PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH

Mirosław Wróblewski

Warszawa, 18 lutego 2026 r.

Sąd Okręgowy w Gdańsku
Wydział I Cywilny
ul. Nowe Ogrody 30/34
80-803 Gdańsk
ePuap

Sygn. akt I C 1281/25

Stanowisko Prezesa Urzędu Ochrony Danych Osobowych zawierające istotny pogląd dla sprawy o sygn. akt I C 1281/25.

Działając na podstawie art. 99 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[1], Prezes Urzędu Ochrony Danych Osobowych (dalej również: „Prezes UODO albo organ nadzorczy") przedstawia **istotny pogląd dla sprawy o sygn. akt I C 1281/25** prowadzonej w Sądzie Okręgowym w Gdańsku, dotyczący wykładni i stosowania przepisów o ochronie danych osobowych.

Przedstawiony poniżej pogląd nie stanowi rozstrzygnięcia indywidualnej sprawy ani wiążącej interpretacji prawa. Został on sformułowany w celu wsparcia Sądu w prawidłowej wykładni i stosowaniu przepisów prawa ochrony danych osobowych, z uwzględnieniem interesu publicznego, konstytucyjnych standardów ochrony praw jednostki oraz dorobku prawa Unii Europejskiej.

W ocenie Prezesa UODO, niniejsza sprawa dotyczy zagadnień o fundamentalnym znaczeniu dla ochrony danych osobowych oraz autonomii informacyjnej obywateli w związku z koniecznością zapewnienia zgodności krajowych przepisów o retencji danych z prawem Unii Europejskiej, co w pełni uzasadnia wyrażenie niniejszego stanowiska organu nadzorczego w granicach interesu publicznego.

[1] Ustawa z 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

Bezpośrednim impulsem do przedstawienia niniejszego istotnego poglądu jest powzięta przez Prezesa UODO informacja o skierowaniu przez Sąd Okręgowy w Gdańsku wniosku o wydanie orzeczenia w trybie prejudycjalnym do Trybunału Sprawiedliwości Unii Europejskiej (TSUE). Sprawa ta, zarejestrowana pod sygnaturą C-741/25 Ranerski, dotyczy kluczowych kwestii interpretacyjnych art. 15 ust. 1 dyrektywy 2002/58/WE w związku z art. 7, 8, 11 i 52 ust. 1 Karty Praw Podstawowych UE, w kontekście krajowych przepisów o retencji danych. Fakt skierowania pytania prejudycjalnego w tej sprawie jest organowi nadzorczemu znany z oficjalnych publikacji, w tym strony internetowej Trybunału, a niniejsze stanowisko ma na celu wsparcie Sądu w procesie wykładni prawa, co będzie miało fundamentalne znaczenie dla rozstrzygnięcia niniejszej sprawy.Należy również wskazać, że Prezes Urzędu Ochrony Danych Osobowych, realizując swoje zadania wynikające z przepisów rozporządzenia 2016/679[2] oraz ustawy o ochronie danych osobowych, przygotował szczegółowe stanowisko w sprawie C-741/25 na potrzeby postępowania przed TSUE, które zostało przekazane Ministerstwu Spraw Zagranicznych[3]. W stanowisku tym Prezes UODO wskazał, że art. 15 ust. 1 dyrektywy 2002/58/WE stoi na przeszkodzie regulacjom krajowym (takim jak art. 47 i 49 Prawa komunikacji elektronicznej), które nakładają na operatorów uogólniony i niezróżnicowany obowiązek zatrzymywania danych o ruchu i lokalizacji. Zbieżność argumentacji przedstawionej w niniejszym piśmie ze stanowiskiem procesowym przygotowanym dla Rządu RP podkreśla wagę problemu i potrzebę zapewnienia pełnej zgodności prawa krajowego ze standardami unijnymi.

Podobne stanowisko Prezes UODO zajmował na etapie prac legislacyjnych nad projektem ustawy – Prawo komunikacji elektronicznej, o której będzie mowa w dalszej części pisma[4], a także w pismach kierowanych do właściwych podmiotów już po wejściu ustawy w życie[5].

I. Ogólne ramy prawne przetwarzania danych osobowych

1. Rozporządzenie 2016/679, zgodnie z art. 1 ust. 1, ustanawia przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych. Rozporządzenie 2016/679 określa obowiązki administratora danych, do których należy przetwarzanie danych osobowych z zachowaniem przesłanek w nim określonych.

2. Przepisem uprawniającym administratorów danych do przetwarzania danych osób fizycznych jest art. 6 ust. 1 rozporządzenia 2016/679, zgodnie z którym przetwarzanie jest

[2] RozporządzenieParlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021, str. 35), dalej jako: RODO albo rozporządzenie 2016/679.
[3] Pismo o sygnaturze DOL.0623.2.2026 z 29.1.2026 r. skierowane do Ignacego Niemczyckiego, Sekretarza Stanu w Ministerstwie Spraw Zagranicznych.
[4] Zob. opinia Prezesa Urzędu Ochrony Danych Osobowych z 7 czerwca 2024 r. udostępniona na stronie uodo.gov.pl/pl/138/3126
[5] Zob. wystąpienie do Ministra Cyfryzacji, udostępnione na stronie https://uodo.gov.pl/pl/138/3850

zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z warunków wymienionych w tym przepisie.

Katalog przesłanek wymienionych w art. 6 ust. 1 rozporządzenia 2016/679 jest zamknięty. Każda z przesłanek legalizujących proces przetwarzania danych osobowych ma charakter autonomiczny i niezależny. Oznacza to, że przesłanki te co do zasady są równoprawne, a wobec tego spełnienie co najmniej jednej z nich stanowi o zgodnym z prawem przetwarzaniu danych osobowych.

3. Niezależnie od zgody osoby, której dane dotyczą (art. 6 ust. 1 lit. a rozporządzenia 2016/679), przetwarzanie danych osobowych jest dopuszczalne między innymi wtedy, gdy jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c rozporządzenia 2016/679), jak również gdy jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora (art. 6 ust. 1 lit. f rozporządzenia 2016/679).

Zgodnie z motywem 45 rozporządzenia 2016/679, jeżeli przetwarzanie odbywa się w celu wypełnienia obowiązku prawnego, któremu podlega administrator, lub jeżeli jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, podstawę przetwarzania powinno stanowić prawo Unii lub prawo państwa członkowskiego. Rozporządzenie nie nakłada wymogu, aby dla każdego indywidualnego przetwarzania istniało szczegółowe uregulowanie prawne. Wystarczyć może to, że dane uregulowanie prawne stanowi podstawę różnych operacji przetwarzania wynikających z obowiązku prawnego, któremu podlega administrator, lub że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej. Prawo Unii lub prawo państwa członkowskiego powinno określać także cel przetwarzania. Ponadto prawo to może doprecyzowywać ogólne warunki określone w niniejszym rozporządzeniu dotyczące zgodności przetwarzania z prawem, określać sposoby wskazywania administratora, rodzaj danych osobowych podlegających przetwarzaniu, osoby, których dane dotyczą, podmioty, którym można ujawniać dane osobowe, ograniczenia celu, okres przechowywania oraz inne środki zapewniające zgodność z prawem i rzetelność przetwarzania.

4. Szczegółowe wymogi dotyczące podstawy przetwarzania danych, gdy jest określona w prawie Unii lub w prawie państwa członkowskiego ustanawia art. 6 ust. 3 rozporządzenia 2016/679. Zgodnie z tym przepisem, podstawa przetwarzania, o której mowa w ust. 1 lit. c i e, musi być określona: a) w prawie Unii; lub b) w prawie państwa członkowskiego, któremu podlega administrator. Cel przetwarzania musi być określony w tej podstawie prawnej lub, w przypadku przetwarzania, o którym mowa w ust. 1 lit. e – musi być ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Zgodnie z art. 6 ust. 3 lit. b rozporządzenia 2016/679, podstawa prawna może zawierać przepisy szczegółowe dostosowujące stosowanie przepisów niniejszego rozporządzenia, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane

osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. **Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.**

5. Zasady przetwarzania danych osobowych uregulowane zostały w art. 5 ust. 1 rozporządzenia 2016/679. Stosownie do powyższego przepisu dane osobowe muszą być: a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość"); b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu"); c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych"); d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość"); e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania"); f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

6. Stosownie do motywu 39 rozporządzenia 2016/679 odnoszącego się do zasad przetwarzania danych osobowych, wszelkie przetwarzanie danych osobowych powinno być zgodne z prawem i rzetelne. Dla osób fizycznych powinno być przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane. Zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich

dotyczących. Osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem. W szczególności konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania. Dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu. Należy podjąć wszelkie rozsądne działania zapewniające sprostowanie lub usunięcie danych osobowych, które są nieprawidłowe.

7. W rozporządzeniu 2016/679 uregulowano również prawa podmiotu danych (art. 12 i n.). Jak wskazano w motywie 65 rozporządzenia 2016/679, każda osoba fizyczna powinna mieć prawo do sprostowania danych osobowych jej dotyczących oraz prawo do "bycia zapomnianym", jeżeli zatrzymywanie takich danych narusza niniejsze rozporządzenie, prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator. Osoba, której dane dotyczą, powinna w szczególności mieć prawo do tego, by jej dane osobowe zostały usunięte i przestały być przetwarzane, jeżeli dane te nie są już niezbędne do celów, w których były zbierane lub w inny sposób przetwarzane, jeżeli osoba, której dane dotyczą, cofnęła zgodę lub jeżeli wniosła sprzeciw wobec przetwarzania danych osobowych jej dotyczących, lub jeżeli przetwarzanie jej danych osobowych nie jest z innego powodu zgodne z niniejszym rozporządzeniem. Niemniej dalsze zatrzymywanie danych osobowych powinno być uznane za zgodne z prawem, jeżeli jest niezbędne do wywiązania się z obowiązku prawnego.

Zgodnie z treścią art. 17 ust. 1 lit. d rozporządzenia 2016/679 osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli dane osobowe były przetwarzane niezgodnie z prawem. Zgodnie jednak z art. 17 ust. 3 lit. b rozporządzenia 2016/679, powyższy przepis nie ma zastosowania, w zakresie w jakim przetwarzanie jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

II. Dane gromadzone na podstawie ustawy - Prawo komunikacji elektronicznej[6] przez przedsiębiorców telekomunikacyjnych jako dane osobowe

[6] Ustawa z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej (Dz. U. z 2024 r. poz. 1221 ze zm.), dalej jako: p.k.e.

9. Operatorzy telekomunikacyjni, wykonując obowiązki określone w art. 47 i 49 p.k.e. oraz w przepisach wykonawczych[7] , zatrzymują i przechowują niezwykle szeroki zakres informacji o użytkownikach usług łączności elektronicznej. Dane te obejmują przede wszystkim tzw. **dane o ruchu i dane o lokalizacji**, czyli informacje generowane lub przetwarzane w toku korzystania z usług telekomunikacyjnych. W praktyce są to m.in. numery telefonów inicjującego i odbierającego połączenie (MSISDN), identyfikatory IMSI (karta SIM) i IMEI (urządzenie końcowe), adresy IP przypisane użytkownikom w czasie rzeczywistym, daty, godziny i czas trwania połączeń, współrzędne geograficzne stacji bazowych (BTS), przez które przechodzi połączenie, dane dotyczące rodzaju połączenia (rozmowa, SMS, połączenie internetowe), a także informacje o numerach i adresach, z którymi zastępowane są połączenia. W przypadku usług internetowych i poczty elektronicznej obejmuje to również identyfikatory użytkownika, loginy, adresy e-mail, znaczniki czasowe logowania i wylogowania oraz dane o wykorzystanych portach sieciowych. W konsekwencji zestaw tych informacji pozwala odtworzyć pełny cyfrowy ślad aktywności użytkownika w przestrzeni telekomunikacyjnej – jego kontakty, częstotliwość komunikacji, miejsca przebywania, a nawet wzorce zachowań.

10. Choć pojedyncza dana, taka jak numer telefonu czy adres IP, może wydawać się neutralna, w rozumieniu art. 4 pkt 1 rozporządzenia 2016/679 stanowi ona dane osobowe, ponieważ umożliwia zidentyfikowanie osoby fizycznej bezpośrednio lub pośrednio. Wystarczy, że operator lub inny podmiot dysponuje dodatkowymi informacjami (np. umową abonenta, kartą SIM, danymi rejestracyjnymi, lokalizacją urządzenia), które pozwalają przyporządkować daną techniczną do konkretnej osoby. W orzecznictwie TSUE (m.in. w wyroku z 19.10.2016 r. w sprawie C-582/14, *Breyer*, EU:C:2016:779) oraz w wytycznych Europejskiej Rady Ochrony Danych[8] przyjmuje się konsekwentnie, że **adres IP, numer IMSI, IMEI, dane lokalizacyjne czy identyfikatory urządzeń końcowych są danymi osobowymi**, o ile można w sposób racjonalny ustalić tożsamość użytkownika, nawet pośrednio, za pomocą środków prawnie dostępnych administratorowi.

11. Co więcej, w przypadku danych o ruchu i lokalizacji, zestawionych w dłuższym okresie, ich wartość identyfikacyjna znacząco rośnie – pozwalają one bowiem na odtworzenie profilu życia osoby, jej relacji społecznych, miejsc przebywania, codziennych nawyków czy przekonań. W tym sensie dane przetwarzane w systemach retencji mają charakter **danych osobowych wrażliwych funkcjonalnie**, ponieważ ujawniają wzorce zachowań i elementy życia prywatnego chronione art. 7 i 8 Karty Praw Podstawowych Unii Europejskiej [9]oraz art. 47 i 51 Konstytucji RP.

---

[7] Rozporządzenie Ministra Infrastruktury z 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania, Dz. U. z 2009 r. Nr 226, poz. 1828), dalej jako: rozporządzenie Ministra Infrastruktury z 2009 r..

[8] Europejska Rada Ochrony Danych (dalej jako: EROD) jest niezależnym unijnym organem, powołanym na mocy RODO (art. 68), w celu zapewnienia jednolitego stosowania przepisów o ochronie danych w EOG. Zob. wytyczne 4/2020, wytyczne 2/2023 czy oświadczenie 5/2024, dostępne na stronie internetowej https://www.edpb.europa.eu/edpb_pl

[9] Dz. Urz. C 202 z 7.6.2016 r., s. 389, dalej jako KPP UE.

12. Z tego względu obowiązek masowego zatrzymywania, analizowania i udostępniania organom państwa tego rodzaju danych – bez powiązania z konkretnym celem lub osobą – stanowi głęboką ingerencję w prawo do prywatności i autonomii informacyjnej jednostki. Wymaga on zatem ścisłego przestrzegania zasad wynikających z rozporządzenia 2016/679, w szczególności zgodności z prawem, ograniczenia celu, minimalizacji i ograniczenia okresu przechowywania danych[10].

III. Przepisy p.k.e. jako podstawa prawna przetwarzania danych osobowych

13. Przedsiębiorcy telekomunikacyjni wywodzą obecnie obowiązek przetwarzania danych o połączeniach z przepisów art. 47 i 49 p.k.e. Zgodnie z art. 47 ust. 1 p.k.e. przedsiębiorca telekomunikacyjny jest obowiązany na własny koszt: 1) zatrzymywać i przechowywać dane, o których mowa w art. 49 ust. 1, generowane w publicznej sieci telekomunikacyjnej lub przez niego przetwarzane, na terytorium Rzeczypospolitej Polskiej, przez okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, a z dniem upływu tego okresu dane te niszczyć, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z przepisami odrębnymi; 2) udostępniać dane, o których mowa w pkt 1, uprawnionym podmiotom, a także sądowi i prokuratorowi, zgodnie z wymaganiami określonymi w przepisach wydanych na podstawie art. 49 ust. 3, oraz na zasadach i w trybie określonych w przepisach odrębnych; 3) chronić dane, o których mowa w pkt 1, przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą, nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem lub ujawnieniem, zgodnie z przepisami ust. 5, art. 386-405 oraz podejmując środki techniczne i organizacyjne, o których mowa w art. 39 ust. 2 pkt 3.

14. Zgodnie z art. 47 ust. 2 p.k.e. obowiązkom, o których mowa w ust. 1, podlegają dane dotyczące połączeń zrealizowanych i nieudanych prób połączeń, o których mowa w art. 386 ust. 1 pkt 5.

Z odesłania do art. 49 ust. 1 p.k.e wynika, iż obowiązkiem retencji objęte są dane dotyczące publicznie dostępnych usług telekomunikacyjnych niezbędne do: 1) jednoznacznego zidentyfikowania zakończenia sieci, telekomunikacyjnego urządzenia końcowego oraz użytkownika końcowego: a) inicjującego połączenie, b) do którego kierowane jest połączenie; 2) określenia: a) daty i godziny połączenia oraz czasu jego trwania, b) rodzaju połączenia, c) lokalizacji telekomunikacyjnego urządzenia końcowego.

15. Wskazane przepisy wyznaczają przedmiotowy zakres przechowywania, udostępniania i ochrony danych, gdyż tylko dane zatrzymane mogą być przedmiotem dalszych czynności[11].

[10] Zob. również rozważania Trybunału Konstytucyjnego w wyroku o sygn. akt K 23/11 z 30 lipca 2014 r. co do istoty przetwarzania danych telekomunikacyjnych w kontekście ochrony prywatności, w związku z przepisami Konstytucji RP.
[11] Por. S. Piątek, Komentarz do art. 47, w: S. Piątek (red.), Prawo komunikacji elektronicznej. Komentarz, Warszawa 2025, dostęp: Legalis.

Zatrzymywanie danych oznacza utrwalenie danych wytworzonych w sieci telekomunikacyjnej lub przetworzonych w związku z wykonywaniem usług. Przedsiębiorca musi w sposób trwały ustalić wymagane informacje i zapisać je w swoich urządzeniach. Zatrzymaniu podlegają dane generowane w publicznej sieci telekomunikacyjnej, czyli dane dotyczące różnych stanów urządzeń pracujących lub obsługiwanych w tej sieci. Ponadto zatrzymaniu podlegają dane przetwarzane przez przedsiębiorców w związku ze świadczeniem usług. Mogą to być dane otrzymywane od użytkownika lub innych przedsiębiorców współdziałających przy świadczeniu usług.

Ponieważ niektóre dane podlegające obowiązkowi zatrzymywania (np. numer abonenta wywołującego) są otrzymywane od przedsiębiorców współpracujących przy wykonywaniu usług, to przedsiębiorca zobowiązany do retencji powinien podjąć niezbędne działania w celu uzyskania tych danych, np. poprzez odpowiednie postanowienia w umowach o połączeniu sieci. Dotyczy to również danych generowanych w związku z usługami transgranicznymi.

Z kolei obowiązek przechowywania danych wykonywany jest przez zachowanie utrwalonych danych w taki sposób, aby przez ustalony ustawą okres mogły być udostępnione uprawnionym podmiotom. Ustawa nie wymaga przechowywania zatrzymanych danych w określonym układzie i porządku, ale wymagania dotyczące sposobu ich udostępniania i ochrony uzasadniają gromadzenie ich w sposób uporządkowany.

16. Prawo komunikacji elektronicznej nie jest pierwszą ustawą, która reguluje obowiązek retencji danych. Wręcz przeciwnie, stanowi kontynuację przepisów Prawa telekomunikacyjnego[12].

Na gruncie przepisów Prawa telekomunikacyjnego sprawy retencji danych telekomunikacyjnych były unormowane w art. 180a-180c. Przepisy te były wynikiem wdrożenia do prawa polskiego dyrektywy 2006/24/WE[13].

17. Nowa ustawa powiela część dotychczasowych regulacji i jednocześnie implementuje do polskiego porządku prawnego przepisy unijne: dyrektywę Parlamentu Europejskiego i Rady (UE) z 11 grudnia 2018 r. 2018/1972 ustanawiającą Europejski kodeks łączności elektronicznej[14] .

18. Do przepisów Prawa telekomunikacyjnego (jako rozwiązań analogicznych) ustawodawca odesłał w uzasadnieniu do projektu ustawy (druk sejmowy nr 423), co uprawnia do stwierdzenia, że **przepisy p.k.e. stanowią kontynuację przepisów Prawa**

[12] Ustawa z 16 lipca 2004 r. – Prawo telekomunikacyjne, ostatnio Dz. U. z 2024 r. poz. 34, uchylona przez p.k.e., dalej jako: Prawo telekomunikacyjne.
[13] Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE, Dz. Urz. L 105 z 13.4.2006 r., s. 54, nieobow., dalej jako: dyrektywa 2006/24/WE.
[14] Dz.Urz. L 321 z 17.12.2018, s. 36 , dalej jako: EKŁE.

telekomunikacyjnego i również wiążą się z przepisami prawa UE, w tym z dyrektywą 2006/24/WE (już nieobowiązującą), ale również z dyrektywą 2002/58/WE[15].

IV. Standard ochrony w świetle prawa UE

19. Skoro genezą przepisów p.k.e. są przepisy prawa Unii Europejskiej, należy przywołać te przepisy. Nie będą w tym miejscu przywoływane przepisy dyrektywy 2006/24/WE, skoro nie obowiązuje ona w tym momencie (o czym będzie mowa dalej). Należy jednak skupić się na innych przepisach prawa UE.

20. W pierwszej kolejności należy przywołać przepisy prawa pierwotnego, w tym art. 7 i 8 KPP UE i art. 16 Traktatu o funkcjonowaniu Unii Europejskiej[16], które dotyczą poszanowania prawa do prywatności i prawa do ochrony danych osobowych i które są przedmiotem wykładni TSUE również w sprawach, do których nastąpi nawiązanie w dalszej części uzasadnienia. Artykuły 7 i 8 KPP UE ustanawiają podwójny, komplementarny standard ochrony prywatności w sferze komunikacji elektronicznej, który ma kluczowe znaczenie dla oceny dopuszczalności retencji danych telekomunikacyjnych. Wspólnie przepisy te tworzą ścisły standard materialny i instytucjonalny ochrony, który wykracza poza tradycyjne rozumienie prawa do prywatności i obejmuje kontrolę nad informacjami o jednostce oraz gwarancje proceduralne zapobiegające ich nadużyciu.

Z tego standardu wynika (por. art. 52 ust. 1 KPP UE), że każda ingerencja w sferę prywatności poprzez gromadzenie, przechowywanie lub udostępnianie danych telekomunikacyjnych musi spełniać trzy podstawowe warunki: po pierwsze – być **przewidziana w ustawie**, po drugie – służyć **realizacji celu o charakterze ogólnym**, a po trzecie – być **konieczna i proporcjonalna** względem tego celu.

21. Dane o ruchu i lokalizacji, które mogą ujawniać szczegółowe informacje o życiu codziennym, relacjach społecznych czy miejscach pobytu jednostki, wkraczają bowiem głęboko w sferę chronioną art. 7 i 8 KPP UE, niezależnie od tego, czy dotyczą treści komunikacji, czy jedynie jej „metadanych". Z punktu widzenia KPP UE, dopuszczalne jest wyłącznie takie zatrzymywanie danych, które ogranicza się do zakresu **ściśle niezbędnego** i które jest otoczone gwarancjami prawnymi zapewniającymi skuteczną kontrolę ich przetwarzania. Artykuły 7 i 8 Karty ustanawiają zatem zasadniczy paradygmat w sprawach retencji danych: ochrona prywatności i autonomii informacyjnej jednostki stanowi punkt wyjścia, a nie wyjątek, od którego bezpieczeństwo publiczne może odstąpić jedynie w granicach ściśle określonych i uzasadnionych prawem.

22. Przypomnieć należy, że KPP UE wiąże państwa członkowskie zgodnie z art. 51 ust. 1. Przepis ten wskazuje, że postanowienia Karty mają zastosowanie m.in. do państw członkowskich wyłącznie w zakresie, w jakim stosują one prawo Unii. W omawianym przypadku nie powinno być wątpliwości co do tej kwestii. Państwa członkowskie (w tym

[15] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz. Urz. L 201 z 31.7.2002 r., s. 37 ze zm., dalej jako: dyrektywa 2002/58/WE.
[16] Dz. Urz. UE C 202z 7.6.2016 r., s. 247, dalej jako: TFUE.

organy państwa) stosują prawo UE m.in. wtedy, gdy implementują prawo UE/WE albo gdy odstępują od jego wymagań[17].

23. W 2002 r. Parlament Europejski i Rada Unii Europejskiej przyjęły wspomnianą wcześniej dyrektywę 2002/58/WE. Ustanawia ona w art. 5 zasadę poufności komunikacji, zakazując co do zasady przechwytywania i przechowywania danych o ruchu bez zgody użytkowników. W art. 15 ust. 1 tej dyrektywy prawodawca przewidział możliwość stosowania przez państwa członkowskie wyjątku od zasady poufności komunikacji, motywowanego względami bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego czy zapobiegania przestępstwom, ich dochodzenia, wykrywania lub karania. W szczególności, przepis ten pozwala na uchwalanie krajowych środków ustawodawczych wprowadzających ogólny obowiązek zatrzymania danych na określony czas. Wskazuje jednocześnie, że **takie środki muszą być niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego**.

24. Również przepisy EKŁE nie zaprzeczają ww. wnioskom. W motywie 6 EKŁE wyraźnie wskazano, że dyrektywa „pozostaje bez uszczerbku dla uprawnień każdego z państw członkowskich do podejmowania środków, mających na celu zapewnienie ochrony jego podstawowych interesów w zakresie bezpieczeństwa, zapewnienie porządku publicznego i bezpieczeństwa publicznego oraz umożliwienie wykrywania lub ścigania przestępstw i prowadzenia dochodzeń w ich sprawie, mając na uwadze, że wszelkie ograniczenia korzystania z praw i wolności uznanych w Karcie, w szczególności jej art. 7, 8 i 11, **takie jak ograniczenia dotyczące przetwarzania danych, muszą być przewidziane prawem, przestrzegać istoty praw i wolności oraz podlegać zasadzie proporcjonalności zgodnie z art. 52 ust. 1 Karty**.” (podkr. wł.).

V. Orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej

25. Kluczowym wyrokiem Trybunału Sprawiedliwości UE jest orzeczenie zapadłe w sprawach połączonych C-293/12 i C-594/12 Digital Rights Ireland[18]. W wyroku tym TSUE dokonał wykładni przepisów KPP UE i stwierdził nieważność dyrektywy 2006/24/WE.

Zdaniem Trybunału, przyjmując dyrektywę 2006/24/WE prawodawca Unii przekroczył granice, które wyznacza poszanowanie zasady proporcjonalności. W wyroku Trybunał w szczególności wyznaczył sposób interpretacji nie tylko dyrektywy, co do której stwierdził nieważność, ale przede wszystkim art. 7 i 8 KPP, w świetle których to przepisów analizował dyrektywę.

Po pierwsze, dyrektywa obejmowała w sposób uogólniony wszystkie jednostki, środki łączności elektronicznej i dane o ruchu, przy czym nie przewidziano jakiegokolwiek

[17] Szerzej A. Wróbel, Komentarz do art. 51, w: A. Wróbel (red.), Karta Praw Podstawowych UE. Komentarz, wyd. 2, Warszawa 2020, dostęp: Legalis. oraz M. Wróblewski, Karta Praw Podstawowych Unii Europejskiej, [w:] „System Prawa Unii Europejskiej. Tom I. Podstawy i źródła prawa Unii Europejskiej”, red. S. Biernat, Warszawa 2020, s. 725-775.

[18] Wyrok z 8.4.2014 r. w sprawach połączonych C-293/12 i C-594/12, Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, The Commissioner of the Garda Síochána, Irlandii i Attorney General oraz Kärntner Landesregierung, Michael Seitlinger, Christof Tschohl i in., EU:C:2014:238, dalej jako: wyrok w sprawie Digital Rights Ireland.

zróżnicowania, ograniczenia lub wyjątku w zależności od celu dotyczącego zwalczania poważnych przestępstw. Po drugie, dyrektywa nie wyróżniała żadnego obiektywnego kryterium, które pozwoliłoby zagwarantować, by właściwe organy krajowe miały dostęp do danych i mogły je wykorzystywać wyłącznie do zapobiegania przestępstwom, które mogą być uważane za wystarczająco poważne, by uzasadnić taką ingerencję, oraz do wykrywania i ścigania karnego takich przestępstw. Przeciwnie, dyrektywa ograniczała się do odesłania w sposób ogólny do pojęcia „poważnych przestępstw" zdefiniowanych przez każde państwo członkowskie w jego prawie krajowym. Ponadto dyrektywa nie przewidywała materialnych i proceduralnych przesłanek dotyczących sytuacji, w których właściwe organy krajowe mogą uzyskać dostęp do danych i je później wykorzystywać. Dostęp do danych nie był w szczególności podporządkowany uprzedniej kontroli sądu lub niezależnego organu administracyjnego. Po trzecie, w odniesieniu do okresu zatrzymania danych, dyrektywa przewidywała okres co najmniej sześciu miesięcy, przy czym nie przeprowadzała jakiegokolwiek rozróżnienia pomiędzy kategoriami danych w zależności od zainteresowanych osób lub ewentualnej użyteczności danych w stosunku do zakładanego celu. Ponadto okres ten wynosił od co najmniej sześciu miesięcy do co najwyżej dwudziestu czterech miesięcy, przy czym dyrektywa nie precyzowała obiektywnych kryteriów, na podstawie których należy ustalić okres zatrzymywania, by zagwarantować jego ograniczenie do tego, co ściśle niezbędne.

26. W połączonych sprawach C-203/15 i C-698/15 Tele2[19], TSUE potwierdził, że krajowe przepisy nakazujące ogólne i niezróżnicowane zatrzymywanie danych są niezgodne z prawem UE. Sąd w wydanym orzeczeniu podkreślił, że retencja musi być ograniczona do tego, co absolutnie niezbędne i proporcjonalne do celu, a jej zakres musi być ściśle zdefiniowany. W kolejnych orzeczeniach TSUE uszczegóławiał ustanowione standardy, bazując w szczególności na przepisach dyrektywy 2002/58/WE (która nadal obowiązuje).

27. Zgodnie z wyrokiem w połączonych sprawach C-511/18, C-512/18 i C-520/18 La Quadrature du Net,[20], , ogólne zatrzymywanie danych jest niedopuszczalne. Dopuszczalne jest jedynie celowe, selektywne zatrzymywanie danych, ściśle ograniczone w czasie i zakresie do zwalczania poważnych przestępstw lub zagrożeń dla bezpieczeństwa narodowego, pod warunkiem uprzedniej kontroli przez niezależny organ sądowy lub administracyjny.

W wyroku tym TSUE orzekł, że art. 15 ust. 1 dyrektywy 2002/58/WE w zw. z art. 4 ust. 2 Traktatu o Unii Europejskiej, a także art. 7, 8 i 11 oraz art. 52 ust. 1 KPP UE **należy interpretować w ten sposób, że stoi on na przeszkodzie uregulowaniu krajowemu umożliwiającemu organowi państwa nałożenie na dostawców usług łączności elektronicznej obowiązku uogólnionego i niezróżnicowanego transmitowania**

[19] Wyrok z 21 grudnia 2016 r. w sprawach połączonych C-203/15 i C-698/15 Tele2 Sverige AB przeciwko Post- och telestyrelsen oraz Secretary of State for the Home Department przeciwko Tom Watson, Peter Brice, Geoffrey Lewis, EU:C:2016:970, dalej jako wyrok Tele2.
[20] Wyrok z 6 października 2020 r., C-511/18, La Quadrature du Net i in. przeciwko Premier Ministre i in., EU:C:2020:791, dalej jako wyrok La Quadrature du Net.

służbom wywiadu i bezpieczeństwa danych o ruchu i danych o lokalizacji do celów ochrony bezpieczeństwa narodowego (por. pkt 168 wyroku i wyjątki tam przewidziane).

28. Zgodnie z wyrokiem w sprawie C-746/18 H.K.[21], dostęp do danych może być przyznany jedynie w celu zwalczania poważnej przestępczości. TSUE wskazał, że art. 15 dyrektywy 2002/58/WE sprzeciwia 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 takich danych, oraz ilości lub rodzaju danych dostępnych przez taki okres.

29. Z kolei w wyroku w sprawie C-140/22 G.D.[22] , Trybunał ponownie wskazał, że art. 15 ust. 1 dyrektywy 2002/58 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 KPP należy interpretować w ten sposób, iż stoi on na przeszkodzie środkom ustawodawczym przewidującym, w celach, o których mowa w art. 15 ust. 1, prewencyjne uogólnione i niezróżnicowane zatrzymywanie danych o ruchu i danych o lokalizacji.

Natomiast art. 15 ust. 1 w związku z art. 7, 8 i 11 oraz art. 52 ust. 1 KPP nie stoi na przeszkodzie przepisom: 1) w których państwo może nakazać dostawcom usług łączności elektronicznej ogólne i niezróżnicowane zatrzymywanie danych. Taki nakaz musi być jednak ograniczony czasowo do tego, co ściśle niezbędne (z możliwością przedłużenia w razie utrzymywania się zagrożenia) oraz podlegać skutecznej kontroli sądu lub niezależnego organu administracyjnego; 2) których celem jest ochrona bezpieczeństwa narodowego, zwalczania poważnej przestępczości oraz zapobiegania poważnym zagrożeniom dla bezpieczeństwa publicznego, dopuszczalne jest ukierunkowane (celowane) zatrzymywanie danych. Musi być ono jednak ograniczone na podstawie obiektywnych i niedyskryminacyjnych kryteriów, np. do określonego kręgu osób lub konkretnego obszaru geograficznego, i trwać tylko tak długo, jak jest to absolutnie konieczne; 3) w celu zwalczania poważnej przestępczości, a tym bardziej w celu ochrony bezpieczeństwa narodowego, właściwe organy mogą wydać dostawcom usług nakaz niezwłocznego zabezpieczenia i przechowania przez określony czas konkretnych danych, którymi ci dostawcy już dysponują. Taka decyzja musi podlegać skutecznej kontroli sądowej.

Wszystkie te dopuszczalne środki muszą być uregulowane **w jasnych i precyzyjnych przepisach krajowych, które gwarantują, że zatrzymywanie danych odbywa się**

[21] Wyrok z 2 marca 2021 r. w sprawie C-746/18, Postępowanie karne przeciwko H.K., EU:C:2021:152, dalej jako wyrok w sprawie H.K.
[22] Wyrok z 5 kwietnia 2022 r. w sprawie C-140/20, G.D. przeciwko The Commissioner of the Garda Sfochana i in., EU:C:2022:258.

zgodnie z materialnymi i proceduralnymi warunkami, a obywatele dysponują skutecznymi środkami ochrony przed ryzykiem nadużyć.

30. Uzupełniająco należy wskazać, że po wyroku z 6.10.2020 r. w sprawach połączonych La Quadrature du Net TSUE również w innych orzeczeniach konsekwentnie doprecyzowywał standardy dotyczące zarówno **dopuszczalności retencji**, jak i **warunków dostępu** do danych. W szczególności w sprawie C-623/17, Privacy International[23] Trybunał zakwestionował krajowe mechanizmy umożliwiające uogólnione i niezróżnicowane przekazywanie danych służbom w kontekście bezpieczeństwa narodowego. Następnie w sprawach C-724/19[24], C-350/21[25] oraz w sprawach połączonych C-339/20 i C-397/20[26] TSUE utrzymał zasadę, że generalna i niezróżnicowana retencja danych o ruchu i lokalizacji co do zasady jest niedopuszczalna, a wszelkie wyjątki wymagają ścisłych gwarancji materialnych i proceduralnych, w tym efektywnej kontroli niezależnego organu oraz realnej ochrony sądowej. Z kolei w wyroku C-162/22[27] Trybunał zaakcentował ograniczenia dotyczące wtórnego wykorzystywania danych – ich użycie musi pozostawać powiązane z celem spełniającym wymogi wynikające z art. 15 ust. 1 dyrektywy 2002/58/WE w świetle KPP UE.

30. Wreszcie, w dniu 30 kwietnia 2024 r. zapadł wyrok w sprawie C-470/21 La Quadrature du Net (EU:C:2024:370; dalej jako: wyrok w sprawie La Quadrature du Net II). Trybunał wskazał w nim, że dopuszczalne jest zatrzymywanie i udostępnianie jedynie danych o tożsamości cywilnej użytkowników, takich jak adresy IP, w ściśle określonych i proporcjonalnych przypadkach, np. dla celów ochrony praw autorskich lub identyfikacji sprawców naruszeń prawa. Jednocześnie TSUE ponownie podkreślił, że ogólna i nieukierunkowana retencja danych o ruchu i lokalizacji pozostaje sprzeczna z art. 7, 8 i 11 KPP UE, a dostęp do danych musi być ograniczony do niezbędnego minimum i poddany skutecznej kontroli.

31. Warto przy tym wskazać, że w doktrynie wskazuje się – jeszcze na gruncie Prawa telekomunikacyjnego – że „Ważne – w tym również dla prawa krajowego i zakresu regulacji krajowej są te fragmenty wyroków, w których TS podkreśla wyraźnie, że wszelkie przetwarzanie danych osobowych przez usługodawców, czy to zwykłe ujawnienie, czy też przekazanie danych osobowych organom państwowym, wchodzi w zakres rozporządzenia 2016/679, a w szczególnym przypadku danych dotyczących łączności elektronicznej – dyrektywy 2002/58/WE. To pociąga za sobą obowiązek stosowania Karty Praw Podstawowych i oceny rozwiązań (również krajowych) w tym kontekście. Nie ma zatem wątpliwości, że przepisy polskiej ustawy Prawo telekomunikacyjne czy też np. ustawy o Policji powinny podlegać ocenie pod kątem zgodności z ww. przepisami i dalsze

[23] Wyrok z 6 października 2020 r. w sprawie C-623/17 Privacy International, EU:C:2020:790.
[24] Wyrok z 16 grudnia 2021 r. w sprawie C-724/19 Postępowanie karne przeciwko HP, EU:C:2021:1020.
[25] Wyrok z 17 listopada 2022 r. w sprawie C-350/21 Postępowanie karne wszczęte przez Spetsializirana prokuratura, EU:C:2022:896.
[26] Wyrok z 20 września 2022 r. w sprawach połączonych C-339/20 i C-397/20 Postępowanie karne przeciwko VD i SR, EU:C:2022:703.
[27] Wyrok z 7 września 2023 r. w sprawie C-162/22 A.G. przeciwko Lietuvos Respublikos generalinė prokuratūra. (EU:C:2023:631)

oczekiwanie na podjęcie stosownych działań przez prawodawcę jest już bezzasadne. Trybunał Sprawiedliwości przy tym zwrócił również uwagę na to, że kiedy państwa członkowskie stosują bezpośrednio środki stanowiące odstępstwo od poufności łączności elektronicznej, bez nakładania obowiązków przetwarzania na dostawców usług łączności elektronicznej, ochrona osób, których dane dotyczą, jest objęta jedynie prawem krajowym. **Stosowane zatem w takim wypadku środki muszą respektować w szczególności prawo krajowe rangi konstytucyjnej i wymogi Konwencji o ochronie praw człowieka i podstawowych wolności** [podkr. wł.][28]. Taka konkluzja wynika również bezpośrednio z art. 51 KPP i orzecznictwa TSUE[29], które wskazuje na konieczność stosowania Karty przez państwa członkowskie w zakresie, w jakim stosują prawo UE (co – jak wykazano wyżej - ma miejsce w niniejszej sprawie).

VI. Przepisy Konstytucji RP

32. Obowiązek zatrzymywania i przechowywania przez operatorów telekomunikacyjnych danych o połączeniach stanowi poważną ingerencję w konstytucyjnie chronione prawa jednostki – w szczególności prawo do prywatności (art. 47 Konstytucji), wolność i tajemnicę komunikowania się (art. 49) oraz autonomię informacyjną (art. 51). Ingerencja taka może być dopuszczalna **jedynie w granicach** określonych przez art. 31 ust. 3 Konstytucji, a zatem musi być ustanowiona w ustawie, niezbędna w demokratycznym państwie prawnym i proporcjonalna wobec realizowanego celu – np. ochrony bezpieczeństwa publicznego lub zwalczania poważnej przestępczości.

33. W świetle art. 8 ust. 1 Konstytucji RP, który stanowi, że Konstytucja jest najwyższym prawem Rzeczypospolitej, wszelkie regulacje ustawowe dotyczące retencji danych muszą być interpretowane w sposób zapewniający poszanowanie jej zasad oraz istoty praw i wolności jednostki.

34. Z kolei zgodnie z art. 91 ust. 3 Konstytucji RP, prawo Unii Europejskiej ma pierwszeństwo przed prawem krajowym w razie kolizji, co oznacza, że także krajowe przepisy o retencji danych – takie jak art. 47 PKE – muszą być stosowane w zgodzie z prawem UE i orzecznictwem Trybunału Sprawiedliwości (m.in. w sprawach *Digital Rights Ireland*, *Tele2 Sverige* i *La Quadrature du Net*). Dodatkowo wzmacnia to art. 9 Konstytucji RP statuujący obowiązek przestrzegania wiążącego RP prawa międzynarodowego (w tym prawa pierwotnego UE).

35. Trybunał Konstytucyjny już przed 2015 r. podkreślał konieczność proporcjonalnego ograniczania sfery prywatności. We wspomnianym już wyroku z 30 lipca 2014 r. (sygn. akt K 23/11) uznał, że przepisy umożliwiające służbom dostęp do danych telekomunikacyjnych bez ustanowienia niezależnej kontroli naruszają art. 47 i 49

[28] Za: A. Grzelak, K. S. Zielińska, Między prawem do prywatności i ochrony danych osobowych a zapewnieniem bezpieczeństwa publicznego i walką z przestępczością. Problemu retencji danych ciąg dalszy. Glosa do wyroku TS z 6 października 2020 r., C-623/17, C-511/18, C-512/18 oraz C-520/18, EPS 2021, nr 8, s. 28-36.
[29] Zob. wyrok z 21 grudnia 2011 r., C-411/10 i C-493/10, N.S. i in., EU:C:2011:865, pkt 119, 120.

Konstytucji RP w związku z art. 31 ust. 3 Konstytucji RP. Wcześniej, w wyroku z 11 maja 2007 r. (sygn. akt K 30/07), Trybunał stwierdził, że ustawodawca musi zapewnić adekwatne i skuteczne mechanizmy ochrony danych, w tym obowiązek niezwłocznego zniszczenia informacji nieistotnych dla prowadzonych postępowań. Wynika z tego, że obowiązek retencji danych – zarówno w Prawie telekomunikacyjnym, jak i w obecnym art. 47 p.k.e. – może być konstytucyjnie dopuszczalny tylko wtedy, gdy jego zakres jest ściśle ograniczony, a dostęp organów państwa do danych objęty kontrolą zewnętrzną i podporządkowany zasadzie proporcjonalności. W przeciwnym razie dochodzi do naruszenia zasady nadrzędności Konstytucji RP (art. 8 ust. 1) oraz obowiązku zapewnienia zgodności prawa krajowego z prawem Unii (art. 91 ust. 3 Konstytucji RP), a tym samym – do podważenia konstytucyjnych gwarancji prawa do prywatności i ochrony danych osobowych.

36. Dodatkowo należy wskazać, że zgodnie z art. 49 ust. 2 p.k.e., minister właściwy do spraw informatyzacji w porozumieniu z ministrem właściwym do spraw wewnętrznych oraz po zasięgnięciu opinii Ministra - Koordynatora Służb Specjalnych, jeżeli został on powołany, określi, w drodze rozporządzenia: 1) szczegółowy wykaz danych, o których mowa w ust. 1, 2) rodzaj przedsiębiorców telekomunikacyjnych niepodlegających obowiązkowi zatrzymywania i przechowywania tych danych. W tym kontekście trzeba podkreślić, że w swoim orzecznictwie Trybunał Konstytucyjny wskazywał na niezgodność takich delegacji z Konstytucją RP przez to, że naruszają wymaganie ustawowej formy dla ograniczeń prawa do prywatności autonomii informacyjnej jednostki (wyrok TK z 18 grudnia 2014 r., sygn. akt. K 33/13). Zgodnie bowiem z art. 51 Konstytucji RP, każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Nikt jednocześnie nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.

VI. Wyrok ETPC z 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce (skargi nr 72038/17 i 25237/18)

Prezes UODO, w piśmie skierowanym do Ministerstwa Spraw Zagranicznych na kanwie sprawy C-741/25 Ranerski wskazał, że przepisy polskiej ustawy Prawo telekomunikacyjne[30], uprawniającej właściwe organy do pozyskiwania danych telekomunikacyjnych były przedmiotem oceny **Europejskiego Trybunału Praw Człowieka, który wyrokiem z 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce** (skargi nr 72038/17 i 25237/18) **orzekł naruszenie art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności** (EKPC), tj. prawa do poszanowania życia prywatnego, rodzinnego oraz korespondencji w odniesieniu do skarg dotyczących reżimu kontroli operacyjnej, tajnego reżimu nadzoru w ramach

[30] Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2024, poz. 1222), nieobowiązująca.

przepisów antyterrorystycznych, a także zatrzymywania danych komunikacyjnych do potencjalnego wykorzystania przez właściwe organy lub władze krajowe[31].

W powołanym wyroku ETPC uznał, że **polskie prawo nie zapewniało wystarczających zabezpieczeń przed nadmierną ingerencją w życie prywatne jednostek, a także w odniesieniu do komunikacji objętej tajemnicą adwokacką**. Jak wskazał Trybunał, brak tych gwarancji nie został dostatecznie zrównoważony przez istniejący mechanizm kontroli sądowej. Trybunał zauważył, że obowiązujące przepisy nie wymagały od sądu rozpatrującego wniosek o zezwolenie na inwigilację potwierdzenia, czy istnieje „uzasadnione podejrzenie" w odniesieniu do osoby, której dotyczy wniosek, a w szczególności zbadania, czy istnieją jakiekolwiek dowody na to, że osoba ta planuje, dokonuje lub dokonała czynów przestępczych lub jakiegokolwiek innego przestępstwa pozwalającego na zastosowanie środków tajnej inwigilacji, takich jak czyny zagrażające bezpieczeństwu narodowemu. Ponadto Trybunał uznał, że istniejąca procedura wydawania zgód powinna zostać uzupełniona o inne mechanizmy kontroli proceduralnej post factum. Zauważając jednocześnie, że w obecnym stanie prawnym, nie przewidziano obowiązku informowania osoby objętej środkiem kontroli, nawet po upływie określonego czasu i nawet w przypadku, gdy nie zagrażałoby to celowi, dla którego zastosowano ww. środek. ETPC wskazał przy tym, że prawo nie przewidywało skutecznego środka odwoławczego dla osób, które uważały, że zostały poddane tajnej inwigilacji.

Ponadto Trybunał uznał, że przechowywanie danych telekomunikacyjnych przez uprawnione organy stanowiło ingerencję w prywatną sferę wnioskodawców. Zdaniem Trybunału **ingerencja wynikająca z obowiązku przechowywania danych komunikacyjnych dla dostawców usług telekomunikacyjnych była bardzo poważna**. Środek ten mógł wywołać u zainteresowanych osób poczucie bezbronności i nadmiernego narażenia na kontrolę ze strony trzeciej, a także mógł negatywnie wpłynąć na skuteczne korzystanie z ich podstawowych praw, w tym prawa do szacunku dla życia prywatnego i korespondencji oraz prawa do nawiązywania relacji z innymi. Trybunał wskazał, że nawet jeśli dostęp organów państwowych do danych udostępnianych im przez dostawców usług telekomunikacyjnych jest podany pewnymi gwarancjami ochrony przed możliwymi nadużyciami, w tym mechanizmem retrospektywnego przeglądu sądowego, te **gwarancje są niewystarczające**, by naprawić stwierdzone niedociągnięcia w reżimie przechowywania danych komunikacyjnych i nie może zatem dostosować reżimu przechowywania danych komunikacyjnych do wymagań artykułu 8 Konwencji.

Trybunał orzekł, że przepisy krajowe, na podstawie których dostawcy usług telekomunikacyjnych zobowiązani byli do zatrzymywania danych komunikacyjnych w

[31] Por. też wyroki ETPC: z 02.08.1984 r. w sprawie Malone przeciwko Zjednoczonemu Królestwu, skarga nr 8691179; z 24.04.1990 r. w sprawie Kruslin przeciwko Francji, skarga nr 11801/85 oraz w sprawie Huvig przeciwko Francji, skarga nr 11105/84; z 29.06.2006 r. w sprawie Weber i Saravia przeciwko Niemcom, skarga 54934/00; z 10.02.2009 r. w sprawie Iordachi i inni przeciwko Mołdawii, skarga nr 25198/02; z 02.09.2010 r. w sprawie Uzun przeciwko Niemcom, skarga nr 35623/05; z 04.12.2015 r. w sprawie Zakharov przeciwko Rosji, skarga nr 47413/06; z 12.01.2016 r. w sprawie Szabó i Vissy przeciwko Węgrom, skarga nr 37138/14; z 25.05.2021 r., w sprawie Big Brother Watch i in. przeciwko Zjednoczonemu Królestwu, skarga nr 58170/13, 62322/14 i 24960/15. z 11 stycznia 2022 r. w sprawie Ekimdzhiev i inni przeciwko Bułgarii, skarga nr 70078/12.

sposób ogólny do ewentualnego wykorzystania w przyszłości przez odpowiednie organy krajowe, są niewystarczające do tego, by móc stwierdzić, że ingerencja w prawo skarżących do poszanowania ich życia prywatnego była ograniczona do tego, co konieczne w demokratycznym społeczeństwie.Trybunał stwierdził tym samym, że **naruszono artykuł 8 Konwencji w zakresie przechowywania danych komunikacyjnych w celu potencjalnego dostępu przez właściwe organy krajowe**.

Wymaga także podkreślenia, że ETPC dopuścił do rozpoznania skargi na polskie ustawodawstwo i uznał, że skarżący mogli twierdzić, iż są ofiarami naruszenia Konwencji, pomimo tego, że nie byli w stanie wykazać, na poparcie swoich wniosków, że zostali poddani konkretnemu środkowi inwigilacji. ETPC wskazał, że samo istnienie zaskarżonych przepisów, w tym w szczególności przepisów dotyczących zatrzymywania danych telekomunikacyjny w sposób ogólny, nieukierunkowany, przez okres 12 miesięcy, stanowiło ingerencję w prawa skarżących na mocy art. 8 Konwencji.

VI. Ocena przepisów p.k.e. w świetle przepisów prawa UE

37. Art. 47 p.k.e. wprowadza obowiązek uogólnionego i prewencyjnego zatrzymywania danych o ruchu i lokalizacji wszystkich użytkowników usług telekomunikacyjnych, niezależnie od ich związku z jakimkolwiek postępowaniem czy podejrzeniem naruszenia prawa. Tymczasem, jak wynika z powyższego, takie rozwiązanie stanowi ingerencję w prawo do ochrony danych osobowych z art. 8 KPP UE, przekraczającą granice proporcjonalności określone w art. 52 ust. 1 KPP. Karta ustanawia bowiem standard, zgodnie z którym każda ingerencja w prawo do prywatności musi być konieczna, proporcjonalna i ściśle określona w czasie, zakresie i celu, co nie jest spełnione w modelu retencji przyjętym w p.k.e.

38. Dyrektywa 2002/58/WE w art. 15 ust. 1 dopuszcza możliwość ograniczenia obowiązku poufności komunikacji jedynie w zakresie niezbędnym, odpowiednim i proporcjonalnym dla ochrony bezpieczeństwa narodowego lub zapobiegania poważnej przestępczości. W ocenie Prezesa Urzędu Ochrony Danych Osobowych, polski ustawodawca nie dokonał rozróżnienia między tymi kategoriami – utożsamiając poważną przestępczość z bezpieczeństwem publicznym – co jest sprzeczne z dyrektywą oraz z interpretacją dokonaną przez TSUE. W efekcie obowiązek retencji przewidziany w art. 47 p.k.e. wykracza poza granice dopuszczone przez prawo UE (dyrektywę 2002/58/WE wraz z wyrokami, w których dokonywana jest wykładnia tych przepisów) i narusza zasadę celowości i minimalizacji danych wynikającą z rozporządzenia 2016/679. Przepisy art. 47 i 49 P.k.e. wprowadzają rozwiązanie, które TSUE uznał już za niedopuszczalne w innych państwach członkowskich. Przewidują bowiem generalny obowiązek przechowywania danych wszystkich użytkowników, bez względu na cel, czas trwania czy istnienie związku z konkretnym zagrożeniem. W ocenie Prezesa UODO, **model masowego** zatrzymywania danych, ich analizowania i udostępniania organom państwa – bez powiązania z konkretnym celem lub osobą – stanowi zatem głęboką ingerencję w prawo do prywatności i autonomii informacyjnej jednostki, **naruszając jednocześnie fundamentalne zasady i warunki legalności wynikające z art. 5 i 6 rozporządzenia 2016/679, o których była mowa wyżej.**

Podsumowanie

Mając na uwadze przedstawione wyżej rozważania, Prezes Urzędu Ochrony Danych Osobowych wskazuje, że ocena zgodności przetwarzania danych osobowych w ramach obowiązków retencyjnych z przepisami rozporządzenia 2016/679 wymaga każdorazowo uwzględnienia standardów wynikających z prawa Unii Europejskiej, w szczególności art. 7 i 8 Karty Praw Podstawowych Unii Europejskiej oraz art. 52 ust. 1 tej Karty, utrwalonego powołanym w niniejszym piśmie orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej, a także art. 8 Europejskiej Konwencji Praw Człowieka wykładanego w powołanym orzecznictwie Europejskiego Trybunału Praw Człowieka, a także norm Konstytucji RP wraz z powołanym orzecznictwem Trybunału Konstytucyjnego.

W ocenie Prezesa Urzędu Ochrony Danych Osobowych przepisy prawa krajowego stanowiące podstawę przetwarzania danych osobowych muszą spełniać wymogi konieczności i proporcjonalności oraz zapewniać poszanowanie istoty prawa do ochrony danych osobowych i prawa do prywatności. W przypadku wątpliwości co do zgodności takich przepisów z prawem Unii Europejskiej sąd krajowy jest zobowiązany do dokonania ich oceny w świetle prawa Unii, z uwzględnieniem wykładni dokonanej przez Trybunał Sprawiedliwości Unii Europejskiej.

Prezes Urzędu Ochrony Danych Osobowych uważa zatem, że art. 15 ust. 1 dyrektywy 2002/58/WE w związku z art. 7, 8 i 11 i 52 ust. 1 KPP UE należy interpretować w ten sposób, że **stoi on na przeszkodzie** uregulowaniu krajowemu, które nakłada na operatorów dostępnych publicznie usług łączności elektronicznej **prewencyjny, niezindywidualizowany, ogólnospołeczny, nieograniczony czasowo bądź miejscowo obowiązek zatrzymywania danych o ruchu i danych o lokalizacji użytkowników końcowych tych usług**, jeżeli obowiązek ten dotyczy danych niezbędnych do określenia daty i godziny połączenia, rodzaju połączenia, lokalizacji telekomunikacyjnego urządzenia końcowego, a przedsiębiorca telekomunikacyjny ma obowiązek na własny koszt zatrzymywać i przechowywać powyższe dane generowane w publicznej sieci telekomunikacyjnej lub przez niego przetwarzane na terytorium Rzeczypospolitej Polskiej, przez okres 12 miesięcy, licząc od dnia połączenia lub nieudanej próby połączenia, a z dniem upływu tego okresu dane te niszczyć, z wyjątkiem tych, które zostały zabezpieczone, zgodnie z przepisami odrębnymi.

Przedstawiony istotny pogląd ma na celu wsparcie Sądu w dokonaniu tej oceny, pozostając w granicach kompetencji Prezesa Urzędu Ochrony Danych Osobowych określonych w art. 99 ustawy o ochronie danych osobowych.

Działając na podstawie art. 99 ustawy o ochronie danych osobowych, w związku z przedstawieniem przez Prezesa Urzędu Ochrony Danych Osobowych istotnego poglądu w niniejszej sprawie, wnoszę o:

- **uwzględnienie udziału Prezesa Urzędu Ochrony Danych Osobowych w postępowaniu głównym w zakresie przedstawionego istotnego poglądu,**

- **przekazanie Trybunałowi Sprawiedliwości Unii Europejskiej informacji o udziale Prezesa Urzędu Ochrony Danych Osobowych w postępowaniu głównym,**
- **powiadomienie Prezesa Urzędu Ochrony Danych Osobowych o dalszym toku postępowania prejudycjalnego przed Trybunałem Sprawiedliwości Unii Europejskiej, celem umożliwienia ewentualnego skorzystania z uprawnień przewidzianych w art. 96–97 Regulaminu postępowania przed TSUE.**

Mirosław Wróblewski

Prezes Urzędu

Ochrony Danych Osobowych

/dokument podpisany elektronicznie/