Marcin Rojszczak

Prawne podstawy prowadzenia masowej inwigilacji obywateli opartej na hurtowym i nieukierunkowanym przechwytywaniu danych w UE z uwzględnieniem dorobku orzeczniczego TSUE i ETPC

Wprowadzenie

Każdy rodzaj inwigilacji prowadzi do naruszenia swobody komunikowania się i prawa do ochrony prywatności. Współczesne państwa demokratyczne w różny sposób wyważają relacje pomiędzy prawami obywateli a celami bezpieczeństwa publicznego, służącego ochronie społeczeństwa jako całości. Historycznie, zasady odnoszące się do stosowania środków inwigilacji określone były przepisami procedury karnej[1] jako element związany z gromadzeniem materiału dowodowego w konkretnych sprawach, w których istniało podejrzenie popełnienia poważnego przestępstwa, a zastosowanie kontroli operacyjnej było uzasadnione oraz podlegało kontroli niezależnego organu[2]. Inwigilacja rozumiana przez pryzmat przepisów karnych była więc – i nadal jest – traktowana jako narzędzie służące wprowadzeniu wyjątków od zasady braku ingerencji państwa w prawo do prywatności obywateli. Bez wątpienia zatem zastosowanie technik inwigilacyjnych w odniesieniu

[1] Na gruncie krajowym zasady realizacji kontroli rozmów telefonicznych oraz komunikacji elektronicznej uregulowane zostały przepisami art. 237 i n. Ustawy z dnia 6 VI 1997 r. Kodeks postępowania karnego (tekst jedn. Dz.U. 2016, poz. 1749).

[2] Por. także D. Kaczorkiewicz, *Granice inwigilacji społeczeństwa w zakresie czynności operacyjno-rozpoznawczych*, w: *Obywatel – państwo – społeczność międzynarodowa*, pod red. E. Cały-Wacinkiewicz, K. Flagi-Gieruszyńskiej, D. Wacinkiewicza, Warszawa 2014.

do nieoznaczonej grupy osób, przy braku istnienia przesłanek co do możliwości popełnienia lub planowania popełnienia jakiegokolwiek przestępstwa, bez nadzoru sądu oraz bezterminowo – tworzyłoby z uprawnienia szczególnego, jakim powinna być kontrola operacyjna, normę prowadzącą do trwałego ograniczenia prawa do prywatności.

Wraz z rozwojem technik służących gromadzeniu i przetwarzaniu dużej ilości danych środki inwigilacji znalazły praktyczne zastosowanie w obszarze bezpieczeństwa narodowego. Możliwość gromadzenia danych na temat członków określonych grup społecznych, czy nawet wszystkich obywateli, i zestawiania tych danych w celu wyszukiwania określonych wzorców zachowania pozwala na przewidywanie bądź zapobieganie poważnym przestępstwom, takim jak zdarzenia o charakterze terrorystycznym. Ponieważ działania takie nie są zazwyczaj związane z prowadzonymi postępowaniami karnymi, ale mają charakter prewencyjny i analityczny, sposób ich przeprowadzania nie jest uregulowany procedurą karną, lecz zazwyczaj przepisami regulującymi uprawnienia służb specjalnych[3], funkcjonowanie rynku telekomunikacyjnego[4] lub specjalnymi przepisami antyterrorystycznymi[5].

W takim przypadku gromadzenie danych może przybrać charakter hurtowy (ang. *bulk*) i nieukierunkowany (ang. *indiscriminate*). Pod terminem hurtowego gromadzenia danych należy rozumieć możliwość przechwytywania wszystkich informacji, które są przekazywane za pośrednictwem określonej sieci łączności. Rejestrowane mogą być zatem wszelkie zdarzenia dotyczące wszystkich użytkowników usługi. Z kolei nieukierunkowany charakter inwigilacji oznacza, że nie stosuje się żadnych filtrów ograniczających zakres przechwytywanych danych (np. występowanie określonych słów kluczowych lub korelacji będących w zainteresowaniu uprawnionych organów). Jako przykład gromadzenia

[3] Na przykład polska Ustawa z dnia 6 IV 1990 r. o Policji (tekst jedn. Dz.U. 2016, poz. 1782) w art. 20c czy Ustawa z dnia 24 V 2002 r. o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu (tekst jedn. Dz.U. 2016, poz. 1897) w art. 28, brytyjska Ustawa z dnia 17 VII 2014 r. o zatrzymywaniu danych i uprawnieniach dochodzeniowych (*Data Retention and Investigatory Powers Act*, publ. 2014 r., c 27), niemiecka Ustawa z dnia 26 VI 2001 r. o ograniczeniu prawa do tajemnicy korespondencji i komunikacji (*Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses*, publ. BGBI, I S, 1254).

[4] Na przykład polska Ustawa z dnia 16 VII 2004 r. Prawo telekomunikacyjne (tekst jedn. Dz.U. 2016, poz. 1489, dalej „pr. tel.") w art. 180 i n., szwedzka Ustawa z dnia 12 VI 2003 r. o łączności elektronicznej (*Lagen om elektronisk kommunikation*, publ. 2003, 389).

[5] Na przykład francuska Ustawa z dnia 19 III 2015 r. o informacjach wywiadowczych (*La loi relative au renseignement*, publ. 2015, 912).

danych, które jest hurtowe, jednak nie jest działaniem nieukierunkowanym, można podać przepisy niemieckiej ustawy o zwalczaniu przestępczości z 1994 r., wprowadzające tzw. monitoring strategiczny polegający na przechwytywaniu treści wybranej komunikacji międzynarodowej, które ze względu na użycie określonych słów kluczowych może stanowić źródło informacji w obszarze bezpieczeństwa narodowego[6]. Z drugiej strony, przykładem krajowego programu inwigilacyjnego zakładającego hurtowe i nieukierunkowane gromadzenie danych jest program PRISM prowadzony przez Narodową Agencję Bezpieczeństwa (ang. National Security Agency, NSA), specjalizowaną agendę rządową Stanów Zjednoczonych dedykowaną do prowadzenia programów rozpoznania elektronicznego (ang. *signal intelligence*, SIGINT).

O skali programów masowej inwigilacji prowadzonej przez państwa mogą wskazywać informacje na temat programu *Tempora* realizowanego przez Centralę Łączności Rządowej (ang. Government Communications Headquarters, GCHQ), brytyjski odpowiednik NSA. Według ujawnionych informacji[7] w ramach projektu *Tempora* przechwytywany jest ruch internetowy transmitowany za pośrednictwem światłowodów przechodzących przez terytorium Wielkiej Brytanii – niezależnie od tego, kto jest nadawcą transmisji, a kto ich odbiorcą, w szczególności niezależnie od tego, czy którakolwiek ze stron komunikacji znajduje się na terytorium Wielkiej Brytanii. Oznacza to, że GCHQ codziennie przetwarza miliardy wiadomości elektronicznych, ma dostęp do danych osobowych milionów użytkowników sieci, w tym informacji wrażliwych – takich jak dotyczące stanu zdrowia czy preferencji politycznych. Informacje te są gromadzone i przetwarzane przez GCHQ, ale także udostępniane innym agencjom wywiadowczym – takim jak amerykańska NSA. Poza Wielką Brytanią wśród państw członkowskich Unii Europejskiej (UE) jako prowadzące własne programy inwigilacyjne zakładające hurtowe i nieukierunkowane gromadzenie danych wskazywane są Francja, Niemcy i Szwecja[8].

---

[6] Zob. także wyrok Europejskiego Trybunału Praw Człowieka (ETPC) z 29 VI 2006 r. w sprawie *Weber i Saravia v. Niemcy*, sygn. 54934/00.

[7] The Guardian, *GCHQ taps fibre-optic cables for secret access to world's communications*, 21 VII 2013, https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa (dostęp: 1 III 2017).

[8] European Parliament Directorate General for Internal Policies, *National programmes for mass surveillance of personal data in EU Member States and their compatibility with EU law*, October 2003, https://goo.gl/d6WSSE (dostęp: 1 III 2017).

Jakkolwiek termin „masowa inwigilacja" nie jest terminem prawniczym i nie został formalnie zdefiniowany, jest jednak powszechnie stosowany w literaturze przedmiotu. Jak wskazuje Komisja Wenecka, masowa inwigilacja jest przeciwieństwem inwigilacji ukierunkowanej, a sam dobór terminu może być związany z określeniami stosowanymi wobec działań państw policyjnych lub podkreślać fakt, że jego przedmiotem jest całe społeczeństwo bądź duża jego część[9].

Skala realizowanych programów inwigilacyjnych stała się przyczyną rosnących wątpliwości w zakresie zgodności stosowanych technik z przepisami prawa, w szczególności z gwarancjami związanymi z ochroną prywatności. Jakkolwiek kwestie dotyczące bezpieczeństwa publicznego należą do sfery imperium każdego państwa, to obszar ochrony prywatności od lat jest przedmiotem standaryzacji w prawie międzynarodowym. Dodatkowo praktyczne znaczenie norm prawa międzynarodowego w tym zakresie związane jest z ponadnarodowym charakterem komunikacji w sieci Internet. Jeżeli użytkownicy Internetu musieliby polegać wyłącznie na przepisach krajowych w zakresie ochrony prywatności, w przypadku jakiejkolwiek transmisji (takiej jak wysłanie e-maila) zastosowanie miałoby wiele, często nawet kilkadziesiąt, różnych jurysdykcji. W praktyce nierzadko nawet komunikacja pomiędzy użytkownikami (odbiorcą i nadawcą informacji) zlokalizowanych w tym samym kraju realizowana jest za pośrednictwem łączy międzynarodowych. Biorąc pod uwagę, że wymiana komunikatów pomiędzy tymi samymi użytkownikami w sieci Internet może być za każdym razem realizowana poprzez inne kanały transmisyjne, określenie prawa właściwego oraz praktyczna realizacja gwarancji związanych z ochroną prywatności byłyby niemożliwe. Podobnie w praktyce znacznie utrudnione byłoby kwestionowanie legalności działań poszczególnych państw w zakresie przechwytywania i gromadzenia łączności elektronicznej.

Kwestia ochrony praw podstawowych, do których zalicza się ochronę prywatności, jest jednym z filarów funkcjonowania Unii Europejskiej. Gwarancje związane z ochroną prywatności są dodatkowo wzmocnione dzięki postanowieniom Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności[10], której stroną są wszystkie państwa członkowskie UE.

[9] Europejska Komisja na rzecz Demokracji przez Prawo, *Report on the democratic oversight of signals intelligence agencies*, 15 XII 2015, sygn. CDL-AD(2015)011, pkt 53.

[10] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z dnia 4 XI 1950 r. (Dz.U. 1993 Nr 61, poz. 284), dalej „EKPC" lub „Konwencja".

Dlatego interesujące wydaje się przeprowadzenie analizy dotyczącej prawnych ram funkcjonowania krajowych programów inwigilacji zakładających hurtowe i nieukierunkowane przechwytywanie danych oraz praktycznego znaczenia ponadnarodowych norm prawa wprowadzających gwarancje w obszarze poszanowania prywatności. Na tym tle możliwe będzie dokonanie także oceny, na ile istniejące środki ochrony prawnej pozwalają na wystarczająco skuteczną ochronę praw jednostki przed działaniami państwa uzasadnianymi interesem ogólnym, jakim jest zapewnienie bezpieczeństwa publicznego.

W ramach powyższych rozważań na szczególne wyróżnienie zasługują dwa zagadnienia prawne towarzyszące programom inwigilacji: wymagania związane z retencją danych oraz ochrona metadanych jako istotnych składników komunikacji.

W kontekście środków związanych z działaniami inwigilacyjnymi pod pojęciem retencji danych należy rozumieć obowiązek zatrzymania przez operatorów telekomunikacyjnych informacji na temat sposobu korzystania z usług (w szczególności np. o wykonanych połączeniach, czasie ich trwania czy o komunikujących się stronach) oraz lokalizacji użytkowników[11]. Zasady związane z retencją danych tym różnią się od kontroli komunikacji realizowanej na podstawie przepisów karnych, że są realizowane w odniesieniu do wszystkich użytkowników, i to bez istnienia jakiegokolwiek postępowania, w którym informacje te miałyby zostać wykorzystane. Celem wprowadzenia ogólnego obowiązku zatrzymania danych jest zapewnienie ich dostępności dla przyszłych działań związanych z dochodzeniem, wykrywaniem i ściganiem przestępstw[12].

Obowiązki związane z zatrzymaniem danych nie dotyczą treści komunikacji, ale tzw. metadanych, przez które należy rozumieć informacje towarzyszące transmisji, lecz niestanowiące merytorycznej treści przekazu (np. dane o lokalizacji, identyfikatorach stron komunikacji, wielkości przekazanych danych czy zastosowanych protokołach komunikacyjnych). Przez ostatnie lata znaczenie metadanych rosło wraz z rozwojem usług elektronicznych, doprowadzając do sytuacji, w której analiza samych metadanych pozwalała na identyfikację tożsamości komunikujących się stron albo ocenę osobistych preferencji czy

[11] Podstawę obowiązku dotyczącego ogólnego obowiązku zatrzymania danych w polskim systemie prawnym stanowi art. 180 pr. tel.

[12] Por. w tym zakresie definicję przedstawioną w art. 1 dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 III 2006 r. (Dz.Urz. UE L 105 z 13 IV 2006 r., s. 54).

zainteresowań. Zakres prawnej ochrony metadanych – w szczególności fakt uznania ich za dane osobowe – ma pierwszorzędne znaczenie z punktu widzenia programów inwigilacyjnych polegających na masowym i nieukierunkowanym przechwytywaniu danych. Brak takiej ochrony w praktyce oznaczałby, że obywatele zostaliby pozbawieni gwarancji oraz praw związanych z przetwarzaniem informacji o nich przez organy ścigania.

1. Podstawy prawne w UE ochrony prywatności w komunikacji elektronicznej

W efekcie reformy Unii Europejskiej, będącej następstwem przyjęcia przez państwa członkowskie traktatu lizbońskiego[13], prawa zagwarantowane w Karcie Praw Podstawowych[14] stały się częścią prawa pierwotnego UE. Chociaż sama Karta została przyjęta już w roku 2011, wcześniej miała charakter wyłącznie deklaracji i nie miała wymiaru prawnie wiążącego. Zgodnie z art. 7 KPP każdy ma prawo do poszanowania swego życia prywatnego i rodzinnego, domu i komunikowania się. Natomiast art. 8 KPP wprowadza gwarancje związane z ochroną danych osobowych. W szczególności zgodnie z art. 8 ust. 2 KPP dane osobowe muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą, a każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do spowodowania ich sprostowania. Ponadto – zgodnie z art. 8 ust. 3 KPP – przestrzeganie zasad określonych w ustępach wcześniejszych podlega kontroli niezależnego organu. W efekcie zarówno ochrona prywatności, jak i ochrona danych osobowych zyskały w UE rangę przepisów konstytucyjnych.

Szczególną rolę w systemie ochrony praw podstawowych zarówno na poziomie Unii, jak i państw członkowskich pełni ponadto Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Formalnie Konwencja jest umową międzynarodową, której stronami są państwa członkowskie Rady Europy (RE), przy czym obecnie przyjęcie Konwencji jest

[13] Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską podpisany w Lizbonie 13 XII 2007 r. (Dz.Urz. UE C 306 z 17 XII 2007 r., s. 1).

[14] Karta Praw Podstawowych Unii Europejskiej z dnia 30 III 2010 r. (Dz.Urz. UE C 83 z 30 III 2010 r., s. 389), dalej „KPP" lub „Karta".

także warunkiem przystąpienia do RE[15]. Ponieważ jednak wszystkie państwa członkowskie UE są stronami Konwencji, jest ona powszechnie stosowana na poziomie krajowych systemów prawnych. Ponadto, zgodnie art. 6 ust. 3 Traktatu o Unii Europejskiej[16], prawa podstawowe zagwarantowane w Konwencji stanowią część prawa Unii jako zasady ogólne prawa. Zamierzeniem twórców traktatu lizbońskiego było także przystąpienie samej UE jako organizacji międzynarodowej do Konwencji – co jednak do tej pory nie nastąpiło[17]. Jednym z praw podlegających ochronie na podstawie przepisów Konwencji jest prawo do poszanowania życia prywatnego i rodzinnego (art. 8).

Badając problematykę możliwości oraz zakresu prowadzenia krajowych programów opartych na hurtowym i nieograniczonym gromadzeniu danych, należy zauważyć, że zarówno KPP, jak i EKPC przewidują możliwość ograniczenia praw jednostek konieczną ze względu na bezpieczeństwo narodowe, ochronę porządku i zapobieganie przestępstwom. W szczególności zgodnie z art. 52 ust. 1 KPP wszelkie ograniczenia wprowadzone przez państwa członkowskie muszą brać pod uwagę zasadę proporcjonalności oraz być konieczne i rzeczywiście odpowiadać celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób. Na zasady proporcjonalności oraz konieczności wskazano także w art. 8 ust. 2 EKPC, doprecyzowując ponadto, że ograniczenia w stosowaniu praw zagwarantowanych Konwencją muszą wynikać z przepisów rangi ustawowej.

Należy podkreślić, że prawa i gwarancje wynikające z KPP mają zastosowanie w obszarze regulowanym przez prawo unijne, w szczególności należy zatem rozważyć obszar kompetencji UE oraz wyłączenia przewidziane w traktatach ustanawiających Unię Europejską. Zgodnie z zasadą przyznania wszelkie kompetencje nieprzyznane Unii w traktatach należą do państw członkowskich (art. 4 ust. 1 w zw. z art. 5 ust. 1 TUE). Kwestię kompetencji w zakresie bezpieczeństwa publicznego rozstrzygnięto w art. 4 ust. 2 Traktatu, wskazując, że jest to wyłączny obszar odpowiedzialności państw członkowskich. Natomiast zgodnie

[15] Rezolucja 1031 (1994) Zgromadzenia Parlamentarnego Rady Europy z dnia 14 IV 1994 r. dotycząca wywiązywania się ze zobowiązań zaciągniętych przez państwa członkowskie wraz z przystąpieniem do Rady Europy, https://goo.gl/AE2Brc (dostęp: 1 III 2017).

[16] Tekst jedn. Dz.Urz. UE C 202 z 7 VI 2016 r., dalej „TUE".

[17] Konwencja, do czasu przystąpienia do niej Unii, nie stanowi aktu prawnego formalnie obowiązującego w porządku prawnym UE (tak: Trybunał Sprawiedliwości Unii Europejskiej w sprawie C-398/13 P, pkt 45).

z art. 6 ust. 1 TUE postanowienia Karty w żaden sposób nie prowadzą do rozszerzenia kompetencji Unii ponad zakres określony w traktatach. Nie ulega zatem wątpliwości, że na gruncie obowiązujących traktatów UE nie ma kompetencji do ingerowania lub regulowania obszaru bezpieczeństwa publicznego poszczególnych państw członkowskich – z którym bez wątpienia są związane prowadzone programy inwigilacji, w tym zakładające hurtowe i nieukierunkowane przechwytywanie danych.

Jak jednak wskazał Trybunał Sprawiedliwości UE (TSUE), uprawnienie państwa członkowskiego do skorzystania z odstępstwa przewidzianego w traktatach nie stoi na przeszkodzie sądowej kontroli działań podjętych w ramach tego odstępstwa[18]. Ponadto, biorąc pod uwagę, że terminy zdefiniowane w art. 4 ust. 2 – takie jak bezpieczeństwo narodowe czy porządek publiczny – nie zostały precyzyjnie zdefiniowane w traktatach, ich rozumienie w kontekście unijnym powinno być interpretowane w sposób wąski, aby jego zasięg nie był określany jednostronnie przez poszczególne państwa członkowskie bez kontroli instytucji UE[19]. Ponadto zastosowanie wyłączenia związane z porządkiem czy bezpieczeństwem publicznym może być uzasadnione tylko w przypadku istnienia rzeczywistego i dostatecznie poważnego zagrożenia podstawowego interesu społeczeństwa. Klauzule te nie mogą być zatem wykorzystywane do wprowadzenia rozwiązań prawnych nieadekwatnych lub nierealizujących celów, dla jakich zostały ustanowione[20]. Nadto podkreślić należy, że wszystkie obszary wskazane w art. 4 ust. 2 TUE są domenami działalności państwowej, odmiennej od dziedzin działalności jednostek. Dlatego adresatem określonych w przepisie wyłączeń jest władza państwowa. Ponadto zakres wyłączenia musi być interpretowany wąsko i obejmować tylko takie działalności, które zostały wyraźnie wymienione lub które mogą być zaliczone do tego samego rodzaju[21].

W efekcie, o ile działalność wywiadowcza czy inwigilacyjna związana z gromadzeniem danych przekazywanych w łączności elektronicznej, prowadzona przez uprawnione do tego organy państwowe, korzysta z wyłączenia określonego w art. 4 ust. 2 TUE, to działania podejmowane

[18] Wyrok TSUE z 4 XII 1974 r. w sprawie *van Duyn*, sygn. 41/74.

[19] Wyrok TSUE z 14 X 2004 r. w sprawie *Omega Spielhallen- und Automatenaufstellungs*, sygn. C-36/02.

[20] Wyrok TSUE z 14 III 2000 r. w sprawie *Association Eglise de scientologie de Paris*, sygn. C-54/99.

[21] Wyrok TSUE z 6 XI 2003 r. w sprawie *Lindqvist*, sygn. C-101/01, pkt 43–44.

przez inne podmioty (np. operatorów telekomunikacyjnych) związane z gromadzeniem czy przechwytywaniem danych nie korzystają z tego wyłączenia, a same przepisy krajowe nakładające takie obowiązki na te podmioty mogą być przedmiotem oceny przez TSUE w zakresie zgodności z prawem UE.

Gwarancje związane z ochroną danych osobowych obywateli UE zostały wzmocnione poprzez przyjęcie dyrektywy 95/46 z 1995 r. (dyrektywa o ochronie danych), której głównym celem było ułatwienie integracji gospodarczej i funkcjonowania rynku wewnętrznego UE poprzez standaryzację poziomu ochrony pomiędzy państwami członkowskimi oraz wprowadzenie mechanizmów kontrolowania transgranicznego przepływu danych[22]. Dyrektywa precyzowała między innymi zasady gromadzenia, przetwarzania i udostępniania danych, a także wprowadzała zbiór obowiązków dla administratorów danych oraz praw dla osób, których dane są przetwarzane. Zgodnie z art. 288 TFUE dyrektywa nie jest bezpośrednio stosowalna i wymaga implementacji do krajowego porządku prawnego. Podkreślenia wymaga jednak fakt, że zgodnie z wyrokiem TSUE w sprawie *van Duyn* brak implementacji przez państwo dyrektywy lub jej niewłaściwe wdrożenie nie ogranicza możliwości podmiotów do powoływania się przed sądem na prawa i zobowiązania wynikające z mocy dyrektywy[23]. Nie można zatem uznać, że sama dyrektywa nie nadaje praw jednostkom, ponieważ jest aktem kierowanym do państw.

Zmierzając do zapewnienia pełnego poszanowania praw określonych w art. 7 i 8 KPP, prawo wtórne UE zostało uzupełnione ponadto o dyrektywę 2002/58/WE z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej. Jest ona znana także w literaturze przedmiotu jako dyrektywa *e-privacy* lub dyrektywa o e-prywatności. Jak słusznie wskazał prawodawca unijny, nie wszystkie informacje, które są wymieniane za pośrednictwem publicznych sieci łączności i publicznie dostępnych usług łączności elektronicznej, można zakwalifikować jako dane osobowe i w związku z tym objąć ochroną na podstawie przepisów dyrektywy 95/46/WE. Pomijając treść samego przekazu, jak wcześniej zaznaczono,

[22] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 X 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.Urz. UE L 281 z 23 XI 1995 r., s. 31); w zakresie celów wprowadzenia tej dyrektywy por. treść motywu (5).

[23] Wyrok TSUE w sprawie *van Duyn*, pkt 12.

równie istotnie na obszar prywatności użytkowników może wpłynąć nieuprawnione przetwarzanie metadanych związanych z łącznością. Dlatego zgodnie z art. 1 ust. 2 przepisy dyrektywy dookreślają i uzupełniają dyrektywę 95/46/WE. Jak ponadto wskazano w motywie 10 dyrektywy, w sektorze łączności elektronicznej dyrektywę o ochronie danych należy stosować zwłaszcza do wszystkich spraw dotyczących ochrony podstawowych praw i wolności, które nie są szczegółowo objęte przepisami dyrektywy o e-prywatności, włączając zobowiązania nałożone na administratora danych oraz prawa jednostek. W efekcie należy uznać, że przepisy dyrektywy 2002/58 stanowią *lex specialis* w odniesieniu do wymagań określonych w dyrektywie 95/46.

Ze względu na fakt wyłączenia obszaru bezpieczeństwa publicznego z kompetencji prawa UE (por. wcześniejsze rozważania dotyczące art. 4 ust. 2 TUE), zarówno w dyrektywie 95/46, jak i dyrektywie 2002/58 wskazano, że ich zakresem stosowania nie jest objęte przetwarzanie danych na rzecz bezpieczeństwa publicznego, obronności czy bezpieczeństwa państwa (art. 3 ust. 2 dyrektywy 95/46 i art. 1 ust. 3 dyrektywy 2002/58).

Zgodnie z art. 5 ust. 1 dyrektywy 2002/58 państwa członkowskie zostały zobowiązane do wprowadzenia ustawodawstwa krajowego zapewniającego poufność komunikacji i związanych z nią danych o ruchu za pośrednictwem publicznie dostępnej sieci łączności i publicznie dostępnych usług łączności elektronicznej. Zobowiązanie to należy rozumieć w szczególności jako zakaz słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez inne osoby, bez zgody zainteresowanych użytkowników. Wyjątkiem od tej zasady jest tryb określony w art. 15 ust. 1, zgodnie z którym państwa członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu enumeratywnie wymienionych praw i obowiązków przewidzianych w dyrektywie, jednak – podobnie jak w zakresie ograniczeń w stosowaniu KPP – tylko wtedy, gdy takie ograniczenia są niezbędne i proporcjonalne do zapewnienia między innymi bezpieczeństwa narodowego, obronności oraz bezpieczeństwa publicznego. Prawodawca unijny określił, że w celu realizacji tego uprawnienia państwa członkowskie mogą w szczególności uchwalić środki ustawodawcze przewidujące przechowywanie danych przez określony czas. W efekcie art. 15 ust. 1 dyrektywy określa zatem warunki realizacji krajowych programów inwigilacyjnych służących bezpieczeństwu publicznemu, których elementem może być gromadzenie danych

o użytkownikach sieci z wyłączeniem praw i gwarancji wynikających z dyrektywy o e-prywatności.

Bez wątpienia, w dalszych rozważaniach nad problematyką prawnego uregulowania prowadzenia krajowych programów zakładających masowe i nieukierunkowane przechwytywanie danych konieczne jest udzielenie odpowiedzi na dwa istotne pytania. Po pierwsze – o możliwość zastosowania przepisów wynikających z dyrektyw 95/46 i 2002/58 w odniesieniu do tych programów, a w szczególności o znaczenie przytoczonych aktów unijnych dla czynności hurtowego przechwytywania i gromadzenia informacji przekazywanych w sieciach telekomunikacyjnych. Dopiero po udzieleniu odpowiedzi na pytanie pierwsze należy przebadać wzajemną zależność art. 1 ust. 3 (przedmiotowe wyłączenie m.in. obszaru bezpieczeństwa publicznego, obronności, bezpieczeństwa państwa) oraz art. 15 ust. 1 dyrektywy 2002/58 (warunki ograniczenia stosowania przepisów dyrektywy w odniesieniu do programów bezpieczeństwa publicznego). Konieczne jest zwłaszcza ustalenie, czy środki ustawodawcze wprowadzone do krajowych porządków prawnych na podstawie art. 15 ust. 1 podlegają ocenie w zakresie zgodności z ograniczeniami przewidzianymi w przywołanym przepisie, skoro należą do obszaru wyłączonego przedmiotowo z zakresu stosowania dyrektywy.

Odpowiadając na pierwsze z pytań, na wstępie należy zauważyć, że przepisem kompetencyjnym dla wydania obu dyrektyw jest art. 114 Traktatu o funkcjonowaniu Unii Europejskiej[24] (wcześniej art. 95 Traktatu ustanawiającego Wspólnotę Europejską), dotyczący harmonizacji rynku wewnętrznego. Celem wprowadzenia dyrektyw nie była zatem ingerencja i sposób regulacji obszarów przynależnych państwom i wyłączonych na podstawie art. 4 ust. 2 TUE, ale wprowadzenie ram prawnych wspólnych w całej Unii dotyczących ochrony danych osobowych i prywatności w sektorze łączności elektronicznej – co w zamierzeniu prawodawcy miało pozwolić na uniknięcie przeszkód uniemożliwiających rozwój wewnętrznego rynku łączności elektronicznej. Dyrektywy nakładają więc obowiązki i ograniczenia nie na władzę państwową, lecz głównie na podmioty przetwarzające dane osobowe (w przypadku dyrektywy 95/46) oraz przedsiębiorstwa sektora telekomunikacyjnego (w przypadku dyrektywy 2002/58). Zgodnie z linią orzeczniczą TSUE dla uzasadnienia zastosowania art. 114 TFUE jako podstawy prawnej

[24] Tekst jedn. Dz.Urz. UE C 202 z 7 VI 2016 r., dalej „TFUE".

istotne jest, by akt wydany na tej podstawie miał rzeczywiście na celu poprawę warunków ustanowienia i funkcjonowania rynku wewnętrznego. Zastosowanie art. 114 nie wymaga natomiast rzeczywistego związku ze swobodnym przepływem w ramach rynku wewnętrznego między państwami członkowskimi w każdej sytuacji objętej zakresem normowania aktu opartego na tej podstawie[25].

Trybunał w swoim orzecznictwie stwierdził ponadto, że w przypadku spełnienia warunków zastosowania art. 114 TFUE jako podstawy prawnej prawodawca unijny nie może zostać pozbawiony możliwości powołania się na to postanowienie tylko z tego względu, że interes publiczny jest rozstrzygający do podejmowania decyzji. Trybunał podkreślił, że art. 114 ust. 3 jest wystarczający do przyjmowania aktów prawnych prowadzących do zbliżania ustawodawstw, które mają na celu ustanowienie i funkcjonowanie rynku wewnętrznego i które jednocześnie służą realizacji celu w zakresie interesu ogólnego, za jaki można uznać wysoki poziom bezpieczeństwa w ramach UE[26].

Przenosząc powyższe rozważania na grunt programów nieukierunkowanej inwigilacji, należy zauważyć, że omawiane dyrektywy będą miały do nich zastosowanie tylko w zakresie nieobjętym wyłączeniem stosowania prawa UE (por. wcześniejsze rozważania dotyczące art. 4 ust. 2 TUE). W szczególności badane dyrektywy nie będą miały zastosowania do czynności związanych z dostępem do danych ani ich wykorzystywaniem przez uprawnione organy państw członkowskich. Jednak już sam proces hurtowego gromadzenia danych, realizowany przez nałożenie przez przepisy krajowe na dostawców usług telekomunikacyjnych obowiązku zatrzymania danych o ruchu i lokalizacji, podlega regulacjom dyrektyw 95/46 oraz 2002/58[27].

Przechodząc do drugiego zagadnienia, dotyczącego wzajemnych relacji pomiędzy art. 1 ust. 3 i art. 15 ust. 1 dyrektywy 2002/58 oraz możliwości oceny przepisów krajowych wprowadzonych na podstawie art. 15 ust. 1 na zgodność z dyrektywą, należy zauważyć, że problem ten był przedmiotem analizy dokonanej przez TSUE w ramach połączonych spraw *Tele2* oraz *SSHD*. Zawisłe przed Trybunałem sprawy dotyczyły pytań prejudycjalnych zadanych przez sądy w Wielkiej Brytanii i Szwecji, a dotyczących zgodności z prawem UE krajowych przepisów

[25] Wyrok TSUE z 12 XII 2006 r. w sprawie *Niemcy v. Komisja Europejska*, sygn. C-380/03.

[26] Por. opinia rzecznika generalnego w sprawie C301/06, pkt 97.

[27] Wyrok TSUE z 21 XII 2016 r. w połączonych sprawach *Tele2* i *SSHD*, sygn. C-203/15 i C-698/15.

wprowadzających mechanizmy uogólnionego i niezróżnicowanego zatrzymywania danych telekomunikacyjnych w celu zwalczania poważnej przestępczości. Trybunał przypomniał, że obszary wymienione w art. 3 ust. 1 należą co do zasady do obszaru działalności władzy państwowej, różnej od dziedziny, w której prowadzą działalność jednostki. Możliwość dostępu do danych przez uprawnione organy mogłaby zatem zostać objęta wyłączeniem przewidzianym w art. 1 ust. 3 dyrektywy. Nie oznacza to jednak, że przepisy wprowadzające obowiązek zatrzymywania danych – realizowany przez firmy telekomunikacyjne, a nie organy władzy publicznej – także znajdują się poza zakresem jej stosowania[28].

Pamiętając o wyborze podstawy prawnej dyrektywy – jakim jest art. 114 TFUE – Trybunał podzielił stanowisko przestawione w sprawie przez rzecznika generalnego o tym, że art. 15 ust. 1 nie może być interpretowany w ten sposób, iż daje on państwom członkowskim uprawnienie do przyjęcia odstępstwa od systemu ustanowionego przez dyrektywę w takim zakresie, który pozbawiłby wysiłek na rzecz harmonizacji wszelkiej skuteczności. Taki bowiem efekt miałoby zaakceptowanie poglądu, że środki przyjęte na podstawie art. 15 ust. 1 nie mogą być oceniane przez pryzmat zgodności z dyrektywą jako korzystające z wyłączenia wprowadzonego art. 1 ust. 3. Konkludując, Trybunał uznał, że skoro zakresem stosowania dyrektywy jest przetwarzanie danych osobowych w związku z dostarczaniem publicznie dostępnych usług łączności elektronicznej w publicznych sieciach łączności, to środki przyjęte na podstawie art. 15 ust. 1 nie mogą być wyłączone spod zakresu stosowania tego aktu.

Powyższa wstępna analiza stała się podstawą do merytorycznej oceny zgodności z prawem UE szwedzkich i brytyjskich przepisów krajowych wprowadzających obowiązek zatrzymania danych telekomunikacyjnych. W szczególności Trybunał dokonał analizy zarzutu nieuzasadnionego naruszenia prawa do prywatności oraz oceny zasadności ograniczenia praw podstawowych względami określonymi w art. 15 ust. 1 dyrektywy 2002/58 – a więc zapewnienia, że wprowadzane ograniczenie odbywa się z zachowaniem zasady proporcjonalności, a nadto że wprowadzane środki są niezbędne i właściwe w ramach społeczeństwa demokratycznego.

Zgodnie z art. 52 ust. 1 KPP wszelkie ograniczenia praw i wolności przewidzianych w Karcie mogą być wprowadzane wyłącznie wtedy, gdy

[28] Por. także opinia rzecznika generalnego w połączonych sprawach *Tele2* i *SSHD*, pkt 92.

są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób. Wskazywanym przez projektodawców celem wprowadzenia krajowych przepisów zakładających hurtowe i nieukierunkowane gromadzenie danych jest ochrona bezpieczeństwa publicznego w szczególności przed najpoważniejszymi przestępstwami, takimi jak zdarzenia o charakterze terrorystycznym. Zgodnie z wyrokiem Trybunału w połączonych sprawach *Kadi* i *Al Barakaat International Foundation*[29] walka z poważną przestępczością prowadzona dla zapewnienia bezpieczeństwa publicznego stanowi cel interesu ogólnego Unii. Z kolei z wyroku w sprawie *Tsakouridis*[30] wynika, że na obszar bezpieczeństwa publicznego mogą także wpływać zdarzenia zagrażające funkcjonowaniu głównych instytucji i służb publicznych oraz życiu ludności, podobnie jak ryzyko poważnego zakłócenia stosunków zagranicznych lub pokojowego współistnienia narodów.

Trybunał miał okazję wcześniej odnieść się do kwestii stosowania środka w postaci hurtowego gromadzenia informacji o wszystkich użytkownikach sieci telekomunikacyjnej i jego celowości oraz zasadności w obszarze bezpieczeństwa publicznego. Stało się to na kanwie sprawy *Digital Rights Ireland Ltd*[31], w ramach której badana była zgodność z prawem UE tzw. dyrektywy retencyjnej[32]. Dyrektywa ta została wprowadzona w celu ujednolicenia obowiązków i zasad związanych z retencją (przechowywaniem) danych o łączności i komunikatach przekazywanych w sieciach telekomunikacyjnych na obszarze UE. Przepisy dyrektywy nie określały sposobu udostępniania danych upoważnionym organom, wskazując w tym obszarze, że każde państwo członkowskie powinno ustalić procedury i warunki uzyskiwania dostępu do zatrzymanych danych, biorąc pod uwagę wymogi konieczności i proporcjonalności.

---

[29] Wyrok TSUE z 3 IX 2008 r. w połączonych sprawach *Kadi* i *Al Barakaat International Foundation*, sygn. C-402/05 P i C-415/05 P.

[30] Wyrok TSUE z 23 XI 2010 r. w sprawie *Tsakouridis*, sygn. C-145/09.

[31] Wyrok TSUE z 8 IV 2014 r. w sprawie *Digital Rights Ireland Ltd*, sygn. C-293/12 i C-594/12.

[32] Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 III 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnieniem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz.Urz. UE L 105 z 13 IV 2006 r., s. 54), dalej „dyrektywa retencyjna".

Trybunał, badając kwestię zgodności dyrektywy retencyjnej z prawem UE, stwierdził, że ze względu na rosnące znaczenie środków komunikacji elektronicznej dane, które mogłyby być zatrzymane na podstawie tej dyrektywy, dają krajowym organom ścigania dodatkowe możliwości – można więc przyjąć, że hurtowe i nieograniczone gromadzenie danych jest odpowiednie do realizacji celu, jakim jest zapewnienie bezpieczeństwa publicznego. Trybunał wszakże jednocześnie zaznaczył, że celowość doboru środka nie przesądza o jego konieczności[33].

Co zaś się tyczy kwestii proporcjonalności krajowych programów inwigilacyjnych w aspekcie nieukierunkowanego gromadzenia danych, to zgodnie z ugruntowanym orzecznictwem TSUE zastosowanie zasady proporcjonalności w odniesieniu do ochrony prywatności wymaga, aby odstępstwa i ograniczenia stosowane były w zakresie, w jakim jest to absolutnie konieczne[34]. Wprowadzenie mechanizmów hurtowego i nieukierunkowanego przechwytywania danych w sposób oczywisty prowadzi do ingerencji w prawo do prywatności wszystkich użytkowników sieci niezależnie od tego, czy jest wobec nich prowadzone postępowanie karne, a także czy w ogóle znajdują się w kręgu osób będących w zainteresowaniu uprawnionych organów. Takie uregulowanie nie wymaga istnienia żadnego związku między danymi, których zatrzymywanie nakazuje, a zagrożeniem dla bezpieczeństwa publicznego. Ponadto, jak wskazał TSUE, brak określenia ograniczeń czasowych czy geograficznych, jak również ograniczeń do grupy osób, które można podejrzewać o taki czy inny rodzaj uczestnictwa w poważnym przestępstwie, tak by obowiązek zatrzymywania danych obejmował tylko te dane, co do których z jakiegoś powodu można zakładać, że mają znaczenie dla walki z przestępczością, powoduje, iż uregulowanie takie wykracza poza granice tego, co jest absolutnie konieczne i uzasadnione w demokratycznym społeczeństwie[35].

Bezpośredni wpływ na ocenę zachowania proporcjonalności przyjętych środków ma także zapewnienie kontroli działań inwigilacyjnych przez niezależny organ. Kontrola ta powinna być rozumiana zarówno na płaszczyźnie weryfikacji celowości oraz konieczności zastosowania rozwiązań prowadzących do ograniczenia prawa do prywatności określonych osób, jak i w zakresie dostępności procedury prawnej umożliwiającej

[33] Wyrok TSUE w sprawie *Digital Rights Ireland Ltd*, pkt 51.
[34] Wyrok TSUE z 16 XII 2008 r. w sprawie *Tietosuojavaltuutettu*, sygn. C-73/07.
[35] Wyrok TSUE w połączonych sprawach *Tele2* i *SSHD*, pkt 107.

uzyskanie odszkodowania lub zadośćuczynienia w przypadku, gdyby zastosowanie środka ingerującego w prywatność okazało się bezprawne. Z treści art. 8 ust. 3 KPP wprost wynika, że przestrzeganie zasad związanych z ochroną danych osobowych podlega kontroli niezależnego organu. Bez wątpienia, wprowadzenie regulacji, które przewidują możliwość nieograniczonego przechwytywania i gromadzenia danych dotyczących wszystkich użytkowników sieci telekomunikacyjnych oraz nie wprowadzają precyzyjnych zasad dostępu do tych danych dla uprawnionych organów, rodzi ryzyko, że kontrola taka nie będzie mogła okazać się skuteczna. Na tle rozważań dotyczących zgodności dyrektywy retencyjnej z prawem Unii Europejskiej TSUE zwrócił uwagę, że uzyskanie dostępu do gromadzonych danych powinno podlegać kontroli sądu lub niezależnego organu administracyjnego, tak aby udostępnianie i wykorzystywanie danych ograniczało się do przypadków, gdy jest to absolutnie konieczne do realizacji zamierzonego celu – jakim jest zapobieganie, wykrywanie lub ściganie przestępstw na gruncie prawa karnego[36].

Biorąc pod uwagę powyższe rozważania, TSUE zarówno w sprawie *Digital Rights Ireland Ltd* (zgodność dyrektywy retencyjnej z prawem UE), jak i w połączonych sprawach *Tele2* oraz *SSHD* (zgodność krajowych programów inwigilacyjnych z prawem UE) orzekł, że wprowadzenie środka w postaci hurtowego i nieograniczonego gromadzenia danych o użytkownikach sieci telekomunikacyjnych narusza zasadę proporcjonalności i z tego względu jego stosowanie nie może być pogodzone z obowiązkami wynikającymi z art. 15 ust. 1 dyrektywy 2002/58, a także postanowieniami art. 52 ust. 1 w zw. z art. 7, 8 i 11 KPP.

Na podstawie orzeczeń TSUE oraz towarzyszących im opinii rzeczników generalnych można wskazać najważniejsze kryteria, jakie powinien spełniać krajowy program inwigilacyjny przewidujący ogólny obowiązek zatrzymania danych, aby można było stwierdzić, że jest on zgodny z prawami podstawowymi oraz gwarancjami wynikającymi z KPP i dyrektyw 95/46 oraz 2002/58. W szczególności obowiązek zatrzymania danych:

1. musi być oparty na podstawie prawnej;
2. musi szanować istotę praw ustanowionych przez Kartę;
3. musi dążyć do osiągnięcia celu interesu ogólnego;
4. musi być właściwy do realizacji tego celu;
5. musi być konieczny do realizacji tego celu;

[36] Wyrok TSUE w sprawie *Digital Rights Ireland Ltd*, pkt 62.

6. musi być w ramach społeczeństwa demokratycznego proporcjonalny do osiągnięcia tego celu.

Jakkolwiek wprowadzenie ogólnego obowiązku gromadzenia danych telekomunikacyjnych niewątpliwie może służyć celowi związanemu z bezpieczeństwem publicznym, kwestią dyskusyjną pozostaje, czy jest to środek właściwy i konieczny. Bez wątpienia natomiast, ze względu na poważną ingerencję prowadzącą do ograniczenia prawa do prywatności wszystkich obywateli – rozwiązanie takie nie może być uznane na gruncie prawa UE za proporcjonalne, w efekcie czego jest z nim niezgodne.

Brak możliwości nałożenia na operatorów telekomunikacyjnych prawnego obowiązku wprowadzenia mechanizmów ogólnego i niewybiórczego zatrzymania danych dotyczących komunikacji wszystkich użytkowników w sposób bezpośredni wpływa na możliwość realizacji masowych programów inwigilacji na obszarze UE. Pamiętając jednak o przedmiotowym wyłączeniu obszaru bezpieczeństwa publicznego z zakresu prawa UE (art. 4 ust. 2 TUE), wskazane orzeczenia TSUE nie ograniczają możliwości prowadzenia działań inwigilacyjnych, w tym zakładających hurtowe i nieukierunkowane gromadzenie danych, jeżeli są one prowadzone przez uprawnione organy państw członkowskich.

2. Dyrektywa retencyjna i implikacje jej nieważności dla przepisów krajowych

Unieważnienie dyrektywy retencyjnej miało także dodatkowy, praktyczny skutek dla prawodawstwa krajów członkowskich. Do czasu ogłoszenia wyroku w sprawie *Digital Rights Ireland Ltd* dyrektywa, jako akt prawny wymagający wdrożenia do porządku krajowego, została zaimplementowana w formie ustaw w części państw członkowskich. Stwierdzenie nieważności dyrektywy jako aktu prawa UE w wyniku wyroku TSUE wydanego w trybie prejudycjalnym stworzyło stan prawny, w którym w krajowych porządkach prawnych nadal obowiązywały przepisy rangi ustawowej implementujące nieważną dyrektywę. Należy podkreślić, że Trybunał Sprawiedliwości, odpowiadając na pytanie prejudycjalne, nie orzeka o ważności prawa krajowego, w tym zakresie pozostawiając rozpoznanie merytoryczne sprawy w gestii sądu krajowego. W rezultacie Trybunał Sprawiedliwości, unieważniając akt prawa unijnego w ramach postępowania wszczętego w trybie prejudycjalnym, nie ma kompetencji do wycofania z porządku prawnego implementujących ją ustaw krajowych.

Stwierdzenie nieważności dyrektywy, które nastąpiło w wyniku rozpatrzenia sprawy *Digital Rights Ireland Ltd*, nie wywarło więc skutków prawnych na przepisy krajowe implementujące tę dyrektywę.

Z drugiej strony, zgodnie z zasadą lojalności wynikającą z art. 4 ust. 3 TUE, wyrok TSUE stwierdzający nieważność aktu prawa UE wiąże nie tylko instytucje Unii, ale także wszystkie organy państw członkowskich, a zatem także organy wymiaru sprawiedliwości (sądy) oraz władzę wykonawczą (organy ścigania). Jeżeli zatem przepisy krajowe były wyłącznie transpozycją normy unijnej (dyrektywy), to powstaje ciekawe zagadnienie prawne, czy i w jakim zakresie krajowe przepisy inwigilacyjne mogą być nadal stosowane – nawet w przypadku braku orzeczenia właściwego sądu konstytucyjnego stwierdzającego ich nieważność.

Częściową odpowiedź na to pytanie można odnaleźć w omawianym wcześniej wyroku w połączonych sprawach *Tele2* oraz *SSHD*. Obie sprawy zostały zainicjowane w wyniku pytań prejudycjalnych skierowanych przez sądy krajowe odpowiednio Szwecji oraz Wielkiej Brytanii i dotyczyły oceny zgodności z prawem UE ustaw krajowych, implementujących unieważnioną wcześniej dyrektywę retencyjną. Zdaniem brytyjskiego sądu krajowego, przed którym zawisła sprawa, która następnie stała się podstawą do sformułowania pytań prejudycjalnych do TSUE, ze względu na to, iż Trybunał uznał we wcześniejszym wyroku, że dyrektywa retencyjna jest niezgodna z zasadą proporcjonalności, przepis krajowy o treści identycznej z tą dyrektywą również nie może być zgodny z tą zasadą[37]. Należy jednak pamiętać, że przepisy krajowe służyły nie tylko transpozycji dyrektywy w zakresie wprowadzenia ogólnego obowiązku zatrzymania danych, ale także wprowadzały zasady dotyczące dostępu do tych danych dla uprawnionych organów. Drugi ze wskazanych obszarów, jako związany z bezpieczeństwem publicznym, mógł zostać uznany za wyłączony z prawa UE (por. wcześniejsze rozważania dotyczące art. 4 ust. 2 TUE oraz art. 1 ust. 3 dyrektywy 2002/58). Dlatego stwierdzenie nieważności dyrektywy, mające wszak skutek *ex tunc*, nie w każdym przypadku można było uznać za wystarczającą przesłankę do unieważnienia przepisów krajowych. Sytuację dodatkowo komplikował fakt, że zgodnie z dominującym w doktrynie poglądem orzeczenie o nieważności aktu prawa UE wydane na podstawie art. 267 TFUE nie skutkuje wycofaniem go z porządku prawnego[38].

[37] Wyrok TSUE w połączonych sprawach *Tele2* i *SSHD*, pkt 53.

[38] J. Michalska, *Pytania prejudycjalne sądów do TS UE*, w: *Zasada pierwszeństwa prawa Unii Europejskiej w praktyce działania organów władzy publicznej RP*, pod red. M. Jabłońskiego, S. Jarosz-Żukowieckiej, Wrocław 2015, s. 268.

Stwierdzenie przez TSUE nieważności aktu jest wystarczające nie tylko do pominięcia go w wyrokowaniu w sprawie, w której zadano pytanie prejudycjalne, ale także we wszystkich innych podobnych sprawach zawisłych przed sądami krajowymi (skutek *erga omnes*)[39]. Wyrok wydany w połączonych sprawach *Tele2* oraz *SSHD* zawiera wykładnię przepisów prawa UE, na podstawie której sądy konstytucyjne bez zadawania dalszych pytań prejudycjalnych mogą stwierdzić niezgodność przepisów krajowych z prawem UE. Jakkolwiek zgodnie z art. 267 TUE sądy, od których orzeczeń nie przysługuje odwołanie, badając sprawę związaną z ważnością lub wykładnią prawa UE, muszą skierować pytanie prejudycjalne do TSUE, to zgodnie z wyrokiem w sprawie *CILFIT* zadanie takiego pytania nie jest konieczne, jeżeli sprawa była już wcześniej badana przez Trybunał i na podstawie wydanego wówczas orzeczenia rozstrzygnięcie w bieżącej sprawie jest oczywiste[40].

Należy także pamiętać, że nawet w przypadku braku stwierdzenia nieważności przepisów krajowych sądy powszechne, których orzeczenia nie są ostateczne, mogą skierować do TSUE wniosek z pytaniem prejudycjalnym dotyczącym wykładni przepisów prawa UE mających zastosowanie w badanej sprawie. Pamiętając o skutku *erga omnes* wyroków wydanych w trybie prejudycjalnym, fakt ten może mieć doniosłe znaczenie praktyczne i w związku z wyrokiem w połączonych sprawach *Tele2* oraz *SSHD* doprowadzić we wszystkich państwach członkowskich do unieważnienia (stwierdzenia braku skuteczności) przepisów krajowych wprowadzających uogólniony obowiązek gromadzenia danych telekomunikacyjnych wszystkich użytkowników – nawet jeżeli właściwe sądy konstytucyjne nie stwierdziły takiej nieważności we właściwym postępowaniu.

3. Masowa inwigilacja w orzecznictwie ETPC

Analizując problematykę prawnych aspektów prowadzenia programów inwigilacyjnych zakładających hurtowe i nieograniczone przetwarzanie danych, należy zwrócić uwagę na wydane w tej materii orzeczenia Europejskiego Trybunału Praw Człowieka. Dorobek orzeczniczy ETPC w tym zakresie ma szczególne znaczenie z kilku powodów. Po pierwsze, wszystkie kraje członkowskie Unii Europejskiej są członkami

[39] Wyrok TSUE z 13 V 1981 r. w sprawie *International Chemical Corporation*, sygn. 66/80, pkt 13.

[40] Wyrok TSUE z 6 X 1982 r. w sprawie *CILFIT*, sygn. 283/81.

Rady Europy oraz stronami Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności. W efekcie wyroki ETPC mają bezpośrednie znaczenie dla kształtowania krajowego porządku prawnego w obszarze gwarancji związanych z prawami podstawowymi jednostek, w tym z wynikającego z art. 8 Konwencji prawa do poszanowania życia prywatnego. Po drugie, prawo pierwotne UE wprost odwołuje się do dorobku wynikającego z EKPC oraz wskazuje, że zagwarantowane w niej prawa podstawowe stanowią część prawa Unii jako zasady ogólne prawa. Nadto, zgodnie z art. 52 ust. 3 KPP, w zakresie, w jakim Karta definiuje prawa, które odpowiadają prawom zagwarantowanym w EKPC, ich znaczenie i zakres są takie same jak praw przyznanych przez tę Konwencję. W efekcie dorobek orzeczniczy EKPC ma istotne znaczenie przy wyrokowaniu przez TSUE we wszystkich sprawach, w których przedmiotem analizy są gwarancje związane z prawami podstawowymi. Przykładem takiego obszaru jest zgodność krajowych programów inwigilacyjnych zakładających hurtowe i nieukierunkowane przechwytywanie danych z art. 8 EKPC wprowadzającym gwarancje związane z poszanowaniem życia prywatnego i rodzinnego.

Przywołując wcześniejsze rozważania dotyczące prawa UE i orzecznictwa TSUE w zakresie programów inwigilacyjnych, należy przypomnieć, że podstawową trudnością w prawnym kwestionowaniu stosowania środków w postaci hurtowego i nieograniczonego przechwytywania danych jest ograniczona stosowalność prawa UE w tym obszarze. Bez zmiany traktatów UE i doprecyzowania bądź zawężenia pojęć związanych z bezpieczeństwem publicznym skuteczna ochrona przed działaniami państw prowadzącymi do naruszenia praw podstawowych na gruncie prawa UE będzie niemożliwa. Problem ten nie występuje w przypadku EKPC, ponieważ Konwencja nie zawiera wyłączenia przedmiotowego związanego z bezpieczeństwem publicznym. Jednostki mają więc możliwość nie tylko skarżenia do ETPC wybranych elementów związanych z prowadzeniem masowej inwigilacji (np. przepisów nakładających na przedsiębiorstwa telekomunikacyjne obowiązku wdrożenia mechanizmów ogólnej retencji danych), ale także kwestionowania legalności całych programów inwigilacyjnych prowadzonych przez organy państwowe.

Zgodnie z art. 8 ust. 2 EKPC państwa-strony Konwencji nie mogą wprowadzać środków ingerujących w prawo do prywatności z wyjątkiem wprowadzonych ustawą i koniecznych w demokratycznym społeczeństwie przypadków związanych w szczególności z bezpieczeństwem

państwowym, bezpieczeństwem publicznym, ochroną porządku i zapobieganiem przestępstwom.

Europejski Trybunał Praw Człowieka wypowiadał się kilkukrotnie w sprawach związanych ze skargami indywidualnymi dotyczącymi krajowych programów inwigilacyjnych. W sprawie *Klass i in. v. Niemcy*[41] Trybunał uznał, że – przy spełnieniu określonych warunków – jednostki mogą skarżyć się na naruszenie swoich praw gwarantowanych Konwencją w wyniku stosowania krajowych przepisów wprowadzających niejawne techniki inwigilacji, nawet jeżeli nie wykazały, że były podmiotem takiej inwigilacji. W tym zakresie Trybunał uznał, że nie można zaakceptować faktu ograniczenia stosowania Konwencji tylko z tego powodu, że osoby zainteresowane nie wiedzą o ograniczeniu swoich praw.

W sprawie *Weber i Saravia v. Niemcy*[42] Trybunał uznał że termin „z wyjątkiem przypadków przewidzianych przez ustawę" wskazany w art. 8 ust. 2 EKPC oznacza, że zastosowanie wyjątku w obszarze zakazu ingerencji w prawo do prywatności musi nie tylko wynikać z prawa krajowego, ale także być zgodne z zasadą rządów prawa. Z tego powodu przepisy krajowe muszą być przystępne dla jednostki oraz zapewniać przewidywalność, rozumianą w tym kontekście jako odpowiednia ochrona przed arbitralnością. Ponadto ze względu na zasadę rządów prawa nadzór nad działaniem upoważnionych organów w zakresie realizacji uprawnień związanych z inwigilacją musi wynikać z przepisów prawa i nie wiązać się z nieograniczoną swobodą podejmowania decyzji[43].

Z kolei w sprawie *Kennedy v. Wielka Brytania*[44] Trybunał uznał brak prawnej możliwości stosowania hurtowego i nieograniczonego przechwytywania danych za jedno z rozwiązań, na podstawie których orzekł o braku naruszenia Konwencji przez badane przepisy inwigilacyjne[45].

Trybunał w swoim dorobku orzeczniczym wskazał również listę minimalnych rozwiązań prawnych, które powinny zostać uwzględnione w przepisach krajowych dotyczących tajnych środków inwigilacji, aby uniknąć nadużycia władzy. W szczególności zastosowanie technik inwigilacji powinno być ograniczone ze względu na:

[41] Wyrok ETPC z 6 IX 1978 r. w sprawie *Klass i in. v. Niemcy*, sygn. 5029/71.
[42] Wyrok ETPC z 29 VI 2006 r. w sprawie *Weber i Saravia v. Niemcy*, sygn. 54934/00.
[43] Wyrok ETPC w sprawie *Weber i Saravia v. Niemcy*, § 92–94.
[44] Wyrok ETPC z 18 V 2010 r. w sprawie *Kennedy v. Wielka Brytania*, sygn. 26839/05.
[45] Wyrok ETPC z 18 V 2010 r. w sprawie *Kennedy v. Wielka Brytania*, § 160.

– kategorie przestępstw, z którymi może wiązać się autoryzacja zastosowania środków inwigilacyjnych;
– kategorie osób, które mogą być jej poddane;
– ograniczenie czasu stosowania środków;
– procedurę określającą zasady badania, przechowywania i wykorzystywania zgromadzonych danych;
– środki ostrożności zastosowane w przekazywaniu zgromadzonych danych innym podmiotom;
– kryteria, według których zebrane dane powinny zostać usunięte bądź zniszczone[46].

Trybunał określił także, w jaki sposób należy interpretować wprowadzony w art. 8 ust. 2 EKPC termin wyjątków „koniecznych w demokratycznym społeczeństwie". W szczególności interesujące są w tym zakresie rozważania dotyczące wyważenia znaczenia norm związanych z bezpieczeństwem publicznym oraz prawem do prywatności. Trybunał zwrócił uwagę na zasadę proporcjonalności, wyrażającą się zachowaniem równowagi pomiędzy wymogami interesu ogólnego a interesem osoby lub osób objętych środkami inwigilacji. W tym zakresie prawodawca krajowy dysponuje znaczącą swobodą w wyborze środków do osiągnięcia tego celu. Trybunał podkreślił jednak, że wprowadzanie tajnych programów inwigilacji uzasadnianych względami bezpieczeństwa narodowego wiąże się z ryzykiem osłabienia lub nawet zniszczenia zasad demokracji. Z tego powodu w ocenie proporcjonalności przyjętego środka znaczącą rolę powinny odgrywać rozwiązania prawne mające na celu wyeliminowanie ryzyka nadużycia władzy[47].

Na podstawie powyższych rozważań Trybunał w sprawie *Zacharow v. Rosja* wskazał, że wprowadzenie przez Rosję obowiązku umożliwienia upoważnionym organom rejestrowania transmisji w sieciach telekomunikacyjnych wobec wszystkich użytkowników, i to w sposób niepozwalający na prześledzenie, jakie dane oraz przez kogo były przechwytywane, nie pozwala na wdrożenie skutecznych mechanizmów kontroli i nadzoru ograniczających ryzyko nadużycia uprawnień.

Do najnowszych orzeczeń Trybunału dotyczących materii przepisów inwigilacyjnych należy zaliczyć sprawę *Szabo i Vissy v. Węgry*[48], której podstawą była skarga dwóch obywateli Węgier na przepisy krajowe nadające szerokie uprawnienia służbie antyterrorystycznej policji,

[46] Wyrok ETPC w sprawie *Weber i Saravia v. Niemcy*, § 95.
[47] Wyrok ETPC z 4 XII 2015 r. w sprawie *Zacharow v. Rosja*, sygn. 7143/06, § 232.
[48] Wyrok ETPC z 12 I 2016 r. w sprawie *Szabo i Vissy v. Węgry*, sygn. 37138/14.

skutkujące, zdaniem skarżących, naruszeniem ich prawa do poszanowania prywatności. W analizowanej sprawie Trybunał doprecyzował wcześniejsze rozważania dotyczące definicji konieczności, wprowadzając termin „ścisłej konieczności" (ang. *strict necessity*), która – jak wskazano – powinna być stosowana w przypadkach związanych z inwigilacją obywateli przez państwo[49]. Ścisłą konieczność należy rozumieć poprzez łączne spełnienie dwóch przesłanek: po pierwsze, konieczności zastosowania danego środka w celu ochrony demokratycznych instytucji państwa (rozumienie węższe, stosowane we wcześniejszych orzeczeniach ETPC), i po drugie, konieczności zastosowania środka w konkretnym przypadku, w związku z potrzebą pozyskania istotnych danych operacyjnych dotyczących inwigilowanych jednostek. W efekcie Trybunał podkreślił, że zdefiniowanie wyjątku od zasady niedopuszczalności ingerencji władzy publicznej w korzystanie z prawa do prywatności jako „koniecznego w demokratycznym społeczeństwie" (art. 8 ust. 2 EKPC) musi odnosić się nie tylko do ochrony interesu społeczeństwa jako całości, ale również być uzasadnione faktyczną potrzebą związaną z uzyskaniem informacji od konkretnych, inwigilowanych osób.

Nadto w sprawie *Szabo i Vissy v. Węgry* Trybunał zauważył, że stosowanie technik inwigilacyjnych musi być ograniczone w czasie i niedopuszczalna jest sytuacja, w której zgoda na stosowanie takich środków jest przedłużana bez odpowiedniej kontroli sądowej. Ponadto Trybunał rozwinął wcześniejsze rozważania dotyczące nadzoru ze strony władzy wykonawczej, zauważając, że wydawanie zgody na stosowanie technik inwigilacyjnych na szczeblu politycznym władzy wykonawczej nie zapewnia gwarancji związanych z ochroną przed nadużyciem władzy[50].

Biorąc pod uwagę szeroki zakres podmiotowy, podejmowanie decyzji na szczeblu politycznym, brak skutecznego nadzoru sądowego oraz niespełnienie kryterium „ścisłej konieczności", Trybunał uznał przepisy węgierskie za naruszające art. 8 Konwencji[51].

Analiza orzecznictwa Trybunału, zwłaszcza niedawnych wyroków w sprawie *Zacharow v. Rosja* (2015) oraz *Szabo i Vissy v. Węgry* (2016), wskazuje na rosnące znaczenie konieczności i proporcjonalności jako warunków niezbędnych do uznania za uzasadnione ograniczenia prawa do prywatności w wyniku działań inwigilacyjnych państw. Ponieważ programy inwigilacji oparte na nieograniczonym i hurtowym

[49] Wyrok ETPC z 12 I 2016 r. w sprawie *Szabo i Vissy v. Węgry*, § 73.
[50] Wyrok ETPC z 12 I 2016 r. w sprawie *Szabo i Vissy v. Węgry*, § 77.
[51] Wyrok ETPC z 12 I 2016 r. w sprawie *Szabo i Vissy v. Węgry*, § 89.

gromadzeniu danych osobowych z definicji nie spełniają tych warunków, nie mogą być uznane za akceptowalne w rozumieniu art. 8 ust. 2 EKPC. Niemniej jednak dotychczasowe orzecznictwo Trybunału nie zawiera jednoznacznego zanegowania możliwości stosowania środków związanych z masowym przechwytywaniem danych. W analizowanych przypadkach Trybunał każdorazowo dokonał analizy przepisów krajowych, wskazując na niewystarczające zabezpieczenia wprowadzone w celu ochrony przed arbitralnymi decyzjami polityków lub uprawnionych organów, a także na brak skutecznych mechanizmów dochodzenia praw przez obywateli, których prawa zostały naruszone.

W chwili obecnej na rozpoznanie przez Trybunał czeka kilka spraw złożonych przez organizacje pozarządowe kwestionujące wprost legalność prowadzenia programów inwigilacyjnych nastawionych na masowe przetwarzanie komunikacji elektronicznej. W ramach sprawy *Big Brother Watch i in. v. Wielka Brytania*[52] wnioskujący wnoszą między innymi o uznanie przepisów krajowych, na podstawie których realizowany jest przez GCHQ program inwigilacyjny *Tempora*, za naruszające art. 8 Konwencji. Z podobnym wnioskiem wystąpiło dziesięć organizacji działających w obszarze ochrony prywatności w ramach sprawy *Amnesty International i in. v. Wielka Brytania*[53], z tą wszakże różnicą, że sprawa ta została wniesiona do Trybunału po wyczerpaniu drogi sądowej przed krajowym Sądem ds. Uprawnień Śledczych (ang. *Investigatory Powers Tribunal*).

Podsumowanie

Według ujawnionych w 2013 r. informacji, dzięki podłączeniu do światłowodowych łączy telekomunikacyjnych przechodzących przez Wielką Brytanię GCHQ każdego dnia miało dostęp do 21 petabajtów informacji, co odpowiada 10 gigabitom danych na sekundę[54]. W tym samym okresie NSA, realizując program *RAMPART-A* polegający na podsłuchu transmisji światłowodowych, miała mieć dostęp do ponad 3 terabajtów danych

[52] Skarga do ETPC z 4 IX 2013 r., sprawa *Big Brother Watch i in. v. Wielka Brytania*, sygn. 58170/13.

[53] Skarga do ETPC z 20 V 2015 r., sprawa *Amnesty International i in. v. Wielka Brytania*, sygn. 24960/15.

[54] The Guardian, *GCHQ taps fibre-optic cables*…

na sekundę (3000 gigabajtów na sekundę)[55]. Dla porównania, *Pionier*, największa polska naukowa sieć teleinformatyczna, dysponuje łączem do światowego Internetu o przepustowości 15 gigabitów na sekundę[56], czyli dwieście razy mniejszym. Z kolei w ramach programu *Muscular*, prowadzonego wspólnie przez GCHQ oraz NSA, a ukierunkowanego na przechwytywanie korespondencji i transmisji innych danych do serwerów Google i Yahoo, w ciągu trzydziestodniowego okresu pomiędzy grudniem 2012 a styczniem 2013 r. z pozyskanych informacji utworzono ponad 180 mln rekordów[57].

Statystyki wskazują na rosnące znaczenie kontroli komunikacji jako źródła pozyskiwania informacji w prowadzonych postępowaniach. Trend ten jest oczywisty, zwłaszcza biorąc pod uwagę dynamiczny rozwój form komunikacji elektronicznej, skutkujący jej coraz powszechniejszym stosowaniem. Prawo do zachowania prywatności – do niedawna utożsamiane głównie z ochroną życia rodzinnego, miru domowego czy tajemnicą korespondencji – coraz częściej musi być odnoszone do mediów elektronicznych. Obszarem szczególnego zainteresowania powinny być w tym zakresie uprawnienia państw pozwalające na stosowanie nieograniczonej kontroli komunikacji elektronicznej. W filozofii oraz literaturze symbolem permanentnej kontroli ze strony władzy jest panoptykon, więzienie doskonałe, w którym każdy nieustannie powinien czuć się obserwowany bez możliwości sprawdzenia, czy rzeczywiście jest. Rozwój techniki spowodował, że programy inwigilacji realizowane przez poszczególne państwa często przypominają „cyfrowy panoptykon". Rolą prawodawcy jest wbudowanie takich zabezpieczeń w mechanizmy stanowionego prawa, aby egzekutywa nie mogła wykorzystać dostępnych technik inwigilacji do realizacji wizji przedstawionej w literaturze.

---

[55] Informacja pochodząca z ujawnionych przez E. Snowdena dokumentów dotyczących finansowania tajnych programów rozpoznania elektronicznego NSA, http://www.statewatch.org/news/2014/jun/usa-nsa-foreignpartneraccessbudgetfy2013-redacted.pdf (dostęp: 1 III 2017).

[56] *Polski Internet Optyczny PIONIER – ogólnopolska szerokopasmowa sieć optyczna nauki*, sekcja „Infrastruktura", http://www.pionier.net.pl/online/pl/projekty/69/ (dostęp: 1 III 2017).

[57] The Washington Post, *How the NSA's MUSCULAR program collects too much data from Yahoo and Google*, 30 IX 2013, http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/#document/p1/a129319 (dostęp: 1 III 2017).

Szukanie prawnej ochrony obywateli przed nadmierną ingerencją w obszar prywatności przez władzę publiczną nie zawsze może być skuteczne na gruncie przepisów krajowych. Przyjmując zasadę legalizmu jako normę w krajach demokratycznych, trudno założyć, aby ustawodawca wprowadził rozwiązania prawne w obszarze inwigilacji w oczywisty sposób naruszające przepisy krajowe czy normy konstytucyjne. Z tego powodu szczególne znaczenie praktyczne mogą mieć normy prawa międzynarodowego czy to związane z funkcjonowaniem w organizacjach międzynarodowych (takich jak Unia Europejska bądź Rada Europy), czy wynikające z przystąpienia do określonych konwencji lub traktatów (jak EKPC). Bogaty dorobek orzeczniczy TSUE oraz ETPC może być pomocny nie tylko przy rozstrzyganiu spraw dotyczących mechanizmów inwigilacji stosowanych w indywidualnych sprawach, ale również przy wyznaczaniu kierunków rozwoju krajowych przepisów w sposób zgodny ze standardami międzynarodowymi.

Przedstawione rozważania można bezpośrednio odnieść do przepisów obowiązujących w Polsce. Kwestia braku zgodności stosowania ogólnego obowiązku przetrzymywania danych telekomunikacyjnych z prawem Unii była już kilkukrotnie badana przez TSUE, a ostatecznie potwierdzona wyrokiem w połączonych sprawach *Tele2* i *SSHD*. W tym kontekście wynikający z art. 180a ust. 1 ustawy Prawo telekomunikacyjne ogólny obowiązek przetrzymywania danych jest wprost niezgodny z art. 15 ust. 2 dyrektywy 2002/58. Przepisy pr. tel. w tym zakresie stanowiły implementację dyrektywy retencyjnej[58], która także została uznana przez TSUE za niezgodną z prawem UE[59]. Trwanie przez polskiego prawodawcę przy przepisach, które bez wątpienia są niezgodne z przepisami wyższego rzędu, wydaje się zatem nieuzasadnione, a biorąc pod uwagę zasadę lojalności oraz prymat prawa UE – także bezcelowe w ewentualnych sporach sądowych. Problem ten dostrzegł także Rzecznik Praw Obywatelskich, występując do minister cyfryzacji z wnioskiem o zajęcie stanowiska w sprawie zgodności pr. tel. w zakresie implementującym dyrektywę retencyjną z przepisami KPP oraz orzecznictwem TSUE[60].

[58] S. Piątek, *Prawo telekomunikacyjne. Komentarz*, Warszawa 2013, komentarz do art. 180a, nb. 1.

[59] Wyrok TSUE z 8 IV 2014 r. w sprawie *Digital Rights Ireland Ltd*.

[60] Wniosek Rzecznika Praw Obywatelskich do Minister Cyfryzacji z 1 II 2017 r., sygn. VII.520.11.2017.AG.

Poważne wątpliwości co do zgodności z art. 8 ust. 2 EKPC dotyczą przepisów uchwalonej w zeszłym roku ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw[61], znaną powszechnie w literaturze przedmiotu jako „ustawa inwigilacyjna". Wynikające z noweli nowe uprawnienia służb umożliwiają dostęp do metadanych dotyczących korzystania z usług internetowych oraz pocztowych bez potrzeby wykazania, że informacje te są konieczne i związane z konkretnym, prowadzonym postępowaniem oraz bez realnej kontroli sądu[62]. Rozwiązanie takie wydaje się w sposób oczywisty niezgodne z – dostępnymi już w czasie uchwalania przepisów – licznymi orzeczeniami ETPC wskazującymi na konieczność i proporcjonalność jako warunki konieczne zastosowania technik inwigilacyjnych. Z kolei TSUE w wyroku w sprawie *Schrems* wskazał, że „w szczególności uregulowanie pozwalające władzom publicznym na uzyskanie powszechnego dostępu do treści wiadomości elektronicznych należy uznać za naruszenie zasadniczej istoty prawa podstawowego do poszanowania życia prywatnego, wynikającego z art. 7 karty"[63].

Tak samo krytycznie należy ocenić zmianę dotyczącą wprowadzenia pozornej kontroli sądowej w zakresie realizacji uprawnień organów ścigania w dostępie do danych telekomunikacyjnych. Warto przy tym wskazać, że wcześniejsze przepisy z powodu braku kontroli sądowej zakwestionował Trybunał Konstytucyjny (TK) w wyroku z 30 lipca 2014 r.[64] Wydaje się jednak, że zaproponowany obecnie model nie realizuje wniosków z wyroku TK, a także jest niezgodny z orzecznictwem zarówno TSUE (por. *Tele2* i *SSHD*, pkt 120), jak i ETPC (por. *Zacharow v. Rosja*, § 233). Problem ten dostrzegła także Komisja Wenecka w opinii wydanej na temat ustawy inwigilacyjnej[65].

Jak słusznie zauważył Naczelny Sąd Administracyjny, „z punktu widzenia demokratycznego państwa prawnego oraz społeczeństwa obywatelskiego niezwykle istotnym jest, aby działalność służb specjalnych […] podlegała społecznej kontroli, ale w obszarach, które

[61] Ustawa z dnia 15 I 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz.U. poz. 147).

[62] Por. znowelizowana treść art. 20c ustawy o Policji czy art. 28 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu.

[63] Wyrok TSUE z 6 X 2015 r. w sprawie *Schrems*, sygn. C-362/14, pkt 94.

[64] Wyrok TK z 30 VII 2014 r., sygn. K 23/11.

[65] Europejska Komisja na rzecz Demokracji przez Prawo, *Opinion on the act of 15 January 2016 amending the police act and certain others acts*, 13 VII 2016, sygn. CDL-AD(2016)012.

nie ograniczają możliwości ich skutecznego działania i nie dotyczą konkretnych prowadzonych postępowań, czy też stosowanych w nich metod operacyjnych"[66]. W demokratycznym państwie prawa nie można jednak przyjąć, że każde działanie służb jest uzasadnione i konieczne, natomiast brak realnej kontroli sądowej powoduje, iż taka ocena jest niemożliwa do przeprowadzenia. Na problem ten wskazuje wprost opublikowany w styczniu 2017 r. raport Fundacji Panoptykon, w którym zaprezentowano praktyczne skutki stosowania przepisów ustawy inwigilacyjnej[67]. W szczególności przedstawiono zestawienie dotyczące informacji nadesłanych przez sądy okręgowe, które zgodnie z art. 16 ust. 4a pkt c ustawy Prawo o ustroju sądów powszechnych[68] powinny pełnić nadzór nad działalnością uprawnionych organów, z którego to zestawienia wynika, że nadzór ten jest realizowany wyłącznie na podstawie zbiorczych informacji nadesłanych przez służby, bez weryfikacji przedstawionych informacji i bez analizy (nawet wyrywkowej) materiałów dotyczących indywidualnych spraw. Bez wątpienia, takie rozwiązanie kwestii niezależnej kontroli nie spełnia standardów wynikających z orzecznictwa EKPC i *per se* stało się jedną z przyczyn uznania przepisów krajowych za niespełniające wymagań Konwencji w sprawie *Zacharow v. Rosja*[69].

Niezależnie od problematyki zgodności krajowych przepisów inwigilacyjnych w obszarze poszanowania prywatności z normami prawa międzynarodowego bez wątpienia interesujący wydaje się kierunek, w jakim zmierza orzecznictwo zarówno TSUE, jak i EKPC. Należy oczekiwać, że w najbliższych latach wyroki zapadające w sprawach zawisłych przed trybunałami doprowadzą do faktycznego utrudnienia bądź uniemożliwienia prowadzenia programów inwigilacyjnych opartych na hurtowym i nieukierunkowanym przechwytywaniu danych.

---

[66] Wyrok Naczelnego Sądu Administracyjnego z 28 IV 2016 r., sygn. I OSK 2620/14.

[67] Fundacja Panoptykon, *Rok z ustawą inwigilacyjną*, 18 I 2017, https://panoptykon.org/sites/default/files/publikacje/fp_rok_z_tzw._ustawa_inwigilacyjna_18–01–2017.pdf (dostęp: 1 III 2017).

[68] Ustawa z dnia 27 VII 2001 r. Prawo o ustroju sądów powszechnych (tekst jedn. Dz.U. 2016, poz. 2062).

[69] Por. § 283 wyroku ETPC w sprawie *Zacharow v. Rosja* w zakresie opierania działań nadzorczych wyłącznie na danych statystycznych, bez analizy indywidualnych przypadków zasadności podejmowania działań inwigilacyjnych.

LEGAL ASPECTS OF CONDUCTING MASS SURVEILLANCE OF CITIZENS AND NON-DIRECTED DATA COLLECTION WITHIN THE EUROPEAN UNION, INCLUDING THE JUDICIAL DECISIONS OF THE CJEU AND THE ECHR

Summary

The activity which States undertake when conducting extensive non-directed surveillance programmes is seen as one of the major threats to privacy at the time of the information society. This problem has a special dimension in the European Union because the surveillance activity of individual Member States may be an obstacle to the functioning of a single internal market, particularly when it comes to ensuring the freedom to transfer personal data.

Due to the supranational character of contemporary means of communication, and especially Internet communication services, guarantees related to the protection of privacy ought to be analysed not only through the prism of domestic regulations but also in the light of international law provisions.

Results of an analysis of the relevant primary and secondary EU law have been presented. A special focus was put on Directive 95/46 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data and Directive 2002/58 on privacy and electronic communications. The formal effects of the rulings of the Court of Justice which determined invalidity of the retention directive have been analysed as well, mainly from the perspective of the validity of national provisions implementing the general obligation to retain the data in legal orders of EU Member States.

Particularly interesting seems to be the analysis of the grounds for non-directed surveillance programmes and comparison of the findings with the rulings of the CJEU and the ECHR, particularly the recent CJEU's judgment in *Tele2* and the ECHR's judgment in *Szabo v. Hungary*. The judicial decisions analysed in the paper may not only be useful in solving matters related to surveillance instruments used in individual cases but may also serve as a helpful tool in establishing the directions of development of domestic regulations in line with international standards. The latter may also be related to the provisions of the surveillance act and anti-terrorist act recently binding in Poland.

Keywords: mass surveillance – general obligation of data retention – data retention – proportionality of surveillance