

Publikacja analizuje wpływ sztucznej inteligencji na handel ludźmi, wskazując, że technologia ta działa jak „miecz obosieczny”. Z jednej strony przestępcy wykorzystują AI do usprawnienia wszystkich etapów swojej działalności – od rekrutacji ofiar po tworzenie fałszywych dokumentów. Z drugiej strony, służby i organizacje pozarządowe mogą wykorzystać te same technologie do lepszej identyfikacji ofiar, analizy danych i wsparcia poszkodowanych. Dokument podkreśla, że kluczowe jest oparcie działań na podejściu skoncentrowanych na prawach człowieka, aby uniknąć działań niosących ze sobą negatywne konsekwencje takie jak dyskryminacja czy naruszenie prywatności.

Zagrożenia: Jak przestępcy wykorzystują SI

Przestępcy, w tym handlarze ludźmi, coraz częściej korzystają z zaawansowanych narzędzi AI, w szczególności z tzw. generatywnej (GenAI), ze względu na jej wszechstronność i łatwość użycia. Do głównych zagrożeń należą:

- **Automatyzacja i skalowanie rekrutacji:** Narzędzia AI pozwalają na automatyzację rozmów i tłumaczenie ich na różne języki w czasie rzeczywistym, co umożliwia handlarzom dotarcie do szerszego grona potencjalnych ofiar w nowych społecznościach.
- **Analiza danych i targetowanie:** Przestępcy wykorzystują AI do analizy aktywności w mediach społecznościowych w celu identyfikowania osób w sytuacjach zagrożenia, co pozwala na precyzyjne manipulowanie nimi.
- **Tworzenie fałszywych tożsamości i treści:** Generatywna AI umożliwia tworzenie realistycznych profili w mediach społecznościowych, stron internetowych oraz ofert pracy, które wyglądają na autentyczne.
- **Deepfakes i sextortion:** Technologia ta pozwala na generowanie materiałów seksualnych z wizerunkiem ofiary (deepfakes), które są następnie wykorzystywane do szantażu (sextortion) lub kontrolowania ofiary poprzez podszywanie się pod znajomych.
- **Model „Crime-as-a-Service”:** Dostępne są specjalistyczne narzędzia przestępcze (np. chatboty typu „FraudGPT”), które pozwalają na wykorzystanie zaawansowanej AI nawet przez osoby bez wiedzy technicznej.

Wykorzystanie AI do zwalczania handlu ludźmi

Autorzy wskazują, że AI może wspierać działania mające na celu przeciwdziałanie handlowi ludźmi w obszarze czterech filarów: prewencji, ścigania, ochrony i partnerstwa.

Prewencja

- **Tłumaczenie i edukacja:** Generatywna AI pozwala na szybkie i skuteczne tłumaczenie kampanii uświadamiających, dzięki czemu docierają one do szerszej publiczności.
- **Moderacja treści:** Narzędzia oparte na uczeniu maszynowym mogą wykrywać nielegalne treści, takie jak materiały przedstawiające wykorzystywanie seksualne dzieci.
- **Odstraszanie sprawców:** Przykładem jest chatbot „Sweetie 2.0”, który podszywa się pod dziecko w pokojach czatów, aby identyfikować potencjalnych sprawców i informować ich o konsekwencjach prawnych.

Ściganie

- **Analiza finansowa:** Uczenie maszynowe pomaga wykrywać wzorce w danych finansowych, oznaczając podejrzone transakcje, które mogą wskazywać na pranie brudnych pieniędzy lub kontrolę nad kontem ofiary.
- **Identyfikacja:** Narzędzia takie jak model AI organizacji Global Fishing Watch analizują dane satelitarne, aby identyfikować statki, na których mogą występować warunki pracy przymusowej.
- **Rozpoznawanie obrazu:** Oprogramowanie takie jak „Traffic Jam” wykorzystuje widzenie m.in. rozpoznawanie twarzy do przeszukiwania dużych zbiorów danych w celu identyfikacji ofiar i sprawców.

Ochrona ofiar

- **Chatboty:** Mogą one dostarczać porad i informacji ofiarom, co jest szczególnie ważne przy ograniczonych zasobach ludzkich.
- **Analiza potrzeb:** Przetwarzanie języka naturalnego (NLP) pozwala analizować notatki z spraw i dzienniki ofiar (np. projekt RESTART), aby lepiej zrozumieć ich potrzeby i usprawnić system wsparcia.

Partnerstwo

- **Wymiana danych:** Platformy takie jak „Traffik Analysis Hub” (stworzona przez IBM i STOP THE TRAFFIK) wykorzystują AI do analizy danych z banków, NGO i policji, pozwalając na lepsze ukierunkowanie zasobów.

Zasady etycznego wykorzystania AI

Publikacja kładzie ogromny nacisk na to, że korzyści z AI wiążą się z ryzykiem błędów etycznych. Aby temu zapobiec, należy przyjąć podejście oparte na prawach człowieka i przestrzegać sześciu kluczowych zasad:

1. **Odpowiedzialność:** Twórcy systemów AI powinni ponosić odpowiedzialność za wpływ swoich narzędzi. Regulacje (np. Akt o AI w UE) mają kluczowe znaczenie dla minimalizowania ryzyka przejęcia nowych technologii przez przestępców.
2. **Przejrzystość i wytłumaczalność:** Użytkownicy powinni rozumieć, w jaki sposób AI dochodzi do swoich wniosków. Brak przejrzystości może prowadzić do podejmowania decyzji w oparciu o niepełne lub błędne założenia algorytmu.
3. **Sprawiedliwość i niedyskryminacja:** Systemy AI mogą dziedziczyć uprzedzenia z danych treningowych (np. dyskryminacja ze względu na płeć czy rasę), co prowadzi do błędnej identyfikacji ofiar lub sprawców. Konieczne jest dzielenie się danymi między sektorami, aby zbiory były reprezentatywne.
4. **Kontrola człowieka nad technologią:** AI powinna być narzędziem wspomagającym i niezastępującym ludzkich decyzji, zwłaszcza w kwestiach dotyczących bezpieczeństwa i praw ofiar. Ostateczna decyzja musi zawsze należeć do człowieka.
5. **Prywatność, bezpieczeństwo i ochrona:** Systemy nie mogą szkodzić osobom, które mają chronić. Ryzyko obejmuje stygmatyzację przez błędną identyfikację, retraumatyzację przez nadmierne poleganie na AI lub wyciek danych osobowych ofiar.

6. **Odpowiedzialność zawodowa:** Deweloperzy muszą dbać o to by minimalizować ryzyko nadużyć. Ofiary i społeczności zagrożone powinny mieć głos na każdym etapie tworzenia narzędzi AI.

Wyzwania: Luki cyfrowe i dostępność

Autorzy zwracają uwagę na problem nierównego dostępu do technologii (tzw. digital divides). Organy ścigania i organizacje w krajach o niskich dochodach mogą mieć trudności z wdrożeniem zaawansowanych narzędzi AI, co osłabia globalne działania mające na celu przeciwdziałanie handlowi ludźmi. Dodatkowo, niski poziom kompetencji cyfrowych w społeczeństwie zwiększa podatność osób na manipulacje ze strony handlarzy wyposażonych w AI. Publikacja postuluje inwestycje w edukację cyfrową i wyrównywanie dostępu do technologii jako kluczowe elementy budowania odporności społeczeństw.

Wnioski

AI zmienia krajobraz handlu ludźmi, dając przestępcom nowe możliwości rozwoju działalności, ale jednocześnie otwierając nowe metody walki z tym zjawiskiem. Kluczem do sukcesu jest odpowiedzialne wykorzystanie technologii z naciskiem na przestrzeganie praw człowieka i przy zachowaniu zasad takich jak przejrzystość, nadzór osobowy i ochrona prywatności. Bez uwzględnienia szerszego kontekstu społecznego, w tym luk cyfrowych, działania te mogą być nieskuteczne lub wręcz szkodliwe.