

The Rise and Rise of Biometric Mass Surveillance in the EU

ANALIZA PRAWNA PRAKTYK MASOWEJ
INWIGILACJI BIOMETRYCZNEJ W NIEMCZECH,
HOLANDII I POLSCE.

Luca Montag, Rory Mcleod, Lara De Mets, Meghan Gauld, Fraser
Rodger i Mateusz Pełka z Edinburgh International Justice Initiative
(EIJI)

Ogólne podsumowanie

W imieniu European Digital Rights (EDRi)

▼ [Przeczytał cały raport tutaj.](#)

Wstęp European Digital Rights (EDRi)

W maju 2020, EDRi opublikowało stanowisko ["Ban Biometric Mass Surveillance" \("Zakazać Masowej Inwigilacji Biometrycznej"\)](#) w odpowiedzi na mrozący wzrost wykorzystywania technologii rozpoznawania twarzy i innych praktyk masowej inwigilacji biometrycznej w Europie. Zarówno w tym stanowisku, jak i w naszej dotychczasowej strategii i działalności, pokazujemy, że jakiegokolwiek wdrażanie technologii biometrycznych w publicznie dostępnych miejscach i wykorzystywanie ich w sposób bezkrytyczny lub arbitralnie namierzających ludzi, skutkuje bezprawną masową inwigilacją - bez względu czy te dane są one wykorzystywane przez policję, administrację publiczną czy korporacje. Pokazaliśmy, że z definicji, **każde wykorzystywanie danych biometrycznych, które może prowadzić do masowej inwigilacji jest zwyczajnie zbędne i nieproporcjonalne w kontekście ochrony europejskich praw człowieka.** Udowodniliśmy także ogrom ryzyk i szkód wyrządzanych ludzkiej prywatności, danym osobowemu, równości, niedyskryminacji i innym podstawowym prawom człowieka bezprawnie naruszanych przez praktyki masowej inwigilacji biometrycznej.

W Holandii i Niemczech, te praktyki są wciąż wykorzystywane w drobnych celach, zupełnie nieproporcjonalnych w szczególności do poważnej skali ingerencji z jakimi się wiążą.

Liczba odkrywanych za ich pośrednictwem powiązań jest znikoma, a nawet jeżeli do nich dochodzi, mają one marginalne znaczenie dla interesu publicznego. **To znaczy, że nawet jeżeli te technologie pracują zgodnie z ich założeniami, nie są w stanie osiągnąć założonych im celów.**

Cytując autorów raportu, obecne praktyki wskazują, że te środki są:

"[S]tosowane rzadziej w odpowiedzi na konkretne i udowodnione zagrożenia, a częściej masowo i bezkrytycznie jako środki zapobiegawcze i odstraszające."

Skoro każda ingerencja w prawo człowieka do ochrony danych biometrycznych powinna spełniać wymóg niezbędności i proporcjonalności, stosowanie tych abstrakcyjnych i rzekomo "zapobiegawczych" środków potwierdza nie tylko fałszywość założenia, że ludzie są bezpieczniejsi w ramach systemu masowej inwigilacji biometrycznej, lecz także, że **dążenie do redukcji kosztów i wzrostu efektywności wciąż nabiera na sile kosztem troski o podstawowe prawa człowieka.**

Kolejnym zaobserwowanym trendem jest **poważny brak środków, uniemożliwiający organom ochrony danych osobowych egzekwowanie istniejących regulacji.**

To dodatkowo pogarsza fakt, że jak wskazuje EDRi, **obowiązujące prawo regulujące dane biometryczne obarczone jest licznymi niedoskonałościami - znacznymi marginesami uznania, kruczkami i lukami prawnymi, szarymi strefami i potencjałem do celowego obchodzenia zasad (tak jak w przypadku nadużywania zgody jako podstawy do przetwarzania danych). Te niedoskonałości skutkują de facto przyzwoleniem na praktyki masowej inwigilacji biometrycznej w Unii Europejskiej.**

Dodatkowo, wdrażanie i rozwijanie praktyk masowej inwigilacji biometrycznej często jest prowadzone w tajemnicy i nazywane "pilotami", by cynicznie unikać kontroli ze strony regulatorów.

W Polsce, dążenia nie skupiają się jeszcze na wdrażaniu systemów rozpoznawania twarzy na żywo w publicznie dostępnych miejscach - tak jak zgodnie z badaniem, jest obecnie powszechne w Niemczech i Holandii - lecz bardziej na tworzeniu baz danych i infrastruktury, która umożliwi i ułatwi masową inwigilację biometryczną w przyszłości (dokładnie tak jak zgodnie z badaniem, miało miejsce kilka lat temu w Niemczech i Holandii). Co więcej, badanie wskazuje, że to rzekome uzasadnienie dla zamieszczania danych biometrycznych w dowodach osobistych, tak jak w Polsce czy Niemczech, jest pozbawione podstaw prawnych.

Ponadto, w Niemczech i w Polsce organy publiczne zdają się traktować pandemię COVID-19 jako przysłowiowego konia trojańskiego, umożliwiającego bezpodstawne rozszerzanie zakresu zastosowania środków inwigilacji.

Przykładowo, polska policja wciąż przeprowadza kontrole w domach ludzi korzystających z "Domowa Kwarantanna", nawet po tym jak ich okres kwarantanny minął. Aplikacja "Domowa Kwarantanna" korzysta z technologii rozpoznawania twarzy.

Kolejnym poważnie niepokojącym trendem wskazanym w raporcie, jest to jak **technologie masowej inwigilacji biometrycznej są nieproporcjonalnie stosowane przeciwko określonym grupom ludzi.**

W Niemczech, społeczności religijne i LGBT+ były celem praktyk rozpoznawania twarzy na żywo. W Holandii, obcokrajowcy zostali włączeni do pseudo-kryminalnej bazy danych biometrycznych, wyłącznie ze względu na fakt, że są "obcy", a dystopijny projekt "Living Labs" traktował całe społeczności jako eksperyment, często bez ich wiedzy, w którym ich dane biometryczne były gromadzone wraz z innymi danymi w celu przewidywania poziomu agresji tych grup, czy życiowych rezultatów (np. edukacji).

To wszystko w sytuacji gdy społeczeństwa i system opieki społecznej już i tak piętnuje i kryminalizuje ludzi biednych, pracujących za minimum, lub przynależących do mniejszości etnicznych.

Mimo że od czasu publikacji "Ban Biometric Mass Surveillance" ("Zakazać Masowej Inwigilacji Biometrycznej") odnotowaliśmy wiele znaczących sukcesów w zapobieganiu bezprawnym zastosowaniu inwigilacji biometrycznej w Europie, problem wciąż narasta, co dokładnie potwierdza dlaczego działania EDRi są ważniejsze niż



kiedykolwiek wcześniej. Autorzy raportu podsumowali, że:

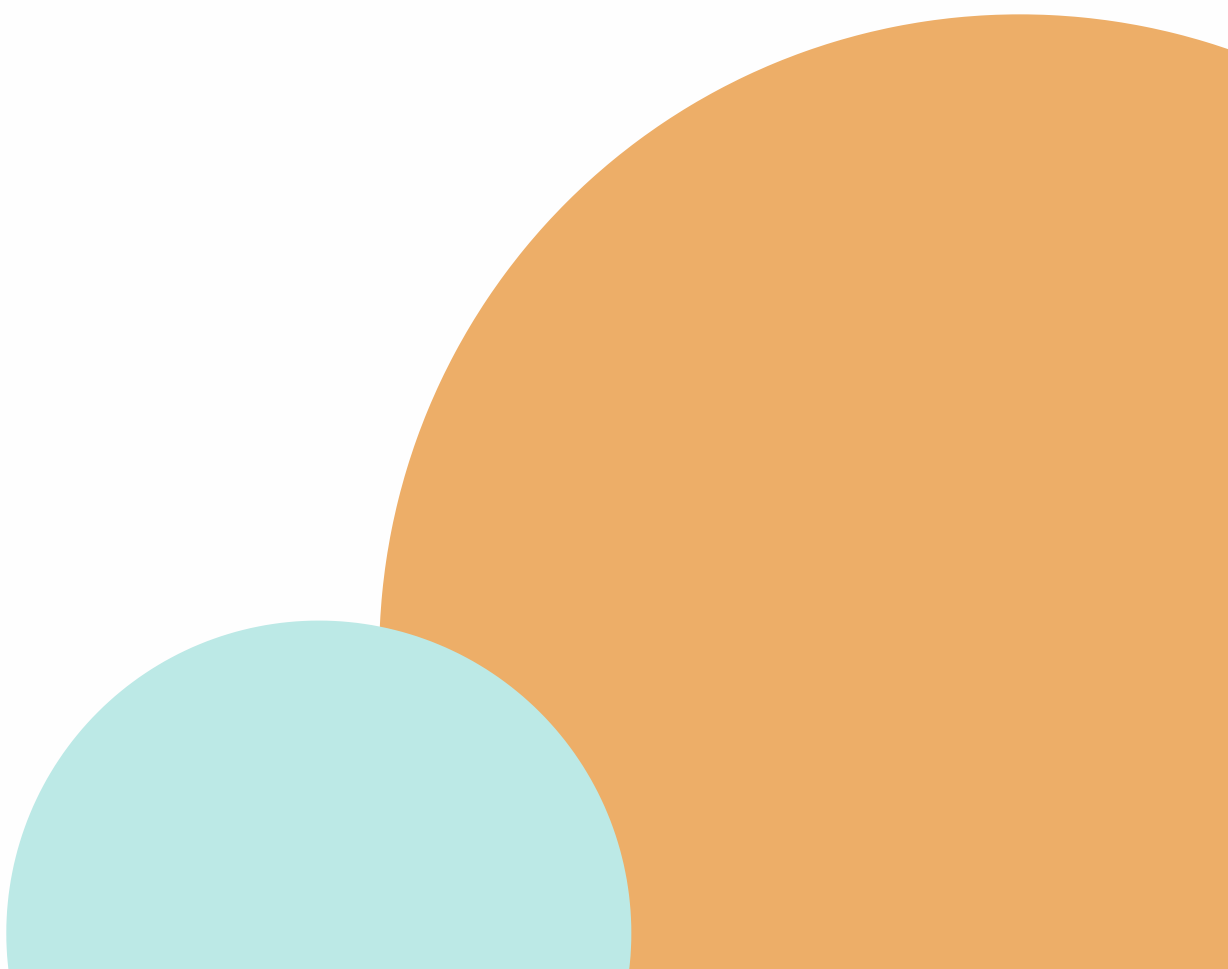
“Wykorzystywanie masowej inwigilacji biometrycznej w miejscach publicznych staje się w ostatnich latach stopniowo i po cichu regularną praktyką.”

W październiku 2020 EDRI rozpoczęło kampanię społeczną zatytułowaną “Reclaim Your Face” / “Odzyskaj swoją twarz” by sprzeciwić się tym praktykom.

Mimo zapewnieniom Komisji Europejskiej, że obecne przepisy i środki prawne są wystarczające, jest wprost przeciwnie.

Autorzy raportu wskazują na lukę pomiędzy prawdziwym zakazem - przy którym szkodliwe i naruszające prawa praktyki nie mogłyby być w ogóle wdrażane - i obecnym Dzikim Zachodem masowej inwigilacji biometrycznej, gdzie prywatne spółki, zysk i impulsywne decyzje państw by monitorować, inwigilować i kontrolować ludzi w każdym czasie, wygrywają.

[Dowiedz się więcej na temat akcji “Reclaim Your Face” / “Odzyskaj swoją twarz” by zakazać praktyk masowej inwigilacji biometrycznej.](#)



Wprowadzenie do Polski, badanie EDRI:

Mimo że praktyki masowej inwigilacji biometrycznej (takie jak zdalna identyfikacja biometryczna ludzi w miejscach publicznych) są mniej rozpowszechnione w Polsce, niż w Holandii czy Niemczech, Polska jest daleko od bycia wolną od masowej inwigilacji biometrycznej. Co więcej, to bardzo prawdopodobne, że Polska będzie podążać wytyczoną przez Holandię i Niemcy ścieżką prowadzącą do przetworzenia baz danych i infrastruktury w system masowej inwigilacji biometrycznej.

Pomimo że Polska Konstytucja uwzględnia poszanowanie godności człowieka i prawo do ochrony danych osobowych, jak i Europejskie prawo do prywatności, ochrony danych osobowych i niedyskryminacji (między innymi), praktyki dążące do stworzenia idealnych warunków do masowej inwigilacji biometrycznej nabierają na sile. Zważywszy na samozwańcze aspiracje Polski by zostać liderem sztucznej inteligencji i cyfryzacji administracji, szczególną obawą napawa fakt, że ów rozwój technologiczny odbywa się na tle odstępstw od zasad demokracji, zagrożeń względem praworządności oraz tłumienia wolności zgromadzeń i wolności słowa, w szczególności względem kobiet i osób LGBT+.

Pierwszy przykład w raporcie, poddający analizie aplikację z 2020 roku "Kwarantanna Domowa", która została wprowadzona w celu egzekwowania kwarantanny na początku pandemii koronawirusa, sugeruje, że Polska nie dysponuje odpowiednimi

instrumentami prawnymi i praktycznymi, by mierzyć się z wyzwaniami stawianymi prawom człowieka przez narastające dążenia do identyfikowania i śledzenia ludzi za pośrednictwem danych biometrycznych. Szybka decyzja Polski by korzystać z technologii rozpoznawania twarzy w celu monitorowania i śledzenia stosowania się populacji do obowiązku kwarantanny nie była ani niezbędna ani proporcjonalna w kontekście zamierzonego celu i stawiała redukcję kosztów i efektywność przed ochroną podstawowych praw człowieka. Dodatkowo, ta obowiązkowa aplikacja została utworzona w ramach lukratywnego partnerstwa publiczno-prawnego które powstało zaledwie w trzy dni, skupiającego się na wykorzystywaniu technologii rozpoznawania twarzy. Szczególnie niepokojący był również fakt, że dane biometryczne były przechowywane tak długo, aż użytkownik ich nie usunął. Dodatkowo to, że policja nadużywała tej aplikacji przeciwko osobom przebywającym dłużej na kwarantannie, oraz że ta początkowo dobrowolna aplikacja szybko i bez jakiegokolwiek uzasadnienia stała się obowiązkowa, potwierdza całkowicie bezpodstawne dążenia do forsowania wdrażania technologii rozpoznawania twarzy w produktach i usługach.

Po drugie, raport analizuje wdrażanie nowych polskich dowodów osobistych z obowiązkową warstwą biometryczną. Wdrażanie dowodów biometrycznych obnaża dążenie do ciągłego i bezpodstawnego zwiększania ilości gromadzonych

danych biometrycznych na temat obywateli i mieszkańców Polski. By uzyskać obowiązkowy dowód osobisty w Polsce, osoby już od 12 roku życia muszą udostępnić organom swoje dane biometryczne. Raport wskazuje na poważną nieścisłość pomiędzy rzekomym dążeniem do uzyskania europejskiej 'korzyści' wykorzystywania tych dowodów osobistych w celu realizowania swobody przemieszczania się i bezpieczeństwa narodowego, a sposobem w jaki te dowody są wykorzystywane w rzeczywistości - czyli w przeważającej mierze w narodowych celach obywatelskich, co podważa konieczność gromadzenia danych biometrycznych w ogóle. Poza tym, rozszerzenie polskich dowodów osobistych o dane biometryczne poszło w parze z nowymi regulacjami przewidującymi kruczki prawne umożliwiające udostępnianie tych danych wielu agencjom rządowym, jak również niepokojącymi przepisami umożliwiającymi bezterminowe przechowywanie danych biometrycznych twarzy.

Po trzecie, mimo że nadzór nad operacjami służb bezpieczeństwa w państwach członkowskich Unii Europejskiej pozostaje w jurysdykcji wyłącznej tego państwa członkowskiego, przykład Polski może dostarczyć nam istotnych informacji na temat tego jak działania służb bezpieczeństwa mogą tworzyć ryzyko masowej inwigilacji biometrycznej wdrażanej przeciwko części lub całej populacji. Po tajnym przetargu wartym ok. 5 milionów euro system szpiegowski "Pegasus" z funkcjonalnością gromadzenia danych biometrycznych został wdrożony w Polsce. Stało się tak mimo absolutnego braku nadzoru i powiązania tego konkretnego systemu z zabójstwami wielu dziennikarzy i tłumieniem obrońców praw człowieka w państwach trzecich. To przestroga przed tym, jak ukierunkowana inwigilacja może, na wiele sposobów, być tak szkodliwa i dyskryminująca jak "niedyskryminująca" inwigilacja biometryczna; oraz jak jej tajne i nieuregulowane zastosowanie - bez kontroli sądowej

i organów nadzoru - może skutkować powszechnym przeświadczeniem o masowej inwigilacji całej populacji.

Przekrój polskich przykładów dostarcza dowodów działań, które mogą prowadzić do normalizacji gromadzenia i przetwarzania danych biometrycznych - sprzecznego z zasadami UE - oraz tworzenia baz danych i infrastruktury gotowej do prowadzenia masowej inwigilacji biometrycznej. Najwyższy czas by odpowiednie organy ograniczyły bazy danych i stosowane praktyki, i proaktywnie ustanowiły zasady, które zapewnią, że praktyki masowej inwigilacji biometrycznej zostaną ostatecznie zakazane. Dlatego właśnie państwa członkowskie i instytucje UE powinny podjąć działania i zakazać praktyki masowej inwigilacji biometrycznej by zagwarantować ochronę podstawowych praw człowieka. Taki zakaz wymagałby, aby takie abuzywne i bezprawne praktyki były absolutnym wyjątkiem, nigdy normą.

▼ [Przeczytał cały raport tutaj.](#)