Kary organów nadzorczych w Unii Europejskiej

Kraj oraz organ nadzorczy

Francja

French Data Protection Authority (CNIL)

Data wydania decyzji

17 październik 2022 r.

Podmiot kontrolowany

Clearview AI Inc.

Wysokość kary

20 000 000 EUR

FORSAFE
BEZPIECZEŃSTWO PONAD WSZYSTKO

Rodzaj naruszenia

Art. 6 RODO, Art. 12 RODO, Art. 15 RODO, Art. 17 RODO, Art. 31 RODO.
Niedostateczna realizacja praw osób, których dane dotyczą.

Przedmiot decyzji

Źródło postępowania:

Francuski organ nadzorczy otrzymał od organizacji Privacy International skargę na Clearview AI Inc. (Clearview).

Opis wydarzeń:

1) Francuski organ nadzorczy zdecydował o dokonaniu czynności kontrolnych w Clearview celem rozpatrzenia przedmiotowej sprawy.

2) W trakcie czynności kontrolnych francuski organ nadzorczy ustalił, iż:

a) Clearview opracowała platformę do rozpoznawania twarzy, która pobierała obrazy z sieci społecznościowych, blogów i ogólnie dostępnych 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: link do źródła, geolokalizacja,

d) Clearview zebrała w swojej bazie danych ponad 20 miliardów zdjęć twarzy z całego świata.

3) Na podstawie zebranego materiału dowodowego francuski organ nadzorczy dopatrzył się naruszenia:

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

b) prawa do dostępu do danych – Clearview nie wykonała żądań o realizację praw podmiotów danych, a czasami wręcz utrudniała ich realizację.

Przyczyna naruszenia:

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

Decyzja:

1) Kara pieniężna w wysokości 20 000 000 EUR.

2) Zakaz dalszego przetwarzania i gromadzenia, za pomocą technik web scrapingu, obrazów i powiązanych metadanych dotyczących osób przebywających na terytorium Francji.

3) Nakaz usunięcie danych, powszechnych i biometrycznych, przetwarzanych za pośrednictwem systemu rozpoznawania twarzy, odnoszących się do osób przebywających na terytorium Francji.

Źródło:

https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000046444859?isSuggest=true

Kompas FORSAFE

JAK UNIKAĆ TAKICH NARUSZEŃ?

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 wykorzystywaniem 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