



„AI”gorytm na miłość

Poradnik (nie)romantyczny UKE

UKE

| Urząd Komunikacji Elektronicznej

JAK SZTUCZNA INTELIGENCJA MOŻE ZŁAMAĆ CI SERCE I POMÓC OPRÓŻNIĆ PORTFEL?

„O królowo wszechpiękności!
Ornamencie człowieczeństwa!
Powiedz: W ogień skocz, Papkinie.
A twój Papkin w ogniu zginie” -
mówi Papkin do Klary w *Zemście*
Aleksandra Fredry. Papkin to postać
tragikomiczna, kreująca się
na uwodziciela i bohatera,
a tak naprawdę tchórz i kłamca
o rozchwianym poczuciu wartości.
Takich bohaterów w literaturze
i filmie znajdziemy miliony. A
jak to jest, gdy szukamy w sieci
wybranki lub wybranka serca?

Miłość to nie tylko uczucia, miłość to dochodowy biznes. Naszym przodkom aranżowano małżeństwa kierując się pozycją społeczną i majątkiem kandydata. Kolejnym etapem były biura matrymonialne z segregatorami i Panią Halinką, która prezentowała zdjęcia oraz opisy kandydatów i kandydatek niczym w polskiej komedii *Nie lubię poniedziałku*. Pamiętacie Francesco Romanelliego, który zamiast na spotkanie biznesowe w Maszynohurcie trafił do biura matrymonialnego, a następnie w objęcia Marianny? To była jeszcze era, w której błąd mógł zakończyć się romansem, a nie wyciekami danych osobowych i opróżnieniem konta bankowego.

Dziś już tak nie wygląda kojarzenie par. **Mamy algorytmy, które śledzą każdy Twój ruch w sieci: ile razy spojrzales na zdjęcie z kotem, jak długo przytrzymałeś palec na profilu bruneta na Insta, czy przeglądasz profile częściej przed śniadaniem czy po lunchu oraz ile lajków zostawiłeś pod zdjęciem Roberta Makłowicza na Make Life Harder.** To na tej podstawie algorytmy decydują, czy jesteś gotowy na związek, czy tylko na krótką przygodę, która skończy się szybciej niż Twoje subskrypcje premium.

Według różnych danych branżowych, globalny rynek usług randkowych generuje rocznie między 6 a 9 miliarda USD, przy tendencji wzrostowej w kolejnych latach. To są liczby, które przyciągają inwestorów i programistów sztucznej inteligencji. A jeśli już mowa o dużych pieniądzach, to obawiam się, że algorytm aplikacji randkowej ma więcej wspólnego z ruletką w Monte Carlo niż z przeznaczeniem – tyle, że przy ruletce przynajmniej serwują drinki.

Takie przychody i zainteresowanie randkami online wykorzystują oszuści internetowi. **Dostęp do internetu, aplikacji i mediów społecznościowych sprawił, że obecnie oszuści działają na globalną skalę.** Coraz częściej oszustwa związane z randkami i romansami są prowadzone przez grupy przestępcze, korzystające ze sztucznej inteligencji, skryptów i szkoleń, pozwalających na dotarcie do wielu potencjalnych ofiar i maksymalizację zysków.



Trzecia edycja *Poradnika (nie)romantycznego UKE* powstała, ponieważ w świecie, gdzie „kocham cię” może napisać bot, a Twoje zdjęcie profilowe jest analizowane przez AI pod kątem zdolności kredytowej, **musimy uzbroić się w wiedzę, odrobinę cynizmu i bardzo silne hasła.**

Epizod I

Aplikacje i portale randkowe

W radiu Leonard Cohen swoim barytonem śpiewa *Dance Me to the End of Love*, a ciotka Maryla po trzech rozwodach, znów na Wigilii pytała, kiedy przyprowadzisz jakąś dziewczynę. Więc postanawiasz poszukać partnerki lub partnera do uprawy ogródka i konsumpcji wigilijnego barszczu.

Co robisz? Rejestrujesz się w aplikacji randkowej.

Masz duży wybór, bo w sieci znajdziesz wiele portali randkowych.

Są popularne aplikacje dostępne na urządzenia mobilne, portale dla różnych grup wiekowych czy skierowane do osób o określonych preferencjach.

Znajdziesz aplikacje i serwisy randkowe kierowane do szerokiego grona użytkowników i te wyspecjalizowane, koncentrujące się na konkretnych potrzebach, np. kojarzeniu par według rasy, religii, wykształcenia, poglądów oraz oferujące dopasowanie do orientacji seksualnej.

Portale i aplikacje oferują podstawowe wersje bezpłatne oraz płatne opcje rozszerzone i pakiety premium. Większość serwisów działa na podobnej zasadzie, a sama rejestracja często jest bezpłatna. Do założenia konta wystarczy wprowadzić podstawowe dane o sobie, ustawić login oraz hasło. Część aplikacji umożliwia rejestrację i logowanie za pośrednictwem portalu społecznościowego. Wybierając taką opcję zezwalasz na dostęp i wykorzystywanie informacji z Twojego konta na danym portalu społecznościowym.



Krok 1 | wybierasz aplikację lub portal

Sprawdź czy ma określony regulamin korzystania z usług

Jeśli na stronie portalu nie znajdziesz regulaminu, nie korzystaj z tego portalu. W regulaminie znajdziesz m.in. informacje o warunkach korzystania z portalu/aplikacji, warunki rozwiązywania umowy, szczegóły dot. subskrypcji, informacje o płatnościach i ograniczeniu odpowiedzialności podmiotów.

Pobieraj aplikacje tylko z legalnych źródeł

Jeśli inni użytkownicy wypowiadają się o aplikacji pozytywnie, a liczba pobrań jest wysoka można przejść do jej instalacji. **Aplikacje pobieraj wyłącznie z legalnych źródeł. Unikaj portali, gdzie nie ma podanych danych kontaktowych podmiotu prowadzącego serwis randkowy.**

Wpisanie imienia, wieku w formularzu i wrzucenie zdjęcia przerobionego przez siedem filtrów, na którym wyglądamy o dziesięć lat młodziej, to moment, w którym podpisujemy cyfrowy cyrograf.

Według raportu Mozilla Foundation *Privacy Not Included 2024*, aplikacje randkowe i romantyczne chatboty AI nie dbają o naszą prywatność¹.

Mozilla przetestowała 25 najpopularniejszych aplikacji i 22 z nich otrzymało ostrzeżenie *Privacy Not Included*². To trochę tak jakby pani w markecie zapytała przy kasie o Waszą orientację seksualną, poglądy polityczne, historię chorób i czy w dzieciństwie lubiliście szpinak, skoro macie go w koszyku.

A potem Waszą historię sprzedała koleżance z innego marketu.

Aplikacje zbierają wszystko. Waszą lokalizację, preferencje (im dziwniejsze, tym cenniejsze dla algorytmu), a nawet to, jak długo zatrzymujecie wzrok na zdjęciu. Jeśli myślicie, że „prywatność” istnieje, to jesteście w większym błędzie niż pewien konsument, który oczekiwał, że UAE na jego żądanie wyłączy internet na całym świecie (uważał, że ma ku temu powód). W temacie przetwarzania danych przypomina mi się cytata dr. Michała Kosińskiego z wywiadu dla *Sztucznej Inteligencji*: „Wojnę o prywatność już przegraliśmy. To, że polubiłaś jakąś restaurację albo zdjęcie twojego bratanka, może zdradzić twoją płć, rasę, orientację seksualną, poglądy polityczne i religijne, cechy twojej osobowości”³.

Pamiętaj: to, co wpiszesz w formularzu, tam zostaje. Nawet jeśli napiszesz, że „szukasz tylko przyjaźni”, algorytm i tak wie, co klikasz. On nie ocenia moralnie, on gromadzi dane.

¹ [Romantic AI Chatbots Don't Have Your Privacy at Heart](#)

² [Dating Apps | Privacy & Security Guide | Mozilla Foundation](#)

³ [Michał Kosiński: Wojnę o prywatność już przegraliśmy – Sztuczna Inteligencja](#)

Krok 2 | zabezpiecz się (także cyfrowo)

Stwórz silne hasło

123456, Hasło!, Zbyszek123, Pusia12, 14.02.2025 itp. to nie są silne hasła. To zaproszenia do włamania, wypisane ozdobną czcionką na stronie logowania.

Obecnie o sile hasła decyduje głównie jego długość, ale potrzeby się zmieniają. Używaj dużych i małych liter, cyfr i znaków specjalnych, ale unikaj najpopularniejszych kombinacji typu „!” zawsze na końcu. Nie podawaj w hasło swojego imienia czy daty urodzenia. Pamiętaj, że nie powinno ono być takie jak login.

Im dłuższe i bardziej skomplikowane hasło, tym trudniej będzie je złamać. Używaj menadżerów haseł i dwuskładnikowego logowania. Jeśli Twoje konto zostanie przejęte, to historia rozmów o „głębokim porozumieniu dusz” trafi w ręce kogoś, kto użyje jej do szantażu szybciej, niż zdążysz powiedzieć „to nie tak, jak myślisz, kotku”.



szukam tylko przyjacieli...

Krok 3 | Uśmiechnij się, pokaż zęby - AI patrzy i analizuje

Wybierz neutralne pytania

Wstawiając zdjęcia na swój profil zwróć uwagę, aby nie pokazywały żadnych identyfikujących szczegółów, np. z nazwą ulicy w tle czy numerem domu. **Nie publikuj intymnych zdjęć i nie przysyłaj takich zdjęć innym użytkownikom serwisów.**

Zdjęcie to nie tylko obrazek. To pakiet metadanych. Sztuczna inteligencja jest wykorzystywana przez niektóre aplikacje randkowe do rozpoznawania twarzy i dopasowywania użytkowników na podstawie cech fizycznych⁴. Systemy AI wbudowane w aplikacje nie tylko sprawdzają, czy nie jesteście botem. One coraz częściej analizują tło. Widzą Twój samochód, markę sprzętu w kuchni i zegarek na nadgarstku. **To nie jest randkowanie, to jest inwentaryzacja zasobów finansowych.**

⁴ [Online Dating Industry Statistics: Market Data Report 2026](#)

Nie publikuj intymnych zdjęć i nie przesyłaj takich zdjęć innym użytkownikom serwisów

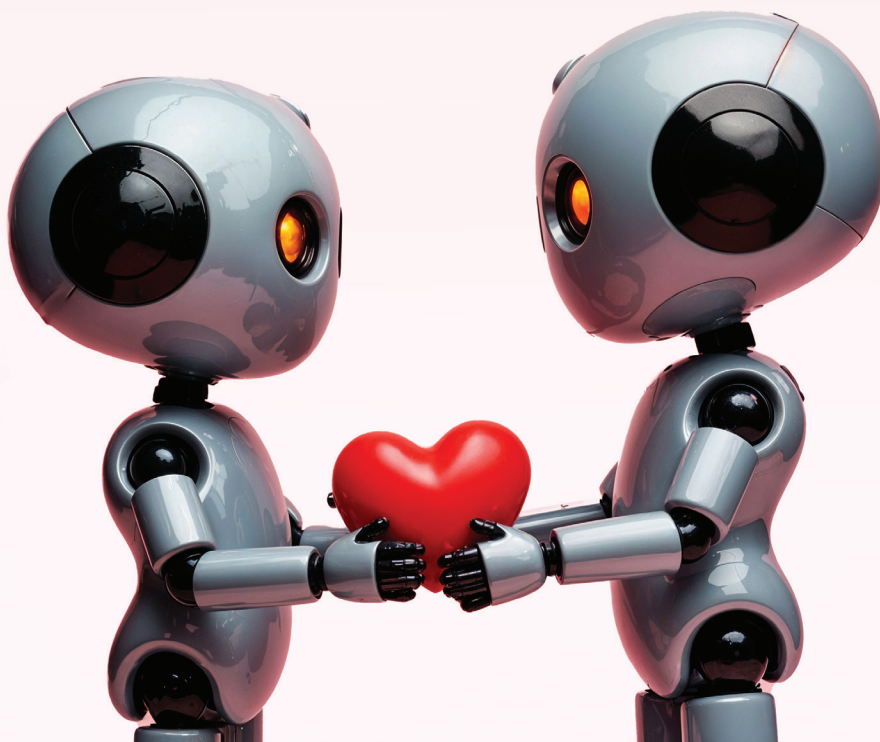
Cyberflashing to wysyłanie nieprzyzwoitych zdjęć swojego nagiego ciała, zwłaszcza narządów płciowych, komuś kogo nie znamy, i kto tego nie chce, często za pośrednictwem transferów Bluetooth lub AirDrop. Przykładowo aplikacja Bumble wykorzystuje AI do wykrywania i rozmycia nieproszonych obrazów z dokładnością do 98%⁵.

W Polsce nie ma przepisów klasyfikujących wprost cyberflashing, jedynie przepisy dotyczące treści pornograficznych: **art. 202 §1 kodeksu karnego - kto publicznie prezentuje treści pornograficzne w taki sposób, że może to narzucić ich odbiór osobie, która tego sobie nie życzy, podlega karze pozbawienia wolności do lat 3.**

Materiały mają charakter pornograficzny w rozumieniu art. 202 kodeksu karnego, gdy treścią prezentacji w tych materiałach jest przedstawienie przejawów płciowości i życia seksualnego człowieka, które koncentruje się wyłącznie na pokazaniu jego techniczno-biologicznych aspektów (z pominięciem jakiegokolwiek warstwy intelektualno-personalistycznej) i zawiera ukazanie narządów płciowych w ich seksualnych funkcjach, jeśli jedyną intencją twórcy tych materiałów było wywołanie podniecenia seksualnego u odbiorcy przekazu⁶.

⁵ [Online Dating Industry Statistics: Market Data Report 2026](#)

⁶ Wyrok Sądu Apelacyjnego w Poznaniu - II Wydział Karny z dnia 24 maja 2012 r., II Aka 75/12



Krok 4 | Polityka prywatności (może to powinien być krok 1, ale kogo chcemy oszukać)

Kto z Was czyta polityki prywatności tych aplikacji? Zapewne cieszą się takim samym zainteresowaniem jak regulaminy. A potem krzyk i oburzenie - skąd oni mają moje dane? Pamiętacie słynne oświadczenia użytkowników serwisów społecznościowy w stylu: „Nie upoważniam Marka Z., ani żadnej organizacji współpracującej z F/M do korzystania z moich obrazów, zdjęć, postów (...) Treść tego profilu jest informacją prywatną i poufną...”? I tu daję Wam trzy minuty na opanowanie ataku śmiechu. Stopień niewiedzy nie przestaje zaskakiwać.

Większość aplikacji randkowych zastrzega sobie prawo udostępniania danych „podmiotom trzecim”. Kim są te podmioty? To głównie reklamodawcy, firmy analityczne, a w skrajnych przypadkach brokerzy danych. Masz doła, w sieci przeglądasz profile adwokatów rozwodowych, to idealny moment by podsunąć Ci reklamę cudownego suplementu na chandrę czy czekoladek, które zawsze poprawią humor.

W Polsce teoretycznie mamy prawo do bycia zapomnianym. Pozwala ono na usunięcie danych osobowych z baz tworzonych przez wszelkie podmioty dysponujące danymi osobowymi. Zgodnie z art. 17 RODO osoby, których dane są przetwarzane mają prawo do zgłoszenia administratorom danych osobowych żądania ich bezzwłocznego usunięcia.

W praktyce usunięcie konta w aplikacji to dopiero początek drogi przez mękę. Dane krążą w ekosystemie reklamowym jeszcze długo po tym, jak odinstalujesz aplikację.

Indywidualne konto

Nie loguj się do konta w aplikacji randkowej przy użyciu profili założonych np. na Facebooku czy Google. W ustawieniach prywatności zablokuj dostęp do danych ze smartfona wszędzie tam, gdzie jest taka możliwość, np. aparat, książka adresowa, lokalizacja. Zakładaj konto na mailu, który nie jest Twoim głównym, powiązanym np. z kontem bankowym ani służbowym.

Zasada ograniczonego zaufania

Ogranicz do minimum przekazywanie wrażliwych informacji na swój temat programom i aplikacjom randkowym. Nie dziel się szczegółami z życia z botami. Aplikacje służące do ulepszania profili na portalach randkowych, czy generowania „lepszych” wiadomości, to narzędzia często wykorzystywane przez cyberoszustów.

Krok 5 | Trzymaj się za cyfrowy portfel, czyli subskrypcja na miłość

Większość aplikacji randkowych oferuje bezpłatną instalację. Możesz przesuwac zdjęcia w lewo i prawo, póki nie rozboli Cię kciuk, ale jeśli chcesz czegoś więcej – płacisz. **Aplikacje oferują konta lub opcje rozszerzone/premium. Pozwalają one korzystać użytkownikom z dodatkowych możliwości, np. niewidoczny profil, który pozwala na sekretne przeglądanie innych profili, lepsze dopasowanie itd.** Konta premium zazwyczaj są oparte o subskrypcje i mają różne koszty w zależności od wybranego wariantu. Chcesz poczuć się wyjątkowo? Możesz przystąpić do elitarnego klubu płatników. Gwarancji znalezienia tego lub tej jedynej nie masz, za to możesz zapłacić równowartość raty kredytu hipotecznego, żeby algorytm łaskawiej na Ciebie spojrział.

Przykłady:

- **Tinder Select** – to „Elitarny Klub dla Naiwnych”. Cena Tinder Select? Koszty poznasz dopiero, gdy zostaniesz zakwalifikowany do klubu. Wiadomo jednak, że członkostwo Tinder Select można łączyć z subskrypcjami Tinder Plus, Gold lub Platinum.
- **Bumble Premium+ i inne „udogodnienia” typu *Spotlights*** (płatna widoczność) i ***Compliments*** (płatne komplementy)⁷. Tak, nawet miłe słowo ma swoją cenę rynkową.

⁷ [Compliments](#) | [Jak wysłać Compliment](#) | Bumble

STUDIUM PRZYPADKU

Wiktor, lat 42, świeżo upieczony singiel z nadmiarem gotówki, bo w 2025 r. jako stolarz wykonał trzy kuchnie na wymiar. Nadmiarowi gotówki towarzyszył deficyt pewności siebie, więc wykupił Tinder Select. Przez miesiąc nie dostał ani jednej odpowiedzi. Dlaczego? Bo żadne dolary nie zastąpią umiejętności prowadzenia rozmowy ciekawszej niż: „Hej, co tam?”. Jediną „osobą”, która do niego napisała, był bot z Azji Południowo-Wschodniej, próbujący namówić go na inwestycję w kryptowaluty. NIE BĄDŹ JAK WIKTOR!

Nie nabieraj się na opcje premium

Zanim wstąpisz do elitarnego klubu wypróbuj podstawowe opcje portali i aplikacji randkowych. Co Ci da „lepsze dopasowanie” skoro i tak wszyscy kłamią w opisach, a barwne, błyskotliwe historie przygotowuje AI? „Bolało, gdy spadałaś z nieba?” nie zadziała, gdy spotkacie się w realu. O ile się w ogóle poznacie bez filtra...

Sprawdź warunki i koszty subskrypcji

W przypadku wykupienia automatycznie odnawialnej subskrypcji, opłata będzie pobierana za pośrednictwem wybranej metody płatności do momentu jej anulowania. **W regulaminie powinieneś znaleźć szczegółowe instrukcje jak zmienić lub zakończyć subskrypcję.** Automatyczne odnawianie subskrypcji to standard. Nie odhaczyłeś ptaszka w trzecim podmenu w siedemnastej zakładce wielkości ziarnka ryżu? Twoja karta kredytowa zostanie obciążona ponownie. Regularnie sprawdzaj listę wszystkich aktywnych subskrypcji. To może zaoszczędzić Ci setki złotych na usługi, o których dawno zapomniałeś.

Usunięcie konta

Odinstalowanie aplikacji nie oznacza usunięcia konta. Przy rejestracji podajemy nasz adres e-mail i możemy się zalogować na konto z innego urządzenia. Dlatego, **gdy chcesz zakończyć przygodę z randkowaniem online, przejdź do ustawień danej aplikacji i usuń konto zgodnie z instrukcją.** Są też aplikacje, które stosują tzw. „dark patterns”. Usunięcie aplikacji z telefonu nie przerywa subskrypcji. Subskrypcja jest przywiązana do Twojego konta w Google Play lub Apple App Store. Aby z niej zrezygnować, musisz przejść przez siedem kręgów piekielnych. O wiele szybciej skręcisz regał z IKEA.

Nie odhaczyłeś ptaszka w trzecim podmenu w siedemnastej zakładce wielkości ziarnka ryżu? Twoja karta kredytowa zostanie obciążona ponownie.



Epizod II

AI w branży randkowej – przyjaciel czy wróg

W ubiegłym roku pisałam, że część firm już korzysta lub testuje funkcje sztucznej inteligencji, np. do selekcji zdjęć lub do wspierania algorytmów wyświetlania poszczególnych profili użytkowników osobom, które mogą być nimi zainteresowane. Czas porzucić złudzenia, teraz robią to już wszyscy liczący się na rynku gracze. Jeśli ktoś odpisuje Wam na wiadomość o trzeciej rano, używając nienagannej polszczyzny i wykazując się błyskotliwością godną Oscara Wilde’a, to z prawdopodobieństwem graniczącym z pewnością rozmawiacie z algorytmem. I ten algorytm prawdopodobnie ma o wiele ciekawsze życie wewnętrzne niż my wszyscy razem wzięci.

Trochę statystyk na początek (z obcego podwórka, ale my jesteśmy światowi):

47%

dorosłych w USA deklaruje, że korzysta z narzędzi AI do pisania swoich bio

51%

randkujących online uważa, że algorytmy są niezbędne do filtrowania dopasowań

1,6 mld

przesunięć dziennie generuje Tinder dzięki algorytmom dopasowania AI⁸

Sztuczna inteligencja weszła do aplikacji randkowych na dobre i przejęła władzę. To AI wybiera Ci kandydata, który w teorii powinien spełnić Twoje najskrytsze fantazje. Zanim jednak pomyślisz by uciekać przed technologią do bieszczadzkiego lasu (co też ma swoje ryzyka, głównie kleszcze), przyjrzyjmy się tej nowej, cyfrowej rzeczywistości.

Twój randkowy asystent, czyli narodziny *Rizz apps*

RIZZ

Siedzisz przed ekranem, gapiąc się na zdjęcie kogoś, kto wygląda jak bóstwo z Twoich marzeń, a jedyną rzeczą, jaką umiesz wykrzesać jest błyskotliwe: „Hej, jak tam?” **Tu na scenę wkraczają tak zwane Rizz apps, czyli asystenci randkowi, których zadaniem jest pomaganie użytkownikom w flirtowaniu i podtrzymywaniu rozmów.** Nazwa pochodzi od słowa charisma, które dzisiejsza młodzież skróciła, bo pełne słowa są najwyraźniej zbyt męczące dla kciuków. Asystenci w cyfrowej przestrzeni zmieniają Cię w charyzmatycznego, pełnego uroku poliglotę, przy którym Pan Darcy wypada blado.

Mechanizm jest prosty jak konstrukcja cepa: robisz zrzut ekranu profilu, rozmowy lub opisu swojej ofiary... przepraszam, wybranki lub wybranka, wrzucasz do aplikacji korzystającej z AI, a ta generuje Ci propozycje zagajenia, gotowe teksty na podryw lub np. cięte riposty.

Możesz mieć wersję dowcipną, intelektualną, romantyczną, co tylko chcesz. Z takim wsparciem ogranicza Cię tylko Twoja wyobraźnia. Zaawansowane algorytmy uczą się stylu komunikacji użytkowników, aby generowane wiadomości brzmiały naturalnie i pasowały do poczucia humoru.

Same zalety? Dla właścicieli tych aplikacji i ich zysków tak, dla użytkowników tylko pozorne. Matchmaking staje się płynniejszy, rozmowy błyskotliwe, a wskaźnik frustracji spada. Tylko **jeśli on używa AI do pisania wierszy, a ona używa AI do ich interpretowania, to w rzeczywistości mamy do czynienia z randką dwóch serwerowni w Iowa (przykładowo), które zużywają gigantyczne ilości prądu i wody.** Tymczasem przed ekranem smartfona dwoje ludzi zastanawia się, skąd w nich nagle taki polot i są gotowi uwierzyć, że to przecież ich własny potencjał, który dotąd pozostawał w ukryciu.

Inwazja botów – *dobry i zły bot*

Boty to idealni pracownicy. Nie śpią, nie chorują, nie mają fochów, utrzymują „zaangażowanie użytkownika” i nie trzeba za nich płacić ZUS-u.

Wykorzystanie botów w aplikacjach randkowych można podzielić na dwie główne kategorie:

- **Wsparcie i optymalizacja, czyli boty „dobre”**

Do tej kategorii zaliczamy wyżej opisanych asystentów randkowych AI i wszystkie rodzaje botów służących do wsparcia technicznego.

- **Oszustwa i wyłudzenia, czyli boty „złe”**

W tej kategorii mamy boty do wyłudzenia danych i phishingu. W skrócie: fałszywe profile, sterowane przez gotowe skrypty, nawiązujące znajomości, a następnie podsyłające podejrzaną linki lub wyłudzające dane osobowe, np. pod pozorem „weryfikacji”. Mamy też boty, które masowo wysyłają wiadomości reklamujące strony dla dorosłych lub platformy inwestycyjne. Kilka kroków i możesz być akcjonariuszem spółki z wysoką dynamiką przychodów i znaczącym wzrostem wartości portfela.

Plotka głosi, że aplikacje randkowe wykorzystują też AI do stymulowania ruchu. Jeśli algorytm widzi, że od trzech dni nikt do Ciebie nie napisał i zaczynasz myśleć o odinstalowaniu aplikacji, nagle pojawia się „Ania, 28 lat, miłośniczka podróży”, która pyta, jak Ci minął dzień. Ania nie istnieje. Ania jest zbiorem danych, który ma Cię zatrzymać w aplikacji na kolejne dziesięć minut, żebyś zdążył zobaczyć trzy reklamy kredytu gotówkowego.



AI-profilowanie: atrakcyjność w oczach kalkulatora

Ocena koni na targu obejmuje budowę anatomiczną, stan kopyt, chód i kondycję w skali BCS. Ty w aplikacji randkowej jesteś trochę jak ten koń. **Algorytmy nie tylko łączą ludzi na podstawie hobby. One oceniają Twoją „atrakcyjność”. AI analizuje dane użytkowników, aby poznać ich preferencje i cechy osobowościowe.** W praktyce ma to służyć temu, byś otrzymał spersonalizowane rekomendacje, które zwiększają szanse na udane połączenie z bratnią duszą w kosmosie. Najpopularniejsze aplikacje korzystają z AI do analizy czasu jaki spędzasz na przeglądaniu profili czy częstotliwość interakcji z innymi użytkownikami. Dzięki tym danym, AI jest w stanie przewidzieć, które profile będą dla Ciebie najbardziej interesujące. Wykorzystując techniki uczenia maszynowego, algorytmy są w stanie uczyć się na podstawie wcześniejszych interakcji, co pozwala im na ciągłe doskonalenie swoich rekomendacji.

Algorytmy są na tyle dobre, jak dobre są dane, na których są trenowane. Jeśli te dane zawierają błędy, uprzedzenia lub stereotypy społeczne, algorytmy będą je powielać. Przykładowo, jeśli dane dotyczące preferencji użytkowników wskazują na dominację pewnych cech, np. rasa czy wiek, algorytmy mogą faworyzować te cechy kosztem innych grup. W takiej sytuacji mimo, że czujesz się jak mustang na prerii, to masz dużo mniejsze szanse w rankingu, który preferuje konie fryzyskie. AI decyduje, w której „lidze” grasz. Jeśli algorytm uzna Cię za „trójkę”, to nie pokaże Ci „dziesiątki”, chyba że zapłacisz za Tinder Select ;-)

To jest cyfrowa segregacja, prowadzona przez bezduszne procesory, które nie mają pojęcia o tym, że masz świetne poczucie humoru i robisz najlepsze pierogi na wschód od Wisły.

AI w randkach to potężne narzędzie, które może nam pomóc wyjść z cyfrowego cienia. **Jednak w świecie, gdzie 60% osób podejrzewa interakcję z botem, naszą największą bronią staje się... autentyczna niedoskonałość.**

STUDIUM PRZYPADKU

Poznajcie Jaśminę. Jaśmina jest poczciwą dziewczyną, ale flirt nigdy nie był jej mocną stroną. Postanowiła więc użyć AI-asystenta, by uwieść Alana. Asystent spisał się świetnie – Alan był zachwycony „głębią intelektualną” Jaśminy i szerokim wachlarzem jej zainteresowań. Do czasu pierwszej randki w kawiarni. Kiedy Jaśmina zamiast cytować egzystencjalistów, zaczęła narzekać na ceny w markecie, sąsiadkę z trzeciego piętra i mlaskać przy jedzeniu szarlotki, Alan zrozumiał jedno: Jaśmina nie ma „Rizzu”. Randka skończyła się po 10 minutach i telefonie ratunkowym od kumpla. Jaśmina to jednak twarda zawodniczka, nie poddaje się łatwo. Postanowiła zawalczyć o uwagę wybranka i wysłała Alanowi zdjęcia prezentujące jej...atrybuty.

NIE BĄDŹ JAK JAŚMINA!



Epizod III

Deepfaki: kiedy zmysły przestają być naturalnym firewallem

Jeśli myśleliście, że wideorozmowa to ostateczny dowód na to, że Wasz interlokutor nie jest „hakerem w kapturze”, to mam dla Was złą wiadomość. Witamy w erze deepfake’ów. Technologia sprawiła, że stare przysłowie: „uwierzę, jak zobaczę na własne oczy” nadaje się dziś do lamusa. Dziś już nie masz gwarancji, że to co widzisz i słyszysz w internecie jest prawdziwe. Możesz widzieć twarz, którą znasz, słyszeć znany Ci głos i to wcale nie będzie ta osoba, tylko sklonowany technologiczny twór, wykorzystywany przez internetowych oszustów. Co mają deepfaki do poradnika (nie)romantycznego? Otóż coraz częściej są wykorzystywane w oszustwach romantycznych i do szantażu seksualnego.

Jak to się zaczęło

Technologia deepfake pojawiła się już w 2015 r. w Hollywood. W filmie *Szybcy i wściekli* wykorzystano technikę syntezy głosu i nałożenia cyfrowej maski. Dzięki temu na wielkim ekranie mogliśmy zobaczyć zmarłego Paula Walkera w roli Briana O’Connera. Historia z nazwą zaczęła się w 2017 r., kiedy na portalu Reddit użytkownik o pseudonimie *deepfakes* uznał, że świat byłby lepszym miejscem, gdyby twarze znanych aktorek „dokleić” do ciał pań występujących w filmach, powiedzmy, mało edukacyjnych. Wtedy było to prymitywne i nie przypominało nawet filmów kategorii B, a zwykły użytkownik, mający prędkość internetu do 10 Mb/s, nawet o takich dziwach nie słyszał. **W 2026 r. doszliśmy do momentu, w którym prawie każdy może stworzyć film, na którym dowolna osoba mówi dowolne bzdury i nie będzie to trudniejsze niż założenie skrzynki do e-doręczeń.**

Jak to działa

Deepfaki to syntetyczne obrazy, filmy i dźwięki wygenerowane przy użyciu sztucznej inteligencji przedstawiające osoby, rzeczy i sytuacje, które nie istnieją lub się nie wydarzyły. To treści, które zostały zmanipulowane. **Deepfaki są tworzone przez algorytmy na podstawie prawdziwych zdjęć, filmów czy próbek głosu.**

Kiedyś wiadomości od „amerykańskiego żołnierza”, „brytyjskiej pielęgniarki” czy „nigeryjskiego księcia” mogliśmy poznać po oczywistych kłamstwach, niechęci do rozmów wideo i błędach ortograficznych. Chociaż w przypadku błędów ortograficznych mamy do czynienia z dwiema przyczynami, pierwsza - słaby translator, druga - brak uwagi na lekcjach języka polskiego w szkole podstawowej. **Oszustwa romantyczne weszły na wyższy poziom, od kiedy AI może wygenerować obraz i dźwięk.**

Dziś oszust może Cię zaczepić na dowolnym portalu, może być wirtualną postacią z wiarygodną twarzą, głosem, skrupulatnie zbudowaną historią i wciągnąć Cię w internetowy romans, który skończy się próbą wyłudzenia pieniędzy.

Technikalia

Zaawansowane deepfaki są najczęściej tworzone przy użyciu Generative Adversarial Networks (GANs). GAN składa się z dwóch sieci neuronowych, które działają przeciwko sobie, aby ulepszać rezultaty. Wyobraź sobie, że wewnątrz komputera siedzi dwóch genialnych oszustów.

- **Oszust pierwszy (Generator):** To taki cyfrowy Hagen, który maluje współczesną *Damę z łasiczką*. Bierze tysiące zdjęć damy z Instagrama (tych z dziubkiem i bez dziubka, z siłowni, z kotłowni, z kawiarni, bawialni, w pociągu, w przeciągu itd.) i próbuje stworzyć jej cyfrową kopię.
- **Oszust drugi (Dyskryminator):** To taki krytyk sztuki, który niczym Barbara Sykalska dostrzeże dodatkowy wąż u łasiczki. Patrzy na dzieło Hageny Generatorsa i mówi: „Nie, nie jest podobna, oczy są martwe, dwie piersi by wystarczyły, ta trzecia jest zbędna, a lewe ucho wyrasta z nosa. Popraw!”



Aby stworzyć przekonujący wideo deepfake danej osoby, AI do niedawna potrzebowała godzin materiału pokazującego daną osobę podczas mówienia, poruszania się i wyrażania emocji. W przypadku audio deepfake'ów system musiał być trenowany na nagraniach głosu w różnych tonach i kontekstach. Po takim treningu algorytmy mają lepszą formę niż Usain Bolt u szczytu kariery i mogą generować treści tak realistyczne, że potrafią one oszukać nie tylko użytkownika portalu randkowego, ale nawet niektóre systemy biometryczne. Skuteczny, ale dość drogi proces. Jeszcze.

Inne popularne techniki tworzenia deepfake'ów to m.in.:

- **Sieci nadawcze** – modele AI generują obrazy i filmy poprzez dodawanie i usuwanie cyfrowego „szumu”, tworząc nowe twarze na podstawie oryginalnych danych.
- **Zamiana twarzy, czyli technika podmiany twarzy**, polegająca na nałożeniu twarzy jednej osoby, na twarz innej osoby na obrazie lub w filmie. Im więcej obrazów i ujęć zostanie użytych do wytrenowania modelu, tym bardziej wiarygodny będzie rezultat.
- **Synchronizacja ust** – technika dostosowująca ruchy ust i głosu do wybranej mowy. Bardzo skuteczna w połączeniu z syntetycznym głosem. Do tego oszuści nie potrzebują komputera niczym z laboratorium NASA, istnieją aplikacje mobilne, które umożliwiają tworzenie filmów deepfake w zaledwie kilka minut. Jakość i realizm są lepsze dzięki połączeniu większej liczby obrazów referencyjnych z lepszym sprzętem.

Podsumowując, wystarczy kilka zdjęć, kilka filmów z serwisów społecznościowych, próbka głosu, by stworzyć cyfrowy awatar, który wyrecytuje *Pana Tadeusza*, poleci znajomym na fejsie inwestycję, zatańczy na rurze w filmie dla dorosłych albo poprosi Waszą babcię o kod BLIK. **Przyszłość wygląda jeszcze gorzej, bo już są testowane deepfake'i głosu generowane w czasie rzeczywistym⁹.**

Historia kobiety, którą uwiódł fałszywy Brad Pitt, obiegła cały świat. Oszust może wyglądać jak hollywoodzki aktor, mieć idealnie zsynchronizowane ruchy warg i mrugać z wdziękiem, podczas gdy w rzeczywistości jest to zorganizowana grupa przestępcza z biurem w odległym zakątku świata.

⁹ [Voice Impersonation and DeepFake Vishing in Realtime | NCC Group](#)

Deepfake Porn i Sextortion: Gdy intymność staje się bronią

Tu kończą się żarty. **Jednym z najgorszych zastosowań AI jest tzw. non-consensual deepfake pornography. Jest to rodzaj syntetycznej pornografii wytworzonej przez modyfikację istniejących zdjęć lub wideo.** Oszust bierze Twoje zdjęcia z portalu randkowego lub serwisu społecznościowego i wrzuca je do algorytmu „undressing AI”. Problemem nie jest już wyciek intymnych zdjęć, wystarczą te zwykłe, w sukience, w garniturze, w świątecznym swetrze. Algorytm „domyśla się”, co jest pod ubraniem (bazując na tysiącach innych zdjęć, więc efekt nie ma nic wspólnego z rzeczywistością) i tworzy spreparowany pornograficzny materiał wykorzystujący Twój wizerunek bez Twojej zgody. Potem dostajesz wiadomość: „Mam Twoje nagie zdjęcia. Jeśli nie przelejesz 5000 zł w kryptowalutach, wyślę je do Twojego szefa, matki i wszystkich znajomych na Facebooku”. Ofiarami tego procederu padają już nie tylko celebryci, ale zwykli użytkownicy aplikacji randkowych. Nawet jeśli ofiara udowodni, że materiał jest fałszywy, trauma pozostanie.

Gdyby szantaż był dyscypliną olimpijską, to walka o medale byłaby zacięta.

Psychologia strachu

Klasyczny sextortion polega na tym, że ofiara, omamiona obietnicą wielkiej miłości lub chociażby upojnego kwadransa, wysyła swoje zdjęcie w stroju Adama lub Ewy. Po czym „druga połówka” pokazuje swoje prawdziwe intencje i pisze: „płać, albo...”. Rozwój technologii, w tym deepfake, napędza ten rodzaj przestępczości. To już jest proceder zautomatyzowany. Boty AI generują tysiące wiadomości szantażujących naraz. Dostajesz na skrzynkę maila w stylu: „Widziałem, co robisz przed kamerką. Mam nagranie”. **Nawet jeśli nigdy nie włączyłeś kamerki, a przed komputerem siedzisz wyłącznie w starym dresie, ziarno niepokoju zostaje zasiane.** A może ktoś się włamał? Czy zawsze mam zasłoniętą kamerkę? A co jeśli faktycznie mają jakieś moje kompromitujące nagrania? A co jeśli je spreparowali i nikt mi nie uwierzy, że to nie ja. **Co robisz?**

***Czy zawsze mam zasłoniętą kamerkę?
A co jeśli faktycznie mają jakieś moje
kompromitujące nagrania?***



STUDIUM PRZYPADKU

Pan Maurycy, lat 52, dyrektor działu logistyki w dużej firmie (człowiek z natury uporządkowany), poznał w sieci piękną „Anastazję”. Anastazja była modelką, która, tu zaskoczenie, pasjonowała się logistyką i optymalizacją łańcucha dostaw. Po dwóch tygodniach wymiany wiadomości, Anastazja zaproponowała wideorozmowę na WhatsAppie. Był tylko jeden haczyk: Anastazja była cnotliwą, wstydliwą kobietą i poprosiła Maurycyego, by ten, by ją ośmielić, pokazał jej „całego siebie”. Maurycy, pod wpływem emocji i koniaku, spełnił prośbę. Nie wiedział, że „Anastazja” to deepfake, a całe nagranie było rejestrowane.

10 minut po zakończeniu rozmowy Maurycy dostał link i wytyczne co dalej. Zobaczył tam siebie w pełnej krasie, obok zdjęcia ze swoją żoną na wakacjach w Egipcie i linku do profilu swojej firmy na LinkedIn. Do tego krótka acz jakże treściwa wiadomość: „10 000 euro do jutra, albo zapraszamy na premierę”. Maurycy niejedną „Anastazję” już w sieci poznał, więc zamiast biec do banku, nie zapłacił. Zamiast tego zablokował konta i zgłosił sprawę na policję. Czy film wyciekł? Nie. Szantażysta nie tracił czasu na kogoś, kto nie płaci. Miał w kolejce stu innych Maurycych.

Pierwszą poradą gwarantującą względne bezpieczeństwo cyfrowe, jaka przychodzi mi do głowy, jest wyrzucenie telefonu i laptopa do Wisły i zamieszkanie w jaskini. Wiem, słaba ta rada. Więc pamiętaj chociaż o tych bardziej standardowych, które przynajmniej pozwolą ograniczyć ryzyka.

Dobre rady

- **Ogranicz do minimum udostępnianie danych**

Tu się powtarzam, ale to jest podstawa. Wręcz może świadczyć o Twojej atrakcyjności, w czasach gdy influencerki i influencerzy relacjonują już wszystko, począwszy od porodu. Czekamy jeszcze na streaming z „zejścia z tego łez padołu”. Zakład Pogrzebowy Bytom lubi to.

- **Nie wysyłaj niczego, czego nie pokazałbyś na billboardzie przy autostradzie**

Internet nie zapomina. Internet jest jak złośliwa sąsiadka, która pamięta Twoje błędy z 1997 roku i wypomni Ci je przy najbliższej okazji.

- **Zanim zaangażujesz się w relację i wyślesz zdjęcia lub udzielisz pożyczki, zrób rekonesans w sieci i sprawdź z kim masz do czynienia:**

- Sprawdź, czy ma konta w innych serwisach, portalach;
- Sprawdź jak długo ma konto i co na nim jest;
- Sprawdź zdjęcia, np. za pośrednictwem zwykłej wyszukiwarki. Skoro przy pomocy obiektywu Google potrafisz znaleźć ekonomiczną wersję lampki nocnej, która przypłynie do Ciebie z Azji, to i z tym sobie poradzisz;
- Sprawdź metadane za pomocą dostępnych narzędzi czy zdjęcia nie są wygenerowane przez AI;
- Weryfikuj rozmówcę „testem ruchu”. Deepfake w czasie rzeczywistym często „gubi” ostrość lub twarz na ułamek sekundy zmienia się w pikselozę;
- Na chłodno zweryfikuj spójność historii rozmówcy. Zwracaj uwagę na niuanse. To przyda się nie tylko przy ochronie przed nigeryjskim łowcą majątków, ale i przed polskim tulipanem.

- **Nie lekceważ red flagów** (określenie sygnałów ostrzegawczych)

Jeśli w wątku przyjacielsko-romantycznym pojawiają się kwestie finansowe, prośby o pożyczkę, propozycje inwestycji albo naciski o utrzymanie znajomości w tajemnicy, to zakończ relację natychmiast i bezdyskusyjnie. Blokuj, urywaj kontakt, nie reaguj na wiadomości.

- **Myśl! Nie wierz w ideały**

Jeśli ktoś jest piękny, bogaty, romantyczny i zbyt chętny, by z Tobą rozmawiać o 4 rano – prawdopodobnie jest zasilany prądem stałym.

Co zrobić, gdy Cię szantażują

- **Nie płać!** Nigdy. Szantażysta nie kasuje materiałów. On tylko odnotowuje w Excelu: „Ofiara nr 482 – płaci, skłonny/a do współpracy, dość dalej”.
- **Zrób zrzuty ekranu.** Zachowaj dowody (rozmowy, linki, żądania okupu, zrzuty profilu, zdjęcia, całą historię).
- **Zerwij kontakt.** Zablokuj szantażystę na wszystkich kanałach komunikacji.
- **Zgłoś sprawę na policję.** Szantaż to przestępstwo.
- **Poszukaj pomocy!** Porozmawiaj z kimś bliskim lub skorzystaj z telefonów zaufania.

Jak na urząd przysłało, dodaję paragrafy, które mogą Ci pomóc:

Kodeks karny określa przestępstwa przeciwko wolności oraz oszustwo i oszustwo komputerowe:

art. 190 § 1 kodeksu karnego: Kto grozi innej osobie popełnieniem przestępstwa na jej szkodę lub na szkodę osoby dla niej najbliższej, jeżeli groźba wzbudza w osobie, do której została skierowana lub której dotyczy, uzasadnioną obawę, że będzie spełniona, podlega karze pozbawienia wolności do lat 3.

art. 190a §2 kodeksu karnego: Kto, podszywając się pod inną osobę, wykorzystuje jej wizerunek lub inne jej dane, za pomocą których jest ona publicznie identyfikowana, w celu wyrządzenia jej szkody majątkowej lub osobistej, podlega karze pozbawienia wolności od 6 miesięcy do 8 lat.

art. 191a §1 kodeksu karnego: Kto utrwała wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej, używając w tym celu wobec niej przemocy, groźby bezprawnej lub podstęp, albo wizerunek nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody rozpowszechnia, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

art. 286 §1 kodeksu karnego: Kto, w celu osiągnięcia korzyści majątkowej, doprowadza inną osobę do niekorzystnego rozporządzenia własnym lub cudzym mieniem za pomocą wprowadzenia jej w błąd albo wyzyskania błędu lub niezdolności do należytego pojmowania przedsiębranego działania, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

art. 287 §1 kodeksu karnego: Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.



Pamiętaj! Ściganie tych przestępstw odbywa się na wniosek pokrzywdzonego.

Sextortion w 2026 roku to nie tylko przestępstwo – to przemysł. Wykorzystanie deepfake'ów sprawiło, że granica między prawdą a fałszem się zaciera.

Bądź czujny, bądź sceptyczny i nie daj się nabrać na „modelki pasjonujące się logistyką”. Prawdziwe modelki są zajęte liczeniem kalorii w liściu sałaty i reklamowaniem „cudownych” kremów.

Poproś o pomoc!

116sos.pl – wsparcie dla osób w kryzysie emocjonalnym

- Zadzwoń: 116123
- Napisz: 116sos.pl | [Formularz kontaktowy](#) | [Pomoc psychologiczna dla dorosłych](#)

Centrum Wsparcia dla Osób Dorosłych w Kryzysie Psychicznym

- Zadzwoń: 800 70 22 22
- Napisz do specjalisty: [Kontakt - Centrum Wsparcia](#)

Fundacja Feminoteka – wsparcie dla kobiet doświadczających przemocy

- Zadzwoń: 888 88 33 88
- Napisz: pomoc@feminoteka.pl

Instytut Przeciwdziałania Wykluczeniom – Telefon Zaufania dla Mężczyzn

- Zadzwoń: 608 271 402
- Napisz: pomoc@pomesku.org