CEST
Centro de Estudos Sociedade e Tecnologia
USP
Universidade de São Paulo
Boletim - Volume 3, Número 11, Dezembro/2018

Considerações sobre *softwares* de policiamento preditivo

Eduardo Bertassi

Alguns veículos de comunicação noticiaram recentemente um caso ocorrido na Itália em que um homem de 55 anos foi preso antes de cometer um crime [1] [2] [3]. A história ganhou atenção porque a polícia italiana utilizou um *software* de combate ao crime com "tecnologia preditiva" chamado "X-Law".

O *software* da polícia de Nápoles é um programa de computador com algoritmos que usam uma grande quantidade de dados para realizar previsões baseadas em estimativas probabilísticas. Em *softwares* similares, os dados mais comuns utilizados são: os antecedentes criminais dos ladrões; o histórico de incidentes em diferentes regiões da cidade; a localização do efetivo policial; o horário de funcionamento e operação de estabelecimentos comerciais; entre outros. A partir desses dados o programa pode indicar à polícia os locais com maior probabilidade de ocorrência de crimes dentro de um intervalo de confiança.

> A tecnologia deve ser empregada como uma ferramenta auxiliar no combate ao crime, mas não como fonte de verdades absolutas (...)

O emprego de *softwares* parecidos com o "X-Law" não é novidade. O PredPol [4] é um programa utilizado pela polícia de Los Angeles com tecnologia de aprendizado de máquina (*machine learning*). Desde que entrou em operação o *software* recebeu elogios, mas também críticas [5] [6]. Uma delas refere-se à possibilidade da existência de "laços de reforço", que fariam com que o programa fornecesse resultados "tendenciosos" à polícia.

Em engenharia de sistemas [7] [8], um laço de reforço (do inglês *reinforcing loops*) é aquele em que uma ação produz um resultado que influencia mais da mesma ação, resultando em taxas de crescimento ou redução. Os laços podem ser dos tipos positivo ou negativo. Um exemplo de laço de reforço positivo é o do crescimento populacional: quanto maior for a população de um país, maior será o aumento de nascimentos e quanto maior for o número de nascimentos, maior será a população de um país. Um exemplo de laço de reforço negativo é o da relação de predação: quanto maior for o número de predadores em uma área, menor será o número de presas e quanto menor for o número de presas, menor será o número de predadores; porém, quando o número de predadores diminuir, o número de presas voltará a aumentar (caso elas não tenham sido extintas), e o número de predadores também aumentará (caso eles não tenham morrido por inanição). Por simplificação, os fatores externos que influenciam as taxas de crescimento ou redução foram desconsiderados.

O receio quanto aos laços de reforço está na possibilidade de o algoritmo indicar sempre os mesmos criminosos, ou as mesmas regiões da cidade, devido à quantidade de ocorrências passadas e recentes registradas [9] [10]. Algumas das consequências desse comportamento "tendencioso" do *software* podem ser, por exemplo: a ineficácia ao identificar novos criminosos e novas regiões com criminalidade; ou o risco de que determinados bairros associados a certos grupos étnicos ou raciais sejam injustamente rotulados, levando a discriminação de seus habitantes.

Defensores dos direitos civis alertam que as justificativas para uso desta tecnologia podem mascarar um problema maior: a discriminação étnica e racial [9]. Há quem defenda que é perigoso retirar totalmente a perspectiva e interações humanas do processo de avaliação de quem pode ou não ser considerado um potencial criminoso. Algoritmos de aprendizagem de máquina fornecem respostas com base em seus dados de treinamento e operação, e se algum tipo de viés for modelado ou

programado no *software* de policiamento preditivo, mesmo que de forma não intencional, os resultados podem ser muito negativos.

A tecnologia deve ser empregada como uma ferramenta auxiliar no combate ao crime, mas não como fonte de verdades absolutas, até porque os dados que alimentam os programas podem estar incorretos. Em 2016, durante uma auditoria feita nos bancos de dados de um *software* de inteligência artificial (IA) da polícia da Califórnia (o *CalGang*), verificou-se que os dados consultados por juízes sobre pessoas que supostamente tinham ligação com gangues estavam errados [10]. Portanto, é recomendável que a capacidade de avaliação humana não seja completamente abandonada e que tanto os *softwares* quanto suas bases de dados possam ser auditados periodicamente por entidades idôneas.

Provavelmente, a adoção de *softwares* de policiamento preditivo aumentará, conforme vem ocorrendo nos Estados Unidos, Canadá e em outras cidades no mundo. Mas é preciso cautela, pois na cidade predominantemente muçulmana de Xinjiang, na China, um *software* desse tipo é empregado há algum tempo e, infelizmente, existem relatos de pessoas detidas de forma arbitrária com justificativas embasadas nos dados do *software* [11]. Inclusive, há indícios de que os dados dos cidadãos coletados a partir de imagens de câmeras de circuito fechado, transações de cartões de crédito, conexões Wi-Fi de telefones e computadores, registros de saúde, dados bancários, entre outros, são utilizados para reprimir os residentes [12].

A aquisição de *softwares* de policiamento preditivo com código-fonte aberto pode ser uma alternativa para tentar evitar que governos usem estes *softwares* como ferramentas de repressão, evitando que sejam compradas "caixas pretas" que não permitam o conhecimento do funcionamento interno do sistema [13]. Em *softwares* de IA é importante que existam certas características como: transparência (possibilidade de consultar e compreender os modelos de tomada de decisão da IA); explicabilidade (possibilidade de compreender os mecanismos de raciocínio da IA); e provabilidade (possibilidade de comprovar matematicamente os resultados de cada decisão do programa). Algumas empresas de consultoria identificaram que a falta de confiança nos modelos de tomada de decisão dos *softwares* de IA é uma oportunidade de negócios, portanto, oferecem serviços para auxiliar a avaliação destes *softwares* antes da compra [14] [15].

Adquirir *softwares* baseados em normas internacionais, também pode amenizar o problema de compras de "caixas pretas". A ISO (*International Organization for Standardization*) é um órgão que vem trabalhando na criação de normas para elaboração de sistemas de IA [16] [17], como é o caso das normas ISO/IEC 23053 (para sistemas que usam aprendizado de máquina) [18] e ISO/IEC 38507 (para padronizar o uso de inteligência artificial pelas organizações) [19]. *Softwares* desenvolvidos e certificados a partir de normas internacionais têm reconhecimento internacional, pois devem seguir padrões de qualidade bem estruturados e processos de desenvolvimento e implantação de conhecimento público, permitindo maior interoperabilidade, consistência e transparência quanto ao produto final. Logo, é interessante que entidades públicas considerem a aquisição de *softwares* de IA baseados em normas internacionais para prover aos cidadãos um grau de transparência que é creditada por uma entidade idônea como a ISO.

O combate ao crime é uma necessidade na maioria das metrópoles e grandes cidades do mundo, portanto, é possível que novas notícias apareçam no futuro sobre iniciativas como: HunchLab [20]; CrimeRadar [21] [22] (protótipo brasileiro usado na cidade do Rio de Janeiro durante as Olimpíadas de 2016); o CompStat [23] [24] [25] (que não é um *software*, mas um conjunto de ferramentas tecnológicas e métodos organizacionais de trabalho voltados para departamentos de polícia), entre outros. A justificativa do emprego desses *softwares* para combater o crime é nobre, mas é preciso que a população, os governantes e, principalmente, os acadêmicos fiquem atentos para a utilização e o desenvolvimento desse tipo de tecnologia, pois apesar dos resultados imediatos serem muito atraentes ainda não se sabe com precisão quais podem ser as consequências para a sociedade no futuro.

Eduardo Bertassi *é mestrando em engenharia da computação pela Escola Politécnica da Universidade de São Paulo e pesquisador do CEST-USP.*

Coordenador Acadêmico: Edison Spina

Este artigo resulta do trabalho de apuração e análise do autor, não refletindo obrigatoriamente a opinião do CEST.

Referências:

[1] Polícia usa algoritmo que prevê crimes para prender ladrão na Itália. BBC Brasil, 19 de nov. de 2018. Disponível em: <https://www.bbc.com/portuguese/internacional-46198655>. Acesso em 26 de nov. de 2018.

[2] BERNASCONI, F. Venezia, ecco il software che predice tutti i reati. Il Giornale, 17 de nov. de 2018. Disponível em: <http://www.ilgiornale.it/news/cronache/venezia-ecco-software-che-predice-tutti-i-reati-1603366.html>. Acesso em 26 de nov. de 2018.

[3] XLAW funziona, il software che "prevede" i furti coglie un ladro sul fatto. Il Gazzettino, 16 de nov. de 2018. Disponível em: <https://www.ilgazzettino.it/nordest/venezia/furto_hotel_sistema_x_law-4111701.html>. Acesso em 26 de nov. de 2018.

[4] BERTASSI, E. Utilização da inteligência artificial para promover a inclusão social. Boletim do CEST, vol. 3, n. 4, mai. de 2018. Disponível em: < http://www.cest.poli.usp.br/download/utilizacao-da-inteligencia-artificial-para-promover-a-inclusao-social/>. Acesso em 26 de nov. de 2018.

[5] LAPOWSKY, I. How the LAPD uses data to predict crime. Wired, 22 de mai. de 2018. Disponível em: < https://www.wired.com/story/los-angeles-police-department-predictive-policing/>. Acesso em 26 de nov. de 2018.

[6] BURRINGTON, A.; BURRINGTON , I. A pioneer in predictive policing is starting a troubling new project. The Verge, 26 de abr. de 2018. Disponível em: < https://www.theverge.com/2018/4/26/17285058/predictive-policing-predpol-pentagon-ai-racial-bias>. Acesso em 26 de nov. de 2018.

[7] HITCHINS, Derek K. Systems engineering: a 21st century systems methodology. John Wiley & Sons, 2008.

[8] HUNTER, J. System Thinking: Feedback loops. The W. Edwards Deming Institute Blog, 28 de abr. de 2016. Disponível em: <https://blog.deming.org/2016/04/systems-thinking-feedback-loops/>. Acesso em 26 de nov. de 2018.

[9] How data-driven policing threatens human freedom. The economist, 4 de jun. de 2018. Disponível em: <https://www.economist.com/open-future/2018/06/04/how-data-driven-policing-threatens-human-freedom>. Acesso em 26 de nov. de 2018.

[10] RIELAND, R. Artificial Intelligence Is Now Used to Predict Crime. But Is It Biased? Smithsonian.com, 5 de mar. de 2018. Disponível em: <https://www.smithsonianmag.com/innovation/artificial-intelligence-is-now-used-predict-crime-is-it-biased-180968337/#jf04gGf6HrOVlqyt.99>. Acesso em 26 de nov. de 2018.

[11] China using big data and 'predictive policing' in Xinjiang region to round up perceived threats: HRW. The Japan Times, 28 de fev. de 2018. Disponível em: <https://www.japantimes.co.jp/news/2018/02/28/asia-pacific/social-issues-asia-pacific/china-using-big-data-predictive-policing-xinjiang-region-round-perceived-threats-hrw/#.W_07AOhKiUk>. Acesso em 26 de nov. de 2018.

[12] 'Big data' predictions spur detentions in China's Xinjiang: Human Rights Watch. Reuters, 27 de fev. de 2018. Disponível em: <https://www.reuters.com/article/us-china-rights-xinjiang/big-data-predictions-spur-detentions-in-chinas-xinjiang-human-rights-watch-idUSKCN1GB0D9>. Acesso em 26 de nov. de 2018.

[13] CAREY, S. How IBM is leading the fight against black box algorithms. Computer World UK, 21 de set. de 2017. Disponível em: <https://www.computerworlduk.com/data/how-ibm-is-taking-lead-in-fight-against-black-box-algorithms-3684042/>. Acesso em 26 de nov. de 2018.

[14] GOLBIN, I.; RAO, A. What it means to open AI's black box. Price Waterhouse Cooper, 15 de mai. de 2018. Disponível em: <https://usblogs.pwc.com/emerging-technology/to-open-ai-black-box/>. Acesso em 26 de nov. de 2018.

[15] DUIN, S. V. Accountability of Artificial Intelligence: how to see what is inside the black box? Disponível em: <https://www2.deloitte.com/nl/nl/pages/data-analytics/articles/accountability-of-artificial-intelligence-how-to-see-what-is-inside-the-black-box.html>. Acesso em 26 de nov. de 2018.

[16] PRICE, A. First International Standards Committee for entire AI ecosystem. International Electrotechnical Commission (IEC). E-tech, vol. 3, 2018. Disponível em: <https://iecetech.org/Technical-Committees/2018-03/First-International-Standards-committee-for-entire-AI-ecosystem>. Acesso em 26 de nov. de 2018.

[17] PRICE, A. How tech savvy leaders stay ahead of the game. International Electrotechnical Commission (IEC). E-tech, vol. 5, 2018. Disponível em: <https://iecetech.org/Technical-Committees/2018-05/How-tech-savvy-leaders-stay-ahead-of-the-game>. Acesso em 26 de nov. de 2018.

[18] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC NP 23053: Framework for Artificial Intelligence (AI) Systems Using Machine Learning (ML), 7 de mar. de 2018 (Preparatory Document). Disponível em: <https://www.iso.org/standard/74438.html>. Acesso em 26 de nov. de 2018.

[19] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC NP 38507: Information technology -- Governance of IT -- Governance implications of the use of artificial intelligence by organizations, 5 de out. de 2018. Disponível em: <https://www.iso.org/standard/56641.html>. Acesso em 26 de nov. de 2018.

[20] AZAVEA. HunchLab, 2018. Next generation predictive policing. Disponível em: <https://www.hunchlab.com/>. Acesso em: 26 de nov. de 2018.

[21] GRIFFITHS, S. CrimeRadar is using machine learning to predict crime in Rio. Wired, 18 de ago. de 2016. Disponível em: <https://www.wired.co.uk/article/crimeradar-rio-app-predict-crime>. Acesso em 26 de nov. de 2018.

[22] CRIMERADAR. Instituto Igarapé, 2018. Disponível em: <https://rio.crimeradar.org/>. Acesso em 26 de nov. de 2016.

[23] Compstat: A Crime Reduction Management Tool. Harvard Kennedy School. Disponível em:<https://www.innovations.harvard.edu/compstat-crime-reduction-management-tool>. Acesso em 26 de nov. de 2018.

[24] O'NEIL, J.; SHEA, D. Crime data helps police thrive: NYPD commissioner. USA Today, 15 de fev. de 2017. Disponível em: <https://www.usatoday.com/story/opinion/policing/2017/02/15/policing-the-usa-crime-compstat-new-york-police-department/97913528/>. Acesso em 26 de nov. de 2018.

[25] Compstat. in: Wikipedia. Disponível em: <https://en.wikipedia.org/wiki/CompStat>. Acesso em 26 de nov. de 2018.