"PONURE ŚWIADECTWO". RPO O ZASADACH POBIERANIA BILINGÓW PRZEZ SŁUŻBY

Policja i służby specjalne mogą w bardzo szerokim zakresie i bez kontroli sprawdzać, z kim obywatel rozmawiał przez komórkę, poznawać lokalizację telefonu czy spis połączeń internetowych - podkreśla Biuro Rzecznika Praw Obywatelskich. Jak dodaje, służby sięgają po takie dane, bo jest to po prostu dla nich najprostsze i najwygodniejsze, a dana osoba nie jest o tym informowana. "Ponure świadectwo o Polsce stanowi utrzymywanie regulacji, która zachęca organy państwa do łamania prawa i zapewnia, że nielegalne działania zostaną usankcjonowane w procesie karnym" – podkreśla Adam Bodnar. Czy interwencja RPO u premiera Mateusza Morawieckiego doprowadzi do zainicjowania odpowiednich zmian legislacyjnych?

"W związku z wyrokiem Trybunału Sprawiedliwości Unii Europejskiej z 2 marca 2021 r. Rzecznik Praw Obywatelskich wystąpił do premiera Mateusza Morawieckiego o zainicjowanie odpowiednich zmian legislacyjnych. Chodzi o wyważanie między potrzebą ochrony bezpieczeństwa obywateli a ich prawem do prywatności" - informuje Biuro RPO. W komunikacie podkreśla również, że od dawna monitoruje kwestie zbierania i wykorzystywania przez policję i służby specjalne danych telekomunikacyjnych, w tym spisów połączeń czy lokalizacji telefonów komórkowych obywateli. "Wymogi bezpieczeństwa państwa nie oznaczają, że prowadzenie takiej inwigilacji ma nie podlegać ograniczeniom wynikającym z konstytucyjnych praw i wolności. A w tym zakresie jednostka ma bardzo ograniczone środki bezpośredniej ochrony prawnej" - czytamy.

Wyrok, o którym wspomina Biuro RPO, mówi że "art. 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 r. o prywatności i łączności elektronicznej oraz art. 52 ust. 1 Karty praw podstawowych UE należy interpretować w ten sposób, że sprzeciwiają się przepisom krajowym umożliwiającym dostęp organów władzy publicznej do zbioru danych o ruchu lub danych o lokalizacji, które mogą dostarczyć informacji o połączeniach wykonywanych przez użytkownika środka łączności elektronicznej lub o lokalizacji używanego przez niego urządzenia końcowego oraz umożliwić wyciągnięcie precyzyjnych wniosków na temat jego życia prywatnego, do celów zapobiegania, dochodzenia, wykrywania i karania przestępstw - bez ograniczania takiego dostępu do postępowań mających na celu zwalczanie poważnej przestępczości lub zapobieganie poważnym zagrożeniom bezpieczeństwa publicznego, niezależnie od długości okresu, na jaki wniesiono o dostęp do danych oraz ich liczby i rodzaju". Co więcej, "art. 15 ust. 1 dyrektywy o prywatności i łączności elektronicznej w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 KPP stoi na przeszkodzie środkom ustawodawczym przewidującym w tych celach prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji". Poważne ingerencje w prawo do poszanowania życia prywatnego i rodzinnego oraz prawo do ochrony danych osobowych, jak pisze Biuro RPO, może uzasadniać jedynie walka z poważną przestępczością i zapobieganie poważnym zagrożeniem bezpieczeństwa publicznego.

TS podkreślił również w wyroku, że ingerencja we wspomniane wyżej prawa w każdym wypadku ma

poważny charakter, niezależnie od długości okresu na jaki się wnosi o dostęp do wspomnianych danych i w każdym wypadku powinno dojść do spełnienia wymogu proporcjonalności, a odstępstwa od poszanowania prywatności czy danych osobowych powinny być ograniczone do tego, co jest ściśle niezbędne do celów danego dochodzenia.

Czytaj też: Adam Bodnar dla InfoSecurity24.pl: policja uznawana jest za emanację państwa

Problem w tym, że "polskie prawo nie spełnia wymogów wynikających z prawa UE, które znalazły odzwierciedlenie w tym wyroku TS UE". Jak relacjonuje Biuro RPO, nowelizacja ustaw "policyjnych" uchwalona w 2016 roku poszerzyła możliwości ingerencji służb w sferę prywatności obywateli i dała służbom prawo do uzyskiwania danych telekomunikacyjnych, internetowych i pocztowych oraz do przetwarzania tych danych bez wiedzy i zgody osoby, której dotyczą. Prawo to przyznane zostało w celu zapobiegania lub wykrywania przestępstw albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych. Nie spełnia ono jednak, jak podkreśla Biuro, kryteriów uzasadniających ograniczenie praw i wolności obywatelskich, wynikających m.in. z Konstytucji. Co więcej, katalog przestępstw, w których przypadku dopuszczalne jest uzyskiwanie i przetwarzanie tych danych przez poszczególne służby jest nadmiernie szeroki.

> *Nie wskazano poszczególnych typów czynów zabronionych, które uzasadniałyby sięgnięcie po tego typu dane o obywatelach, lecz użyto ogólnego określenia "przestępstwa". Oznacza to możliwość uzyskiwania danych w odniesieniu do wszystkich czynów spełniających znamiona jakiegokolwiek przestępstwa, w tym ściganego na wniosek lub z oskarżenia prywatnego. To nadmierna ingerencja w prawo do prywatności i w prawo do ochrony danych osobowych, a także naruszenie zasady autonomii informacyjnej, wyrażone w art. 47, 49 oraz 51 ust. 2 Konstytucji, przez co naruszona jest również zasada godności człowieka (art. 30 Konstytucji).*
>
> *fragment komunikatu Biura Rzecznika Praw Obywatelskich*

Jak podkreśla Biuro, daje to służbom możliwość uzyskiwania danych w postępowaniach w sprawie bliżej nieokreślonych czynów zabronionych, bez względu na ich szkodliwość społeczną i otwiera szansę do wykorzystywania danych telekomunikacyjnych, pocztowych i internetowych nie tylko wówczas, gdy jest to rzeczywiście konieczne do wykrywania lub zapobiegania przestępstwom, ale także wtedy, gdy jest to po prostu najprostsze i najwygodniejsze. Na konieczność precyzyjnego uregulowania zakresu przestępstw, w których dopuszczalne jest sięganie po te dane, wskazywały Europejski Trybunał Praw Człowieka (ETPC) i TS UE.

Czytaj też: Dane specjalnej troski. RPO apeluje o kontrolę NIK

Inny zarzut wobec nowelizacji, jak czytamy w komunikacie, to "nieproporcjonalnie długi czasu trwania kontroli operacyjnej - do 18 miesięcy". Co więcej, znowelizowane przepisy ograniczyły chronioną prawem tajemnicę zawodów zaufania publicznego, m.in. adwokatów, radców prawnych, lekarzy i

dziennikarzy. Zdobyte podczas inwigilacji tajemnice mogą bowiem być wykorzystane w postępowaniu karnym, gdy "jest to niezbędne ze względu na dobro wymiaru sprawiedliwości, a okoliczność ta nie może być ustalona na podstawie innego dowodu".

> *Rozwiązania polskie są niezgodne z wyrokiem TSUE, który podkreślił, że dyrektywa o prywatności i łączności elektronicznej stoi na przeszkodzie środkom ustawodawczym nakładającym na dostawców usług łączności elektronicznej obowiązek prewencyjnego, uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych o lokalizacji. Są one też niezgodne z tą dyrektywą w zakresie w jakim pozwalają na korzystanie z tego typu danych w każdym postępowaniu, a nie jedynie w postępowaniu zmierzającym do zwalczania poważnej przestępczości lub zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego. Tylko bowiem to ostatnie może uzasadniać dostęp organów władzy publicznej do zbioru danych, które umożliwiają wyciągnięcie precyzyjnych wniosków na temat życia prywatnego osób, których dane dotyczą.*
>
> *fragment komunikatu Biura Rzecznika Praw Obywatelskich*

Z wyroku TSUE wynika także konieczność wykluczenia informacji i dowodów uzyskanych z naruszeniem przepisów prawa Unii. "Powinny być one wyeliminowane z materiału dowodowego stanowiącego podstawę rozstrzygnięcia. Postulować należy zatem pilną zmianę art. 168a k.p.k., przywracającą mu treść sprzed nowelizacji z 2016 r. W obecnym brzmieniu przepis ten jest bowiem jawnie i oczywiście niekonstytucyjny" - pisze BRPO.

Niewystarczająca kontrola

"Obecna forma kontroli jest niewystarczająca" - czytamy w komunikacie Biura RPO, nie przewiduje przeprowadzenia kontroli uprzedniej. Dzięki niej "sięganie po dane mogłoby podlegać rzetelnej ocenie pod względem spełniania kryteriów niezbędności, adekwatności i celowości".

> *Polskie regulacje nie przewidują jednak realnej kontroli pobierania danych obywateli. Sąd okręgowy ma wprawdzie prawo do kontroli, ale jedynie na podstawie ogólnych, zbiorczych półrocznych sprawozdań służb. Sąd nie musi, ale tylko może weryfikować, czy dane pobrano zasadnie.*
>
> *fragment komunikatu Biura Rzecznika Praw Obywatelskich*

Jak tłumaczy Biuro RPO, po kontroli sąd może jedynie poinformować daną służbę o jej wynikach, ale nie może zarządzić np. zniszczenia zgromadzonych danych lub innych działań naprawczych, co w praktyce "ma zatem charakter iluzoryczny". "Tajne sprawozdania służb nie są informacją publiczną, choć zawierają informacje dotyczące liczby pozyskanych danych telekomunikacyjnych, pocztowych

lub internetowych i kwalifikacji prawnej czynów, w związku z którymi o nie wystąpiono" - dodano.