PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa, 18.06.2024 r.

DOL.0623.11.2022

Pani

Sekretarz Stanu
w Ministerstwie Spraw Zagranicznych

Szanowna Pani Minister,

w odpowiedzi na korespondencję z 17 maja 2024 r. dotyczącą skutków wyroku Trybunału Sprawiedliwości Unii Europejskiej (dalej jako: TSUE) z dnia 30 kwietnia 2024 r. w sprawie **C- 178/22, Procura della Repubblica presso il Tribunale di Bolzano**, uprzejmie informuję, że w ocenie Prezesa Urzędu Ochrony Danych Osobowych **orzeczenie to pociąga za sobą konieczność rozważenia zmiany obowiązujących przepisów prawa.**

W sentencji wyroku TSUE uznał, że artykuł 15 ust. 1 dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywy o prywatności i łączności elektronicznej), zmienionej dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r., w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej, należy interpretować w ten sposób, że nie stoi on na przeszkodzie przepisowi krajowemu zobowiązującemu sąd krajowy, orzekający w ramach uprzedniej kontroli dokonywanej po przedstawieniu przez właściwy organ krajowy w ramach karnego postępowania przygotowawczego uzasadnionego wniosku o dostęp do zbioru danych o ruchu lub danych o lokalizacji mogących pozwolić na

wyciągnięcie precyzyjnych wniosków dotyczących życia prywatnego użytkownika środka łączności elektronicznej, które to dane są zatrzymywane przez dostawców usług łączności elektronicznej, do wydania zgody na udzielenie tego dostępu, jeżeli zażądano go do celów dochodzenia przestępstw zagrożonych w prawie krajowym karą pozbawienia wolności, której górna granica ustawowego zagrożenia wynosi nie mniej niż trzy lata, z zastrzeżeniem, że istnieją wystarczające przesłanki popełnienia takich przestępstw i że dane te są istotne dla ustalenia okoliczności faktycznych, pod warunkiem jednak, iż ów sąd jest uprawniony do odmowy udzielenia wspomnianego dostępu, jeżeli jest on wnioskowany w ramach dochodzenia dotyczącego przestępstwa, które w sposób oczywisty jest przestępstwem mniejszej wagi w świetle warunków społecznych panujących w danym państwie.

TSUE wskazał, że art. 15 ust. 1 dyrektywy 2002/58 stoi na przeszkodzie środkom ustawodawczym przewidującym prewencyjne, tzn. ujęte w sposób generalny i niezróżnicowany, przesłanki zatrzymywania przez dostawców danych o ruchu i danych o lokalizacji. Dostępu do tych danych nie uzasadnia również cel polegający na zapobieganiu, dochodzeniu, wykrywaniu i karaniu ogółu przestępstw, gdyż jest on uzasadniony wyłącznie w przypadku zwalczania poważnej przestępczości lub zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego.

TSUE wypowiedział się również odnośnie do tego czy tak poważna ingerencja w prywatność może być dozwolona w odniesieniu do przestępstw określonych wyłącznie prawem krajowym, uznając że zdefiniowanie „poważnego przestępstwa" do celów stosowania art. 15 ust. 1 dyrektywy 2002/58 należy do kompetencji państw członkowskich, przy czym uznanie za poważne przestępstwo czynów zagrożonych karą pozbawienia wolności, której górna granica ustawowego zagrożenia wynosi nie mniej niż przewidziany w ustawie okres, jest oparta na kryterium obiektywnym przyznania dostępu do danych.

Co istotne, z treści orzeczenia TSUE wynika, że prawo krajowe w przedmiocie uzyskiwania dostępu do danych o ruchu i lokalizacji podmiotu objętego postępowaniem karnym powinno spełniać określone warunki, tj. przepisy krajowe powinny zawierać jasne i precyzyjne przepisy regulujące zakres i przesłanki stosowania dostępu do danych. Co do zasady dostęp powinien być przyznany jedynie w odniesieniu do danych dotyczących osób podejrzewanych o udział w poważnym przestępstwie. Jednocześnie dostęp do danych przez organy krajowe powinien być uzależniony od uprzedniej kontroli sądu lub niezależnego organu administracyjnego, które powinny mieć zapewnioną możliwość podjęcia decyzji odmownej.

W odniesieniu do polskiego prawa wskazać należy, że kwestia dotycząca możliwości pozyskania na potrzeby postępowania karnego tzw. danych telekomunikacyjnych przez sąd i prokuratora została uregulowana przepisem art. 218 § 1 Kodeksu postępowania karnego, zgodnie z którym urzędy, instytucje i podmioty prowadzące działalność w dziedzinie poczty lub działalność telekomunikacyjną, urzędy celno-skarbowe oraz instytucje i przedsiębiorstwa transportowe obowiązane są wydać sądowi lub prokuratorowi, na żądanie zawarte w postanowieniu,

korespondencję i przesyłki oraz dane, o których mowa w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. z 2022 r. poz. 1648, 1933 i 2581 oraz z 2023 r. poz. 1394, 1703 i 2005), jeżeli mają znaczenie dla toczącego się postępowania. Tylko sąd lub prokurator mają prawo je otwierać lub zarządzić ich otwarcie.

Dane telekomunikacyjne podlegające udostępnieniu przez podmioty prowadzące działalność telekomunikacyjną sądowi lub prokuratorowi na jego żądanie obejmują, zgodnie z art. 180c ust. 1 Prawa telekomunikacyjnego, dane niezbędne do: ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego, inicjującego połączenie, do którego kierowane jest połączenie; określenia: daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia, lokalizacji telekomunikacyjnego urządzenia końcowego.

Z kolei zgodnie z przepisem art. 180d Prawa telekomunikacyjnego, przedsiębiorcy telekomunikacyjni są obowiązani do zapewnienia warunków dostępu i utrwalania oraz do udostępniania uprawnionym podmiotom, a także sądowi i prokuratorowi, na własny koszt, przetwarzanych przez siebie danych, o których mowa w art. 159 ust. 1 pkt 1 i 3-5, w art. 161 oraz w art. 179 ust. 9, związanych ze świadczoną usługą telekomunikacyjną, na zasadach i przy zachowaniu procedur określonych w przepisach odrębnych.

Jak wskazuje przepis art. 159 ust. 1 pkt 1, 3-5 Prawa telekomunikacyjnego, tajemnica komunikowania się w sieciach telekomunikacyjnych, zwana dalej "tajemnicą telekomunikacyjną", obejmuje: dane dotyczące użytkownika, z zastrzeżeniem art. 161 ust. 2; dane transmisyjne, które oznaczają dane przetwarzane dla celów przekazywania komunikatów w sieciach telekomunikacyjnych lub naliczania opłat za usługi telekomunikacyjne, w tym dane lokalizacyjne, które oznaczają wszelkie dane przetwarzane w sieci telekomunikacyjnej lub w ramach usług telekomunikacyjnych wskazujące położenie geograficzne urządzenia końcowego użytkownika publicznie dostępnych usług telekomunikacyjnych; dane o lokalizacji, które oznaczają dane lokalizacyjne wykraczające poza dane niezbędne do transmisji komunikatu lub wystawienia rachunku, a także dane o próbach uzyskania połączenia między zakończeniami sieci, w tym dane o nieudanych próbach połączeń, oznaczających połączenia między telekomunikacyjnymi urządzeniami końcowymi lub zakończeniami sieci, które zostały zestawione i nie zostały odebrane przez użytkownika końcowego lub nastąpiło przerwanie zestawianych połączeń.

W tym miejscu należy wskazać na art. 18 ust. 6 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344), stanowiący, że usługodawca nieodpłatnie udostępnia dane, o których mowa w ust. 1-5, organom państwa uprawnionym na podstawie odrębnych przepisów na potrzeby

prowadzonych przez nie postępowań[1]. Z powyższego przepisu nie wynikają szczegółowe zasady udostępniania danych uprawnionym organom przez podmiot świadczący usługi drogą elektroniczną, ani też nie została przewidziana kontrola zasadności uzyskania takiego dostępu przez niezależny sąd lub organ administracyjny

Z powołanych przepisów prawa wynika, że **w prawie polskim dostęp organów prowadzących postępowanie karne nie odpowiada standardom ochrony danych określonym w analizowanym wyroku TSUE, ponieważ nie ma określonych przesłanek dotyczących wagi przestępstw i ich rodzaju, w odniesieniu do których można byłoby uznać pozyskanie danych objętych tajemnicą telekomunikacyjną za proporcjonalne i zasadne w świetle art. 7, 8 i 11 Karty praw podstawowych UE**. Ponadto, wniosek organu ścigania o dane osobowe nie jest poddawany weryfikacji sądu lub niezależnego organu publicznego, który miałby zapewnioną możliwość w określonych warunkach odmówienia dostępu do takich danych. W demokratycznym państwie prawa zasadność udostępnienia danych telekomunikacyjnych powinna być poddana takiej kontroli, wzmocniłaby ona zaufanie obywateli do państwa i eliminowałaby ryzyko nieproporcjonalnej ingerencji w prawa podstawowe, jak i pewność stosowania prawa, na co wskazywał TSUE w innych swoich wyrokach, jak np. w wyroku z dnia 8 kwietnia 2014 r. w sprawach połączonych Digital Rights Ireland Ltd (C-293/12) i Kärntner Landesregierung (C-594/12). Jednocześnie sama kontrola przeprowadzana przez sąd lub niezależny organ administracyjny powinna być konieczna i adekwatna w demokratycznym

[1] Art. 18 ust. 1-6 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną stanowi:
1. Usługodawca może przetwarzać następujące dane osobowe usługobiorcy niezbędne do nawiązania, ukształtowania treści, zmiany lub rozwiązania stosunku prawnego między nimi:
1) nazwisko i imiona usługobiorcy;
2) numer ewidencyjny PESEL lub - gdy ten numer nie został nadany - numer paszportu, dowodu osobistego lub innego dokumentu potwierdzającego tożsamość;
3) adres zameldowania na pobyt stały;
4) adres do korespondencji, jeżeli jest inny niż adres, o którym mowa w pkt 3;
5) dane służące do weryfikacji podpisu elektronicznego usługobiorcy;
6) adresy elektroniczne usługobiorcy.
2. W celu realizacji umów lub dokonania innej czynności prawnej z usługobiorcą, usługodawca może przetwarzać inne dane niezbędne ze względu na właściwość świadczonej usługi lub sposób jej rozliczenia.
3. Usługodawca wyróżnia i oznacza te spośród danych, o których mowa w ust. 2, jako dane, których podanie jest niezbędne do świadczenia usługi drogą elektroniczną.
4. Usługodawca może przetwarzać, za zgodą usługobiorcy i dla celów reklamy, badania rynku oraz zachowań i preferencji usługobiorców z przeznaczeniem wyników tych badań na potrzeby polepszenia jakości usług świadczonych przez usługodawcę, inne dane dotyczące usługobiorcy, które nie są niezbędne do świadczenia usługi drogą elektroniczną.
5.Usługodawca może przetwarzać następujące dane charakteryzujące sposób korzystania przez usługobiorcę z usługi świadczonej drogą elektroniczną (dane eksploatacyjne):
1) oznaczenia identyfikujące usługobiorcę nadawane na podstawie danych, o których mowa w ust. 1;
2) oznaczenia identyfikujące zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, z którego korzystał usługobiorca;
3) informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną;
4) informacje o skorzystaniu przez usługobiorcę z usług świadczonych drogą elektroniczną.
6. Usługodawca nieodpłatnie udostępnia dane, o których mowa w ust. 1-5, organom państwa uprawnionym na podstawie odrębnych przepisów na potrzeby prowadzonych przez nie postępowań.

porządku, a także przeprowadzona zgodnie z zasadą proporcjonalności (zgodnie z wyrokiem TSUE z dnia 2 marca 2021 r. w sprawie C-746/18 Prokuratuur). Ponadto Prezes UODO w wyrażanych przez siebie stanowiskach podnosił kilkukrotnie, że TSUE w swoich orzeczeniach – tj. w wyroku z dnia 6 października 2020 r., La Quadrature du Net i in. przeciwko Premier ministre i in., sprawy połączone C-511/18, C-512/18 i C-520/186, wyroku z dnia 6 października 2020 r., Privacy International przeciwko Secretary of State for Foreign and Commonwealth Affairs i in., sprawa C-623/177 oraz wyroku w sprawie Trybunału Sprawiedliwości z dnia 30 kwietnia 2024 r. w sprawie C-470/21 La Quadrature du Net i in. przeciwko Premier ministre i Ministère de la Culture – stwierdził, że niezróżnicowane gromadzenie danych przez przedsiębiorców telekomunikacyjnych o wszystkich użytkownikach jest niezgodne z Kartą Praw Podstawowych Unii Europejskiej.

W świetle powyższego zmianie powinny zatem ulec przepisy ustawy Prawo telekomunikacyjne w zakresie zasad dostępu „uprawnionych podmiotów" do danych objętych tajemnicą telekomunikacyjną. Należy przy tym zwrócić uwagę na to, że zawarte w projekcie ustawy Prawo komunikacji elektronicznej (druk sejmowy nr 423), mającej docelowo zastąpić obowiązującą ustawę Prawo telekomunikacyjne, przewidują identyczny, niezgodny z orzecznictwem TSUE, model retencji danych telekomunikacyjnych oraz zasad dostępu do tych danych, na co organ ochrony danych osobowych także zwrócił uwagę w swojej niedawnej opinii[2].

Wnioski:

Analiza stanowiska TSUE, wyrażonego w wyroku z dnia 30 kwietnia 2024 r. w sprawie **Procura della Repubblica presso il Tribunale di Bolzano, C-178/22,** oraz polskiego prawa prowadzi do wniosku, że konieczna jest zmiana właściwych przepisów regulujących dostęp organów prowadzących postępowanie karne do danych osobowych chronionych tajemnicą telekomunikacyjną.

Łączę wyrazy szacunku,

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych

[2] Opinia Prezesa UODO z 7 czerwca 2024 r., sygn. spraw DOL.401.60.2024.WL.PM i DOL.401.62.2024.WL.PM.