GDAŃSKIE STUDIA PRAWNICZE, TOM XL, 2018

Marek Zubik*
Uniwersytet Warszawski
Jan Podkowik**
Uniwersytet Warszawski
Robert Rybski***
Uniwersytet Warszawski

PRYWATNOŚĆ. WOLNOŚĆ U PROGU D-DAY[1]

Dzień 25 maja 2018 r. z pewnością przejdzie do historii jako istotny punkt w rozwoju ochrony prywatności w państwach Unii Europejskiej. Chociaż poniższe refleksje powstały jeszcze przed tą datą, to już wówczas można, bez szczególnego narażenia się na przesadę, wskazać ją jako doniosłą. W tym dniu weszło w życie kilka aktów prawodawczych Unii Europejskiej, które porządkują oraz aktualizują dotychczasowe podejście do regulowania ochrony prywatności w cyberrzeczywistości.

Przejrzenie dotychczasowego podejścia prawodawcy unijnego do wypracowanych standardów ochrony prywatności było konieczne z kilku powodów. Po pierwsze, dotychczasowe rozwiązania mogły być ocenione z perspektywy praktyki oraz orzecznictwa sądowego tak państw członkowskich, jak i Europejskiego Trybunału Praw Człowieka[2] oraz Trybunału Sprawiedliwości Unii Europejskiej[3].

* m.zubik@wpia.uw.edu.pl
** j.podkowik@wp.pl
*** robert.rybski@wpia.uw.edu.pl

1 Tekst powstał w ramach realizacji programu badawczego finansowanego przez NCN (2015/17/B/H55/01408) „Wpływ orzecznictwa europejskich sądów konstytucyjnych i Trybunału Sprawiedliwości UE na kształtowanie uniwersalnej treści wolności komunikowania się w Europie w dobie rozwoju technologicznego".

2 Z najnowszych warto tu przywołać orzeczenia ETPC – z dnia 25 października 2016 r. *Bašić przeciwko Chorwacji* (wniosek nr 22251/13), z dnia 8 listopada 2016 r. *Figueiredo Teixeira przeciwko Andorze* (wniosek nr 72384/14), z dnia4 kwietnia 2017 r. *Matanović przeciwko Chorwacji* (wniosek nr 2742/12), z dnia 22 czerwca 2017 r. *Aycaguer przeciwko Francji* (wniosek nr 8806/12), z dnia 7 listopada 2017 r. *Zubkov i inni przeciwko Rosji* (wnioski nr 29431/05, 7070/06 i 5402/07) czy z dnia 8 lutego 2018 r. *Ben Faiza przeciwko Francji* (wniosek nr 31446/12).

3 Tutaj podstawowe znaczenie miały dwa orzeczenia w połączonych sprawach: z dnia 8 kwietnia 2014 r. *Digital Rights Ireland i Seitlinger i inni* (C-293/12 i C-594/12) oraz z dnia 21 grudnia 2016 r. *Tele2 Sverige AB i Secretary of State for the Home Department* (C-203/15 i C-698/15).

Szczególnie orzecznictwo przyniosło sporo ustaleń. Warto chociażby przypomnieć, że ostatni z przywołanych organów sądowych uznał nieważność całej dyrektywy 2006/24/WE w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej. Tym samym ta sfera społeczna nie była już obecnie *terra incognita* dla prawodawcy. Po drugie, pojawiły się nowe możliwości technologiczne zarówno w komunikowaniu się, jak i związane z nimi zagrożenia dla prywatności. Szybki postęp techniczny i globalizacja przyniosły nowe wyzwania. Zradykalizowała się skala zbierania informacji i wymiany danych osobowych. Uznano co prawda dotychczasowe ogólne zasady ochrony prywatności w łączności elektronicznej w prawie UE za nadal „rozsądne". Jednocześnie dostrzeżono jednak, że nie w pełni nadążają już one za rozwojem technologicznym i rzeczywistością rynkową, co skutkuje z kolei niespójną lub niedostatecznie skuteczną ochroną prywatności i poufności danych osobowych[4]. Po trzecie, zrewidowano nieco dotychczasowe podejście co do zróżnicowania ochrony prywatności jednostek oraz osób prawnych. Po czwarte, chciano uelastycznić mechanizmy ochrony, tak by były one bardziej adekwatne, a również odpowiadały faktycznemu, zróżnicowaniu stopnia i form zagrożeń. Po piąte, zauważono nowe wyzwania, jak chociażby urealnienie się mechanizmów sztucznej inteligencji, która na trwałe wkroczyła w sferę zachowań ludzkich, przekształcając ją niekiedy bez woli, wiedzy i pełnej kontroli człowieka. Wreszcie – faktycznie doszło do tak daleko idących przemian w sferze łączności elektronicznej, które, za sprawą nowinek technologicznych, zmieniły niekiedy radykalnie zachowania społeczne. W tym sensie 25 maja 2018 r. – to niewątpliwie swoisty D-Day dla prawnej ochrony wolności prywatności, o skali przełomu, na miarę owego dnia z 1944 r.

1. Dzień 25 maja 2018 r. to początek obowiązywania trzech doniosłych aktów normatywnych przyjętych na poziomie prawodawczym Unii Europejskiej: rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW (tzw. dyrektywa policyjna) oraz Rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia pry-

[4] Zob. motyw 6 projektu Rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE COM (2017) 10 final; 2017/03 (COD).

watnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), które w momencie pisania tego tekstu, jeszcze nie przeszło całej ścieżki legislacyjnej. Należy do tego dodać, że na wniosek Komisji Europejskiej toczą się również prace nad przyjęciem dyrektywy Parlamentu Europejskiego i Rady (UE) wprowadzającej Europejski kodeks łączności elektronicznej, zawierający wiele definicji legalnych, rzutujących na znaczenie pojęć ujętych w pozostałych aktach normatywnych[5].

W dużej mierze nowe rozwiązania prawodawcze UE znajdą bezpośredni efekt regulacyjny w polskim porządku prawnym. Część jednak z nich, chociażby ze względu na przejrzystość i spójność systemu prawa, wymaga wszakże interwencji prawodawcy krajowego. Wszystkie razem wzięte z kolei – co nie mniej zasadnicze – muszą się spotkać z praktycznym przyswojeniem.

2. Unormowanie kwestii przetwarzania informacji o osobach musi być w taki sposób dokonywane, by ostatecznie dobrze służyło ludziom. Prawodawca unijny traktuje dane osobowe jako przedłużenie tożsamości osoby – cień tożsamości (Shadow-ID), a zatem za należące do sfery chronionej jako prywatność[6]. Informacje te należą do osoby, której dotyczą. Jednakże po ich przetworzeniu w cyberrzeczywistości najczęściej osoba ta przestaje mieć na nie wpływ. Prawodawca unijny stara się zatem wyważyć różne dobra prawie chronione. Z jednej strony wychodzi z założenia, że Internet i telefonia komórkowa są usługami świadczonymi w interesie ogólnym. Tym samym dostęp do nich musi być powszechny i cenowo przystępny. Z drugiej strony celem nowych regulacji ma być stworzenie jednolitego rynku cyfrowego zapewniającego bezpieczeństwo usług cyfrowych i dającego poczucie zaufania po stronie użytkowników. Nowe prawodawstwo ma chronić prawa użytkowników, przy jednoczesnym zapewnieniu stabilności prawnej niezbędnej do prowadzenia działalności gospodarczej. Kładzie też nacisk na ochronę konsumentów, szczególnie przed niechcianymi informacjami komercyjnymi, starając się też wyważyć interesy przedsiębiorców, szczególnie małych i średnich.

Trafnie prawodawca unijny wychodzi z założenia, że prywatności nie można traktować jako bezwzględnie chronioną wolność. Widzi ją w kontekście jej społecznej funkcji, jaką pełni, oraz relacji z innymi wolnościami i prawami. Nowe prawodawstwo stara się zapewnić wysoki i spójny stopień ochrony osób fizycznych, a jednocześnie usuwać przeszkody w przepływie danych osobowych. Przyjmuje jako cel stworzenie w państwach członkowskich możliwie jednakowego standardu ochrony wolności i praw osób w związku z przetwarzaniem ich danych. Ochrona ta ma być niezależna od obywatelstwa. Podlegać jej mają

[5] COM/2016/0590.

[6] Zob. też J. Taczkowska-Olszewska, *Autonomia informacyjna jednostki a zarządzanie cyfrową tożsamością. Granice autokreacji* [w:] *Prawo prywatności jako reguła społeczeństwa informacyjnego*, red. K. Chałubińska-Jentkiewicz, K. Kakareko, J. Sobczak, Warszawa 2017, s. 33 i nn.

wszelkie informacje o zidentyfikowanych lub możliwych do zidentyfikowania osobach fizycznych. Spseudonimizowane dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, mają być uznawane za informacje o osobie fizycznej możliwej do zidentyfikowania. Nowe rozwiązania starają się też zapobiec ryzyku obchodzenia prawa przez podmioty przetwarzające dane osobowe osób fizycznych. Przyjmują założenie, że ochrona ta ma przybrać postać neutralną pod względem technicznym, a zatem nie być uzależniona od stosowanych technik[7].

Już na poziomie prac prawodawczych UE dostrzeżono jednak słabsze strony nowych regulacji. Przede wszystkim nakładanie się na siebie odrębnych aktów prawodawczych, ich dużą objętość i wzajemne przeplatanie się rozwiązań. Taka technika legislacyjna niewątpliwie utrudnia chociażby zapoznanie się z tymi rozwiązaniami. Za ułomność przyjętych regulacji wskazuje się pozostawienie nieuregulowanymi dwóch doniosłych, a zarazem nowych zjawisk technologicznych. Chodzi o kwestię ochrony prywatności w kontekście przekazywania danych między urządzeniami (M2M) oraz przechowywania danych osobowych w chmurze obliczeniowej. Szczególnie w pierwszym wypadku może to rodzić poważne zagrożenia. Internet świata urządzeń jest bardzo inwazyjny i może otwierać drogę do naruszenia prywatności podczas transmisji danych w łączności elektronicznej. Pozwala też przekształcić obecnie duże zbiory danych (BigData) w wielkie zbiory danych (HugeData), a to może następnie doprowadzić do powstania środowiska opartego w całości na danych (AllData). Nie bez znaczenia dla ochrony prywatności w cyberświecie jest zatem okoliczność, że także urządzenia elektroniczne przekazują sobie dane osobowe, a dzięki inteligentnemu przetwarzaniu mogą „sprofilować" i „utowarowić" osoby fizyczne i prawne oraz zarabiać pieniądze, nawet bez wiedzy użytkowników. Zwraca się także uwagę na zjawisko przekształcania dotychczasowych aplikacji cyfrowych w platformy cyfrowe[8].

3. Nowe technologie w sferze elektronicznej komunikacji są wykorzystywane nie tylko jako narzędzia ułatwiającego porozumiewanie się jednostek. Stwarzają nowe możliwości nabywania dóbr i usług lub decydowania o realizowaniu własnych potrzeb. Są nieocenione w zapewnieniu bezpieczeństwa osobom i mieniu, umożliwiając monitoring osób i miejsc oraz ich elektroniczny nadzór. Szczególną rolę odgrywa w tym zakresie Internet. Jest on nie tylko nośnikiem komunikatów przekazywanych między jednostkami. Stał się wielowymiarowym narzędziem tworzenia, przechowywania i przekazywania danych o zróżnicowanym

[7] Zob. np motywy 4, 10, 13 i 26 rozporządzenia z dnia 27 kwietnia 2016 r.

[8] Zob. np. motywy 1.3.9, 3.3, 4.17, 5.1.5, 6.12 i 6.13 opinii Europejskiego Komitetu Ekonomiczno-Społecznego „Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej)" z dnia 5 lipca 2017 r. (Dz. Urz. UE C 345/23 z 13.10.2017 r.).

charakterze, a zarazem narzędziem umożliwiającym funkcjonowanie jednostki w nowoczesnym społeczeństwie. Dzięki nowym technologiom zarówno przedsiębiorstwa prywatne, jak i organy publiczne mogą na niespotykaną dotąd skalę wykorzystywać informacje o osobach w swojej działalności.

Nowe technologie mają niestety też swoją ciemniejszą stronę. Coraz szerzej stanowią narzędzia wykorzystywane przez osoby fizyczne, państwa jak i podmioty niepaństwowe do wpływania poprzez cyberoperacje na życie demokratycznych wspólnot i ich destabilizowanie, także w innych krajach, cyberszpiegostwa czy cyberprzestępczości[9]. Zaczęto nawet rozważać kwestie realności cyberwojny[10]. Nowe technologie mogą być wykorzystywane do nieuprawnionego pozyskiwania wiedzy o zachowaniach współobywateli, w tym o treściach i formach przekazywanych komunikatów, gromadzenia tych danych na własne potrzeby i ich przetwarzania. Mogą dodatkowo stanowić narzędzie służące popełnianiu specjalistycznych przestępstw zagrażających różnym dobrom oraz służyć komunikowaniu się lub integracji środowisk przestępczych. Rozwój technologiczny doprowadził wreszcie do wykształcenia się nowych form popełniania tradycyjnych przestępstw. Internet i środki komunikowania się na odległość są dodatkowym, specjalistycznym narzędziem w rękach przestępców, istniejącym niejako równolegle do dotychczas wykorzystywanych technik. Wykształciły się ponadto nowe, nieistniejące dotychczas rodzaje przestępstw, możliwe do popełnienia wyłącznie z użyciem nowych technologii.

Komunikowanie się za pomocą nowych technologii i przestępstwa popełniane z ich wykorzystaniem generalnie wymykają się spod kontroli społeczeństwa. Niejednokrotnie jest utrudnione ustalenie tożsamości osób naruszających prawo, a w konsekwencji zapobieżenie i wykrycie zagrożeń. Okoliczność ta powinna być uwzględniona przez ustawodawcę i służby, które są zobowiązane zapewnić bezpieczeństwo obywatelom i mechanizmom demokratycznego i praworządnego sprawowania władzy w państwie. Demokratyczne państwo prawne nie może bowiem ignorować rosnącego znaczenia nowych technologii, a ponadto skali ich wykorzystywania, niekiedy w celu naruszania prawa. Służby stojące na straży tych wartości winny nie tylko móc wykrywać już popełnione przestępstwa. W warunkach globalnej przestępczości i przekraczającego granice państw terroryzmu czy przestępczości zorganizowanej istotna jest również prewencja zagrożeń, których wystąpienie może wyrządzić nieodwracalne straty dla dóbr prawnie chronionych.

Nie jest kwestionowane, że „walka z poważną przestępczością, a zwłaszcza z przestępczością zorganizowaną i terroryzmem, z pewnością ma pierwszorzędne znaczenie dla zagwarantowania bezpieczeństwa publicznego, zaś jej skutecz-

[9] Zob. szerzej D.R. Coats, *Worldwide Threat Assessment of the US Intelligence Community*, 13.02.2018.

[10] UN, *Human Rights Council, Report of the Special Rapporteur on the right to privacy*, A/HRC/37/62, 28.02.2018, s. 14. W myśl ustaleń tego raportu w więcej niż 33% z 193 państw członków Narodów Zjednoczonych (ponad 70 państw) nie ma w swoim porządku prawnym rozwiązań chroniących prywatność (s. 28).

ność może w znacznym stopniu zależeć od wykorzystania nowoczesnych technik dochodzeniowo-śledczych"[11]. Jednakże tego rodzaju doniosły społecznie cel, mimo że ma fundamentalne znaczenie, sam w sobie nie był dla TSUE wystarczający dla przyjęcia poglądu, że uogólniony system zatrzymywania wszelkich informacji pochodzących z łączności elektronicznej jest konieczny do celów tej walki. Wyraźnie też daje się zauważyć, coraz większe napięcie między ochroną prywatności a zapewnieniem przez władze publiczne bezpieczeństwa publicznego[12]. Wreszcie świadomość dokonywanej przez władze publiczne ingerencji w prywatność w komunikacji elektronicznej nie pozostaje bez wpływu na zachowania społeczne oraz korzystanie przez jednostki z ich wolności i praw[13]. Próbę zrównoważenia tych doniosłych dóbr i wartości podjęła UE po raz kolejny właśnie w nowej dyrektywie 2016/680.

4. W prawoznawstwie rozróżnia się wolności, prawa oraz obowiązki[14]. Podobnie czyni to i polski ustrojodawca w rozdziale II Konstytucji[15]. Kategorie te odnoszą się do jednostek, ściślej poszczególnych osób i niekiedy tworzonych przez nie swobodnie podmiotów zbiorowych. Dwa pierwsze pojęcia zbiorczo z czasem zaczęto ujmować jako prawa człowieka. Brak jest jednak pełnej jednolitości w posługiwaniu się tymi pojęciami oraz jednoznacznych konstrukcji doktrynalnych[16]. Niejednolitość języka prawnego i prawniczego przeniósł się na język publicystyki. Brak ogólnej wizji, niestaranność, mniejszy stopień precyzji, chęć łatwego przekazu, a być może także inne czynniki przeniosły i utrwaliły w języku potocznym, z którego z kolei zaczął czerpać prawodawca, zamykając intelektualne koło.

Prywatność człowieka jest w kontekście owego podziału niewątpliwie wolnością. Zasadne jest mówienie o prawnej jej ochronie czy też o szczegółowych prawach, które temu służą, a także o obowiązkach z tego ciążących na innych. Co

---

[11] Motyw 51 wyroku TSUE w połączonych sprawach C-293/12 i C-594/12.

[12] Por. F.H. Cate, J.X. Dempsey, *Introduction and Background* [w:] *Bulk Collection. Systematic Government Access to Private-Sector Data*, eds. F.H. Cate, J.X. Dempsey, Oxford University Press, 2017, s. XXV i nn.

[13] O tym efekcie i badaniach nad nim, szczególnie po opublikowaniu informacji przez E. Snowdena na temat szerokiego zbierania informacji przez państwo, zob. np. A. Marthews, C. Tucker, *The impact of Online Surveillance on Behavior* [w:] *Surveillance Law*, eds. D. Gray, S.E. Henderson, Cambridge University Press 2017, s. 437 i nn.

[14] Zob. M. Zubik, *„Wolność" a „prawo" (pięć hipotez o stosowaniu pojęć konstytucyjnych dotyczących praw człowieka)*, „Państwo i Prawo" 2015, z. 9, s. 3 i nn. Nauka teorii prawa niekiedy postrzega te zagadnienia w sposób bardziej złożony, opisując najczęściej poglądy poszczególnych uczonych-prawników, niż przedstawiając odpowiedzi na praktyczne problemy związane z typologią praw człowieka. Warto tu dodać, że pojawiają się też pewne specyficzne koncepcje, które np. w miejsce „praw" podmiotowych wprowadzają konstrukcję „potrzeb", zob. np. J. Waldron, *The Role of Rights in practical reasoning: „Rights" versus „Needs"*, „The Journal of Ethics" 2000, No. 4, s. 115 i nn.

[15] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483, ze zm.).

[16] Zob. np. A. Wróbel, *Prawo podmiotowe publiczne* [w:] *Instytucje prawa administracyjnego,* t. 1, Warszawa 2015, s. 325 i nn. Pozostaje otwartym pytanie, czy takie podejście służy uchwyceniu istoty problemu i naukowemu wyjaśnieniu zagadnienia, co z kolei domaga się sprowadzania zagadnienia badawczego do możliwie najbardziej prostej postaci.

do swojej istoty prywatność człowieka jest wolnością, czyli tę sferą swobodnego działania nas wszystkich tak długo, jak prawo opatrzone sankcją ze strony organów państwa nam czegoś nie nakazuje lub zakazuje i to wyłącznie w granicach określonych zasadami pomocniczości i proporcjonalności. Gdyby była „tylko" prawem, musielibyśmy wówczas odnaleźć wyraźną regulację ustawową, która pozwalałaby nam wskazać, dlaczego się domagamy, by nikt, nie tyko państwo, nie ingerował w to, gdy decydujemy o sowim życiu osobistym, z kim i jak się komunikujemy, kogo wybieramy na parterów życiowych, skąd mamy możliwość swobodnego wyboru, jakie informacje przekażemy o sobie samym innym itd. Zrozumienie tej doniosłej różnicy w kategoriach prawnych ma doniosłe konsekwencje i znaczenie praktyczne.

Władze publiczne mają obowiązek zapewnić podmiotom efektywne mechanizmy ochrony prywatności. Pamiętać jednak należy, że żadna z wolności – w tym prywatność - nie ma charakteru absolutnego. Istnieją w demokratycznym państwie prawa wartości, w tym takie jak: bezpieczeństwo, porządek i zdrowie publiczne, które mogą nakazywać pewne ograniczenia obowiązki, przełamujące ochronę płynącą z realizacji danej wolności. Niekiedy także taka interwencja ustawodawcza będzie konieczna ze względu na zapewnienie realizacji tej wolności przez inne podmioty. Wówczas władze publiczne muszą starannie dokonać wyważenia poszczególnych wolności i praw ze sobą. Najczęściej ingerencja ta będzie polegać na stworzeniu prawnych, formalnych i organizacyjnych elementów systemu prawnego, regulującego daną sferę życia społecznego, w interesującym nas zakresie – żądaniu podania, zakresu przekazywania danych osobowych, ich przetwarzania, ochrony, udostępniania, korygowania, niszczenia, czy nawet zakresu ponoszenia odpowiedzialności za naruszenie prywatności.

Władze publiczne nie mogą naruszać prywatności obywateli, zbierać niepotrzebnych mu informacji, ale też mają obowiązek chronić prywatność obywateli, także przed naruszeniem prywatności ze strony innych podmiotów prawa prywatnego, czy także zagrożeniami płynącymi spoza terytorium państwa. Również współobywatele nie mogą sobie dowolnie postępować z danymi osobowymi innych podmiotów. Chroniąc prywatność, mówimy zatem o złożoności relacji: władza jednostka, jednostka–jednostka, czy podmioty zewnątrz kraju a obywatele. W każdym jednak razie w odniesieniu do regulowania prawnych kwestii prywatności pozostają w pełni granice wyznaczone dla prawodawcy – zachowanie kryterium konieczności ingerencji w demokratycznym państwie, ze względu na uznany konstytucyjnie ważny interes publiczny, z uwzględnieniem zasad pomocniczości i proporcjonalności oraz zachowaniem zakazu naruszania istoty wolności, jaką jest prywatność i tą jej część, którą jest autonomia informacyjna jednostki (por. art. 31 ust. 3 Konstytucji).

5. Jakkolwiek obowiązująca Konstytucja nie odnosi się do występowania ludzi w wirtualnym świecie, to należy – co podkreślał Trybunał Konstytucyjny[17] – zreinterpretować obowiązujące przepisy konstytucyjne tak, by zapewnić im ochronę prawną i w tej sferze. W konsekwencji ochrona konstytucyjnych wolności i praw jednostek w związku z korzystaniem z Internetu oraz innych elektronicznych sposobów porozumiewania się na odległość nie może różnić się od ochrony dotyczącej tradycyjnych form komunikowania się czy innej aktywności. Dane przekazywane za pomocą Internetu nie mogą być wszakże postrzegane jako funkcjonujące obok czy na marginesie konstytucyjnie chronionych form aktywności człowieka. Aktywność jednostek w tej sferze odpowiada więc odpowiednim postaciom tradycyjnej aktywności od dawna chronionej konstytucyjnie. Przekazywanie korespondencji drogą elektroniczną (np. e-mail) podlega zatem takiej samej ochronie konstytucyjnej jak przekazywanie listu w tradycyjnie formie papierowej (art. 47, 49, 51). Przekazywanie informacji obrońcy za pomocą Internetu i innych środków komunikacji elektronicznej – takim samym gwarancjom jak przekazanie ich w rozmowie osobistej (art. 42). Ochrona poufności kontaktów z osobami wykonującymi zawód zaufania publicznego jest jednakowa bez względu na ich formę (art. 47). Wyrażanie poglądów, pozyskiwanie oraz rozpowszechnianie informacji drogą elektroniczną podlega w pełni ochronie przewidzianej w art. 54 Konstytucji. Podobnie ochrona wolności prasy i środków społecznego przekazu jest taka sama, bez względu na formę korzystania z tej wolności (art. 14, 54). Konstytucyjna ochrona wolności działalności gospodarczej (art. 20 i 22) obejmuje swym zakresem również podejmowanie oraz prowadzenie tej działalności w Internecie lub za pomocą innych form komunikacji elektronicznej. To samo dotyczy też ochrony wolności wyboru i wykonywania zawodu (art. 65), wolności twórczości artystycznej, badań naukowych oraz ogłaszania ich wyników, jak również wolności nauczania i wolności korzystania z dóbr kultury (art. 73) czy prawa składania petycji, wniosków i skarg do organów władzy publicznej (art. 63). Na obecnym etapie rozwoju elektronicznych form komunikowania się nie jest zatem dopuszczalne przeciwstawianie ustawowej ochrony korespondencji tradycyjnej pozostałym formom korespondencji przekazywanej za pomocą sieci telekomunikacyjnych.

Trybunał Konstytucyjny w dotychczasowym orzecznictwie – nawiązując do bogatego dorobku ETPC, a zwłaszcza orzecznictwa Federalnego Sądu Konstytucyjnego RFN – uznawał, że konstytucyjną ochroną wynikającą z art. 47, 49 i 51 ust. 1 Konstytucji są objęte wszelkie sposoby przekazywania wiadomości, w każdej formie komunikowania się, bez względu na fizyczny ich nośnik (np. rozmowy osobiste i telefoniczne, korespondencja pisemna, faks, wiadomości tekstowe i multimedialne, poczta elektroniczna). Ochrona konstytucyjna obejmuje nie tylko treść wiadomości, ale także wszystkie okoliczności procesu porozumiewania

[17] Ta część opracowania szeroko referuje ustalenia zawarte w części III uzasadnienia wyroku TK z dnia 30 lipca 2014 r., K 23/11, OTK ZU 2014, nr 7/A, poz. 80.

się, do których zaliczają się dane osobowe uczestników tego procesu, informacje o wybieranych numerach telefonów, przeglądanych stronach internetowych, dane obrazujące czas i częstotliwość połączeń czy umożliwiające lokalizację geograficzną uczestników rozmowy, wreszcie dane o numerze IP i numerze IMEI. W ramach konstytucyjnie gwarantowanej wolności człowieka i jego autonomii informacyjnej mieści się nadto ochrona przed niejawnym monitorowaniem jednostki oraz prowadzonych przez nią rozmów, nawet w miejscach publicznych i ogólnie dostępnych. Nie ma przy tym relewantnego znaczenia, czy wymiana informacji dotyczy życia prywatnego, czy prowadzonej działalności zawodowej.

6. Przepisy regulujące zatrzymywanie oraz udostępnianie przez operatorów publicznej sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych (operatorów telekomunikacyjnych) danych telekomunikacyjnych w celach związanych z zapewnieniem bezpieczeństwa i porządku publicznego zostały wprowadzone do polskiego systemu prawnego jeszcze przed uzyskaniem członkostwa w Unii Europejskiej[18]. Wraz z uchwaleniem prawa telekomunikacyjnego dokonano nowelizacji ustaw regulujących czynności operacyjno-rozpoznawcze Policji i Urzędu Ochrony Państwa będącego wówczas cywilną służbą wywiadowczą. W przepisach tych ustaw wprost przyznano funkcjonariuszom uprawnienie do dostępu do danych telekomunikacyjnych zatrzymywanych przez operatorów oraz dostawców. W ustawach nie przewidziano jednak żadnej zewnętrznej kontroli pozyskiwania danych telekomunikacyjnych. Kolejnym krokiem rozwoju prawodawstwa krajowego była nowelizacja kodeksu postępowania karnego w 2003 r.[19] Na jej podstawie przyznano sądowi i prokuratorowi uprawnienie do żądania – w toku procesu karnego – wykazu połączeń telekomunikacyjnych z uwzględnieniem czasu ich dokonania i innych informacji związanych z połączeniem niestanowiących treści rozmowy telefonicznej. Podobne uprawnienie przyznano później pozostałym służbom policyjnym i wywiadowczym, w tym nieistniejącym już obecnie: kontroli skarbowej[20] i Wojskowym Służbom Informacyjnym[21]. Organizacyjne zmiany służb policyjnych i ochrony państwa w latach 2005–2009 doprowadziły do poszerzania zakresu dostępu do danych telekomunikacyjnych zatrzymywanych przez operatorów lub dostawców usług telekomunikacyjnych.

---

[18] Ustawa z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz. U. Nr 73, poz. 852, ze zm.).

[19] Ustawa z dnia 10 stycznia 2003 r. o zmianie ustawy – Kodeks postępowania karnego, ustawy – Przepisy wprowadzające kodeks postępowania karnego, ustawy o świadku koronnym oraz ustawy o ochronie informacji niejawnych (Dz. U. Nr 17, poz. 155).

[20] Ustawa z dnia 27 czerwca 2003 r. o utworzeniu Wojewódzkich Kolegiów Skarbowych oraz o zmianie niektórych ustaw regulujących zadania i kompetencje organów oraz organizację jednostek organizacyjnych podległych ministrowi właściwemu do spraw finansów publicznych (Dz. U. Nr 137, poz. 1302).

[21] Ustawa z dnia 9 lipca 2003 r. o Wojskowych Służbach Informacyjnych (Dz. U. Nr 139, poz. 1326, ze zm.).

Dalsze modyfikacje ustawowej regulacji zatrzymywania danych telekomunikacyjnych nastąpiły wraz z uchwaleniem nowego prawa telekomunikacyjnego w 2004 r.[22] Wprowadzono wówczas ustawowy obowiązek przechowywania danych transmisyjnych dotyczących abonentów i użytkowników końcowych przez 12 miesięcy i udostępniania tychże danych na żądanie uprawnionych organów. W 2006 r. – niemalże równolegle z pracami legislacyjnymi nad dyrektywą 2006/24/WE – znowelizowano polskie prawo telekomunikacyjne[23]. Wydłużono obowiązek przetrzymywania danych do 2 lat. Istotniejsze zmiany, mające bezpośrednio na celu dostosowanie polskiego prawa do wymagań dyrektywy 2006/24/WE, zostały wprowadzone w 2009 r.[24] Uchylono dotychczas obowiązujące przepisy, wprowadzając w ich miejsce regulację zupełnie nową pod względem konstrukcji legislacyjnej. Prawo telekomunikacyjne nałożyło na operatorów publicznej sieci telekomunikacyjnej oraz dostawców publicznie dostępnych usług telekomunikacyjnych obowiązek zatrzymywania i przechowywania danych generowanych w sieci telekomunikacyjnej lub przez nich przetwarzanych na terytorium Polski przez okres 24 miesięcy, licząc od dnia połączenia bądź od nieudanej próby połączenia. Zatrzymaniu miały podlegać dane niezbędne do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego zarówno inicjującego połączenie, jak i do którego kierowane jest połączenie. Zatrzymywane miały być ponadto dane niezbędne do określenia daty i godziny połączenia oraz czasu jego trwania, rodzaju połączenia, a także lokalizacji telekomunikacyjnego urządzenia końcowego. Po upływie dwuletniego okresu dane te miały podlegać niszczeniu. Ustawodawca zobowiązał również operatorów i dostawców usług do udostępniania zatrzymanych dane uprawnionym podmiotom (funkcjonariuszom Policji, Straży Granicznej, Żandarmerii Wojskowej, kontroli skarbowej, Agencji Bezpieczeństwa Wewnętrznego, Centralnemu Biuru Antykorupcyjnemu oraz Służbie Celnej, a także sądowi i prokuratorowi). Szczegółowe zasady udostępniania tych danych określiły przepisy ustaw regulujących zadania i kompetencje poszczególnych służb. Ponadto operatorzy i dostawcy zostali zobowiązani chronić te dane przed przypadkowym lub bezprawnym zniszczeniem, utratą lub zmianą, nieuprawnionym lub bezprawnym przechowywaniem, przetwarzaniem, dostępem i ujawnieniem. W ustawach regulujących zadania i kompetencje poszczególnych służb doprecyzowano zasady dostępu funkcjonariuszy poszczególnych służ do danych telekomunikacyjnych objętych obowiązkiem ich zatrzymania. Co do zasady, dostęp odbywał się zdalnie – za pomocą specjalnego interfejsu – na żądanie upoważnionych funkcjonariuszy. Przesłanką żądania danych było, co do zasady, zapobieganie i wykrywanie

[22] Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. Nr 171, poz. 1800, ze zm.).

[23] Ustawa z dnia 29 grudnia 2005 r. o zmianie ustawy – Prawo telekomunikacyjne oraz ustawy – Kodeks postępowania cywilnego (Dz. U. Nr 12, poz. 66).

[24] Ustawa z dnia 24 kwietnia 2009 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz. U. Nr 85, poz. 716).

przestępstw lub przestępstw skarbowych, niekiedy także naruszeń prawa niebędących przestępstwami, a w wypadku cywilnych i wojskowych służb kontrwywiadowczych – realizacja ustawowych zadań m.in. zapewnienia bezpieczeństwa, przeciwdziałania terroryzmowi i szpiegostwu oraz zadań analitycznych. Od 2013 r. skrócono obowiązek retencji z 24 miesięcy do 12 miesięcy[25]. Analiza wykorzystania danych retencyjnych zawarta w informacji rocznej Prezesa Urzędu Komunikacji Elektronicznej wskazywała, że największe znaczenie i wartość mają dane pochodzące z ostatniego roku. Dlatego biorąc pod uwagę koszty ponoszone przez przedsiębiorców telekomunikacyjnych związane z dwuletnim obowiązkiem przechowywania danych, jak również sugestie płynące z raportu Komisji Europejskiej[26], uznano dwuletni obowiązek retencyjny za nieznajdujący merytorycznego uzasadnienia.

Oceniając implementację dyrektywy 2006/24/WE, należy zważyć, że polski ustawodawca implementował ją w sposób ekstensywny[27], na co zwrócił także uwagę Trybunał Konstytucyjny w wyroku z dnia 30 lipca 2014 r. (K 23/11). Po pierwsze, początkowo przewidział obowiązek przetrzymywania danych przez maksymalny okres dopuszczalny dyrektywą. Po drugie, ustawodawca upoważnił do żądania danych telekomunikacyjnych nie tylko w celu dochodzenia, wykrywania i ścigania poważnych przestępstw, jak stanowiła dyrektywa, lecz także w celu zwalczania przestępstw o stosunkowo niskim stopniu szkodliwości, a także czynów niebędących przestępstwami bądź w celu wykonywania zadań analityczno-planistycznych służb. Po trzecie, kompetencję do żądania dostępu do zatrzymanych danych telekomunikacyjnych przyznano relatywnie dużej grupie organów państwa w porównaniu z pozostałymi państwami UE. Dostęp do tych danych mają bowiem wszystkie sądy i prokuratorzy w toku postępowania karnego, a ponadto kilka służb policyjnych i ochrony państwa.

7. Przepisy regulujące zatrzymywanie danych telekomunikacyjnych, a szczególnie praktyka udostępniania zatrzymanych danych służbom, wzbudzały ożywioną dyskusję na temat skali niejawnej kontroli polskich obywateli[28]. Potęgowały ją coroczne informacje Prezesa Urzędu Komunikacji Elektronicznej sporządzane w wykonaniu art. 10 dyrektywy 2006/24/WE obrazujące liczbę zapytań o dane

---

[25] Ustawa z dnia 16 listopada 2012 r. o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw (Dz. U., poz. 1445).

[26] Opublikowanego przez Komisję Europejską w dniu 18 kwietnia 2011 r. oraz propozycjami przedstawionymi w dniu 29 września 2011 r. w „Sprawozdaniu z pracy Zespołu do spraw pozyskiwania danych telekomunikacyjnych".

[27] Zob. np. A. Adamski, *The telecommunication data retention in Poland: does the legal regulation pass the proportionality test?*, „ICT Law Review" 2013, Vol. 1; tenże, *Retencja danych o ruchu telekomunikacyjnym – polskie rozwiązania i europejskie dylematy*, „Acta Universitatis Wratislaviensis. Przegląd Prawa i Administracji" 2005, nr 70, s. 173.

[28] W tym zakresie szczególną aktywnością wykazały się helsińska Fundacja Praw Człowieka i Fundacja Panoptykon.

telekomunikacyjne[29]. Warto odnotować, że postępowanie funkcjonariuszy służb w zakresie dostępu i wykorzystania danych telekomunikacyjnych zostało, co do zasady, pozytywnie ocenione przez Najwyższą Izbę Kontroli[30].

Nic też dziwnego, że rozwiązania te stały się przedmiotem oceny ze strony Trybunału Konstytucyjnego. Pierwszy wniosek do TK kwestionujący m.in. ustawowy obowiązek zatrzymywania przez operatorów danych telekomunikacyjnych obywateli oraz ich udostępniania funkcjonariuszom Policji i Służby Ochronyppaństwa został złożony do Trybunału 28 stycznia 2011 r. Wnioskodawcą była grupa posłów. Postępowanie przez TK w tej sprawie zostało umorzone 30 listopada 2011 r. z powodów formalnych – upływu kadencji Sejmu i wygaśnięcia mandatów wnioskodawców[31].

Istotniejsze znaczenie dla rozpoznania przez Trybunał Konstytucyjny kwestii konstytucyjności polskich rozwiązań dotyczących przetrzymywania danych telekomunikacyjnych oraz udostępniania ich organom Policji oraz Służby Ochrony Państwa miało łącznie siedem wniosków pochodzących od grupy posłów, Rzecznika Praw Obywatelskich oraz Prokuratora Generalnego. Wnioski te zostały połączone do wspólnego rozpoznania pod sygn. K 23/11. Trybunał rozpoznał je w pełnym składzie.

We wnioskach zakwestionowano przepisy regulujące niejawne pozyskiwanie informacji o jednostkach przez siedem ówczesnych służb policyjnych i ochrony państwa. Zarzuty skierowano wobec przepisów regulujących kontrolę operacyjną (w tym stosowanie podsłuchu i rejestrowania rozmów oraz korespondencji elektronicznej), jak również regulacje dotyczące udostępniania danych telekomunikacyjnych.

Żaden z wnioskodawców nie kwestionował ustawowego ogólnego obowiązku przetrzymywania danych telekomunikacyjnych przez przedsiębiorców świadczących usługi telekomunikacyjne. Zarzuty wnioskodawców dotyczyły stosunkowo wąskiego problemie udostępniania służbom policyjnym i ochrony państwa przetrzymywanych danych tego rodzaju. Wnioskodawcy nie kwestionowali również możliwości żądania udostępnienia danych telekomunikacyjnych na wniosek sądu lub prokuratora. W konsekwencji to zakres zaskarżenia zdeterminował ramy wypowiedzi polskiego sądu konstytucyjnego.

Istota zarzutów odnoszących się do przepisów regulujących udostępnianie danych telekomunikacyjnych sprowadzała się do czterech zasadniczych kwestii:

---

[29] Zob. Informacja dla Komisji Europejskiej, dotyczącą udostępniania danych telekomunikacyjnych, zatrzymywanych przez przedsiębiorców telekomunikacyjnych i operatorów w roku 2013, https://archiwum.uke.gov.pl/informacja-o-rocznym-sprawozdaniu-dotyczacym-udostepniania-danych-telekomunikacyjnych-13495 [dostęp: 1.04.2018].

[30] Zob. Informacja o wynikach kontroli. Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180c i d ustawy – Prawo telekomunikacyjne, znak: KPB-P/12/191, wersja jawna, podpisana w dniu 12 czerwca 2013 r.

[31] Zob. postanowienie TK z dnia 30 listopada 2011 r., K 2/11, OTK ZU 2011, nr 9/A, poz. 108.

Po pierwsze, zaskarżone przepisy upoważniały funkcjonariuszy Policji oraz Służby Ochrony Państwa do pozyskanie danych telekomunikacyjnych w celu zapobiegania wszelkim czynom stanowiącym przestępstwo oraz ich wykrywania, bez względu na doniosłość czynu, a niekiedy nawet czynom niebędącym w świetle prawa przestępstwami. Po drugie, pozyskiwanie danych telekomunikacyjnych na podstawie zakwestionowanych przepisów nie miało charakteru subsydiarnego. Było to dopuszczalne w każdym wypadku, gdy tylko zwrócą się o to odpowiednie służby. Warunkiem uzyskania dostępu do tych danych nie było zatem wyczerpanie innych środków prawnych, mniej ingerujących w sferę prywatności oraz w tajemnicę komunikowania się. Po trzecie, ustawodawca nie przewidział obowiązku uzyskania zgody sądu ani innego niezależnego organu na pozyskanie tych danych. Po czwarte, nieuregulowanie w przepisach odnoszących się do niektórych służb ochrony państwa procedury weryfikacji i niszczenia danych zbędnych dla prowadzonego postępowania.

8. Trybunał Konstytucyjny w wyroku o sygn. K 23/11 podzielił część zarzutów wnioskodawców dotyczących przepisów o udostępnianiu danych telekomunikacyjnych.

Za niezgodne z Konstytucją uznano przepisy przyznające funkcjonariuszom Policji i Służby Ochrony Państwa kompetencje do pozyskiwania danych telekomunikacyjnych bez zapewnienia mechanizmu niezależnej kontroli udostępniania tych danych. Ponadto uznał, że narusza Konstytucję brak procedury niszczenia danych telekomunikacyjnych pozyskanych w toku realizowanych działań, niemających znaczenia dla prowadzonego postępowania.

Trybunał zwrócił uwagę na znaczenie mechanizmu kontrolnego nad służbami w demokratycznym państwie. Ponieważ pozyskiwanie danych telekomunikacyjnych dokonuje się w sposób niejawny, tj. bez wiedzy i woli podmiotów, o których informacje są gromadzone, a zarazem przy ograniczonej kontroli opinii publicznej, to brak niezależnej i zewnętrznej kontroli organów państwa nad tym procesem stwarza ryzyko nadużyć. Może to nie tylko przyczyniać się do nieuzasadnionej ingerencji w wolności i prawa człowieka, lecz także stanowić zagrożenie dla demokratycznych mechanizmów sprawowania władzy w państwie. W ocenie TK im szerszy jest zakres kompetencji do sięgania po dane telekomunikacyjne, tym bardziej restrykcyjna powinna być kontrola nad tym procesem.

Trybunał nie przesądził jednak jak ma być ukształtowana procedura dostępu do danych telekomunikacyjnych. Z uzasadnienia wyroku daje się wyprowadzić wniosek, że zakres i charakter kontroli może być zróżnicowany w zależności od rodzaju danych telekomunikacyjnych, które są pozyskiwane przez służby, a także od specyfiki działalności poszczególnych służb oraz sytuacji, w jakich pozyskiwane są te dane. Według Trybunału nie jest całkowicie wykluczone wprowadzenie kontroli następczej (*ex post*). Zgodnie z konstytucyjną zasadą sprawności działania instytucji publicznych (wstęp do Konstytucji) należy wykreować mechanizm,

który umożliwi służbom odpowiedzialnym za bezpieczeństwo państwa i porządek publiczny efektywną walkę z zagrożeniami. W niektórych wypadkach kontrola uprzednia ograniczałaby skuteczność działań operacyjnych. Trybunał dostrzegł jednakże argumenty za wprowadzeniem jako zasady kontroli uprzedniej w niektórych wypadkach. W szczególności kontrola uprzednia powinna dotyczyć pozyskiwania danych osób wykonujących zawody zaufania publicznego (adwokatów, radców prawnych, dziennikarzy itp. zobowiązanych do zachowania tajemnicy zawodowej) oraz wypadków, w których nie ma konieczności pilnego działania służb[32]. Trybunał nie uznał natomiast za bezwzględnie konieczne wprowadzenie kontroli sądowej nad pozyskiwaniem danych. Konieczne jest, by kontroli tej dokonywał organ niezależny od rządu oraz niepozostający w bezpośredniej lub pośredniej relacji zwierzchności z podmiotami pozyskującymi te dane.

Odnosząc się do zarzutu braku procedury postępowania ze zgromadzonymi i przetwarzanymi dalej danymi, Trybunał stwierdził, że konstytucyjnym warunkiem niejawnego uzyskiwania informacji o jednostkach, w tym dotyczących ich danych telekomunikacyjnych, jest ustanowienie procedury niezwłocznej selekcji oraz niszczenia materiałów zbędnych i niedopuszczalnych. Rozwiązanie to zapobiegać ma nieuprawnionemu wykorzystywaniu przez organy państwa legalnie już zebranych informacji i ich przechowywaniu na wszelki wypadek, gdyby w przyszłości okazały się przydatne do innych celów. Ingerencją w sferę prywatności jest bowiem nie tylko jednorazowe pozyskanie danych o jednostce, lecz również kolejne operacje na tych danych, w tym przechowywanie czy wtórne wykorzystywanie (przetwarzane) w toku innych postępowań.

Trybunał Konstytucyjny dopuścił – w pewnym zakresie – zróżnicowanie standardu ochrony autonomii informacyjnej obywateli polskich oraz osób niemających obywatelstwa polskiego. Przemawiać ma za tym treść art. 51 ust. 2 Konstytucji, który zakazuje władzom publicznym gromadzenia innych informacji o obywatelach niż konieczne w demokratycznym państwie oraz art. 37 ust. 2 Konstytucji uzasadniający możliwość wprowadzenia wyjątkowych ograniczeń wolności i praw konstytucyjnych w stosunku do cudzoziemców, w stosunku do pozostałych podmiotów. W szczególności powinno to dotyczyć sytuacji, w których istnieją poważne i uzasadnione podejrzenia co do ich zaangażowania w działalność zagrażającą bezpieczeństwu państwa, w tym terroryzm i przestępczość zorganizowana. Trybunał zastrzegł przy tym, że silniejsza ingerencja w autonomię informacyjną cudzoziemców nie może być traktowana jako zasada, a w każdym wypadku – nie może prowadzić do arbitralnego różnicowania podmiotów tych konstytucyjnych wolności i praw, których sam ustrojodawca nie scharakteryzował jako obywatelskich. Konstytucja nie stoi także na przeszkodzie odmiennemu określeniu przesłanek pozyskiwania danych i postępowania z nimi w stosunku

[32] Zob. jednak uwagi J. Podkowik, *Niezależna kontrola udostępniania danych telekomunikacyjnych*, „Przegląd Legislacyjny" 2015, nr 2, s. 23 i nn.

do osób niepodlegających polskiemu prawu (np. danych pozyskiwanych przez służby wywiadu o działalności obcych podmiotów za granicą), chociaż w każdym wypadku takie działania władz publicznych muszą mieścić się w ramach standardów państwa prawnego.

9. Orzeczenie Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. istotnie rozwinęło dotychczasową linię orzeczniczą sądu konstytucyjnego w zakresie ochrony wolności komunikowania się i prywatności jednostek w dobie cyfrowej[33]. Stanowiło także przykład dialogu polskiego Trybunału z pozostałymi sądami konstytucyjnymi orzekającymi o przepisach implementujących dyrektywę 2006/24/WE oraz Trybunału Sprawiedliwości UE. W wyroku obszernie nawiązano do orzeczeń sądów konstytucyjnych lub sądów najwyższych innych państw członkowskich orzekających wcześniej o przepisach krajowych implementujących dyrektywę 2006/24/WE oraz orzeczenia TSUE w sprawie *Digital Rights Ireland*. Ponadto TK przeanalizował dotychczasowe orzecznictwo ETPC dotyczące niejawnych czynności operacyjnych wobec jednostek. Stanowiły one tło rekonstrukcji standardu konstytucyjnego odnoszącego się do ochrony wolności komunikowania się i przesłanek jej ograniczenia w imię bezpieczeństwa państwa i porządku publicznego

Uwzględniając wymagania wynikające z wcześniejszego swojego orzecznictwa, a także standardy wypracowane przez ETPC i TSUE – Trybunał skonstruował swoisty test oceny regulacji upoważniających organy władzy publicznej do niejawnego pozyskiwania oraz przetwarzania informacji o osobach demokratycznym państwie prawa (pkt. III.5.3 uzasadnienia wyroku). Wymagania te są następujące:

- gromadzenie, przechowywanie oraz przetwarzanie danych dotyczących jednostek, a zwłaszcza sfery prywatności, dopuszczalne jest wyłącznie na podstawie wyraźnego i precyzyjnego przepisu ustawy[34];
- konieczne jest precyzyjne określenie w ustawie organów państwa upoważnionych do gromadzenia oraz przetwarzania danych o jednostce, w tym do stosowania czynności operacyjno-rozpoznawczych;
- w ustawie – jako akcie uchwalonym przez parlament i mogącym być podstawą ograniczeń wolności i praw jednostek – muszą zostać precyzyjnie określone przesłanki niejawnego pozyskiwania informacji o osobach, którymi są: wykrywanie i ściganie wyłącznie poważnych przestępstw oraz zapobieganie im; ustawa powinna wskazywać rodzaje takich przestępstw[35];

---

[33] Na temat niejawnego pozyskiwania informacji o osobach TK wypowiadał się dotychczas w wyrokach z dnia: 20 kwietnia 2004 r., K 45/02, OTK ZU 2004, nr 4A, poz. 30; 12 grudnia 2005 r., K 32/04; 23 czerwca 2009 r., K 54/07; a także postanowieniach z dnia 25 stycznia 2006 r., S 2/06, OTK ZU 2006, nr 1A, poz. 13; 15 listopada 2010 r., S 4/10, OTK ZU 2010, nr 9A, poz. 111.

[34] Zob. m.in. wyroki TK z dnia: 12 grudnia 2005 r., K 32/04; 23 czerwca 2009 r., K 54/07.

[35] Zob. np. postanowienie TK z dnia 15 listopada 2010 r., S 4/10; orzeczenia ETPC z dnia: 29 czerwca 2006 r. w sprawie *Weber i Saravia przeciwko Niemcom*, (wniosek nr 54934/00); 10 lutego 2009 r. w sprawie *Iordachi i inni przeciwko Mołdawii* (wniosek nr 25198/02).

- ustawa musi określać kategorie podmiotów, wobec których mogą być podejmowane czynności operacyjno-rozpoznawcze[36];
- pożądane jest określenie w ustawie rodzajów środków niejawnego pozyskiwania informacji, a także rodzajów informacji pozyskiwanych za pomocą poszczególnych środków;
- czynności operacyjno-rozpoznawcze muszą być subsydiarnym środkiem pozyskiwania informacji lub dowodów o jednostkach, gdy nie da się ich uzyskać w inny, mniej dolegliwy dla nich sposób[37];
- w ustawie należy określić maksymalny okres prowadzenia czynności operacyjno-rozpoznawczych wobec jednostek, który nie może przekraczać ram koniecznych w demokratycznym państwie prawa;
- niezbędne jest precyzyjne unormowanie w ustawie procedury zarządzenia czynności operacyjno-rozpoznawczych, obejmującej w szczególności wymóg uzyskania zgody niezależnego organu na niejawne pozyskiwanie informacji[38];
- precyzyjne określenie w ustawie zasad postępowania z materiałami zgromadzonymi w toku czynności operacyjno-rozpoznawczych, zwłaszcza zasad ich wykorzystania oraz niszczenia danych zbędnych i niedopuszczalnych[39]
- zagwarantowanie bezpieczeństwa zgromadzonych danych przed nieuprawnionym dostępem ze strony innych podmiotów;
- unormowanie procedury informowania jednostek o niejawnym pozyskaniu informacji na ich temat, w rozsądnym czasie po zakończeniu działań operacyjnych i zapewnienie na wniosek zainteresowanego poddania sądowej ocenie legalności zastosowania tych czynności; odstępstwo jest dopuszczalne wyjątkowo[40];
- zagwarantowanie transparentności stosowania czynności operacyjno-rozpoznawczych przez poszczególne organy władzy publicznej, przejawiające się w publicznej jawności i dostępności zagregowanych danych statystycznych, nadających się do porównania, o ilości i rodzaju stosowanych czynności operacyjno-rozpoznawczych;
- nie jest wykluczone zróżnicowanie intensywności ochrony prywatności, autonomii informacyjnej oraz tajemnicy komunikowania się z uwagi na to, czy dane o osobach pozyskują służby wywiadowcze i zajmujące się ochroną bezpieczeństwa państwa, czy też czynią to służby policyjne;

---

[36] Zob. wyrok TK z dnia 12 grudnia 2005 r., K 32/04; orzeczenia ETPC z dnia: 16 lutego 2000 r. w sprawie *Amann przeciwko Szwajcarii* (wniosek nr 27798/95); 10 lutego 2009 r. w sprawie *Iordachi i inni przeciwko Mołdawii* (wniosek nr 25198/02).

[37] Zob. wyroki TK z dnia: 12 grudnia 2005 r., K 32/04; 23 czerwca 2009 r., K 54/07.

[38] Zob. np. wyrok TK z dnia 12 grudnia 2005 r., K 32/04; orzeczenia ETPC z dnia: 29 czerwca 2006 r. w sprawie *Weber i Saravia przeciwko Niemcom* (wniosek nr 54934/00); 2 września 2010 r. w sprawie *Uzun przeciwko Niemcom* (wniosek nr 35623/05).

[39] Zob. np. wyrok TK z dnia 12 grudnia 2005 r., K 32/04.

[40] Zob. np. postanowienie TK z dnia 25 stycznia 2006 r., S 2/06.

- zróżnicowanie poziomu ochrony prywatności, autonomii informacyjnej oraz tajemnicy komunikowania się może także nastąpić z uwagi na to, czy niejawne pozyskiwanie informacji dotyczy obywateli, czy osób niemających polskiego obywatelstwa.

10. Trybunał Konstytucyjny, stwierdzając niekonstytucyjność przepisów o udostępnianiu danych telekomunikacyjnych służbom policyjnym i ochrony państwa, skorzystał z kompetencji do odroczenia terminu utraty mocy obowiązującej o 18 miesięcy od dnia ogłoszenia orzeczenia w Dzienniku Ustaw. Rozstrzygnięcie to było umotywowane koniecznością ograniczenia wystąpienia ryzyka braku efektywnych mechanizmów walki z zagrożeniami, a w efekcie wzrostu przestępczości bądź choćby osłabienia ich wykrywalności. W konsekwencji – pomimo orzeczonej niekonstytucyjności – ustawowa podstawa dostępu do danych telekomunikacyjnych w dalszym ciągu istniała, a przepisy te mogły być stosowane przez organy państwa aż do dnia 6 lutego 2016 r.

Mimo wyznaczenia maksymalnego osiemnstomiesięcznego terminu na dostosowanie stanu prawnego do wymagań konstytucyjnych ustawodawca nie podjął niezwłocznie działań legislacyjnych. Projekt ustawy w tym zakresie został przygotowany w Senacie i skierowany do Sejmu w dniu 24 lipca 2015 r.[41]. Zaproponowane tam rozwiązania m.in. odnoszące się do kontroli nad udostępnianiem danych telekomunikacyjnych służbom, spotkały się z krytyką opinii publicznej, ekspertów Biura Analiz Sejmowych i instytucji zewnętrznych opiniujących projekt. Do projektu wniesiono też szereg uwag i propozycji zmian merytorycznych. Z uwagi na zbliżające się zakończenie kadencji izb parlamentu i zaplanowane na październik 2015 r. wybory parlamentarne oraz biorąc pod uwagę zarzuty dotyczące niekonstytucyjności planowanych przepisów, prac ustawodawczych nie sfinalizowano w VII kadencji Sejmu.

Zmiany zostały wprowadzone dopiero ustawą z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U., poz. 147) i zaczęły obowiązywać z dniem 7 lutego 2016 r. Uchwalono je niedługo po rozpoczęciu VIII kadencji Sejmu[42]. Przyjęte rozwiązania, co do zasady, bazowały na zgłoszonym w lipcu 2015 r. projekcie senackim[43]. W ustawie z 2016 r. zawarto także inne, nieprzewidziane w projekcie Senatu z dnia 24 lipca 2015 r. oraz niewynikające z wyroku TK o sygn. K 23/11 rozwiązania, w tym prawo funkcjonariuszy służb do żądania dostępu do tzw. danych internetowych obejmujących m.in. informacje o rozpoczęciu i zakończeniu transmisji internetowej lub zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną. Ustawa ta wzbudziła duże kontrowersje w opinii publicznej. W związku z formułowanymi publicz-

[41] Sejm RP VII kadencji, druk sejmowy nr 3765.

[42] Sejm RP VIII kadencji, druk sejmowy nr 154.

[43] Szczegółową analizę projektu zawiera raport Fundacji Panoptykon, https://panoptykon.org/sites/default/files/publikacje/fp_rok_z_tzw._ustawa_inwigilacyjna_18-01-2017.pdf [dostęp: 1.04.2018].

nie poglądami, że zawarte w nim rozwiązania stanowią wykonanie wyroku TK o sygn. K 23/11, Trybunał Konstytucyjny udostępnił na swoich stronach internetowych komunikat prasowy przypominający o zakresie wymagań wynikających z orzeczenia Trybunału[44]. Komunikat prostował też liczne nieścisłości co do treści orzeczenia, jakie pojawiały się w debacie politycznej.

Przepisy ustawy z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw zostały zaskarżone przez Rzecznika Praw Obywatelskich do Trybunału Konstytucyjnego[45]. Początkowo Trybunał zapowiadał rozpoznanie sprawy w lutym 2018 r. Rozprawa została jednak przełożona, a wniosek RPO o zmianę w składzie orzekającym został odrzucony. Rzecznik wycofał swój wniosek w połowie marca 2018 r. Jako powód podał m.in., że „nie widzi jednak szansy na niezależne i merytoryczne rozpoznanie tej sprawy przez Trybunał"[46]. Niezależnie od tej sprawy czas pokaże, gdyby pojawił się nowy wniosek, pytanie prawne czy skarga konstytucyjna kwestionujące nowe rozwiązania prawne dotyczące ogólnego zatrzymywania i dostępu do danych telekomunikacyjnych w Polsce przez funkcjonariuszy Policji i Służby Ochrony Państwa, czy i ewentualnie w jakim zakresie Trybunał Konstytucyjny podtrzyma dotychczasowe ustalenia oraz w jakim zakresie skorzysta z nowego podejścia prawodawcy unijnego z dyrektywy 2016/680 w tej sferze.

11. Trudno jest jednoznacznie powiedzieć, czy współczesny, nawet dobrze wykształcony i świadomie funkcjonujący człowiek, w pełni zdaje sobie sprawę z konsekwencji i zasad funkcjonowania cyberrzeczywistości. Prywatność jest dobrem, które chcą pozyskać nie tylko władze publiczne, ale i podmioty prywatne. Co więcej, faktyczny charakter tych podmiotów niekiedy niełatwo jest rozróżnić. Problemy i zagrożenia potęguje bowiem praktyka państw, które wyzbywają się bądź przenoszą własne obowiązki na podmioty formalnie należące do sfery prawa prywatnego. Wszystkich przedstawianych tu zjawisk nie należy lekceważyć, chociażby po to, by z prawnej ochrony prywatności nie pozostała nam tylko regulacyjna atrapa.

---

[44] Zob. Komunikat Biura Trybunału Konstytucyjnego w związku z nowelizacją ustawy o Policji, http://trybunal.gov.pl/uploads/media/Komunikat_BTK_w_zwiazku_z_nowela_ustawy_o_Policji.pdf [dostęp: 1.04.2018].

[45] Wniosek RPO z dnia 18 lutego 2016 r., który zawisł pod sygnaturą K 9/16.

[46] https://www.rpo.gov.pl/pl/content/rpo-wycofuje-wniosek-do-trybuna%C5%82u-konstytucyjnego-w-sprawie-inwigilacji [dostęp: 1.04.2018]..