Paulo Sá Elias: Inteligência artificial requer atenção do Direito

O comitê de Ciência e Tecnologia do Parlamento da Inglaterra abriu inquérito[1] para examinar o uso crescente de algoritmos (e inteligência artificial) na tomada de decisões públicas e privadas, com o objetivo de avaliar como os algoritmos são formulados, os erros e possíveis correções — bem como o impacto que eles podem ter nos indivíduos e sua capacidade de entender ou desafiar decisões tomadas com base no uso da inteligência artificial.

Em primeiro lugar, é importante entendermos o que são os algoritmos (*Algorithms*) aplicados na informática e telemática, inteligência artificial (*Artificial Intelligence*), aprendizado de máquina (*Machine Learning*), aprendizado profundo (*Deep Learning*), redes neurais (*Neural Networks*), Internet das coisas (*Internet of Things*) e outros — que impressionam em razão dos recentes e incríveis avanços e da importância cada vez maior que passaram (e passarão) a ter em nossas vidas.

Algoritmo (*algorithm*), em sentido amplo, é um conjunto de instruções, como uma receita de bolo, instruções para se jogar um jogo, etc. É uma sequência de regras ou operações que, aplicada a um número de dados, permite solucionar classes semelhantes de problemas. Na informática e telemática, o conjunto de regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número de etapas. Em outras palavras mais claras: são as diretrizes seguidas por uma máquina. Na essência, os algoritmos são apenas uma forma de representar matematicamente um processo estruturado para a realização de uma tarefa. Mais ou menos como as regras e fluxos de trabalho, aquele passo-a-passo que encontramos nos processos de tomada de decisão em uma empresa, por exemplo.

A inteligência artificial (*Artificial Intelligence* – ou simplesmente AI), em definição bem resumida e simples, é a possibilidade das máquinas (computadores, robôs e demais dispositivos e sistemas com a utilização de eletrônica, informática, telemática e avançadas tecnologias) executarem tarefas que são características da inteligência humana, tais como planejamento, compreensão de linguagens, reconhecimento de objetos e sons, aprendizado, raciocínio, solução de problemas, etc. Em outras palavras, é a teoria e desenvolvimento de sistemas de computadores capazes de executar tarefas normalmente exigindo inteligência humana, como a percepção visual, reconhecimento de voz, tomada de decisão e tradução entre idiomas, por exemplo.

O aprendizado de máquina (*Machine Learning*) é uma forma de conseguir a inteligência artificial. É um ramo da inteligência artificial que envolve a criação de algoritmos que podem aprender automaticamente a partir de dados. Ao invés de os desenvolvedores de software elaborarem enormes códigos e rotinas com instruções específicas para que a máquina possa realizar determinadas tarefas e conseguir resultados (e com isso limitar drasticamente o seu campo de atuação e resultados), no aprendizado de máquina treina-se o algoritmo para que ele possa aprender por conta própria, e até mesmo conseguir resultados que os desenvolvedores dos algoritmos nem mesmo poderiam imaginar. Neste treinamento, há o envolvimento de grandes quantidades de dados que precisam ser alimentadas para o algoritmo (ou aos algoritmos envolvidos), permitindo que ele (o algoritmo) se ajuste e melhore cada vez mais os seus resultados.

O aprendizado profundo (*Deep Learning*) é uma das várias abordagens para o aprendizado de máquinas. Outras abordagens incluem aprendizagem por meio de árvores de decisão (*decision tree learning*), programação de lógica indutiva (*inductive logic programming*), agrupamento (*clustering*), aprendizagem de reforço (*reinforcement learning*), redes bayesianas (*Bayesian networks*), entre outras. A aprendizagem profunda foi inspirada na estrutura e nas funções do cérebro humano, na interligação dos neurônios. As redes neurais artificiais (*Artificial Neural Networks* – ANNs) são algoritmos que imitam a estrutura biológica do cérebro humano. Nas ANNs, existem "neurônios" (entre aspas) que possuem várias camadas e conexões com outros "neurônios". Cada camada (*layer*) escolhe um recurso específico para aprender, como curvas e bordas no reconhecimento de uma imagem, por exemplo. A aprendizagem profunda tem o seu nome em razão dessas várias camadas. A profundidade é criada com a utilização de múltiplas camadas em oposição a uma única camada de aprendizado pelo algoritmo. Esses algoritmos de aprendizado profundo formam as "redes neurais" e estas rapidamente podem ultrapassar a nossa capacidade de compreender todas as suas funções.

A inteligência artificial e a Internet das coisas (*Internet of things*)[2] estão intrinsecamente entrelaçadas. É como se fosse a relação entre cérebro e o corpo humano. Nossos corpos coletam as entradas sensoriais, como visão, som e toque. Nossos cérebros recebem esses dados e dão sentido a eles, por exemplo, transformando a luz em objetos reconhecíveis, transformando os sons em discursos compreensíveis e assim por diante. Nossos cérebros então tomam decisões, enviando sinais de volta para o corpo para comandar movimentos como pegar um objeto ou falar.

Todos os sensores conectados que compõem a Internet das coisas (Internet of things) são como nossos corpos, eles fornecem os dados brutos do que está acontecendo no mundo. A inteligência artificial é como nosso cérebro, dando sentido a esses dados e decidindo quais ações executar. E os dispositivos conectados da Internet das coisas são novamente como nossos corpos, realizando ações físicas ou se comunicando com os outros.[3]

Os inúmeros dispositivos construídos atualmente, tais como aparelhos médicos, relógios inteligentes, veículos, eletrodomésticos, enfim, todos os itens construídos com componentes eletrônicos, software, sensores e que possuam a capacidade de coletar e transmitir dados à Internet, capazes de serem identificados de maneira única, formam o que é conhecido como a Internet das coisas (*Internet of things*).

Grande parte dos algoritmos produzidos por meio de *Machine Learning*, notadamente aqueles baseados em "*deep learning*" ou redes neurais (*neural networks*), não são totalmente compreendidos. Nenhum ser humano é capaz de dizer por quê determinado algoritmo desta natureza faz o que faz, nem pode prever totalmente o que o algoritmo poderá fazer em dados diferentes daqueles utilizados para o treinamento da máquina, ao longo do tempo.[4]

Até mesmos os maiores defensores desses sistemas, admitem essa fraqueza. Embora as redes neurais profundas (DNN – *Deep Neural Networks*) tenham demonstrado uma grande eficácia em uma ampla gama de tarefas, quando eles falham, muitas vezes falham espetacularmente, produzindo resultados inexplicáveis e incoerentes que podem deixar o ser humano perplexo, sem conseguir entender a razão pela qual o sistema tomou tais decisões.

Os professores devem estar atentos ao fato de que a Internet (em grande parte dirigida por processos

algorítmicos) pode também ser injustamente prejudicial ou manifestar-se contra alguém ou alguma coisa em suas escolhas, especialmente em vídeos, textos e imagens selecionadas pelos algoritmos. Os consultores escolares, bem como os de carreira, também devem estar atentos ao fato de que determinados serviços de Internet são suscetíveis de serem tendenciosos.

A discussão atual em relação aos riscos da inteligência artificial surge em parte por causa do crescente uso de dados e processos totalmente automatizados (com o elemento humano fora da equação) e também naqueles em que há utilização de algoritmos secretos, como os do Google.

Mas atenção: algoritmos não são imparciais. Os próprios algoritmos podem conter os preconceitos presentes nos criadores do algoritmo ou nos dados que foram usados para treinar o algoritmo. O desempenho dos algoritmos depende muito dos dados utilizados para desenvolvê-los. Os preconceitos que estão presentes nos dados serão refletidos pelos algoritmos. Todos devem se lembrar do resultado inadequado dos algoritmos utilizados pelo Google, quando classificou os negros como gorilas. (*Artificial Intelligence's White Guy Problem – Kate Crawford, The New York Times, 25th June 2016*). Tais desvios, intencionais ou não, podem ser inerentes aos dados, como também oriundos do próprio desenvolvedor do algoritmo. Isso pode ter efeitos tão ruins como os vícios que eles pretendiam eliminar. Alguns denominam este fenômeno como "*Machine bias*", "*Algorithm bias*" ou simplesmente, Bias. É o viés tendencioso. A remoção de tal viés tendencioso em algoritmos não é trivial e é um campo de pesquisa em andamento. Os desvios são difíceis de serem descobertos se o algoritmo for muito complexo (como são os utilizados pelo Google e Facebook), pior ainda se forem secretos. Se o algoritmo é simples e auditável, especialmente publicamente auditável, então haverá em tese (vou explicar adiante a razão do "em tese") maiores chances de que as decisões baseadas em tais algoritmos possam ser mais justas. Igualmente em relação aos dados utilizados para "treinar" o algoritmo. Se eles forem auditáveis (e anônimos quando apropriados) poderão ser identificados desvios desta natureza.

Provedores de serviços de aplicações de Internet e também de acesso, cada vez mais reúnem grandes coleções de dados comportamentais que podem ser recolhidos a partir dos inúmeros sensores que estão acompanhando a Internet das coisas (Internet of things – of everything), os telefones celulares, relógios inteligentes e demais produtos portáteis, tais como GPS, acelerômetros, etc. Esses dados geralmente produzem um perfil muito detalhado e pessoal, provavelmente maior do que a maioria dos cidadãos pode imaginar e compreender.

O vasto volume de dados criado pela Internet e o crescimento gigantesco de dados coletados por inúmeros sensores nos mais variados itens e equipamentos mudará muito o mundo dos negócios e o dia a dia das pessoas. E isto tem profundo impacto em relação a autodeterminação informativa, o direito constitucional da intimidade e a privacidade. Novas leis são necessárias, sim, em alguns aspectos específicos, como o projeto de lei de proteção de dados pessoais (Projeto de Lei 5.276/2016), capitaneado pelo excelente Danilo Doneda. Mas todo cuidado é pouco, tendo em vista o que ocorreu com o Marco Civil da Internet (Lei 12.965/2014) – que sofrendo influência do pernicioso lobby de empresas multinacionais, provedores de aplicações de Internet – criou uma aberração jurídica em relação a responsabilidade civil para protegê-los em detrimento da teoria de responsabilidade civil adotada no Direito Brasileiro, o que exige, sem dúvida, urgente alteração para que se compatibilize com as normas de regência.[5]

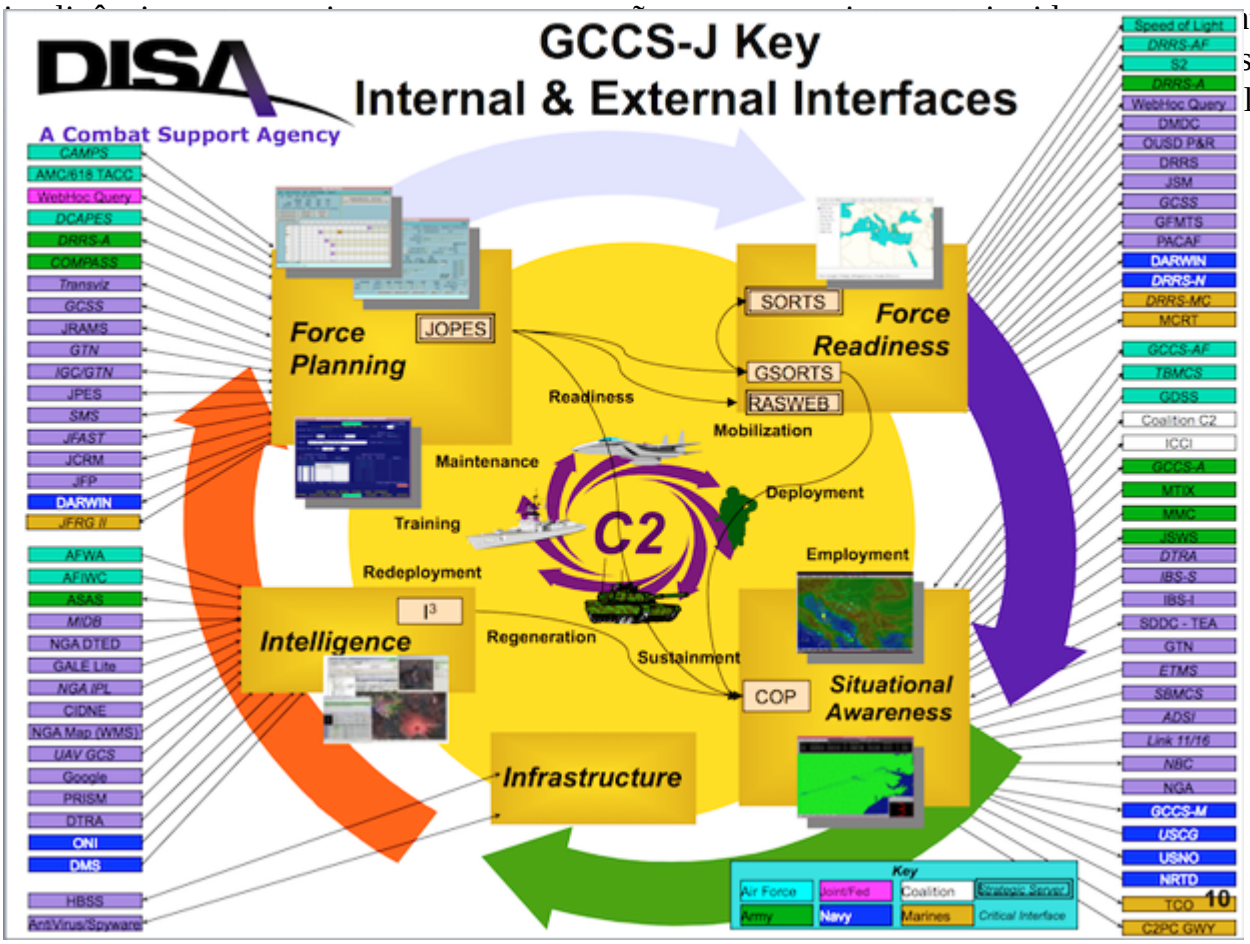
Aliás é grave assistir jovens professores, que aparentemente desconhecendo a amplitude do direito

brasileiro, defendem a criação de novas leis a todo instante. Mas por trás disso, existe o patrocínio de empresas interessadas, como vimos no recente escândalo envolvendo o Google, publicado pelo Wall Street Journal.[6] Saiba mais detalhes também aqui: http://googletransparencyproject.org/

Classificadores baseados em redes neurais equivalem-se ou superam a precisão do nível humano em muitas tarefas comuns, no entanto, redes neurais são suscetíveis ao que se denomina como "exemplos contraditórios". Dados cuidadosamente adulterados podem provocar um comportamento ruim, levando a escolhas arbitrárias e equivocadas.[7]

É notório que os algoritmos estão sendo utilizados extensivamente pelas agências de segurança e inteligência para analisar o público e a comunicação dos cidadãos. A coleta o processamento das comunicações e dados de milhões de pessoas deveria ocorrer para monitorar conhecidos alvos e suspeitos – e também para descobrir novos – mas com certas restrições e controle judicial, no entanto, a técnica de encontrar uma agulha no palheiro, invertendo a relação entre a tradicional vigilância de suspeitos e suas relações para o monitoramento indiscriminado é extremamente preocupante.

A propósito, naquele período do escândalo envolvendo a *National Security Agency* (NSA) e o analista Edward Snowden, enquanto o mundo voltava os olhos para o programa PRISM da agência de



Observe que na apresentação da DISA (*Defense Information Systems Agency*) – órgão integrante do sistema de inteligência militar norte-americano, o programa PRISM aparece como a interface e a empresa Google, como a responsável pela coleta das informações no item "*Intelligence*". Há um livro muito esperado, escrito pelo excelente jornalista Yasha Levine chamado *Surveillance Valley – The Secret Military History of the Internet* [8] que promete trazer revelações importantes. Sugiro ao leitor que também assista o vídeo *Secret History of Silicon Valley* oferecido pelo *Computer History Museum*, apresentado pelo professor Steve Blank.[9] E também o texto elaborado por Julian Assange do Wikileaks – *Google Is Not What It Seems*.[10]

A análise do big data e o processamento algorítmico deveriam ser realizados em dados relevantes de grupos de suspeitos, como mencionei, no entanto, nossos telefones registram onde vamos, com quem falamos, mídias sociais armazenam até como nos sentimos, nossos cartões bancários e de crédito registram uma grande quantidade de informações da nossa atividade, medidores inteligentes até gravam quando estamos em casa e quanto de energia utilizamos. Snowden garantiu (e comprovou pelos documentos que vazou) que os aparelhos de celular inteligentes podem gravar o ambiente, mesmo desligados. Grande parte desses dados estão disponíveis para o Estado que procura incansavelmente "pegadas digitais abrangentes" em vez de partir de uma avaliação cuidadosa das evidências relevantes.

Existem processos algorítmicos sendo utilizados para influenciar comportamentos de pessoas. Processamento algorítmico não deve ser a única base para uma decisão que produza efeitos jurídicos ou possa impactar os direitos de qualquer indivíduo.

Os criadores de algoritmos devem sempre manter a capacidade de fornecer transparência em relação a todo o processo algorítmico envolvido e explicações para as decisões e resultados atingidos. As decisões algorítmicas que envolvem os direitos e as liberdades dos indivíduos devem ser sempre desafiáveis.

A regulação, como sugerida por alguns, parece ser utópica. Impossível regulamentar um segmento que sofre modificações impressionantes a cada dia, a cada instante. O que sabemos, é que os algoritmos, embora "vendidos" por essas grandes empresas como sendo imunes ao viés político, tendencioso, aos interesses econômicos, políticos, militares, estratégicos, de inteligência e tudo mais – na realidade não são. É difícil provar a afirmação dessas empresas (que subestimam a inteligência de alguns) sem uma supervisão significativa dos algoritmos complexos, muitas vezes secretos, incluindo o conjunto de dados, a forma e as fontes de coleta que consideraram para chegar a determinados resultados.

Mesmo que seja compreensível que os controladores de dados tenham um interesse legítimo em não divulgar segredos comerciais, esse interesse não deve superar o desejo de entender como os algoritmos tomam decisões sobre os seres humanos. Para equilibrar esses interesses concorrentes, governos devem explorar a necessidade da criação de um Watchdog (órgão fiscalizador) em Inteligência Artificial, ou outro organismo regulador de confiança e totalmente independente.

Há um grande potencial para que os algoritmos e a inteligência artificial possam ser usados para o bem de toda a sociedade. Na verdade, há uma oportunidade para tornar o mundo mais justo e menos tendencioso com a utilização dos algoritmos e da inteligência artificial. As leis não devem travar e dificultar a inovação, mas, reitera-se, não podemos ser ingênuos e deslumbrados com as novas tecnologias, deixando de perceber o que está por trás de tudo isso.

Clique aqui para ler a íntegra do texto.

---

1 Veja os detalhes aqui: http://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/inquiries/parliament-2017/algorithms-in-decision-making-17-19/

2 Também chamada de “Internet of everything” (Internet de tudo, de todas as coisas)

3 Ref. Calum McClelland / AI/ML/DL – differences.

4 Knight,W., The Dark Secret at the Heart of AI. https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/

5 http://www.direitodainformatica.com.br/?p=1794

6 https://www.wsj.com/articles/paying-professors-inside-googles-academic-influence-campaign-1499785286

7 https://arxiv.org/pdf/1707.07397.pdf

8 https://surveillancevalley.com/

9 https://www.youtube.com/watch?v=ZTC_RxWN_xo

10 https://wikileaks.org/google-is-not-what-it-seems/

Date Created
20/11/2017