Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy	**Wielka Brytania** Information Commissioner (ICO)
Data wydania decyzji	**18 maja 2021 r.**
Podmiot kontrolowany	**Clearview AI Inc.**
Wysokość kary	**9 000 000 EUR**

Rodzaj naruszenia

Naruszenie art. 5 (1) a), e), art. 6, art. 9, art. 14, art. 15, art. 16, art. 17, art. 21, art. 22, art. 35 RODO.
Nieprzestrzeganie ogólnych zasad przetwarzania danych.

Przedmiot decyzji

Źródło postępowania:

Brytyjski organ nadzorczy dokonał czynności kontrolnych w Clearview AI Inc. (Clearview).

Opis wydarzeń:

1) W trakcie czynności kontrolnych brytyjski organ nadzorczy ustalił, iż:

a) Clearview opracowała platformę do rozpoznawania twarzy, która pobierała obrazy z sieci społecznościowych, blogów i ogólnie z serwisów za pomocą technik web scrapingu,

b) wszystkie pozyskane obrazy były przetwarzane za pomocą technik biometrycznych w celu wydobycia cech identyfikacyjnych pozwalających na opracowanie wzorców biometrycznych,

c) każdy z obrazów posiadał dodatkowo takie metadane, jak: tytuł obrazu lub strony internetowej, link do źródła, geolokalizację, płeć, datę urodzenia, narodowość, język,

d) baza danych Clearview zawiera obecnie około 20 miliardów obrazów,

e) co najmniej 5 brytyjskich organów ścigania korzystało z usługi podczas tzw. „brytyjskiej fazy testowej",

f) naruszenie trwa nadal od 25 maja 2018 r.

2) Na podstawie zebranego materiału dowodowego brytyjski organ nadzorczy dopatrzył się naruszeń następujących zasad:

a) legalność – Clearview nie dysponuje przesłanką legalizującą przetwarzanie danych osobowych zwykłych i szczególnej kategorii,

b) przejrzystość – Clearview nie informowała użytkowników o przetwarzaniu ich danych osobowych oraz utrudniała realizację praw podmiotów danych,

c) celowość – Clearview przetwarzała dane użytkowników w celach innych niż te, dla których zostały one udostępnione przez samych użytkowników,

d) ograniczenie przechowywania – Clearview nie określiła okresu przechowywania danych.

4) Ponadto Clearview nie przeprowadził oceny skutków dla ochrony danych.

5) Brytyjski organ nadzorczy uznał, że publiczna dostępność danych w Internecie nie oznacza legalności ich gromadzenia oraz możliwości ponownego ich wykorzystania przez osoby trzecie.

Przyczyna naruszenia:

Clearview opracowywała wzorce biometryczne obrazów pozyskanych z ogólnie dostępnych źródeł łamiąc podstawowe zasady przetwarzania danych osobowych.

Decyzja French Data Protection Authority (CNIL)

Kara pieniężna w wysokości 9 000 000 EUR (7 552 800 GBP).

Kompas FORSAFE

Zgodnie z „Wytycznymi dotyczącymi rozpoznawania twarzy" opracowanymi przez Komitet Konsultacyjny Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych Konwencja 108:

1) przetwarzanie szczególnych kategorii danych, takich jak dane biometryczne, jest dozwolone tylko wtedy, gdy takie przetwarzanie opiera się na odpowiedniej podstawie prawnej, a prawo krajowe zapewnia uzupełniające i odpowiednie zabezpieczenia,

2) konieczność stosowania technologii rozpoznawania twarzy należy oceniać wraz z proporcjonalnością do celu i wpływem na prawa osób, których dane dotyczą,

3) wykorzystywanie obrazów cyfrowych, które zostały umieszczone w Internecie, w tym w mediach społecznościowych lub internetowych witrynach do zarządzania zdjęciami, lub zostały przechwycone przez obiektyw monitorujących kamer wideo, nie może być uznane za zgodne z prawem wyłącznie na tej podstawie, że dane osobowe zostały w sposób oczywisty udostępnione przez osoby, których dane dotyczą,

4) przetwarzanie danych biometrycznych przez technologie rozpoznawania twarzy do celów identyfikacji w kontrolowanym lub niekontrolowanym środowisku powinno być ogólnie ograniczone do celów egzekwowania prawa oraz powinno być prowadzone wyłącznie przez właściwe organy w zakresie bezpieczeństwa,

5) wykorzystywanie technologii rozpoznawania twarzy przez podmioty prywatne, z wyjątkiem podmiotów prywatnych uprawnionych do wykonywania podobnych zadań jak organy publiczne, wymaga wyraźnej, konkretnej, dobrowolnej i świadomej zgody osób, których dane dotyczą, których dane biometryczne są przetwarzane,

6) podmioty prywatne nie mogą wdrażać technologii rozpoznawania twarzy w niekontrolowanych środowiskach, takich jak centra handlowe, zwłaszcza w celu identyfikacji osób będących przedmiotem zainteresowania, do celów marketingowych lub do celów bezpieczeństwa prywatnego.

Zgodnie z Rezolucją Parlamentu Europejskiego z dnia 6 października 2021 r. w sprawie sztucznej inteligencji w prawie karnym i jej stosowania przez policję i organy wymiaru sprawiedliwości w sprawach karnych:

1) korzystanie z systemów rozpoznawania twarzy przez organy ścigania powinno być ograniczone do ściśle określonych celów przy pełnym poszanowaniu zasad proporcjonalności i konieczności oraz obowiązującego prawa,

2) wykorzystanie technologii rozpoznawania twarzy musi co najmniej spełniać wymogi minimalizacji danych, dokładności danych, ograniczenia ich przechowywania, bezpieczeństwa danych i odpowiedzialności za nie, a także być zgodne z prawem, sprawiedliwe, przejrzyste i zgodne z konkretnym, wyraźnym i uzasadnionym celem, który jest jasno określony w obowiązującym prawie,

3) niedopuszczalne jest wykorzystywanie przez organy ścigania i służby wywiadowcze prywatnych baz danych służących do rozpoznawania twarzy pozyskanych nielegalnie z sieci społecznościowych i innych miejsc ogólnie dostępnych w Internecie,

4) niedopuszczalne jest stosowanie w przestrzeni publicznej systemów automatycznej analizy i/lub rozpoznawania nie tylko twarzy, ale także innych cech ludzkich takich jak chód, odciski palców, DNA, głos oraz inne sygnały biometryczne i behawioralne,

5) stosowanie identyfikacji biometrycznej w kontekście ścigania przestępstw i sądownictwa powinno zawsze być uznawane za „wysokie ryzyko" i w związku z tym podlegać dodatkowym wymogom, zgodnie z zaleceniami powołanej przez Komisję grupy ekspertów wysokiego szczebla ds. sztucznej inteligencji.

Materiał edukacyjny przygotowany przez FORSAFE

Opracowanie merytoryczne
Katarzyna Cieślak