

Black Lives Matter zmusza IBM do obrotu o 180 stopni w kwestii technologii rozpoznawania twarzy

5 sierpnia 2020

„W wyniku ostatnich protestów ruchu Black Lives Matters, które poruszyły kwestie rasizmu i działań policji w Stanach Zjednoczonych i na świecie, firma technologiczna IBM ogłosiła zawieszenie swoich działań na rynku rozwiązań technologii rozpoznawania twarzy ogólnego zastosowania. Czy oznacza to punkt zwrotny w stosowaniu przez służby bezpieczeństwa tej, mającej obecnie swoje wady, technologii?” – ta wiadomość przeszła prawie bez echa.

Z jednej strony tej historii, mamy nieudaną walkę z kryzysem COVID-19. Z drugiej, protesty i gniew wzniecany przez skandaliczną brutalność policji, która przywróciła do życia ruch Black Lives Matter na całym świecie. Pomiedzy tymi wydarzeniami, IBM ogłosiło 8 czerwca decyzję o wycofaniu się z planów dostarczania technologii rozpoznawania twarzy, z uwagi na obecne protesty, które wymusiły na nich dostosowanie się do własnych zasad etycznych.

„Technologia może wpłynąć na poprawę przejrzystości działań policji i pomóc im w służbie społecznościom, ale nie powinna promować dyskryminacji, lub nierówności na tle rasowym” – skomentował Arvind Krishna, dyrektor generalny spółki IBM.

Ta wypowiedź nie wywołała wielu reakcji, poza kilkoma ze strony analityków polityki gospodarczej, entuzjastów technologii i aktywistów. Mimo wszystko może to oznaczać znaczące zmiany w tym, jak duży wpływ na nasze życia ma technologia.

Kontrowersyjna technologia

Oprogramowanie do rozpoznawania twarzy pozwala na automatyczną identyfikację osób na podstawie zdjęć lub nagrań wideo. Do osiągnięcia tego celu technologia ta wykorzystuje dwa główne elementy: bazę danych zebranych wcześniej zdjęć oraz dużą moc obliczeniową. Oba elementy to obszary, w których ostatnimi czasy został poczyniony ogromny postęp, a to dzięki rozwojowi w takich dziedzinach jak technologia dużych zbiorów danych i Sztuczna Inteligencja (AI). Umożliwiło to tym samym rozwój technologii rozpoznawania twarzy na dużą skalę.

Przez ostatnie kilka lat na świecie nastąpił wysyp przypadków użycia tej technologii. Już w lutym 2005 roku wydział policji z Los Angeles stosował system stworzony przez General Electric i Hamilton Pacific. Od tamtego czasu tego typu działania zostały mocno rozpowszechnione, a ich rozwój przyspieszył. W 2019 Chiny miały w sumie 200 milionów kamer monitoringu, na terenie swojego państwa. Nawet bardziej gęsta siatka kamer monitoringu powstaje właśnie w Rosji. Nie wspominając o inicjatywach miast takich jak Nicea, która obecnie testuje[fr] tę technologię, lub Londyn, gdzie kamery analizują twarze przechodniów (bez ich wiedzy) w celu zlokalizowania osób poszukiwanych przez służby.

Służby obstają przy wykorzystaniu tego typu automatycznej inwigilacji, argumentując, że przynosi ona korzyści dla bezpieczeństwa: w drugiej połowie 2016 roku, Międzynarodowa Organizacja Policji Kryminalnej, Interpol, ogłosiła identyfikację tożsamości „ponad 650 przestępców, zbiegów, podejrzanych i zaginionych osób [...]”. Te działania mają na celu walkę z przestępczością, terroryzmem, czy ostatnio, rozprzestrzenianiem się koronawirusa.

Tak jak wiele innych nowoczesnych technologii rozpoznawanie twarzy to miecz obosieczny. Korzyści, jakie przynosi, wiążą się także z zagrożeniami, szczególnie, w stosunku do

podstawowych swobód obywatelskich.

Niektóre z organizacji zajmujących się prawami cyfrowymi ostrzegają przed potencjalnymi zagrożeniami i nadużyciami, które wiążą się z zastosowaniem technologii rozpoznawania twarzy. Te organizacje to między innymi, Electronic Frontier Foundation (EFF) i La Quadrature du Net. Ta druga koordynuje kampanię pod nazwą Technopolice, która jest inicjatywą mającą na celu katalogowanie i ujawnianie planów automatycznego nadzoru we Francji oraz wzywanie do systematycznego oporu.

Ograniczona niezawodność

Najbardziej szkodliwą wadą, jaką może posiadać technologia rozpoznawania twarzy, jest stronnictwo. Tego typu narzędzia identyfikują ludzi na podstawie próbek, czyli tak zwanych „zestawów danych treningowych”. Jeśli te są niekompletne lub niestosowne, wówczas narzędzie nie dokona prawidłowego rozpoznania. To zjawisko określane jest mianem odchylenia wywiedzionego.

W zeszłym miesiącu, w celu zademonstrowania wspomnianego odchylenia, użytkownicy „Twittera” przetestowali AI, które rekonstruuje portrety na podstawie rozmazanych obrazów i opublikowali wyniki nietypowe rezultaty w internecie. Algorytm zawodzi dużo częściej w przypadku Afroamerykanów i Latynosów. Przykładami są Barack Obama i Alexandria Ocasio-Cortez. Zbiór danych, który składał się głównie z portretów białych ludzi, sprawił, że rekonstrukcje zostały wykonane nieprawidłowo, bo skupiały się tylko na najczęściej występujących cechach charakterystycznych.

Poniższe zdjęcie przedstawiające białego Baracka Obamę pokazuje w skrócie problem odchylenia wywiedzionego, z którym boryka się AI.

Istnieje prawdopodobieństwo, że wykorzystanie AI do identyfikacji osób ze zdjęć o normalnej jakości, tj. nierozmazanych, będzie wiązało się z podobnym odchyleniem.

„Założmy, że decyzja o oszacowaniu skłonności danej osoby do przestępczości jest określana na podstawie takich danych jak wiek, adres, kolor skóry, edukacja... a dane użyte do rozwoju oprogramowania pochodzą z zakładów karnych i więzień. Istnieje więc wysokie prawdopodobieństwo, że to oprogramowanie znacząco zaniży ryzyko, które stanowią biali ludzie, a wywinduje je dla innych”.

Fakty mówią same za siebie. W Londynie system rozpoznawania twarzy w czasie rzeczywistym wykazał 81% błędnych rozpoznań; w Detroit, Afroamerykanin podzielił się historią o swoim bezprawnym aresztowaniu wynikającym z błędnego rozpoznania.

Wątpliwa zasadność

Technologia rozpoznawania twarzy jest nie tylko zawodna, ale prowadzi też do większej dyskryminacji, jak potwierdziło w 2016 roku śledztwo dociekliwych autorów portalu „Pro Publica”. „Zdjęcia Google dodały tag „goryle” do zdjęcia dwójga Afroamerykanów [...] narzędzie używane w procesie rekrutacji przez firmę Amazon wpływało na niekorzyść kobiet.”

Warto zauważyć, że w przypadku oskarżeń służb policyjnych o dyskryminację, technologia rozpoznawania twarzy często pojawia się jako dodatkowa, silnie poróżniająca, kwestia.

Śmierć George’a Floyda, spowodowana incydentem brutalności policji z 25 maja w Minneapolis, wywołała falę demonstracji najpierw w Stanach Zjednoczonych, a potem na całym świecie. Rozpoczęto od piętnowania dyskryminacji mniejszości rasowych. Jednak eskalacja brutalności doprowadziła do żądań ze strony demonstrantów, którzy mówili o konieczności demilitaryzacji organów ścigania, skandując slogan „Zaprzestać finansowania policji”. Tym samym, narzędzia masowej inwigilacji oraz prywatne firmy je dostarczające również znalazły się pod lupą. Dlatego też w związku z naciskiem aktywistów ruchu Black Lives Matter, spółka IBM ogłosiła swoje częściowe wycofanie się z rynku technologii rozpoznawania twarzy.

Nie jest przypadkiem, że to właśnie niebieski gigant (popularne określenie opisujące IBM) zareagował jako pierwszy. Spółka ma długą, momentami wstydliwą, historię, z którą musiała jakoś nauczyć się żyć. W roku 1934 IBM współpracowało z nazistowskim reżimem poprzez podległe spółki niemieckie. Dużo później, w roku 2013, było również zamieszczone w sprawie programu inwigilacji PRISM, co zostało ujawnione przez Edwarda Snowdena. Może właśnie dzięki tym doświadczeniom IBM było w stanie odnaleźć się w obecnym konflikcie pomiędzy nastawionym na bezpieczeństwo państwem i aktywistami praw człowieka. Oczywiście, można też zastanowić się nad bardziej prozaicznymi argumentami obecnej strategii IBM, które bardzo chętnie chciałoby uniknąć wszelkich przyszłych spraw sądowych i związanych z nimi wydatków.

Mimo wszystko zmiana kierunku działań IBM okazała się na tyle prawdziwa, że wznieciła inicjatywę, za którą podążają też inni giganci przemysłu. Microsoft zadeklarował 12 czerwca, że nie zamierza sprzedawać swojej technologii rozpoznawania twarzy służbom policji; Amazon, w wyniku poczucia presji grupy, ogłosił moratorium na swoje narzędzie Rekognition.

Krok w kierunku wolności?

Potrzeba stworzenia ram prawnych stała się oczywista. W swojej wypowiedzi Arvind Krishna, dyrektor generalny IBM, wezwał Kongres Stanów Zjednoczonych do “rozpoczęcia dialogu narodowego, żeby ustalić, czy i jak technologie rozpoznawania twarzy mają być wykorzystywane przez organy ścigania”.

To wezwanie zostało wysłuchane. Członkowie Kongresu ogłosili 25 czerwca ustawę mającą zakazać stosowania technologii rozpoznawania twarzy przez policję. Dzień wcześniej, zakaz ten został wprowadzony w Bostonie przez tamtejszą radę miasta.

Bez wątpienia to dopiero początek długiej walki prawnej i politycznej o stworzenie procedur zastosowania technologii rozpoznawania twarzy, które będą szanowały prawa obywateli. Po

raz pierwszy jednak ruchy obrony praw człowieka wydają się być na pozycji, która pozwala im wpływać na gigantów technologicznych i elity polityczne, przybliżając im obraz wspólnego dążenia do technologii, która przyniesie korzyść dla wszystkich.

Autorstwo: Rémy Vuong

Tłumaczenie: Rafał Myśliwczyk

Źródło: [pl.GlobalVoices.org](https://pl.globalvoices.org)

Licencja: [CC BY 3.0](https://creativecommons.org/licenses/by/3.0/)

Bibliografia

1.
<https://www.ibm.com/blogs/policy/facial-recognition-sussex-racial-justice-reforms/>
2.
<https://www.forbes.com/sites/glenngow/2020/06/23/why-are-technology-companies-quitting-facial-recognition/#5b151bc96994>
3.
<https://mapr.com/blog/big-data-key-unlocking-facial-recognition-business/>
4.
<https://www.npr.org/2019/12/16/788597818/how-china-is-using-facial-recognition-technology>
5.
<https://www.themoscowtimes.com/2019/11/12/russia-building-one-of-worlds-largest-facial-recognition-networks-a68139>
6. <https://www.lebigdata.fr/nice-test-reconnaissance-faciale>
7.
<https://techcrunch.com/2020/01/24/londons-met-police-switches-on-live-facial-recognition-flying-in-face-of-human-rights-concerns/>

8.

<https://www.interpol.int/en/How-we-work/Forensics/Facial-Recognition>

9.

<https://www.dailymail.co.uk/sciencetech/article-8046325/Chinese-facial-recognition-identify-people-wearing-masks.html>

10. <https://www.eff.org/pages/face-recognition>

11.

<https://www.laquadrature.net/en/2020/02/27/first-success-against-facial-recognition/>

12. <https://technopolice.fr/>

13.

https://twitter.com/tg_bomze/status/1274098682284163072?s=20

14.

<https://twitter.com/Chicken3gg/status/1274314622447820801?s=20>

15.

<https://twitter.com/osazuwa/status/1274444300894572546?s=20>

16. <https://intelligence-artificielle.agency/les-biais/>

17.

<https://www.technologyreview.com/2019/07/04/134296/london-polices-face-recognition-system-gets-it-wrong-81-of-the-time/>

18.

<https://www.washingtonpost.com/opinions/2020/06/24/i-was-wrong-fully-arrested-because-facial-recognition-why-are-police-allowed-use-this-technology/>

19.

<https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>

20.

<https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>

21.

<https://digital-society-forum.orange.com/fr/les-actus/1166-ia-quand-la-reconnaissance-faciale-a-des-biais-racistes>

22.

<https://www.tellerreport.com/news/2020-06-11-tn-rabiot-police-officiel-the-shocking-article-from-streetpress.rkwwwD1TU.html>

23.

<https://www.washingtonpost.com/technology/2020/06/12/facial-recognition-ban/>

24.

<https://www.msn.com/en-us/news/technology/microsoft-wont-sell-police-its-facial-recognition-technology-following-similar-moves-by-amazon-and-ibm/ar-BB15lTVy>

25. <https://twitter.com/wusa9/status/1277389149289484293>

26.

<https://blog.aboutamazon.com/policy/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition>

27.

<https://www.techrepublic.com/article/congress-proposes-ban-on-government-use-of-facial-recognition-software/>

28.

<https://www.boston.com/news/local-news/2020/06/24/boston-face-recognition-technology-ban>