

Dlaczego TSUE powinien zająć się inwigilacją w Polsce

11 kwietnia 2022

Czy impuls do zmiany polskich przepisów dotyczących inwigilacji może popłynąć z Trybunału Sprawiedliwości Unii Europejskiej? W postępowaniu przed stołecznym sądem walczy o to dziennikarka, która pozwała państwo, ponieważ nie została poinformowana, czy była inwigilowana. Oczekuje od sądu, że ten skieruje sprawę do Luksemburga. Z orzecznictwa TSUE wynika bowiem szereg warunków, jakie musi spełniać prawo UE w obszarze dostępu służb do billingów. To próba włączenia instytucji unijnych w walkę z niekontrolowaną inwigilacją w Polsce. Na razie zaangażowanie zadeklarował Parlament Europejski, który powołał komisję śledczą ds. Pegasus.

Dyskusję o inwigilacji w ostatnim czasie zdominowała kwestia Pegasus. Jest to zrozumiałe, biorąc pod uwagę skrajny stopień ingerencji w prywatność, jaki ten system umożliwia, oraz profil osób, które były jego ofiarami. Pegasus to jednak tylko wierzchołek góry lodowej. Służby dysponują też innymi instrumentami inwigilacji i – jak pokazują informacje uzyskane przez Fundację Panoptikon – chętnie z nich korzystają. Co roku zakładanych jest ok. 8–10 tys. podsłuchów, a policja i służby pozyskują ok. 1,35 mln danych telekomunikacyjnych, czyli przede wszystkim billingów i informacji o lokalizacji. Dane telekomunikacyjne są prawdziwą kopalnią wiedzy: dają wgląd w to, z kim się kontaktujemy, jak często i kiedy, a także gdzie przebywamy o określonych godzinach.

Zgodnie z dyrektywą e-privacy państwa członkowskie mają obowiązek zapewnienia poufności komunikacji elektronicznej (telefonicznej, internetowej) i związanych z nią danych. Dyrektywa ta pozwala przyjąć państwom środki ustawodawcze ograniczające zasadę poufności w celu ochrony m.in. bezpieczeństwa publicznego czy ściganiu przestępstw – ale

tylko pod warunkiem, że środki te są niezbędne i towarzyszą im odpowiednie gwarancje mające chronić przed nadużyciami. Trybunał Sprawiedliwości wielokrotnie (m.in. w orzeczeniach La Quadrature du Net i in., C-511/18 i C-512/18, Privacy International, C-623/17) definiował warunki dopuszczalności ingerencji w poufność komunikacji. Zdaniem Trybunału dostęp do danych powinien być możliwy po uzyskaniu zgody niezależnego organu i musi być ograniczony do wyjątkowych przypadków (poważne przestępstwa czy zagrożenia dla bezpieczeństwa). Innym mechanizmem chroniącym przed nadużyciami, który można wywnioskować z orzeczeń TSUE, jest wymóg informowania o tym fakcie osób, których dane zostały pozyskane, gdy przekazanie takich informacji nie zaszkodzi już prowadzonym postępowaniom. Celem tej gwarancji jest stworzenie osobom, których dane były pozyskane, realnej możliwości zażądania niezależnej kontroli tego, czy inwigilacja była zgodna z prawem.

Czy wymogi te mają uniwersalny charakter? Niektóre państwa członkowskie wskazywały bowiem w postępowaniach przed TSUE, że dyrektywa e-privacy nie ma zastosowania m.in. do działalności dotyczącej obronności i bezpieczeństwa państwa. Trybunał stwierdził jednak, że jeżeli państwo przyjmuje środki ograniczające poufność komunikacji elektronicznej, które nakładają jednocześnie obowiązki przetwarzania danych na operatorów telekomunikacyjnych i dostawców internetowych, to są one objęte zakresem dyrektywy e-privacy także wtedy, gdy służby sięgają po dane np. w celu zapewnienia bezpieczeństwa narodowego, które – co do zasady – nie jest objęte prawem UE.

Polskie przepisy zakładają, że wszystkie dziewięć instytucji uprawnionych do pozyskiwania danych raz na sześć miesięcy przedstawia informację zbiorczą na temat swojej aktywności sądom, które mają na podstawie tej zbiorczej informacji weryfikować legalność działania służb. Dostęp do danych możliwy jest nie tylko w sprawie poważnych przestępstw, ale też np. w ramach prowadzenia przez CBA działalności analitycznej. W oczywisty sposób jest to niezgodne z prawem

unijnym (orzecznictwo TK i ETPC pozostawiamy tu na marginesie) i samo w sobie stanowi podstawę do uznania niezgodności krajowych przepisów z prawem UE.

Przywołana na wstępie sprawa redaktor Ewy Siedleckiej przeciwko Komendantowi Głównemu Policji i Szefom ABW i CBA, rozpoznawana przez Sąd Okręgowy w Warszawie, jest szansą na kolejne istotne orzeczenie Trybunału w Luksemburgu oraz klarowne przedstawienie przez niego jeszcze jednego warunku zgodności z prawem UE zasad pozyskiwania danych. Jeżeli warszawski sąd przychyli się do wniosku dziennikarki i skieruje do TSUE pytanie prejudycjalne, ten będzie miał okazję rozstrzygnąć, czy prawo krajowe, które (tak jak w Polsce) umożliwia służbom dostęp do danych telekomunikacyjnych i internetowych, nie przewidując jednocześnie wymogu późniejszego informowania osób, których dane pozyskano, jest zgodne z dyrektywą e-privacy. Wyrok TSUE potwierdzający niezgodność takich regulacji z prawem unijnym mógłby być impulsem do zmiany prawa w Polsce i wprowadzenia – nareszcie – jednoznacznych gwarancji prawa do informacji o byciu inwigilowanym w przeszłości.

Przed wytoczeniem powództwa dziennikarka próbowała uzyskać informację, czy była inwigilowana w latach 2012–2016. Zwróciła się z takim pytaniem bezpośrednio do służb, a także spytała operatorów telekomunikacyjnych, czy przekazywali jej dane organom państwa. Za każdym razem spotykała się z odmową udzielenia takich informacji. Negatywne decyzje były podtrzymywane przez GIOiO oraz sąd administracyjny. W końcu w sierpniu 2020 r. dziennikarka reprezentowana pro bono przez mec. Macieja Dudka z kancelarii LSW Leśnodorski Ślusarek Wspólnicy, wspierana przez Helsińską Fundację Praw Człowieka, złożyła pozew, w którym wskazała, że odmowa przekazania jej takich informacji narusza jej dobra osobiste w postaci prawa do informacji o stosowanych wobec niej środkach inwigilacji, a także prawa do niezaburzonego spokoju psychicznego i emocjonalnego, związanego z niepewnością, czy była

inwigilowana, jak również – czy w związku z tym udało się zachować w tajemnicy tożsamość jej źródeł dziennikarskich. Ponieważ prawo do informacji o stosowanych wobec jednostki środkach inwigilacji objęte jest prawem UE co najmniej w zakresie pozyskiwania danych telekomunikacyjnych i danych internetowych, dziennikarka wskazała, że wykładnia prawa unijnego ma kluczowe znaczenie dla rozstrzygnięcia, czy władze bezprawnie naruszyły jej dobra osobiste. Dlatego zawnioskowała, by sąd w trybie prejudycjalnym skierował pytanie do TSUE. Jej wniosek poparli uczestnicy postępowania: Fundacja Panoptikon i Rzecznik Praw Obywatelskich.

Kwestia podniesiona we wniosku Ewy Siedleckiej o pytanie prejudycjalne nie jest jedynym mankamentem polskiego prawa, które sprawia, że inwigilacji w Polsce nie towarzyszą odpowiednie mechanizmy chroniące przed nadużyciami, wymagane przez regulacje unijne. Tych braków jest więcej i nie wiążą się tylko z dyrektywą e-privacy, ale także z niewłaściwą implementacją tzw. dyrektywy policyjnej (która mogłaby być szczególnie ważna dla pozostałych środków inwigilacji, takich jak np. podsłuchy). Zmiana prawa w tym zakresie stanowiłaby prawdziwą rewolucję dla ochrony praw człowieka w kontekście działalności służb w Polsce. Czy tak się stanie? Zależy to nie tylko od dalszego losu pytania prejudycjalnego i reakcji polskiego ustawodawcy na ewentualny wyrok TSUE, ale także od woli działania jeszcze jednego podmiotu, którego rolą jest zapewnianie, by prawo UE było stosowane prawidłowo i terminowo – „strażniczki traktatów”, czyli Komisji Europejskiej. Jak dotąd, mimo apeli europejskich organizacji społecznych, Komisja nie podejmowała żadnych realnych kroków wobec państw, których prawo krajowe odnoszące się do danych telekomunikacyjnych jest niezgodne z prawem UE. Wobec wojny na Ukrainie istnieje ryzyko, że Komisja wciąż nie podejmie działań związanych z kontrolą nad działalnością służb ze względu na ryzyko zarzutu osłabiania potencjału obronnego państw członkowskich. Decyzja Parlamentu Europejskiego o powołaniu komisji śledczej ds. Pegasus pokazuje jednak, że

poza absolutnie kluczowym tematem działań za naszą wschodnią granicą aktualne pozostają problemy związane z brakiem kontroli nad służbami specjalnymi państw członkowskich.

Autorstwo: Wojciech Klicki (Fundacja Panoptikon), Konrad Siemaszko (Helsińska Fundacja Praw Człowieka)

Tekst ukazał się 05.04.2022 r. w papierowym wydaniu oraz na stronie [„Dziennika Gazety Prawnej”](#)

Źródło: [Panoptikon.org](https://panoptikon.org)