsidiar os serviços que prestam ou oferecem gratuitamente. Apenas recuperar despesas ou lucrar com tais informações não viola por si só seu dever fiduciário<sup>56</sup>.

Segundo, muitos provedores online, como mecanismos de busca e sites de mídia social, ganham dinheiro porque os usuários finais produzem um fluxo constante de conteúdo e links. Assim, ao contrário dos profissionais tradicionais, essas empresas têm interesse em fazer com que as pessoas revelem o máximo possível sobre si mesmas – ou de outra forma se expressem publicamente o máximo possível – para que suas atividades gerem conteúdo e dados que as empresas possam indexar e analisar.<sup>57</sup>

Terceiro, as pessoas esperam que os médicos façam muito mais do que simplesmente não as prejudicar; as pessoas também esperam que os médicos zelem por

---

<sup>50</sup> PASQUALE, Frank. **The Black Box Society**: the secret algorithms that control money and information. 2015. Discute-se o segredo envolvido na coleta, análise e uso corporativos de dados pessoais.

<sup>51</sup> BALKIN, Jack M. Information fiduciaries and the First Amendment. **U.C. Davis Law Review**, v. 49, p. 1221-1222 e 1228, 2015.

<sup>52</sup> *Ibidem*, p. 1207.

<sup>53</sup> *Idem*.

<sup>54</sup> *Ibidem*, p. 1207.

<sup>55</sup> *Ibidem*, p. 1225-1226.

<sup>56</sup> *Ibidem*, p. 1225-1227.

<sup>57</sup> *Idem*.



seus interesses e as alertem sobre possíveis riscos para sua saúde, sua dieta, etc. As pessoas não esperam tais obrigações abrangentes de cuidado de seus provedores de serviços de internet, mecanismos de busca e sites de mídia social.<sup>58</sup>

Devido a essas diferenças, os fiduciários de informação digital devem ter diferentes e menores obrigações do que os fiduciários profissionais tradicionais, como médicos, advogados e contadores. Eles são fiduciários de informação com finalidades específicas, e os tipos de deveres que é razoável impor a eles devem depender da natureza dos serviços que prestam.

A obrigação central dos fiduciários de informação digital é que eles não podem agir como vigaristas – induzindo confiança em seus usuários finais para obter informações pessoais e depois usar essas informações de maneiras que traíam essa confiança e trabalhem contra os interesses de seus usuários finais.<sup>59</sup> Empresas online não devem ser capazes de se apresentar como fornecedoras de segurança digital e respeitar a privacidade digital e depois manipular e discriminar seus usuários finais; nem devem ser capazes de vender ou distribuir dados sobre seus usuários finais para empresas que não respeitem deveres semelhantes de cuidado e boa-fé.<sup>60</sup> Atualmente, a lei não trata essas empresas digitais como fiduciárias. Mas argumentei que deveria. A lei deve estender obrigações fiduciárias a essas empresas e esclarecer os deveres que as empresas online devem aos seus clientes e usuários finais<sup>61</sup>.

Agora, pense em robôs domésticos e casas inteligentes. Robôs domésticos e casas inteligentes coletam uma enorme quantidade de informações sobre nós que, teoricamente, podem ser correlacionadas com informações sobre muitas outras pessoas armazenadas na nuvem. Robôs domésticos e casas inteligentes, em outras palavras, não são simplesmente produtos independentes. Eles são entidades sempre conectadas à nuvem interconectada que dependem e contribuem para enormes bancos de dados. Embora possamos confiar no robô doméstico e na casa inteligente – na verdade, temos que confiar

---

<sup>58</sup> BALKIN, Jack M. Information fiduciaries and the First Amendment. *U.C. Davis Law Review*, v. 49, p. 1183-1234, 2015, p. 1226-1227.

<sup>59</sup> *Ibidem*, p. 1224-1225.

<sup>60</sup> *Ibidem*, p. 1224-1225 e 1227. Argumenta-se que os fiduciários de informações digitais “também podem ter o dever de garantir que, quando vendem ou transmitem essas informações a outros, os deveres de não divulgação e não manipulação acompanhem os dados”.

<sup>61</sup> *Ibidem*, p. 1223-1224, 1226-1229. Veja também: BALKIN, Jack M.; ZITTRAIN, Jonathan. Grand bargain to make tech companies trustworthy, *The Atlantic*, oct. 3, 2016. Disponível em: <https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/>. Defende-se um novo “Digital Millennium Privacy Act”.



– a entidade em que realmente temos que confiar não é o robô ou a casa. É a empresa por trás do robô e da casa que coleta os dados do robô e dos sensores da casa. E essa empresa, argumento, deve ser um fiduciário de informação.

O proprietário do dever fiduciário, em outras palavras, não é o robô. É a empresa que fabrica, instala, vende e opera o robô em nossa casa. É o Rabino, e não o Golem, que nos deve obrigações fiduciárias. A primeira lei da robótica para a era algorítmica, portanto, é que aqueles que usam robôs, sistemas autômatos de IA e algoritmos têm deveres de boa-fé e confiança para com seus usuários finais e clientes. Deveres fiduciários se aplicam se uma empresa ou entidade usar robôs, sistemas autômatos de IA ou algoritmos de aprendizado de máquina na prestação de serviços.

Robôs domésticos e casas inteligentes são exemplos óbvios. Outros exemplos podem ser serviços como Airbnb, Uber, OKCupid, Match.com e 23 and Me. O que importa em cada caso é que as empresas induzam confiança e coletem informações pessoais sobre nós e possam usá-las de maneiras que traiam nossa confiança e/ou criem um conflito de interesses.

Anteriormente, notei que os exemplos clássicos de obrigações fiduciárias surgem nas profissões. Na verdade, robôs, sistemas autômatos de IA e algoritmos provavelmente serão cada vez mais empregados nas operações tradicionais de fiduciários tradicionais – médicos, advogados, contadores e gerentes de dinheiro. O governo federal recentemente emitiu novas regras através do Departamento de Trabalho que tratarão consultores de investimento que lidam com contas de aposentadoria como fiduciários.<sup>62</sup> Esses consultores, por sua vez, estão recorrendo cada vez mais a IA e algoritmos para fazerem seus trabalhos.<sup>63</sup>

A ideia de obrigações fiduciárias também se estende a governos que usam robôs, sistemas autômatos de IA e algoritmos em suas funções cotidianas, incluindo a prestação

---

<sup>62</sup> Definição do Termo "Fiduciário"; Regra de Conflito de Interesse – Aconselhamento de Investimento para Aposentadoria; Isenção de Contrato de Melhor Interesse (Isenção de Transação Proibida 2016-01); Isenção de Classe para Transações Principais em Certos Ativos entre Fiduciários de Aconselhamento de Investimento e Planos de Benefícios para Funcionários e IRAs (Isenção de Transação Proibida 2016-02); Isenções de Transação Proibida 75-1, 77-4, 80-83, 83-1, 84-24 e 86-128, 82 Fed. Reg. 16,902, 16,902 (7 de abril de 2017). Codificado em 29 C.F.R pt. 2510.

<sup>63</sup> Veja O'CONNELL, Brian. Will robo-advisors benefit from the fiduciary rule? **The Street**, 23 fev. 2017. Disponível em: <https://www.thestreet.com/story/14009692/1/will-robo-advisors-benefit-from-the-fiduciary-rule.html>. "Empresas de robôs estão em boa posição para assumir e atrair clientes deixados para trás por empresas maiores, que podem direcionar seu foco de negócios para clientes maiores e mais afluentes à medida que se ajustam à nova regra fiduciária".



de serviços sociais. Governos têm deveres de cuidado e lealdade para com as populações que governam.

## 7.SEGUNDA LEI: OPERADORES ALGORÍTMICOS TÊM DEVERES PARA COM O PÚBLICO GERAL

Como os governos têm obrigações fiduciárias para com as pessoas que governam, as entidades públicas e os governos que utilizam algoritmos são fiduciários da informação para com as populações que governam.

E quanto aos atores privados? Alguns atores, como vimos, são fiduciários da informação relativamente aos seus clientes, pacientes e usuários finais. Mas nem todo negócio online privado que utiliza robôs, sistemas autômatos de IA ou algoritmos é um fiduciário de informações. Talvez igualmente importante, os deveres fiduciários geralmente estendem-se apenas aos clientes e usuários finais de uma empresa, e não ao público em geral como um todo<sup>64</sup>.

Portanto, a ideia de fiduciários da informação não é suficiente para explicar todas as diversas obrigações das empresas privadas que utilizam algoritmos, sistemas autômatos de IA e robôs. As empresas que empregam algoritmos em suas operações ainda podem causar danos a pessoas que não são seus clientes ou clientes, e com as quais não possuem relação contratual. Exemplos são os empregadores que estão a decidir se contratam pessoas ou lhes emprestam dinheiro – isto é, estabelecem relações contratuais com elas – e as empresas de relatórios de crédito, que criam as nossas reputações online que outros irão empregar<sup>65</sup>.

Se excluíssemos simplesmente todas as empresas que afetam as pessoas mas que não têm relações contratuais com elas, replicaríamos um problema que surgiu no início do século XX. Numa economia industrial moderna, as empresas geravam bens produzidos em massa que já não eram vendidos aos consumidores que os contratavam diretamente.<sup>66</sup>

<sup>64</sup> BALKIN, Jack M. Information fiduciaries and the First Amendment. *U.C. Davis Law Review*, v. 49, p. 1183-1234, 2015, p. 1232.

<sup>65</sup> *Ibidem*, p. 1232-1233.

<sup>66</sup> Veja, por exemplo, GRAHAM, Kyle. Strict products liability at 50: four histories. *Marquette Law Review*, v. 98, p. 555-567, 2014. Reconta-se a história padrão.





Em vez disso, uma cadeia de intermediários trouxe estes bens para o mercado<sup>67</sup>. As proteções do consumidor baseadas na privacidade do contrato eram inadequadas às novas realidades econômicas. Como resultado, os tribunais, começando com a famosa decisão de Cardozo em 1916 no caso *MacPherson v. Buick Motor Company*<sup>68</sup>, aboliram a regra da privacidade e consideraram que os fabricantes tinham deveres públicos, não apenas para com os consumidores diretos que compraram os produtos de intermediários, mas também deveres para com suas famílias, membros e para espectadores que acabaram sendo feridos por produtos defeituosos<sup>69</sup>.

Se quisermos articular as regras da Sociedade Algorítmica, precisamos de algo como *MacPherson v. Buick Motor Company* para a era algorítmica. Ou seja, precisamos reconhecer que o uso de algoritmos pode prejudicar não apenas o usuário final de um serviço, mas também muitas outras pessoas na sociedade. Por exemplo, Jonathan Zittrain apontou como o Facebook pode usar os seus dados sobre os usuários finais para os manipular, a fim de influenciar uma eleição nacional.<sup>70</sup> Se isso acontecesse, afetaria não apenas as pessoas com contas no Facebook, mas todas as pessoas no país. Da mesma forma, quando as empresas utilizam algoritmos em negociações de alta velocidade, podem precipitar uma quebra do mercado que afeta não apenas as pessoas com quem negociam, mas todas as pessoas no país e, na verdade, no mundo.

Segue-se então que as empresas têm deveres para com o público quando empregam robôs, sistemas autômatos de IA e algoritmos. Mas não podemos descrever os deveres que devem ao público em termos de quebra de confiança para com clientes, pacientes e usuários finais. Mas se estes deveres não têm como premissa a traição da confiança, em que se baseiam? Isso me leva à terceira lei da Sociedade Algorítmica.

---

<sup>67</sup> GRAHAM, Kyle. Strict products liability at 50: four histories. **Marquette Law Review**, v. 98, p. 555-567, 2014. Veja também *RANDY KNITWEAR, INC. v. AM. CYANAMID CO.*, 181 N.E.2d p. 399 e 402 (N.Y. 1962). “O mundo do comércio já não é mais um mundo de contrato direto”.

<sup>68</sup> 111 N.E. p. 1050 (1916).

<sup>69</sup> 111 N.E. p. 1050 (1916).

<sup>70</sup> ZITTRAIN, Jonathan. Engineering an election: digital gerrymandering poses a threat to democracy, **Harvard Law Review**, v. 127, n. 08, p. 335-341, jun. 2014, p. 335-336. Disponível em: <http://harvardlawreview.org/2014/06/engineering-an-election/>; ZITTRAIN, Jonathan. Facebook could decide an election without anyone ever finding out. **The New Republic**, 1 jun. 2014. Disponível em: [http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-dig ital-gerrymandering](http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering).



## 8. TERCEIRA LEI: OPERADORES ALGORÍTMICOS TÊM O DEVER PÚBLICO DE NÃO SE ENVOLVEREM EM INCÔMODO ALGORÍTMICO

O que quero dizer com incômodo algorítmico? Aqui faço uma analogia com os incômodos públicos e privados – cheiros, fumaça, sons, venenos e especialmente poluição. Tradicionalmente, estes eram danos associados à utilização (e utilização indevida) de bens imóveis, mas a ideia expandiu-se nos últimos tempos para incluir uma vasta gama de danos.<sup>71</sup> Um incômodo privado prejudica os interesses jurídicos reconhecidos de um grupo relativamente pequeno de pessoas,<sup>72</sup> um incômodo público difunde os danos por uma população indefinida, e cabe às autoridades estaduais decidirem se devem iniciar uma ação para diminuir o incômodo.<sup>73</sup> Como alternativa, o governo deve decidir se cria um esquema de regulamentação governamental semelhante à proteção do consumidor ou à proteção ambiental<sup>74</sup>.

Obviamente, não estou afirmando que os danos algorítmicos sejam incômodos no sentido tradicional desse termo pelo direito consuetudinário. Em particular, não estou

<sup>71</sup> Veja RESTATEMENT (SECOND) OF TORTS § 821A cmt. b (AM. LAW INST. 1979). “Atividade humana ou uma condição física que seja prejudicial ou irritante para os outros”.

<sup>72</sup> RESTATEMENT (SECOND) OF TORTS § 821E & cmt. a (AM. LAW INST. 1979). “A responsabilidade por perturbações privadas existe apenas para a proteção de pessoas que tenham ‘direitos e privilégios de propriedade’, isto é, interesses legalmente protegidos, no que diz respeito ao uso ou gozo específico que foi afetado”.

<sup>73</sup> RESTATEMENT (SECOND) OF TORTS § 821B(1). “Interferência não razoável com um direito comum ao público em geral”; RESTATEMENT (SECOND) OF TORTS § 821C(1). Estabeleceu-se que oficiais públicos devem ajuizar ações para eliminar um incômodo público, a menos que um indivíduo privado sofra um dano diferente em espécie daquele sofrido pelo público em geral. Nos últimos vinte anos, Procuradores Gerais Estaduais tentaram expandir o conceito de incômodo público para criar um remédio para danos em massa, problemas de saúde pública e poluição ambiental. Veja, por exemplo, *CONNECTICUT v. Am. Elec. Power Co.*, 582 F.3d 309 (2009), que determinou que estados poderiam processar empresas de energia por emissões excessivas de dióxido de carbono sob a lei comum federal de incômodo público; FAULK, Richard O.; GRAY, John S. *Alchemy in the courtroom? The transmutation of public nuisance litigation.* **Michigan State Law Review**, v. 207, p. 941, 943-944, 2007. “A jurisprudência americana tem experimentado outro ‘assalto à cidadela’ em ações contra fabricantes de amianto, armas e antigas tintas com chumbo... [usando] o menos conhecido delito de ‘incômodo público’”; GIFFORD, Donald G. *Public nuisance as a mass products liability tort.* **University of Cincinnati Law Review**, v. 71, p. 741, 743-744, 2003. Descreveu-se o uso recente de ações de incômodo público tanto por oficiais estaduais quanto por litigantes privados para recuperar danos supostamente decorrentes de doenças relacionadas ao tabaco, violência com armas de fogo e envenenamento infantil por chumbo; veja também SCHWARTZ, Victor E.; GOLDBERG, Phil; SCHAECHER, Corey. *Game over? why recent state Supreme Court decisions should end the attempted expansion of public nuisance law.* **Oklahoma Law Review**, v. 62, p. 629, 629-631, 2010. Descreveu-se e criticou-se a expansão da lei de incômodo público além de suas fronteiras doutrinárias tradicionais.

<sup>74</sup> Veja RESTATEMENT (SECOND) OF TORTS § 821B (2)(b) & cmt. c (1979). Observou-se que os órgãos legislativos e as agências administrativas podem determinar que determinada conduta constitui um incômodo público, evitando assim a necessidade de uma demonstração adicional de interferência irracional.



dizendo que os danos algorítmicos sejam invasões não transgressivas do uso e gozo privado de bens imóveis.<sup>75</sup> Em vez disso, defendo que a melhor maneira de pensar sobre esses danos é por analogia com atos ilícitos como incômodo.

Por que faço uma analogia entre os danos causados pelos algoritmos e o incômodo? Faço isso por três razões. A primeira é a falácia do homúnculo. Não podemos argumentar que o próprio algoritmo tenha más intenções. Em vez disso, o algoritmo é usado por seres humanos que desejam atingir algum conjunto específico de metas gerenciais, mas, no processo, acabam prejudicando vários grupos de pessoas. Algumas destas vítimas são fáceis de identificar, mas os danos causados a outras são mais difusos.

Em essência, estamos falando sobre o uso socialmente injustificado das capacidades computacionais que externaliza custos sobre pessoas não envolvidas. No direito civil, poderíamos denominar essa externalização de incômodo, sendo ela pública ou privada<sup>76</sup>. E na verdade, um artigo recente sobre como regular o policiamento algorítmico, Andrew Selbst argumenta que o remédio apropriado é requerer aos departamentos policiais a criação de declarações de impacto sobre discriminação semelhante às discriminações de impacto ambiental.<sup>77</sup> Segundo Selbst, o que é característica da discriminação algorítmica é que não pode ser facilmente identificada com malícia ou más intenções, tanto por parte das autoridades oficiais que usam os programas quanto pelos próprios programas.<sup>78</sup>

O algoritmo não possui intenções, vontades ou desejos. Esta é a falácia do homúnculo. Não há nenhuma pessoa dentro do algoritmo que o direciona. Portanto, é inútil modelar o dever ou a responsabilidade dos operadores de algoritmo com base em uma

---

<sup>75</sup> RESTATEMENT (SECOND) OF TORTS § 821D & cmt. a (1979). Observou-se que o incômodo privado tradicionalmente se preocupa com invasões não invasivas de interesses no uso e gozo da terra. O incômodo público, por outro lado, pode estar preocupado com questões mais amplas, como saúde pública, segurança ou moral.

<sup>76</sup> Fazendo uma análise crítica das novas ações de aplicação baseadas em incômodo público, Keith Hylton argumenta que há uma racionalidade coerente para a expansão do incômodo público, embora nem sempre refletida na jurisprudência: “A lei de incômodo induz os atores a escolherem níveis de atividade socialmente ótimos, impondo responsabilidade quando os custos externalizados estão muito acima dos benefícios externalizados ou muito acima dos custos externos de fundo” (HYLTON, Keith N. the economics of public nuisance law and the new enforcement actions. **Supreme Court Economic Review**, v. 18, p. 43-44, 2010).

<sup>77</sup> SELBST, Andrew D. Disparate impact in big data policing. **Georgia Law Review**, v. 49, 2017, p. 44. Disponível em: <https://ssrn.com/abstract=2819182>.

<sup>78</sup> *Ibidem*, p. 32. “Os problemas de discriminação na mineração de dados, no entanto, não são os de motivo, consciente ou inconsciente”. Muitas vezes, os efeitos discriminatórios surgem da forma como um problema específico é formulado para o algoritmo resolver, em vez de motivações inconscientes por parte da polícia ou programadores.



teoria de resposta superior – você não pode imputar intenções, negligência, ou malícia do algoritmo ao operador, mesmo – e especialmente – um algoritmo de autoaprendizagem.

Pelo contrário, temos que focar nos efeitos sociais do uso de um algoritmo específico, e se os efeitos são razoáveis e justificáveis do ponto de vista da sociedade como um todo. Ao invés de fazer analogias com o direito penal ou com a lei de tratamento díspar na lei de antidiscriminação, as melhores analogias são as do incômodo e da lei ambiental.<sup>79</sup>

A segunda razão para comparar o problema com o incômodo é que os danos dos algoritmos são uma questão de grau. Além disso, os danos do incômodo algorítmico resultam dos efeitos cumulativos da coleta, análise e tomada de decisões sobre as identidades digitais das pessoas.

Selbst pontua que os danos causados por discriminação algorítmica não se encaixam perfeitamente em uma categorização binária de sim ou não – ou seja, ou você discriminou ou não. Em vez disso, existem compensações inevitáveis no design e na forma na qual os programadores formulam o problema que um algoritmo foi solicitado a resolver.<sup>80</sup> Pode ser difícil determinar uma base de ação não discriminatória contra a qual medir a operação do algoritmo, e pode ser difícil, se não impossível, isolar os efeitos das operações algorítmicas em uma única causa.<sup>81</sup> Em última análise, a pergunta relevante é se você impôs muitos custos injustificáveis a terceiros. A discriminação algorítmica, tal como a poluição, é uma questão de grau.

A terceira razão para a analogia com o incômodo é que ela nos ajuda a compreender como os danos da Sociedade Algorítmica surgem da tomada de decisões e julgamentos cumulativos por parte de uma ampla gama de atores públicos e privados. As

---

<sup>79</sup> Veja FROOMKIN, A. Michael. Regulating mass surveillance as privacy pollution: learning from environmental impact statements. **University of Illinois Law Review**, v. 2015, n. 04, p. 1713-1715, 2015. “Falhas de mercado, problemas de ação coletiva e especialmente assimetrias de informação – incluindo, como recentemente aprendemos, uma surpreendente falta de transparência do governo sobre vigilância doméstica – caracterizam a crise atual de privacidade, assim como caracterizaram o problema ambiental na década de 1960”; HIRSCH, Dennis D. Protecting the inner environment: what privacy regulation can learn from environmental law. **Georgia Law Review**, v. 41, n. 01, p. 23, 2006. Argumentou-se que “os danos à privacidade da Era da Informação são estruturalmente semelhantes aos danos ambientais da era das chaminés” devido às externalidades negativas e aos problemas de ação coletiva. Compare com HIRSCH, Dennis D. The law and policy of online privacy: regulation, self-regulation, or co-regulation? **Seattle University Law Review**, v. 34, n. 03, p. 465-466, 2011. Observou-se como os modelos de correção no direito ambiental podem ser relevantes para a proteção da privacidade.

<sup>80</sup> SELBST, Andrew D. Disparate impact in big data policing. **Georgia Law Review**, v. 49, 2017, p. 46-47. Disponível em: <https://ssrn.com/abstract=2819182>.

<sup>81</sup> *Ibidem*, p. 47-48; BAROCAS, Solon; SELBST, Andrew D. Big data’s disparate impact. **California Law Review**, v. 104, n. 03, p. 671-692, 718-719, 2016.



empresas e os governos utilizam *Big Data* e algoritmos para fazer julgamentos que constroem as identidades, características e associações das pessoas. Estas construções digitais de identidade e características afetam as oportunidades das pessoas – em termos de emprego, crédito, ofertas e posições financeiras. Também moldam as vulnerabilidades delas – ao aumento da vigilância, discriminação, manipulação e exclusão. Empresas e governos coletam dados sobre pessoas de diversas fontes e processam os dados para produzir novos dados. Ao processar dados e tomar decisões, as empresas e os governos contribuem para a construção cumulativa das identidades, características e associações digitais das pessoas, o que, por sua vez, constrói as oportunidades futuras das pessoas e molda as suas vulnerabilidades.

Outras empresas baseiam-se nestas coleções de dados, pontuações e avaliações de risco e nas construções digitais resultantes de características, associações e identidade. As empresas e os governos empregam toda esta informação de forma criativa em contextos de julgamento sempre novos, gerando novas percepções, decisões e previsões. Desta forma, a vida das pessoas está sujeita a uma torrente de julgamentos algorítmicos que moldam identidades, oportunidades e vulnerabilidades ao longo do tempo. Imagine, se puder, sua identidade digital sendo usada como um fluxo de informações no qual uma coleção de novas decisões, pontuações e avaliações de risco está constantemente sendo lançadas.

À medida que mais e mais empresas participam no processo coletivo de formação da identidade digital, esta torrente de julgamentos molda cada vez mais a vida das pessoas. Pode transferir uma vasta gama de custos socialmente injustificados para as pessoas, sob a forma de oportunidades limitadas e vulnerabilidades crescentes. O conceito de incômodo algorítmico tenta capturar esses efeitos sobre os indivíduos, à medida que os atores públicos e privados lançam cada vez mais decisões no fluxo de informações que representa os indivíduos e é usado para julgá-los, classificá-los e controlá-los.

O problema central que enfrentamos hoje, portanto, não é a discriminação intencional, mas sim o dano cumulativo à identidade e às oportunidades. A utilização repetida e generalizada de algoritmos em áreas como o policiamento, o emprego, a habitação e o acesso ao crédito terão efeitos cumulativos nas populações, à medida que os decisores recorrem a múltiplas fontes de dados para construir as identidades e reputações digitais das pessoas.



Em alguns casos, os danos podem ser atribuídos a uma programação e operação descuidadas – erros de código, suposições irracionais ou dados tendenciosos. Ou pode resultar da utilização irracional de algoritmos, fontes de dados, classificações anteriores e categorizações para novos fins para os quais não foram concebidos. Mas, em muitos casos, o programador e o utilizador podem ser capazes de fazer uma afirmação plausível de que o seu modelo inicial é razoável, dada a tarefa em questão, os dados analisados e os pressupostos de base do modelo. Mesmo assim, transferir a tomada de decisões para algoritmos ao longo do tempo irá, previsivelmente, causar uma ampla gama de danos a indivíduos e membros de grupos específicos.

Uma preocupação central é como a identidade – a associação de pessoas com associações e características positivas e negativas – é construída e distribuída na Sociedade Algorítmica. Os decisores economizam na tomada de decisões não só fazendo os seus próprios julgamentos algorítmicos, mas também importando julgamentos algorítmicos que outras partes fizeram sobre os atributos, a fiabilidade e a reputação das pessoas<sup>82</sup> (as pontuações de crédito são um exemplo simples, mas são apenas um exemplo primitivo do que uma Sociedade Algorítmica pode realizar ao longo do tempo).

Em vez de começar do zero, desenvolvendo os seus próprios algoritmos de pontuação, os decisores podem economizar utilizando pontuações e julgamentos já criados por outros algoritmos utilizados em diferentes contextos e para diferentes fins, e modificando-os e atualizando-os para atender às suas necessidades.<sup>83</sup> Alguns dos *insights* mais importantes da Sociedade Algorítmica provêm da reinterpretação de como os dados coletados para um propósito poderiam ser usados para lançar luz sobre o que inicialmente parecia ser um fenômeno ou problema não relacionado.

As empresas especializam-se na coleta, comparação e distribuição das identidades das pessoas a outros decisores, que acrescentam as suas decisões a um crescente fluxo ou dossiê digital.<sup>84</sup> Isto significa que as identidades das pessoas – incluindo as

---

<sup>82</sup> Veja ROBINSON, Yu. **Knowing the score**: new data, underwriting, and marketing in the consumer credit marketplace. 2014. Disponível em: [https://www.teamupturn.com/static/files/Knowing\\_the\\_Score\\_Oct\\_2014\\_v1\\_1.pdf](https://www.teamupturn.com/static/files/Knowing_the_Score_Oct_2014_v1_1.pdf). Descreveu-se a coleta de informações sobre e avaliações de indivíduos a partir de múltiplas fontes de relevância e importância amplamente divergentes.

<sup>83</sup> *Idem*; BECKETT, Lois. Everything We know about what data brokers know about you. **ProPublica**, 13 jun. 2014. Disponível em: <https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you>. Explicou-se como os corretores de dados coletam e vendem informações obtidas de muitas fontes diferentes para muitos propósitos diferentes.

<sup>84</sup> *Idem*.





características positivas e negativas que lhes são atribuídas – são construídas e distribuídas através da interação de muitas bases de dados, programas e algoritmos de tomada de decisão diferentes. E, desta forma, as identidades e reputações construídas por algoritmos das pessoas podem espalhar-se ampla e generalizadamente pela sociedade, aumentando o poder da tomada de decisões algorítmicas sobre as suas vidas. À medida que os dados se tornam um recurso comum para a tomada de decisões, constroem reputação digital, oportunidades práticas e vulnerabilidade digital.

Neste mundo, focar em atos ilícitos intencionais ou mesmo na construção e supervisão negligentes de algoritmos pode ser inadequado. Em vez disso, a melhor analogia na teoria da responsabilidade civil pode ser com os custos sociais que surgem de níveis de atividade socialmente injustificados. O aumento dos níveis de atividade produz custos sociais crescentes, mesmo quando uma atividade é conduzida com o devido cuidado. Mesmo assumindo que a empresa exerce o devido cuidado – o que, claro, pode não acontecer – os efeitos cumulativos do aumento da atividade podem, no entanto, causar demasiados danos ao resto da sociedade.<sup>85</sup> São situações características do incômodo algorítmico.

O aumento dos níveis de atividade e o aumento dos custos sociais podem surgir quando as empresas adotam novas tecnologias que lhes permitam aumentar os seus níveis de atividade.<sup>86</sup> Neste caso, a mudança para uma nova tecnologia – a tomada de decisões algorítmica – permite que os governos e as empresas tomem mais decisões que afetam mais vidas, de forma mais generalizada e mais barata. A Sociedade Algorítmica aumenta a rapidez, o escopo e a difusão da categorização, classificação e decisão; ao fazê-lo, também aumenta os efeitos secundários da categorização, classificação e decisão nas vidas humanas. Esses efeitos colaterais são análogos ao aumento dos níveis de poluição causados pelo aumento da atividade fabril.

Com certeza, é preciso duas pessoas para criar um conflito. Os custos sociais da tomada de decisões algorítmicas também decorrem das ações das partes lesadas. Talvez, então, devêssemos também dar incentivos aos cidadãos para se exporem menos aos efeitos secundários do julgamento algorítmico. Mas na Sociedade Algorítmica, as partes lesadas não podem facilmente ausentar-se da procura de emprego, habitação, cuidados

<sup>85</sup> HYLTON, Keith N. the economics of public nuisance law and the new enforcement actions. **Supreme Court Economic Review**, v. 18, p. 48, 2010.

<sup>86</sup> *Idem*.



médicos e da participação nas características cotidianas da vida diária. Na Sociedade Algorítmica, as pessoas descartam os dados que mais tarde serão utilizados para julgá-las simplesmente por viverem num mundo digital. Nem as pessoas podem contratar facilmente para evitar os danos do julgamento algorítmico. Os problemas de ação coletiva são enormes, para não falar dos custos de obtenção de informação sobre a sua situação. Na Sociedade Algorítmica, as identidades digitais das pessoas são produzidas por muitos atores diferentes, as suas identidades digitais fluem para uma vasta gama de decisores e as decisões são tomadas por entidades sobre as quais as pessoas sabem pouco.

Se seguirmos a analogia com o incômodo, então a Terceira Lei da Robótica estabelece que os operadores de algoritmos têm o dever de não “poluir” o público, ou seja, de não externalizar injustificadamente os custos da tomada de decisão algorítmica para outras pessoas. Assim como a transformação para uma sociedade industrial aumentou previsivelmente a quantidade de poluição social, a mudança para uma Sociedade Algorítmica aumentará previsivelmente os efeitos colaterais da coleta de dados, computação e julgamento algorítmico.

Quais são esses custos ou danos? Considere alguns dos danos mais comuns criados pela Sociedade Algorítmica. Devo sublinhar que estes danos se somam aos danos físicos tradicionais, como os causados por carros autônomos ou robôs industriais, e aos danos a dignitários causados pela vigilância e exposição:

**Danos à reputação** – existem duas maneiras principais pelas quais os algoritmos afetam a reputação: a primeira é a *classificação*; a segunda é a *avaliação de riscos*. Os algoritmos afetam a reputação ao rotular você e outras pessoas como você como arriscados. Ou seja, o que significa para você ser você é um certo tipo de risco ou propensão. A forma como o risco se manifesta será diferente em diferentes contextos. Pode incluir a ideia de que você (ou as pessoas que vivem numa determinada área) cria um risco financeiro, um risco de emprego, um risco de cometer um crime futuro, um risco de gastar muitos serviços sociais, um risco de devolver itens ou ser um cliente caro, um risco de desperdiçar dinheiro em publicidade porque você não comprará nada e assim por diante. Nesse caso, o dano algorítmico é a imputação de que você é uma pessoa arriscada, o que é uma espécie de estigma.

A avaliação de risco geralmente acompanha a classificação; o algoritmo afeta sua reputação ao colocá-lo em uma categoria ou classe, o que não é necessariamente uma



avaliação de risco. O algoritmo constrói grupos nos quais você é colocado e através dos quais você é conhecido e, portanto, potencialmente estigmatizado. A classificação pode afetar a sua reputação sem uma avaliação de risco porque diz que tipo de pessoa você é e a quem você é tratado como equivalente (e, implicitamente, melhor ou pior do que de acordo com alguma métrica).

**Discriminação** – devido à avaliação do risco e/ou devido ao trabalho de classificação, a empresa que emprega o algoritmo nega-lhe oportunidades que oferece a outros (um cartão de crédito, um empréstimo, uma oportunidade de emprego, uma promoção); ou impõe custos especiais (susceptibilidade para parar e revistar dados, vigilância, preços mais elevados, exclusão da posse de armas ou do acesso a viagens aéreas, etc.) que não impõe a outras pessoas.

**Normalização ou Conformação** – o algoritmo faz com que você internalize suas classificações e avaliações de risco, fazendo com que você altere seu comportamento para evitar vigilância ou evitar ser categorizado como de risco. Isso faz com que você altere sua identidade, comportamento ou outros aspectos de autoapresentação pessoal para parecer menos arriscado para o algoritmo que não presta atenção<sup>87</sup>.

**Manipulação** – os seres humanos e as organizações podem usar algoritmos para levar você e outras pessoas como você a fazer escolhas (mais ou menos) previsíveis que beneficiam o operador do algoritmo, mas não melhoram o seu bem-estar e podem, na verdade, reduzi-lo. Além disso, a análise algorítmica torna mais fácil para as empresas descobrirem quais pessoas são mais suscetíveis à manipulação e como podem ser manipuladas de maneira mais fácil e eficaz.

**Falta do devido processo/transparência/interpretabilidade** – o algoritmo toma decisões que afetam o seu bem-estar de uma das maneiras mencionadas acima: sem transparência e compreensibilidade, sem explicação clara das entradas e saídas em termos leigos, sem capacidade de monitorar suas operações, sem fornecer meios de refutação ou sem um método para responsabilizar o algoritmo.<sup>88</sup>

---

<sup>87</sup> Note que ao conformar seu comportamento ao julgamento algorítmico ou se ocultar da coleta de dados e da análise algorítmica, partes potencialmente prejudicadas podem alterar seus próprios níveis de atividade e, assim, reduzir os custos sociais totais do julgamento algorítmico. Como observado anteriormente, são necessárias duas partes para criar um dano. Mas essa forma de redução de custos levanta uma questão importante. Primeiro, deve-se demonstrar que a sociedade pode razoavelmente exigir uma determinada forma de conformação social ou isolamento social de seus cidadãos.

<sup>88</sup> Há agora uma importante literatura lidando com os problemas do devido processo na tomada de decisões algorítmicas e como melhor abordá-los. Veja BAROCAS, Solon *et al.* *Accountable algorithms*. **University of**



Poderíamos resumir esta discussão dizendo que os algoritmos (a) constroem identidade e reputação através de (b) classificação e avaliação de risco, criando a oportunidade para (c) discriminação, normalização e manipulação, sem (d) transparência, responsabilização e monitoramento adequados ou devido processo.

Como esses danos estão relacionados à ideia de incômodo algorítmico? Esses danos são efeitos colaterais da tomada de decisões informatizada. São os custos sociais da atividade algorítmica.

A adoção generalizada de algoritmos aumenta muito o nível e a difusão da tomada de decisões computacionais em nossas vidas. A utilização de algoritmos poupa dinheiro aos decisores e, portanto, pode ser razoável do ponto de vista de uma empresa individual ou de um decisor, mas no processo pode impor danos cumulativos a indivíduos e grupos<sup>89</sup>.

Imagine, por exemplo, um conjunto de algoritmos usado para identificar potenciais funcionários. O algoritmo pode ser bom o suficiente para preencher o pequeno número de vagas disponíveis com pessoas qualificadas, mas exclui muitas pessoas que também seriam qualificadas (neste caso, diríamos que cria muito poucos falsos negativos, mas muitos falsos positivos). Mesmo assim, os dados e pontuações reputacionais usados e produzidos pelo algoritmo podem alimentar bancos de dados usados por outros, incluindo não apenas futuros empregadores, mas muitos outros tomadores de decisão operando em muitos outros contextos. Ou imagine um algoritmo policial que envia policiais para bairros onde a polícia já vem prendendo pessoas, reforçando assim a noção de que a área é especialmente alta em crimes e precisa de vigilância policial adicional.

O ponto da Sociedade Algorítmica é aumentar a oportunidade, velocidade e eficácia na tomada de decisões. As empresas empregam algoritmos para economizar dinheiro e realizar tarefas e cálculos repetitivos em uma escala vasta que seria proibitivamente cara, ou até mesmo impossível, para os humanos realizarem. Isso permite às empresas fazer

---

**Pennsylvania Law Review**, v. 165, p. 633, 2017; BAROCAS, Solon; SELBST, Andrew D. Big data's disparate impact. **California Law Review**, v. 104, n. 03, p. 671-692, 718-719, 2016; CITRON, Danielle Keats. Technological due process. **Washington University Law Review**, v. 85, p. 1249, 2008; CITRON, Danielle Keats; PASQUALE, Frank. The scored society: due process for automated predictions. **Washington Law Review**, v. 89, p. 01, 2014; CRAWFORD, Kate; SCHULTZ, Jason. Big data and due process: toward a framework to redress predictive privacy harms. **Boston College Law Review**, v. 55, p. 93, 2014; KIM, Pauline T. Data-driven discrimination at work. **William & Mary Law Review**, v. 58, p. 857, 2017; SELBST, Andrew D. Disparate impact in big data policing. **Georgia Law Review**, v. 49, 2017, p. 44. Disponível em: <https://ssrn.com/abstract=2819182>.

<sup>89</sup> Veja HYLTON, Keith N. the economics of public nuisance law and the new enforcement actions. **Supreme Court Economic Review**, v. 18, p. 48, 2010. Note-se como a mudança tecnológica pode aumentar os níveis de atividade e custo social.



perguntas que anteriormente teriam sido impossíveis de responder e tomar decisões que anteriormente teriam sido financeiramente caras de formular e adotar.

Esse fenômeno – mais tipos de decisões feitas de forma mais barata – é apenas mais um exemplo do efeito de substituição que é característico da robótica em geral. Substituímos juízes e tomadores de decisão humanos por algoritmos. No entanto, a escolha dos algoritmos, a escolha das categorias, o tipo de dados coletados e a criação e manutenção distribuída de identidades digitais têm custos sociais, cujo peso é transferido para outros — para a população em geral, ou para segmentos específicos da população, como os pobres ou as comunidades minoritárias.

Ao abordar os danos algorítmicos e a discriminação algorítmica, nosso objetivo não é descobrir más intenções. Colocar a questão dessa forma é apenas mais um exemplo da falácia do homúnculo. Em vez disso, o objetivo, à medida que mais e mais empresas migram para a tomada de decisões algorítmicas e aumentam seus níveis de atividade de tomada de decisões, é exigir que as empresas adotem métodos que sejam justificados do ponto de vista da sociedade como um todo. Assim como no caso de perturbação pública, o estado deve decidir como fazer com que as empresas internalizem seus custos.

Frank Pasquale também apontou que, na medida em que usamos essa abordagem de perturbação algorítmica, devemos ser capazes de identificar as pessoas ou organizações que estão usando o algoritmo que está impondo custos ao resto da sociedade.<sup>90</sup> Ou seja, os algoritmos devem ser projetados de forma que possamos dizer quais pessoas ou organizações os estão empregando. O Golem deve ser rastreável até um Rabino ou grupo de Rabinos. Em muitos casos – finanças, emprego, policiamento – a identificação do usuário não será difícil, porque a organização que está usando o algoritmo se identifica. Mas em muitos casos, o algoritmo e os dados que ele usa terão sido construídos por muitas organizações trabalhando juntas. Também pode haver casos em que a tomada de decisões algorítmicas é feita por pessoas ou organizações anônimas ou pseudônimas. Então, a lei terá que exigir a divulgação de quem está por trás do algoritmo para cumprir um dever público.

---

<sup>90</sup> PASQUALE, Frank. **Toward a fourth law of robotics: preserving attribution, responsibility, and explainability in an algorithmic society.** 2017, p. 10-12. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3002546](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3002546)



## 9. CONSIDERAÇÕES FINAIS

A esperança e o medo da robótica e da inteligência artificial estão conosco desde os primeiros dias da literatura. Mesmo hoje, os jornalistas escrevem histórias levantando o espectro de robôs, sistemas autômatos de IA e algoritmos fora de controle que em breve dominarão nosso mundo. Meu objetivo neste trabalho foi oferecer uma correção. Falar assim localiza o perigo da Sociedade Algorítmica nos próprios robôs, sistemas autômatos de IA e algoritmos. Mas o verdadeiro perigo está, e sempre esteve, nas pessoas – nas organizações e empresas que adotam e empregam esses dispositivos e os usam para afetar, controlar e manipular outros seres humanos. Se fôssemos todos tão piedosos quanto o Maharal, não precisaríamos temer o Golem. Como não somos, precisamos aprender a nos conter.

## REFERÊNCIAS

- ANGELO, Joseph A. **Robotics**: a reference guide to the new technology. 2006.
- ASIMOV, Isaac. Mirror image. *In: Robot Visions*. 1990.
- ASIMOV, Isaac. **Robots and empire**. 1985.
- ASIMOV, Isaac. Runaround. *In: I Robot*. 1950.
- ASIMOV, Isaac. **The caves of steel**. 195.
- ASIMOV, Isaac. The last question. *In: Robot dreams*. 1995.
- ASIMOV, Isaac. The machine and the robot. *In: WARRICK, P. S.; GREENBERG, M. H.; OLANDER, J. D. (Eds.). Science Fiction: contemporary mythology*. 1978.
- ASIMOV, Isaac. **The naked sun**. 1957.
- ASIMOV, Isaac. **The robots of dawn**. 1983.
- BALKIN, Jack M. Information fiduciaries and the First Amendment. **U.C. Davis Law Review**, v. 49, p. 1183-1234, 2015.
- BALKIN, Jack M. The path of robotics law. **California Law Review Circuit**, v. 05, p. 45-60, 2015.





BALKIN, Jack M.; ZITTRAIN, Jonathan. Grand bargain to make tech companies trustworthy, *The Atlantic*, oct. 3, 2016. Disponível em: <https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/>.

BAROCAS, Solon *et al.* Accountable algorithms. **University of Pennsylvania Law Review**, v. 165, p. 633, 2017.

BAROCAS, Solon; SELBST, Andrew D. Big data's disparate impact. **California Law Review**, v. 104, n. 03, p. 671-692, 718-719, 2016.

BAROCAS, Solon; SELBST, Andrew D. Big data's disparate impact. **California Law Review**, v. 104, n. 03, p. 671-692, 718-719, 2016.

BARTHELMESS, Ulrike; FURBACH, Ulrich. Do we need Asimov's Laws? Cornell University Library, 2014, p. 11. Disponível em: <https://arxiv.org/ftp/arxiv/papers/1405/1405.0961.pdf>.

**BEAUTY.AI**. Welcome to the first international beauty contest judged by artificial intelligence. Disponível em: <http://beauty.ai/>.

BECKETT, Lois. Everything We know about what data brokers know about you. **ProPublica**, 13 jun. 2014. Disponível em: <https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you>.

CELLAN-JONES, Rory. Stephen Hawking warns artificial intelligence could end mankind. **BBC**, 2 dez. 2014. Disponível em: <http://www.bbc.com/news/technology-30290540>.

CITRON, Danielle Keats. Technological due process. **Washington University Law Review**, v. 85, p. 1249, 2008.

CITRON, Danielle Keats; PASQUALE, Frank. The scored society: due process for automated predictions. **Washington Law Review**, v. 89, p. 01, 2014.

COMAY, Joan; COHN-SHERBOK, Lavinia. **Who's who in Jewish history**: after the period of the Old Testament. 2. ed. Londres: Routledge, 2001.

CRAWFORD, Kate; SCHULTZ, Jason. Big data and due process: toward a framework to redress predictive privacy harms. **Boston College Law Review**, v. 55, p. 93, 2014.

DENG, Boer. Machine ethics: the robot's dilemma. *Revista Nature*, v. 523, p. 24-26, jul. 2015. Disponível em: <http://www.nature.com/news/machine-ethics-the-robot-s-dilemma-1.17881>.

ELSWIT, Sharon Barcan. **The Jewish story finder**: a guide to 668 tales listing subjects and sources. 2012.

FAULK, Richard O.; GRAY, John S. Alchemy in the courtroom? The transmutation of public nuisance litigation. **Michigan State Law Review**, v. 207, p. 941, 943-944, 2007.



FROOMKIN, A. Michael. Regulating mass surveillance as privacy pollution: learning from environmental impact statements. **University of Illinois Law Review**, v. 2015, n. 04, p. 1713-1715, 2015.

GANDOMI, Amir; HAIDER, Murtaza. Beyond the hype: Big data concepts, methods, and analytics. **International Journal of Information Management**, v. 35, n. 02, p. 137-144, 2015. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0268401214001066>.

GIBBS, Samuel. Elon Musk: artificial intelligence is our biggest existential threat. **The Guardian**, 27 out. 2014. Disponível em: <https://www.theguardian.com/technology/2014/oct/27/elon-musk-artificial-intelligence-ai-biggest-existential-threat>.

GIFFORD, Donald G. Public nuisance as a mass products liability tort. **University of Cincinnati Law Review**, v. 71, p. 741, 743-744, 2003.

GRAHAM, Kyle. Strict products liability at 50: four histories. **Marquette Law Review**, v. 98, p. 555-567, 2014.

HAVASI, Catherine. Who's common-sense reasoning and why it matters. **Techcrunch**, 9 ago. 2014. Disponível em: <https://techcrunch.com/2014/08/09/guide-to-common-sense-reasoning-whos-doing-it-and-why-it-matters/>.

HIRSCH, Dennis D. Protecting the inner environment: what privacy regulation can learn from environmental law. **Georgia Law Review**, v. 41, n. 01, p. 23, 2006.

HIRSCH, Dennis D. The law and policy of online privacy: regulation, self-regulation, or co-regulation? **Seattle University Law Review**, v. 34, n. 03, p. 465-466, 2011.

HYLTON, Keith N. the economics of public nuisance law and the new enforcement actions. **Supreme Court Economic Review**, v. 18, p. 43-44, 2010.

JESTICE, Phyllis G. **Holy people of the world: a cross-cultural encyclopedia**. Santa Barbara: ABC-CLIO, 2004.

KANT, Immanuel. **Critique of pure reason**. Editores e tradutores: Paul Guyer e Allen W. Wood. Cambridge: Cambridge University Press, 1998.

KAREL, Capek. **RUR**. 1921.

KEHOE, Ben *et al.* A survey of research on cloud robotics and automation. **Institute of Electrical and Electronics Engineers**, 2015. Disponível em: <http://goldberg.berkeley.edu/pubs/T-ASE-Cloud-RA-Survey-Paper-Final-2015.pdf>.

KEHOE, Ben; PATIL, Sachin; ABBEEL, Pieter; GOLDBERG, Ken. A survey of research on cloud robotics and automation. **IEEE Transactions on Automation Science and Engineering (T-ASE): Special Issue on Cloud Robotics and Automation**, v. 12, n. 02,



abr. 2015. Disponível em: <http://goldberg.berkeley.edu/pubs/T-ASE-Cloud-RA-Survey-Paper-Final-2015.pdf>.

KIM, Pauline T. Data-driven discrimination at work. **William & Mary Law Review**, v. 58, p. 857, 2017.

LEIVICK, H. O Golem. *In: Golem: a new translation of the classic play and selected short stories*. Tradução de Joachim Neugroschel. 2006.

LEVIN, Sam. A beauty contest was judged by AI and the robots didn't like dark skin. **The Guardian**, 8 set. 2016. Disponível em: <https://www.theguardian.com/technology/2016/sep/08/artificial-intelligence-beauty-contest-doesnt-like-black-people>.

LOIZOS, Connie. This famous roboticist doesn't think Elon Musk understands AI. Tech Crunch, 19 jul. 2017. Disponível em: <https://techcrunch.com/2017/07/19/this-famous-roboticist-doesnt-think-elon-musk-understands-ai/>.

MARX, Karl. Capital: A critique of political economy. *In: The fetishism of commodities and the secret thereof*. ENGELS, Friedrich (Ed.). Tradução de Samuel Moore e Edward Aveling. Mineola: Dover Publications, Inc., 2011.

MCCAULEY, Lee. The Frankenstein Complex and Asimov's Three Laws. *In: Association for the Advancement of Artificial Intelligence*. 2007, p. 09-14. Disponível em: <https://perma.cc/AJ9F-FHTJ>.

**O exterminador do futuro**. Direção de James Cameron. Hermdale Film Corporation, Pacific Western Productions Cinema, 1984.

O GOLEM DE PRAGA. *In: AUSUBEL, Nathan (Ed.). A treasury of Jewish folklore*. 1948.  
O'CONNELL, Brian. Will robo-advisors benefit from the fiduciary rule? **The Street**, 23 fev. 2017. Disponível em: <https://www.thestreet.com/story/14009692/1/will-robo-advisors-benefit-from-the-fiduciary-rule.html>.

PASQUALE, Frank. **The Black Box Society: the secret algorithms that control money and information**. 2015.

PASQUALE, Frank. **Toward a fourth law of robotics: preserving attribution, responsibility, and explainability in an algorithmic society**. 2017. Disponível em: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=3002546](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3002546).

RASTOGI, Anupam. Artificial intelligence: human augmentation is what's here and now. **Medium**, 12 jan. 2017. Disponível em: <https://medium.com/reflections-by-ngp/artificial-intelligence-human-augmentation-is-whats-here-and-now-c5286978ace0>.

ROBINSON, Yu. **Knowing the score: new data, underwriting, and marketing in the consumer credit marketplace**. 2014. Disponível em: [https://www.teamupturn.com/static/files/Knowing\\_the\\_Score\\_Oct\\_2014\\_v1\\_1.pdf](https://www.teamupturn.com/static/files/Knowing_the_Score_Oct_2014_v1_1.pdf).



SCHWARTZ, Victor E.; GOLDBERG, Phil; SCHAECHER, Corey. Game over? why recent state Supreme Court decisions should end the attempted expansion of public nuisance law. **Oklahoma Law Review**, v. 62, p. 629, 629-631, 2010.

SELBST, Andrew D. Disparate impact in big data policing. **Georgia Law Review**, v. 49, 2017. Disponível em: <https://ssrn.com/abstract=2819182>.

SINTEF. Big Data, for better or worse: 90% of world's data generated over last two years. **Science Daily**, 22 maio 2013. Disponível em: <https://www.sciencedaily.com/releases/2013/05/130522085217.htm>.

**THE ECONOMIST**. Combustível do futuro: dados estão dando origem a uma nova economia. 6 maio 2017. Disponível em: <https://www.economist.com/news/briefing/21721634-how-it-shaping-up-data-giving-rise-new-economy>.

VIOLINO, Bob. Big data and robotics: a long history together. **ZDNet**, 12 ago. 2016. Disponível em: <http://www.zdnet.com/article/big-data-and-robotics-a-long-history-together/>.

ZITTRAIN, Jonathan. Engineering an election: digital gerrymandering poses a threat to democracy, **Harvard Law Review**, v. 127, n. 08, p. 335-341, jun. 2014. Disponível em: <http://harvardlawreview.org/2014/06/engineering-an-election/>.

ZITTRAIN, Jonathan. Facebook could decide an election without anyone ever finding out. **The New Republic**, 1 jun. 2014. Disponível em: <http://www.newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering>.

RECEBIDO EM 04/06/2024  
APROVADO EM 23/08/2024  
RECEIVED IN 04/06/2024  
APPROVED IN 23/08/2024