

Retencja danych oznacza zatrzymywanie przez dostawców usług łączności elektronicznej danych o ruchu i lokalizacji w celu umożliwienia dostępu właściwym organom krajowym na potrzeby zwalczania przestępczości i ochrony bezpieczeństwa narodowego. Takie dane stanowią obecnie jedno z kluczowych narzędzi do skutecznego ścigania przestępczości i zapobiegania zagrożeniom bezpieczeństwa narodowego (w tym terroryzmowi). Prawna ocena retencji jest jednak kłopotliwa.

Na początku XXI wieku, w efekcie 9/11, w wielu państwach - w tym również w UE, panowało przekonanie o konieczności masowej, obowiązkowej retencji danych wszystkich użytkowników usług elektronicznych. Jednak rewolucja cyfrowa i idące za nią zorientowanie na prywatność i ochronę danych osobowych doprowadziły do ponownej kalibracji retencji przez Trybunał Sprawiedliwości Unii Europejskiej (dalej: TSUE). I tak, Trybunał orzekł, że jedynie szczególne okoliczności uzasadniają zastosowanie retencji (zarówno ukierunkowanej na konkretną osobę lub lokalizację, jak i masowej). Do okoliczności tych zalicza się poziom pewności, że dane państwo jest skonfrontowane z zagrożeniem, lub że dana osoba/obszar rzeczywiście ujawnią związek z przestępstwem. TSUE nakreślił więc ogólne reguły i standardy, pozostawiając UE i państwa członkowskie z trudnym zadaniem wprowadzenia „jasnych i precyzyjnych przepisów” wdrażających owe standardy w życie.

Jak dotąd zarówno w UE, jak i w państwach członkowskich, nie udało się przełożyć standardów TSUE na funkcjonalny, a zarazem gwarancyjny kompromis legislacyjny, który pozwoli na stosowanie retencji jedynie w granicach uznanych za konieczne w państwie demokratycznym.

Dlatego projekt oferuje nowatorskie podejście do problemu retencji, które wykorzystuje dorobek obliczeniowych nauk społecznych (dalej: CSS). Jest to dyscyplina krzyżująca naukę o danych, modelowaniu obliczeniowym i nauki społeczne, która stara się wykorzystać rosnącą dostępność danych i potencjał obliczeniowy do opisywania społecznych fenomenów, trudnych do uchwycenia tradycyjnymi środkami i metodami. W przedmiotowym projekcie przełoży się to na zastosowanie sztucznej inteligencji do analizy publicznie dostępnych danych o terroryzmie i przestępczości w celu wyodrębnienia cech charakterystycznych i powiązań pozwalających zawęzić zakres sytuacji uzasadniających retencję danych.

Dzięki komponentowi CSS, projekt dostarczy szeregu danych empirycznych konkretyzujących wymogi TSUE. To z kolei wypełni wskazywaną w nauce lukę w dowodach na rzeczywistą użyteczność retencji i pomoże rozwiązać impas naukowo-legislacyjny, który trwa w UE trwa już od prawie 10 lat, stawiając pod znakiem zapytania ochronę prywatności użytkowników łączności elektronicznej.