Michał Kamiński

Zagadnienie retencji danych w Unii Europejskiej z perspektywy orzeczenia Tele2

1. Wprowadzenie

W dniu 21 grudnia 2016 r. Trybunał Sprawiedliwości Unii Europejskiej (dalej: TSUE) wydał wyrok w sprawach połączonych C-203/15 Tele2 *Sverige AB/Post-ochtelestyrelsen* i C-698/15 *Secretary of State for the Home Departament/Tom Watson i inni*[1].

Wyrok, o którym mowa, został wydany na skutek złożenia wniosków o orzeczenie w trybie prejudycjalnym, na podstawie art. 267 *Traktatu o Funkcjonowaniu Unii Europejskiej* (dalej: TFUE), przez administracyjny sąd apelacyjny w Sztokholmie w Królestwie Szwecji i sąd apelacyjny dla Anglii i Walii (wydział cywilny) Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej. Jest to drugie orzeczenie TSUE dotyczące zagadnienia retencji danych telekomunikacyjnych oraz dostępu do nich organów właściwych do zwalczania przestępczości, po orzeczeniu *Digital Rights Ireland i inni* CV-293/12 i C-594/12 z 8 kwietnia 2014 r.[2], które unieważniło dyrektywę retencyjną[3]. Potencjalne skutki ostatniego orzeczenia dla możliwości korzystania z danych telekomunikacyjnych przez policję i służby specjalne państw członkowskich Unii Europejskiej mogą być jednak poważniejsze.

W tym orzeczeniu TSUE dokonał wykładni art. 15 ust. 1 dyrektywy 2002/58/WE z 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)[4], zmienionej dyrektywą 2009/136/WE z 25 listopada 2009 r.[5], w związku z art. 7, 8, 11 i art. 52 Karty praw podstawowych Unii Europejskiej.

Dyrektywa 2002/58/WE (dalej: dyrektywa o e-prywatności) jest aktem wydanym w celu harmonizacji przepisów krajowych państw członkowskich Unii Europejskiej dla zapewnienia równoważnego poziomu ochrony podstawowych praw i wolności, szczególnie prawa do prywatności i poufności, w odniesieniu do przetwarzania danych osobowych w sektorze łączności elektronicznej oraz w celu zapewnienia swobodnego przepływu we Wspólnocie tego typu danych oraz urządzeń i usług łączności elektronicznej[6].

---

[1] LEX nr 2202679.

[2] LEX nr 1444266.

[3] *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*.

[4] *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. UE L 201 z 31 VIII 2002 r., s. 37–47.

[5] *Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów* **(**Dz. Urz. UE L z 2002 r. nr 201, s. 37, z 2006 r. nr 105, s. 54 oraz z 2009 r. nr 337, s. 11).

[6] Art. 1 ust. 1 dyrektywy 2002/58/WE.

Jednocześnie z zakresu przedmiotowej dyrektywy, zgodnie z jej art. 1 ust. 3, miała być wyłączona działalność pozostająca poza zakresem *Traktatu Ustanawiającego Wspólnotę Europejską* – działalność w zakresie Wspólnej Polityki Zagranicznej i Bezpieczeństwa oraz współpraca policyjna i sądowa w sprawach karnych[7], a także działalność dotycząca bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa i działalność państwa w obszarze prawa karnego.

Przepis art. 15 ust. 1 dyrektywy o e-prywatności stanowi:

> 1. Państwa Członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1–4, i art. 9 tej dyrektywy, gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (i.e. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej (...). W tym celu Państwa Członkowskie mogą, między innymi, uchwalić środki ustawodawcze przewidujące przechowywanie danych przez określony czas uzasadnione na podstawie zasad ustanowionych w niniejszym ustępie. Wszystkie środki określone w niniejszym ustępie są zgodne z ogólnymi zasadami prawa wspólnotowego, w tym zasadami określonymi w art. 6 ust. 1 i 2 Traktatu o Unii Europejskiej.

Spośród przytoczonych przepisów art. 5 dyrektywy o e-prywatności nakazuje państwom członkowskim zapewnienie poufności komunikacji, art. 6 – niezwłoczne usuwanie lub anonimizację danych o ruchu w sieci, art. 8 reguluje oferowanie użytkownikowi wyświetlania i ograniczenie identyfikacji rozmów przychodzących i wychodzących, art. 9 zaś – ograniczenie przetwarzania danych o lokalizacji. Art. 15 ust. 1 pozwala państwom członkowskim na ograniczenie tych zasad w swoim ustawodawstwie w celu ochrony wymienionych w tym przepisie prawnie chronionych wartości związanych z bezpieczeństwem i ściganiem przestępczości. Reasumując, omawiany przepis pozwala państwom członkowskim na uregulowanie przepisami krajowymi kontroli treści przekazów telekomunikacyjnych i retencji danych dotyczących tych przekazów.

Warto zauważyć, że unieważniona przez TSUE dyrektywa retencyjna dodała do art. 15 dyrektywy o e-prywatności ust. 1b, który wskazywał, że ustępu 1 nie stosuje się do danych zatrzymywanych na jej podstawie.

Przepisy Karty Praw Podstawowych Unii Europejskiej, które TSUE wziął pod uwagę w swoim orzeczeniu, to: art. 7 (prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się), art. 8 (prawo każdej osoby do ochrony danych osobowych jej dotyczących), art. 11 (prawo do wolności wypowiedzi) i art. 52 (zakres i wykładnia praw i zasad) przewidujący, że wszelkie ograniczenia w korzystaniu z praw i wolności uznanych w Karcie muszą być przewidziane ustawą, szanować istotę tych praw i wolności oraz mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób.

W orzeczeniu TSUE, które jest tematem niniejszego artykułu, wskazano, że przepis art. 15 dyrektywy o e-prywatności należy interpretować w ten sposób, że:

[7] Dyrektywa o e-prywatności odsyła do traktatów europejskich w brzmieniu sprzed wejścia w życie *Traktatu z Lizbony*.

1) stoi na przeszkodzie uregulowaniom krajowym, w których przewidziano uogólnione i niezróżnicowane zatrzymywanie wszystkich danych o ruchu oraz danych dotyczących lokalizacji wszystkich abonentów i zarejestrowanych użytkowników wszystkich środków łączności elektronicznej – do celów zwalczania przestępczości,
2) stoi na przeszkodzie obowiązywaniu uregulowań krajowych dotyczących ochrony i bezpieczeństwa danych o ruchu i danych o lokalizacji, a zwłaszcza dostępu właściwych organów władz krajowych do przechowywanych danych, które to przepisy, w ramach zwalczania przestępczości, nie ograniczają tego dostępu jedynie do celów walki z poważną przestępczością, nie uzależniają przyznania go od uprzedniej kontroli sprawowanej przez sąd lub niezależny organ administracyjny i nie ustanawiają wymogu, aby te dane były przechowywane na obszarze Unii

Najważniejszą tezą wyroku jest stwierdzenie przez TSUE, że państwa członkowskie nie mogą nakładać na dostawców usług komunikacji elektronicznej ogólnego obowiązku retencji danych. Prawo UE nie pozwala na ogólną i nieselektywną retencję danych o ruchu i danych dotyczących lokalizacji. Państwa członkowskie mogą jednak przyjmować przepisy przewidujące ukierunkowaną retencję tego rodzaju danych wyłącznie w celu zwalczania poważnej przestępczości, przy założeniu, że te przepisy ograniczają kategorie danych podlegających retencji, objęte nimi środki komunikacji i osoby oraz okres retencji danych do tego, co jest niezbędne dla osiągnięcia celu tych przepisów. Dostęp właściwych organów narodowych do danych podlegających retencji musi być poddany określonym warunkom, w tym ocenie sądu lub niezależnego organu administracyjnego.

2. Geneza orzeczenia – sprawa *Digital Rights Ireland*

Omawiane orzeczenie należy rozpatrywać w kontekście konsekwencji wynikających z wyroku *Digital Rights Ireland i inni* CV-293/12 i C-594/12 z 2014 r.[8], w którym TSUE orzekł o nieważności dyrektywy retencyjnej z uwagi na to, że dopuszczony przez nią stopień ingerencji w prawa i wolności gwarantowane zarówno przez pierwotne, jak i wtórne źródła prawa UE – związany z ogólnym obowiązkiem retencji danych o ruchu i danych dotyczących lokalizacji – nie był ograniczony do tego, co niezbędnie konieczne do osiągnięcia celu tego rodzaju regulacji. Zasadniczym celem wyżej wymienionego aktu prawnego była harmonizacja przepisów państw członkowskich w dziedzinie zatrzymywania danych wytwarzanych lub przetwarzanych przez dostawców ogólnie dostępnych usług komunikacji elektronicznej lub publicznych sieci łączności. Przepisy dyrektywy nakazywały zapewnienie organom ścigania dostępu do powyższych danych zarówno do celów zapobiegania poważnym przestępstwom, takim jak przestępczość zorganizowana i terroryzm, jak i do celów dochodzenia, wykrywania i ścigania takich przestępstw. Nakazywały również przyjęcie środków nakładających na dostawców usług telekomunikacyjnych na terenie Unii Europejskiej obowiązek zatrzymywania danych o ruchu i lokalizacji oraz powiązanych danych niezbędnych do identyfikacji abonenta lub użytkownika.

W wyniku procesu implementacji dyrektywy do krajowych porządków prawnych wdrożono rozwiązania ustawowe stanowiące podstawę prawną do przechowywania przez operatorów telekomunikacyjnych danych o połączeniach telefonicznych obywa-

[8] LEX nr 1444266.

teli UE (m.in. danych o ruchu w sieci, danych lokalizacyjnych) oraz podstawę dostępu do tych danych przez sądy, organy ścigania i służby specjalne państw członkowskich.

Trybunał przeprowadził badanie przepisów dyrektywy w dwóch aspektach: w zakresie naruszenia praw podstawowych do poszanowania życia prywatnego i ochrony danych podstawowych oraz pod kątem zgodności regulacji prawnych zawartych w dyrektywie z zasadą proporcjonalności.

W omawianym wyroku TSUE uznał, że nakładając obowiązek zatrzymywania danych i umożliwiając dostęp do nich właściwym organom krajowym, dyrektywa zbyt mocno ingerowała w prawa podstawowe do poszanowania życia społecznego i do ochrony danych osobowych. Ponadto, zdaniem Trybunału, okoliczność, że zatrzymywanie i późniejsze wykorzystywanie danych było dokonywane bez poinformowania o tym abonenta i zarejestrowanego użytkownika, może wywołać u zainteresowanych osób poczucie, że ich życie prywatne podlega stałemu nadzorowi.

Jednakże biorąc pod uwagę to, że przepisy dyrektywy nie zezwalały na zapoznawanie się z treścią komunikatów elektronicznych jako taką i nakazywały dostawcom usług i sieci przestrzeganie określonych zasad ochrony i bezpieczeństwa danych, Trybunał uznał, że przewidziane przepisami dyrektywy zatrzymywanie danych nie naruszało zasadniczej treści praw podstawowych do poszanowania życia prywatnego i do ochrony danych osobowych. Ponadto Trybunał przyznał, że zatrzymanie danych w celu ich ewentualnego udostępnienia właściwym organom krajowym rzeczywiście odpowiadało celowi w postaci interesu ogólnego, jakim jest zwalczanie poważnej przestępczości, a w konsekwencji – zapewnienie bezpieczeństwa wewnętrznego.

Zdaniem TSUE prawodawca Unii, przyjmując dyrektywę retencyjną, przekroczył jednak granice, które wyznacza poszanowanie zasady proporcjonalności. Trybunał zauważył, że przy uwzględnieniu znaczącej roli, jaką odgrywa ochrona danych osobowych w odniesieniu do prawa podstawowego do poszanowania życia prywatnego, oraz zakresu i znaczenia ingerencji w to prawo, do której prowadziła dyrektywa, uprawnienia dyskrecjonalne prawodawcy Unii powinny być ograniczone, do tego, co ściśle niezbędne. Powyższy warunek nie został jednak spełniony w przypadku omawianego aktu prawnego.

Trybunał stwierdził ponadto, że zapisy dyrektywy nie przewidywały żadnego kryterium gwarantującego, że właściwe organy krajowe, które miałyby dostęp do danych, będą je wykorzystywać wyłącznie do zapobiegania przestępstwom, uważanym – w świetle zakresu i znaczenia ingerencji w omawiane prawa podstawowe – za wystarczająco poważne, by uzasadnić taką ingerencję. Przeciwnie, dyrektywa ograniczała się do odesłania w sposób ogólny do pojęcia p o w a ż n e p r z e s t ę p s t w a, zdefiniowanych przez każde państwo członkowskie w prawie krajowym, co, zdaniem Trybunału, było niewystarczające.

Dyrektywa nie przewidywała również materialnych i proceduralnych przesłanek dostępu właściwych organów do danych podlegających retencji. Dostęp do danych nie został podporządkowany uprzedniej kontroli sądu lub niezależnego organu administracyjnego. Trybunał uznał, że dyrektywa nie przewidywała wystarczających gwarancji umożliwiających zapewnienie skutecznej ochrony danych przed niebezpieczeństwem nadużycia oraz przed jakimkolwiek dostępem do danych i ich wykorzystywaniem w sposób niedozwolony.

Trybunał wskazał również, że dyrektywa przewidywała okres co najmniej sześciu miesięcy na zatrzymanie danych, przy czym nie przeprowadzała jakiegokolwiek rozróżnienia między kategoriami danych w zależności od zainteresowanych osób lub ewentu-

alnej użyteczności danych w stosunku do zakładanego celu. Ponadto, okres ten wynosił od co najmniej sześciu do dwudziestu czterech miesięcy, przy braku obiektywnych kryteriów, na podstawie których należało ustalić okres zatrzymywania, aby zagwarantować jego ograniczenie do tego, co ściśle niezbędne.

Wydanie przez TSUE wskazanego orzeczenia nie miało bezpośredniego skutku dla obowiązywania przepisów krajowych państw członkowskich przewidujących obowiązek retencji danych, wydanych w celu implementacji unieważnionej dyrektywy. Dlatego pojawiły się wątpliwości co do tego, czy uznanie dyrektywy za nieważną oznacza powrót do możliwości samodzielnego regulowania tych zagadnień przez państwa członkowskie. Państwa członkowskie pozostawały jednak związane Kartą Praw Podstawowych, a łącznikiem uzasadniającym jej stosowanie był art. 15 dyrektywy o e-prywatności określający zakres dopuszczalnych wyjątków od poufności w komunikacji elektronicznej[9].

Określenie przez Trybunał elementów wzorca zgodności z Kartą Praw Podstawowych, który, jego zdaniem, naruszała unieważniona dyrektywa, stworzyło poręczne argumenty do kwestionowania uregulowań krajowych dotyczących retencji danych telekomunikacyjnych.

3. Stan faktyczny

Jedną z konsekwencji powyższego orzeczenia było skierowanie przez sądy Szwecji i Wielkiej Brytanii niezależnych od siebie wniosków o wydanie orzeczenia w trybie prejudycjalnym, w celu ustalenia, czy na dostawcach usług elektronicznych w dalszym ciągu spoczywa obowiązek retencji danych wynikający z unieważnionej dyrektywy.

Po wydaniu orzeczenia *Digital Rights* szwedzkie przedsiębiorstwo telekomunikacyjne Tele2 poinformowało miejscowy Urząd Pocztowy i Telekomunikacyjny, że nie zamierza prowadzić dalej retencji danych oraz że dokona zniszczenia danych uzyskanych w okresie poprzedzającym wydanie wyroku (sprawa C-203/15)[10]. Należy wspomnieć, że szwedzki system prawny nakładał na dostawców usług elektronicznych obowiązek systematycznego i ciągłego zatrzymywania danych o ruchu i danych dotyczących lokalizacji wszystkich abonentów oraz zarejestrowanych użytkowników w odniesieniu do wszelkich środków komunikacji elektronicznej, bez żadnych wyjątków, oraz przechowywania ich przez sześć miesięcy[11].

Pytanie prejudycjalne w sprawie C-689/15 jest konsekwencją rozpatrywanego przez Sąd Najwyższy Anglii i Walii wniosku o ocenę legalności sekcji 1 tzw. ustawy DRIPA[12], w którym podniesiono m.in. że ta ustawa jest niezgodna z art. 7, 8 Karty Praw Podstawowych i z art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności. Zaskarżone przepisy DRIPA upoważniały sekretarza stanu w Departamencie Spraw Wewnętrznych do żądania od publicznych operatorów telekomunikacyjnych retencji ww. danych, z wyłączeniem treści komunikacji.

---

[9] A. Grzelak, *Glosa do wyroku TS z dnia 21 grudnia 2016 r. C-203/15 oraz C-698/15. Trybunał Sprawiedliwości ponownie o relacji między koniecznością zwalczania przestępczości a prawem do prywatności*, „Europejski Przegląd Sądowy" 2017, nr 3, s. 31–36, LEX nr 316663.

[10] Teza 44 orzeczenia C-203/15, LEX nr 2202679.

[11] Tezy 15–19 orzeczenia C-203/15.

[12] *The Data Retention and Investigatory Powers Act 2014* – ustawa Parlamentu Zjednoczonego Królestwa, która uzyskała Sankcję Królewską 17 VII 2014 r., po uchwaleniu 14 VII 2014 r. Celem ustawy było zapewnienie służbom bezpieczeństwa dostępu do danych telekomunikacyjnych i internetowych wobec unieważnienia tzw. dyrektywy retencyjnej przez Trybunał Sprawiedliwości Unii Europejskiej, uchylonej i zastąpionej 31 XII 2016 r. przez ustawę I*nvestigatory Powers Act*.

Na podstawie wniosków o wydanie orzeczenia w trybie prejudycjalnym złożonych przez sądy szwedzki i brytyjski, TSUE został zobowiązany do udzielenia odpowiedzi na pytanie, czy przepisy prawa krajowego nakładające na operatorów telekomunikacyjnych ogólny obowiązek nieselektywnej retencji danych – zezwalające na dostęp do tych danych właściwym organom narodowym, jeżeli obowiązek ten nie jest ograniczony wyłącznie do zwalczania poważnej przestępczości – są zgodne z prawem Unii Europejskiej, zwłaszcza z dyrektywą 2002/58 dotyczącą prywatności w sektorze łączności elektronicznej, interpretowaną w świetle Karty Praw Podstawowych UE[13].

4. Główne tezy orzeczenia

Trybunał stwierdził w wyroku, że prawo UE nie pozwala na przyjmowanie przepisów prawa krajowego przewidujących ogólny obowiązek nieselektywnej retencji danych. Zgodnie z argumentacją Trybunału ingerencja w prawa i wolności gwarantowane przez system prawa UE, wynikająca z obowiązywania tego rodzaju przepisów, ma niezwykle poważny charakter. Z tego względu taką ingerencję może uzasadniać wyłącznie cel, jakim jest zwalczanie poważnej przestępczości[14].

Trybunał podkreślił również, że podlegające jego ocenie przepisy krajowe przewidujące powyższy obowiązek nie wymagają, aby istniał jakikolwiek związek między danymi podlegającymi retencji a zagrożeniem bezpieczeństwa publicznego i nie jest on ograniczony do zatrzymywania danych dotyczących określonego okresu, miejsca czy osób, o których można sądzić, że są powiązane z usiłowaniem dokonania, przygotowywaniem lub dokonywaniem poważnego przestępstwa. W konsekwencji, normy tego rodzaju wykraczają poza zakres tego, co jest absolutnie konieczne i może być uznane za uzasadnione w demokratycznym społeczeństwie, jak wymaga tego dyrektywa 2002/58 interpretowana w świetle Karty Praw Podstawowych[15].

W ocenie Trybunału nie powinno budzić wątpliwości to, że dyrektywa o e-prywatności nie stoi na przeszkodzie funkcjonowaniu w krajowych porządkach prawnych przepisów nakładających na operatorów telekomunikacyjnych obowiązek ukierunkowanej retencji dla celów zwalczania poważnej przestępczości, pod warunkiem że zawiera ona odpowiednie ograniczenia powodujące, że zakres zatrzymywania danych jest zawężony do tego, co absolutnie konieczne dla realizacji tego celu[16].

W odniesieniu do dostępu właściwych organów narodowych do danych retencyjnych Trybunał potwierdził, że właściwe przepisy prawa krajowego nie mogą ograniczać się do stwierdzenia, że dostęp jest uzasadniony jednym z celów wskazanych w dyrektywie, nawet gdy tym celem jest zwalczanie poważnej przestępczości. Podstawą tych przepisów muszą być obiektywne kryteria w celu dokładnego określenia, w jakich okolicznościach i na jakich warunkach uprawnione organy mogą uzyskać dostęp do danych podlegających retencji[17].

Dostęp uprawnionych organów do danych, z wyjątkiem szczególnie pilnych przypadków, powinien podlegać uprzedniej kontroli niezależnego organu administracyjnego

[13] Orzeczenie C-203/15, tezy 51 i 59.
[14] Tamże, teza 102.
[15] Tamże, tezy 105–107.
[16] Tamże, teza 108.
[17] Tamże, tezy 109–111.

lub sądu[18]. Właściwe organy narodowe, które uzyskały zgodę na dostęp do danych po weryfikacji przez ww. sąd lub organ, są zobowiązane do poinformowania zainteresowanej osoby o dostępie do danych retencyjnych jej dotyczących[19].

Przepisy narodowe muszą stanowić, że dane mogą być przechowywane wyłącznie na terytorium UE oraz że podlegają nieodwracalnemu zniszczeniu po upływie okresu retencji[20].

5. Skutki wyroku TSUE wydanego w trybie prejudycjalnym dla prawa krajowego państw członkowskich

Zgodnie z art. 19 ust. 3 lit. b *Traktatu o Unii Europejskiej* (dalej: TUE) TSUE orzeka w trybie prejudycjalnym (wydaje tzw. *preliminary ruling*) na wniosek sądów państw członkowskich, w sprawie wykładni prawa Unii lub ważności aktów przyjętych przez instytucje. Wymieniona kompetencja została doprecyzowana w art. 267 *Traktatu o Funkcjonowaniu Unii Europejskiej*, zgodnie z którym TSUE jest właściwy do orzekania w trybie prejudycjalnym o wykładni traktatów oraz o ważności i wykładni aktów przyjętych przez instytucje, organy lub jednostki organizacyjne Unii Europejskiej. Co istotne – postępowanie o wydanie orzeczenia w trybie prejudycjalnym z art. 267 nie jest ani powództwem, ani skargą. Stanowi ono formę współpracy między sądem krajowym państwa członkowskiego, przed którym toczy się postępowanie w sprawie, a TSUE[21]. Powyższe oznacza, że bieg tego postępowania określa zarówno prawo UE, jak i przepisy proceduralne państwa członkowskiego, którego sąd rozstrzyga daną sprawę.

Jednocześnie należy dodać, że w związku z tym, że w świetle art. 267 akapit 1 lit. b TFUE sąd krajowy może zwracać się z wnioskiem o dokonanie wykładni aktów przyjętych przez instytucje, organy lub jednostki organizacyjne Unii, to najczęściej przedmiotem wykładni są akty prawne wymienione w art. 288 TFUE, czyli rozporządzenia, dyrektywy i decyzje, łącznie z niewiążącymi opiniami i zaleceniami, gdyż i one mogą mieć znaczenie dla wykładni i stosowania prawa przez organy krajowe.

Niniejszy wyrok (w sprawach połączonych C-203/15 *Tele2 Sverige AB/Post-ochtelestyrelsen* i C-698/15 *Secretary of State for the Home Departament/Tom Watson i inni*) zapadł na skutek pytań prejudycjalnych skierowanych właśnie w trybie art. 267 TFUE (a nie w trybie art. 263 TFUE, czyli skargi bezpośredniej na nieważność aktu prawa UE).

Nie budzi wątpliwości to, że orzeczenie TSUE o wykładni jest wiążące dla sądu, który zwrócił się z pytaniem prejudycjalnym. To związanie nie wynika, co prawda, z brzmienia art. 267, ale zostało jednoznacznie przesądzone w orzecznictwie TSUE (*Postanowienie Trybunału z dnia 5 marca 1986 r. w sprawie 69/85 Wünsche*, pkt 13)[22]. Obejmuje ono nie tylko sąd, który zwrócił się z pytaniem, lecz także wszystkie sądy krajowe orzekające w danej sprawie (np. w wyższej instancji lub instancji ponownej).

Należy również pamiętać, że orzeczenie TSUE nie ma skutku *erga omnes*. Nie stanowi też formalnego precedensu o skutkach wykraczających poza sprawę, w związku z którą zostało wydane, i wobec osób trzecich. Skuteczność orzeczenia TSUE wynika z doktryny

[18] Tamże, teza120.
[19] Tamże, teza 121.
[20] Tamże, teza 122.
[21] M. Szpunar, *Komentarz do art. 267 Traktatu o funkcjonowaniu Unii Europejskiej,* w: *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz,* t. 3, A. Wróbel (red.), WKP 2012, pkt 1.
[22] Tamże, pkt 9.1.

acte éclairé, która skutkuje m.in. tym, że sąd krajowy może odstąpić od przedłożenia pytania, jeżeli Trybunał rozstrzygał już w analogicznej sprawie. Jeśli sąd krajowy zada w takiej sprawie pytanie, TSUE może odesłać go do wcześniejszego orzecznictwa[23].

Wyrok w trybie prejudycjalnym TSUE po ogłoszeniu jest ostateczny i skuteczny *erga omnes*. Należy przy tym pamiętać, że orzeczenie wydane w trybie prejudycjalnym na podstawie art. 267 TFUE ma charakter wpadkowy w stosunku do postępowania toczącego się przed sądem krajowym. TSUE nie odnosi się do ważności aktów prawa krajowego (np. polskiego) ani też nie orzeka o sprzeczności prawa krajowego z prawem Unii Europejskiej. Po wyroku w trybie prejudycjalnym to sąd krajowy ustala konsekwencje prawne wynikające z prawa krajowego, mogące wiązać się ze wskazaną przez TSUE interpretacją określonych przepisów aktów prawa pochodnego UE. Powyższe odnosi się także do ustalenia na płaszczyźnie krajowej ewentualnych konsekwencji wynikających z krajowego prawa konstytucyjnego, czego powinny dokonać właściwe organy krajowe, w tym krajowe sądy konstytucyjne.

Należy również zaznaczyć, że – co do zasady – w razie uprzedniej implementacji zakwestionowanego przepisu dyrektywy do prawa krajowego państwa członkowskiego, w tym zakresie prawo krajowe implementujące dyrektywę podlega wciąż regulacjom prawa krajowego wyższego rzędu (np. normom konstytucyjnym) i nie traci *ex officio* mocy obowiązującej.

Istotny jest również aspekt skutków orzeczenia zapadłego w trybie art. 267 TFUE w odniesieniu do obowiązywania zakwestionowanych przepisów na płaszczyźnie prawa UE. Jest to o tyle istotne, że konsekwencje orzeczenia wydanego w trybie prejudycjalnym nie są tak oczywiste i jednoznaczne, jak w przypadku stwierdzenia nieważności w trybie art. 263 TFUE (czyli skargi na nieważność aktu prawa UE). W tym drugim przypadku (art. 263 TFUE) nieważny akt prawa UE przestaje automatycznie obowiązywać w systemie prawnym UE, aczkolwiek w przypadku rozstrzygnięcia na podstawie art. 267 TFUE nie ma już tak jednoznacznej interpretacji skutków prawnych na płaszczyźnie UE. Warto również wskazać, że istotą wyroku prejudycjalnego jest to, że pozostaje on wiążący nie tylko dla tego sądu krajowego, który skierował do TSUE pytanie prejudycjalne, lecz także dla każdego innego sądu krajowego tego państwa członkowskiego. Z tego wynika, że sądy krajowe mają uprawnienia, aby w toczącym się przed nimi postępowaniach uwzględnić skutki orzeczenia, które TSUE wydał w innym postępowaniu między innymi stronami.

Z samej istoty dyrektywy jako aktu prawa UE (zgodnie z art. 288 TFUE) wynika, że wymaga ona implementacji przez ustawodawcę krajowego. Tym samym należy przyjąć, że w prawie krajowym państwa członkowskiego UE istnieje akt prawny, który transponuje postanowienia dyrektywy do prawa krajowego. Wyrok TSUE w trybie prejudycjalnym nie będzie mieć więc bezpośredniego przełożenia w prawie polskim na ważność aktu prawa krajowego (np. ustawy) implementującego postanowienia danej dyrektywy. Tym samym z wyroku TSUE nie wynika bezpośrednio automatyczna nieważność aktu prawa krajowego, który transponował do krajowego porządku prawnego regulacje danej dyrektywy.

Reasumując, polski Trybunał Konstytucyjny, w świetle dotychczasowego orzecznictwa, nie uznaje pierwszeństwa prawa UE przed Konstytucją Rzeczypospolitej Polskiej (szczególnie w zakresie tych przepisów Konstytucji, które odnoszą się do ochrony praw odstawowych jednostki), co również ma znaczenie dla przedmiotowej sprawy.

[23] Tamże.

Przy rozważaniu możliwych skutków prawnych omawianego orzeczenia TSUE należy również rozważyć możliwość skorzystania na jego podstawie z mechanizmów prawnych służących ochronie osób w razie niewłaściwej implementacji dyrektywy. W świetle wyroku C-203/15 Trybunał wskazał, jaka powinna być właściwa interpretacja przepisów art. 15 ust. 1 dyrektywy 2002/58. W związku z zapadłym wyrokiem można uznać, że na płaszczyźnie prawa krajowego pojawił się problem niewłaściwej transpozycji dyrektywy 2002/58 do krajowych porządków prawnych państw członkowskich.

W takiej sytuacji należy rozważyć ewentualne konsekwencje postaci bezpośredniego skutku dyrektywy. Zgodnie z orzeczeniem w sprawie 41/74 van Duyn[24], Trybunał stwierdził wyraźnie, że wykluczenie możliwości powołania się przez jednostkę, której dyrektywa dotyczy, na wynikające z dyrektywy obowiązki państwa byłoby nie do pogodzenia z wiążącym charakterem dyrektywy wynikającym z art. 288 zdanie 3 TFUE.

Co do zasady – dyrektywa wywołuje skutki od momentu jej implementacji do prawa krajowego. W opinii Trybunału dyrektywa, która nie została implementowana do krajowego porządku prawnego może powodować określone skutki, jeżeli:

a) implementacja do prawa krajowego nie została dokonana lub została dokonana w sposób niewłaściwy,
b) przepisy dyrektywy mają charakter bezwarunkowy oraz są dostatecznie jasne i precyzyjne,
c) przepisy dyrektywy nadają określone prawa osobom.

Po spełnieniu tych warunków osoby mogą powoływać się na dyrektywę w postępowaniu przeciwko państwu przed sądem krajowym. Niemożliwe jest dochodzenie roszczeń przeciwko innym osobom w związku z jej bezpośrednią skutecznością, jeżeli dyrektywa nie została implementowana (wyrok C-91/92 Paola Faccini Dori v Recreb Srl z 14 czerwca 1994 r.).

Trybunał dopuszcza, pod pewnymi warunkami, uzyskanie odszkodowania za szkody wynikłe w związku z niewłaściwą lub opóźnioną implementacją dyrektywy (wyrok C-6/90 i C-9/90 Francovich i Bonifaci z 19 listopada 1991 r.).

6. Polskie przepisy o retencji danych telekomunikacyjnych a tezy orzeczenia Tele2

Obowiązujące w Polsce przepisy dotyczące retencji danych telekomunikacyjnych, tj. art. 180a i 180c *Ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne*[25] (dalej: „Pt"), zostały do tej ustawy wprowadzone na mocy *Ustawy z dnia 24 kwietnia 2009 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw*[26], wydanej w celu implementacji do polskiego porządku prawnego postanowień dyrektywy retencyjnej. Siłą rzeczy polskie przepisy zawierają rozwiązania odpowiadające przepisom tej dyrektywy zakwestionowanej przez TSUE w wyroku wydanym przez TSUE w sprawie *Digital Rights Ireland*.

Artykuł 180a ust. 1 pkt 1 Pt nakłada na operatorów publicznych sieci telekomunikacyjnych oraz dostawców publicznie dostępnych usług telekomunikacyjnych obowiązek zatrzymywania i przechowywania przez 12 miesięcy – licząc od dnia połączenia lub nieudanej próby połączenia – danych określonych w art. 180c Pt, generowanych w sieci telekomunikacyjnej. Zgodnie natomiast z art. 180c ust. 1 obowiązkiem określo-

[24] LEX nr 84379.
[25] T.j. Dz.U. z 2016 r. poz. 1489, ze zm.
[26] Dz.U. z 2009 r. nr 85 poz. 716.

nym w art. 180a ust. 1 są objęte dane niezbędne do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego inicjującego połączenie oraz do którego jest kierowane połączenie, a także dane niezbędne do określenia daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia oraz lokalizacji telekomunikacyjnego urządzenia końcowego. Jednocześnie w ust. 2 art. 180c Pt zawarto upoważnienie dla ministra właściwego do spraw informatyzacji do określenia, w formie rozporządzenia wydanego w porozumieniu z ministrem właściwym do spraw wewnętrznych, szczegółowego wykazu danych określonych w ust. 1 oraz rodzajów operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do zatrzymywania i przechowywania tych danych. Czynnikami, które organ wydający rozporządzenie jest zobowiązany wziąć pod uwagę, są: rodzaj wykonywanej działalności telekomunikacyjnej przez operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych, dane określone w ust. 1, koszty pozyskania i utrzymania danych oraz potrzeba unikania wielokrotnego zatrzymywania i przechowywania tych samych danych. Nie można zatem ustanowić na podstawie rozporządzenia generalnych wyłączeń spod obowiązku retencji danych telekomunikacyjnych. Na podstawie przedmiotowej delegacji ustawowej zostało wydane *Rozporządzenie Ministra Infrastruktury z dnia 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*[27]. Niniejsze rozporządzenie wyłączyło z obowiązku retencji jedynie dwie kategorie operatorów publicznej sieci telekomunikacyjnej oraz dostawców publicznie dostępnych usług telekomunikacyjnych: prowadzących działalność polegającą wyłącznie na dostarczaniu udogodnień towarzyszących oraz rozpowszechnianiu lub rozprowadzaniu programów radiofonicznych lub telewizyjnych.

Należy zatem stwierdzić, że retencja danych telekomunikacyjnych w Polsce ma charakter ogólny i nieselektywny, a więc przepisy art. 180a i 180c nie spełniają określonych w sentencji omawianego orzeczenia wymogów niezbędności i proporcjonalności.

Zasady dostępu właściwych służb państwowych do danych telekomunikacyjnych wraz z regułami wewnętrznej kontroli zostały ustalone przepisami *Ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw*[28]. Przedmiotowa ustawa wprowadziła zmiany w następujących przepisach: *Ustawie z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych*[29] – art. 3–30b, *Ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[30] – art. 28a–28b, *Ustawie z dnia 21 sierpnia 1997 r. – Prawo o ustroju sądów wojskowych* [31] – art. 6a, *Ustawie z dnia 27 sierpnia 2009 r. o Służbie Celnej*[32] – art. 75d–75da, *Ustawie z dnia 28 września 1991 r. o kontroli skarbowej*[33] – art. 36b–36bb, *Ustawie z dnia 6 kwietnia 1990 r. o Policji*[34] – art. 20c–20cb, *Ustawie z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych*[35] – art. 16 § 4a pkt 3 i art. 175b, *Ustawie z dnia 9 czerwca 2006 r.*

[27] Dz.U. Nr 226, poz. 1828.
[28] Dz.U. poz. 147.
[29] Dz.U. z 2016 r. poz. 96.
[30] Dz.U. z 2015 r. poz. 1929.
[31] Dz.U. z 2015 r. poz. 1198.
[32] Dz.U. z 2015 r. poz. 990.
[33] Dz.U. z 2015 r. poz. 553.
[34] Dz.U. z 2015 r. poz. 355.
[35] Dz.U. z 2015 r. poz. 133.

o Centralnym Biurze Antykorupcyjnym[36] – art. 18–18b, *Ustawie z dnia 12 października 1990 r. o Straży Granicznej*[37] – art. 10 b–10bb, *Ustawie z dnia 9 czerwca 2009 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego*[38].

Cel, w jakim jest dopuszczalne pozyskiwanie danych telekomunikacyjnych, został określony w różny sposób w poszczególnych ustawach pragmatycznych. Policja może te dane pozyskiwać, aby zapobiegać lub wykrywać przestępstwa, ratować życie lub zdrowie ludzkie bądź wspierać działania poszukiwawcze lub ratownicze. Dotyczy to również Żandarmerii Wojskowej. Straż Graniczna jest ograniczona do zapobiegania bądź wykrywania przestępstw, Służba Celna natomiast – do zapobiegania lub wykrywania przestępstw skarbowych (podobnie Kontrola skarbowa).

Agencja Bezpieczeństwa Wewnętrznego może te dane uzyskiwać, jeśli są jej niezbędne do realizacji zadań, o których mowa w art. 5 ust. 1 ustawy o ABW oraz AW. Równie szerokie uprawnienia do pozyskiwania danych telekomunikacyjnych, obejmujące całość zadań ustawowych danej służby, polski ustawodawca przyznał Centralnemu Biuru Antykorupcyjnemu oraz Służbie Kontrwywiadu Wojskowego.

Wykonując wytyczne zawarte w wyroku Trybunału Konstytucyjnego K 23/11, wśród których znalazł się postulat wprowadzenia mechanizmu niezależnej kontroli nad wykorzystaniem przez służby właściwe w zakresie przeciwdziałania i zwalczania przestępczości danych telekomunikacyjnych, polski ustawodawca wprowadził do ustaw pragmatycznych poszczególnych służb, a także do przepisów ustrojowych sądów powszechnych i sądów wojskowych, regulacje dotyczące kontroli wykorzystania danych telekomunikacyjnych przez sądy. Ustawą wprowadzającą te mechanizmy była ustawa z 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw. Ponieważ Trybunał Konstytucyjny nie przesądził, że mechanizm kontroli nad wykorzystaniem danych telekomunikacyjnych musi mieć charakter uprzedni, polski ustawodawca zdecydował o wprowadzeniu mechanizmu następczej kontroli sądowej. Takie też zapisy znalazły się w wymienionych wyżej ustawach pragmatycznych właściwych służb, w tym Agencji Bezpieczeństwa Wewnętrznego. Kontrola jest sprawowana przez sąd okręgowy, któremu wskazany w ustawie organ przesyła w okresach półrocznych sprawozdania obejmujące liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych, a także kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o te dane.

Według TSUE kontrola sądu lub innego niezależnego organu nad wykorzystaniem przez odpowiednie służby danych retencyjnych powinna mieć jednak charakter uprzedni.

Zgodnie z treścią art. 180a ust. 1 Pt operatorzy publicznych sieci telekomunikacyjnych i dostawcy publicznie dostępnych usług telekomunikacyjnych są obowiązani przechowywać dane telekomunikacyjne, podlegające obowiązkowi retencji na terytorium Rzeczpospolitej Polskiej, a zatem wymóg przechowywania danych wyłącznie na terytorium UE został spełniony.

7. Podsumowanie. Wnioski *de lege ferenda*

Wydając przedmiotowe orzeczenie, TSUE uznał, że mimo wcześniejszego stwierdzenia nieważności tzw. dyrektywy retencyjnej uregulowanie retencji danych telekomunikacyjnych pozostaje objęte kompetencją prawodawczą Unii Europejskiej.

[36] Dz.U. z 2014 r. poz. 1402.
[37] Dz.U. z 2014 r. poz. 1402.
[38] Dz.U. z 2014 r. poz. 253.

Należy podkreślić, że to orzeczenie nie ma bezpośredniego skutku w zakresie obowiązywania polskich przepisów regulujących retencję danych telekomunikacyjnych. Polskie przepisy regulujące retencję danych telekomunikacyjnych oraz dostęp do nich odpowiednich służb będą obowiązywały do momentu ich zmiany. Nie można wykluczyć, że na niniejsze orzeczenie będą się powoływały w postępowaniach sądowych podmioty zobowiązane do retencji danych telekomunikacyjnych, jeśli zechcą kwestionować nałożone na nie obowiązki, bądź też podmioty tych danych uznające, że państwo polskie narusza ich prawa. Jest możliwe, że w takiej sytuacji polski sąd zada pytanie prawne Trybunałowi Konstytucyjnemu w trybie art. 193 Konstytucji, a ten wydając orzeczenie, może wziąć pod uwagę zgodność polskich przepisów o retencji danych telekomunikacyjnych z prawem europejskim, stosownie do art. 9 Konstytucji (*Rzeczpospolita Polska przestrzega wiążącego ją prawa międzynarodowego*), biorąc pod uwagę tezy orzeczenia TSUE C-203/15 i C-698/15.

W przypadku gdy polskie przepisy dotyczące retencji danych telekomunikacyjnych nie ulegną zmianie, będzie istniało potencjalnie niebezpieczeństwo pozwania Polski przed TSUE przez Komisję bądź inne państwo członkowskie z powodu naruszenia przez nasz kraj zobowiązań ciążących na nim na mocy traktatów. Należy jednak zważyć, że w chwili obecnej problem niezgodności krajowych przepisów dotyczących retencji danych telekomunikacyjnych z prawem europejskim, w świetle wytycznych zawartych w omawianym orzeczeniu, dotyczy nie tylko Polski, lecz także większości państw członkowskich Unii Europejskiej. Taka perspektywa wydaje się zatem dość odległa.

W swojej glosie do niniejszego orzeczenia Agnieszka Grzelak podnosi jednak, że:

> Ponieważ wyrok TS nie pozostawia wątpliwości, że przepisy ustaw regulujących dostęp organów do danych (telekomunikacyjnych – przyp. aut.) leżą w zakresie zastosowania prawa unijnego w rozumieniu art. 51 Karty, zarówno ustawa inwigilacyjna, jak i inne ustawy regulujące dostęp do danych muszą zostać jak najszybciej zbadane w formalnych procedurach pod kątem zgodności z prawem unijnym, z uwzględnieniem wykładni poczynionej w sprawie Tele2. System retencji i udostępniania danych, uregulowany przepisami prawa telekomunikacyjnego, oraz ustaw regulujących dostęp właściwych organów do tych danych wymaga daleko idących zmian, uwzględniających wnioski płynące z wyroków Trybunału Sprawiedliwości w sprawach *DRI* i *Tele2*. Konieczność analizy, weryfikacji i zmiany regulacji krajowych odnoszących się do przechowywania danych jest konieczna, a długotrwały brak reakcji ze strony danego państwa członkowskiego może skutkować reakcją Komisji Europejskiej, która, jako strażnik Traktatów, ma obowiązek monitorowania zgodności prawa krajowego z prawem UE. W sytuacji wątpliwości, Komisja może wszcząć procedurę zmierzającą do weryfikacji naruszenia na podstawie art. 259 Traktatu o funkcjonowaniu Unii Europejskiej[39].

W chwili obecnej rozważenia wymaga to, czy sytuacja spowodowana orzeczeniem TSUE w sprawie Tele 2 wymaga od polskiego ustawodawcy inicjatywy mającej na celu dostosowanie polskiego prawodawstwa do tez niniejszego orzeczenia czy też Polska powinna czekać na inicjatywę ustawodawczą na szczeblu unijnym. Każde z tych rozwiązań ma pewne wady i zalety.

[39] A. Grzelak, *Glosa do wyroku TS z dnia 21 grudnia 2016 r. C-203/15 oraz C-698/15*…

W dniu 10 stycznia 2017 r. rozpoczęły się prace nad rozporządzeniem w sprawie prywatności i łączności elektronicznej mającym zastąpić dyrektywę 2002/58/WE[40], której interpretacja przepisów stała się podstawą orzeczenia Tele2. W tej sytuacji podejmowanie przez polskiego ustawodawcę inicjatywy legislacyjnej w obszarze retencji danych mogłoby się okazać przedwczesne, ponieważ przyjęte teraz przepisy mogłyby okazać się sprzeczne z nowym rozporządzeniem. Wymaga przy tym podkreślenia, że przedstawiony przez Komisję Europejską projekt zawiera podobne jak dyrektywa o e-prywatności wyłączenie z zakresu przewidzianych jego przepisami gwarancji poufności danych telekomunikacyjnych. Tę rolę odgrywa artykuł 11 ust. 1:

> Zakres zobowiązań i praw przewidzianych w art. 5–8 można ograniczyć w drodze środka legislacyjnego w ramach prawa Unii lub prawa krajowego, w sytuacji gdy takie ograniczenie odbywa się z poszanowaniem istoty podstawowych praw i wolności oraz gdy jest to środek konieczny, właściwy i proporcjonalny w demokratycznym społeczeństwie do zabezpieczenia jednego interesu publicznego lub wielu interesów publicznych, o których mowa w art. 23 ust. 1 lit. a)–e) rozporządzenia (UE) 2016/679 lub realizacji funkcji monitorowania, inspekcji lub regulacji w związku z wykonywaniem władzy publicznej na potrzeby takich interesów.

Powyższy przepis nie definiuje nawet bezpośrednio, tak jak czyniła to dyrektywa e-prywatnosci, prawnie chronionych interesów, które uzasadniają ograniczenie zawartych w danym akcie prawnym gwarancji praw podmiotu danych, lecz odsyła w tym zakresie do stosownego przepisu rozporządzenia ogólnego o ochronie danych osobowych. Należy dodać, że w zakresie interesów uzasadniających ograniczenie praw podmiotu danych, skatalogowanych w art. 23 ust. 1 lit. a)–e) rozporządzenia (UE) 2016/679 uwzględniono bezpieczeństwo narodowe, obronność, bezpiczeństwo publiczne i zapobieganie przestępczości. Trudno jednak oczekiwać, aby TSUE uznał, że tak sformułowane wyłączenie z gwarancji praw podmiotu danych telekomunikacyjnych mogło być interpretowane szerzej, niż to wynikające z art. 15 ust. 1 dyrektywy o e-prywatności.

Należy zatem uznać, że przed polskim ustawodawcą stoi wyzwanie w postaci dostosowania przepisów o retencji danych telekomunikacyjnych i dostępie do nich uprawnionych podmiotów do standardów zgodności z Kartą Praw Podstawowych, określonych przez TSUE w orzeczeniu Tele2.

Niezależnie od sposobu takiego dostosowania jest pewne, że ograniczy ono możliwość pozyskiwania danych telekomunikacyjnych przez uprawnione podmioty i tym samym nie wpłynie korzystnie na efektywność pracy operacyjnej organów policyjnych i służb specjalnych. Działania ustawodawcy muszą być nakierowane na zminimalizowanie ewentualnych szkód dla pracy wykrywczej służb powołanych do zwalczania przestępczości przez takie działania dostosowawcze.

Bez wątpienia dostosowanie polskiego prawa do standarów orzeczania Tele2 oznaczałoby konieczność organiczenie zakresu przedmiotowego możliwości korzystania przez uprawnione podmioty z danych telekomunikacyjnych. Trybunał stoi na stanowisku, że wykorzystywanie tego typu danych powinno być ograniczone do zwalczania

[40] Wniosek. Rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52017PC0010 [dostęp: 23 IX 2017].

poważnej przestępczości. Jak wskazano, niektóre z polskich służb mogą występować o przekazanie danych telekomunikacyjnych również w innych celach. Należałoby rozważyć pozostawienie możliwości tego rodzaju danych również w celu rozpoznawania i zwalczania zagrożeń dla bezpieczeństwa państwa, mając na uwadze, że bezpieczeństwo narodowe znajduje się w sferze wyłącznej odpowiedzialności państw członkowskich. Tak więc Unia Europejska, jej prawo i instytucje nie powinny ingerować w działania państwa podejmowane w tym obszarze.

Konieczne byłoby również poddanie wniosków uprawnionych podmiotów o udostępnienie danych telekomunikacyjnych uprzedniej kontroli niezależnego organu. Do decyzji ustawodawcy będzie należało, czy tym organem będzie sąd, prokurator czy inny niezależny organ, być może w tym celu powołany.

W uzasadnieniu do omawianego wyroku TSUE wspomniał również o zasadności wprowadzenia obowiązku notyfikacyjnego: właściwe organy ochrony bezpieczeństwa i proządku publicznego, które korzystały z dostępu do danych podlegajacych retencji, powinny poinformować zainteresowane osoby, zgodnie z właściwymi przepisami krajowymi, gdy tylko udzielenie tego rodzaju informacji nie będzie już stanowiło potencjalnego zagrożenia dla prowadzonych przez nie czynności. To, zdaniem Trybunału, jest niezbędne do umożliwienia tym osobom skorzystania z prawa do wniesienia środka zaskarżenia. Co istotne – TSUE nie odniósl się do istnienia tego obowiazku w sentencji wyroku, a jedynie w jednym z motywów uzasadnienia.

Najtrudniejsze do praktycznej realizacji byłoby wprowadzenie selektywnej w miejsce generalnej retencji danych telekomunikacyjnych. Powyższe wynika między innymi ze wskazania przez TSUE, że krajowe instrumenty prawne dotyczące danych telekomunikacyjnych – obejmujace swym zakresem, w sposób uogólniony, wszystkich abonentów i zarejestrowanych użytkowników oraz wszystkie środki łącznosci elektronicznej, jak również dane o ruchu – powinny przewidywać zróżnicownie oraz ograniczenia w zależności od tego, jakiemu celowi mają służyć[41]. Jednocześnie TSUE wskazuje, że musi istnieć związek między danymi podlegającymi retencji a zagrożeniem bezpieczeństwa publicznego. Ponadto TSUE określa, że retencja danych powinna być ograniczona przez zastosowanie:

- kryterium przedmiotowego,
- kryterium podmiotowego,
- kryterium geograficznego,
- kryterium czasowego[42].

Kryterium przedmiotowe odnosi się do wskazania, że retencja ma istotne znaczenie dla ochrony bezpieczeństwa publicznego lub może mieć istotne znaczenie dla zwalczania poważnych przestępstw.

Kryterium podmiotowe oznacza, że retencja może znaleźć zastosowanie wobec tych osób, co do których istnieją poważne przesłanki mogące sugerować, że ich zachowanie może mieć związek, nawet pośredni i daleki, z poważnymi przestępstwami lub z określonym kręgiem osób mogących, w taki czy inny sposób, mieć związek z poważnym przestępstwem, lub z osobami, których zatrzymane dane mogłyby z innych powodów przyczynić się do zapobiegania, wykrywania lub ścigania poważnych przestępstw.

Kryterium geograficzne wskazuje, że zatrzymywane dane powinny być związane z określonym obszarem geograficznym.

[41] Orzeczenie C-203/15, teza 105.

[42] Tamże, teza 106.

Kryterium czasowe określa, że zatrzywane dane powinny być związane z określonym okresem.

Należy wskazać, ze literalne zastosowanie wskazanych kryteriów w prawie krajowym zbliżyłoby metodologię retencji danych do kontroli operacyjnej. Dotyczyłaby ona tylko danych telekomunikacyjnych wygenerowanych od momentu zarządzenia stosowania retencji. Niemożliwe byłoby sięgnięcie przez uprawniony podmiot do danych historycznych, ponieważ te dane nie byłyby zatrzymywane i nie istniałyby już w momencie złożenia wniosku o ich udostępnienie, chyba że byłyby przechowywane przez operatora telekomunikacyjngo do innych celow. Taka sytuacja przyniosłaby nieoszacowane szkody pracy wykrywczej służb powołanych do zwalczania przestępczości. Dlatego rozważenia wymaga to, czy nie byłoby zgodne z określonymi przez TSUE standardami utrzymanie obowiązku retencji danych telekomunikacyjnych, z jednoczesnym ograniczeniem dostępu do nich uprawnionych podmiotów, na podstawie kryteriów przedmiotowych, podmiotowych i czasowych, z równoczesnym stworzniem mechanizmu uprzedniej kontroli nieznależnego organu nad sięganiem przez nie po te dane.

Ten problem wymaga dalszych pogłębionych analiz. Wypracowane ostateczne rozwiazanie musi uwzgledniać zarówno potrzebę ochrony prawa jednostki do prywatności, gwarantowaną w prawie Unii Europejskiej, jak i możliwość zagwarantowania jednostce innych podstawowych praw. Dotyczy to m.in. praw gwarantowanych przez Kartę Praw Podstawowych Unii Europejskiej, jak prawo do życia (art. 2 ust. 1), integralność fizyczna (art. 3 ust. 1), bezpieczeństwo osobiste (art. 6) i nienaruszalność mienia (art. 17 ust. 1), których nie da zagwaratnować się bez umożliwienia organom odpowiedznialnym za bezpieczeństwo publiczne i bezpieczeństwo państwa skutecznej realizacji ich ustawowych obowiązków.