Jędrzej SKRZYPCZAK
Uniwersytet im. A. Mickiewicza w Poznaniu

DOI 10.14746/ps.2016.1.22

BEZPIECZEŃSTWO PAŃSTWA I DOSTĘP ORGANÓW ŚCIGANIA DO DANYCH INTERNETOWYCH A OCHRONA PRYWATNOŚCI W ORZECZNICTWIE TRYBUNAŁU KONSTYTUCYJNEGO

Przedmiotem niniejszego opracowania jest próba ukazania konfliktu pomiędzy wartościami chronionymi w demokratycznych państwach, a mianowicie z jednej strony sferą prywatności jednostki a koniecznością zapewnienia przez państwo bezpieczeństwa swoich obywateli, m.in. poprzez możliwość zapewnienia dostępu odpowiednim organom ścigania do danych internetowych. Stąd też konieczne jest poszukiwanie odpowiedniego balansu pomiędzy tymi dwoma normami chronionymi prawnie. Jako materiał badawczy posłużyło orzecznictwo Trybunału Konstytucyjnego oraz regulacje prawne Rady Europy i Unii Europejskiej.

Warto rozpocząć od podkreślenia, iż sfera prywatności jest dobrem chronionym aktami prawa międzynarodowego, europejskiego, jak i krajowego. Przywołać tu trzeba art. 12 *Powszechnej Deklaracji Praw Człowieka*[1], art. 17 *Międzynarodowego Paktu Praw Obywatelskich i Politycznych*[2] oraz art. 8 *Europejskiej Konwencji Praw Człowieka*[3] (Garlicki, 2010: 490–500; Nowicki, 1999: 330–331; Nowicki, 2005: 765–921), a także art. 7 *Karty Praw Podstawowych Unii Europejskiej*[4]. Jest to także dobro prawnie chronione normą konstytucyjną (*Konstytucja*, 1977: art. 47; Tarnacka, 2009: 276–284). Prawo do prywatności, definiowane jest jako jedno z chronionych dóbr osobistych, na które składa się wszystko to, co ze względu na uzasadnione odosobnienie się jednostki od ogółu społeczeństwa służy jej do rozwoju fizycznego i psychicznego (Sobczak, 2008: 570–576). W doktrynie życie prywatne definiowane jest jako „przy-

[1] Przepis ten stanowi, iż „Nie wolno ingerować samowolnie w czyjekolwiek życie prywatne, rodzinne, domowe, ani w jego korespondencję, ani też uwłaczać jego honorowi lub dobremu imieniu. Każdy człowiek ma prawo do ochrony prawnej przeciwko takiej ingerencji lub uwłaczaniu".

[2] Zgodnie z tym przepisem „1. Nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję ani też na bezprawne zamachy na jego cześć i dobre imię. 2. Każdy ma prawo do ochrony prawnej przed tego rodzaju ingerencjami i zamachami".

[3] W myśl tego przepisu „Każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób".

[4] Art. 7 tego dokumentu stanowi „Każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się".

mioty, wewnętrzne przeżycia osobiste (jednostkowo) człowieka i ich oceny, refleksje dotyczące wydarzeń zewnętrznych i jego wrażenia zmysłowe, a także stan zdrowia" (Banaszak, 2009: 246).

Koncepcja ochrony życia prywatnego, najczęściej ujmowana jest w doktrynie jako kategoria nadrzędna, chroniąca wiele jednostkowych dóbr osobistych. Wskazuje się zatem na następujące możliwe sytuacje naruszające tak nakreślone prawo: a) ingerencja w życie prywatne, rodzinne, domowe; b) naruszenie integralności psychofizycznej jednostki; c) naruszenie wolności przekonań lub obyczajów człowieka; d) ukazanie innej osoby w niekorzystnym dla niej świetle; e) ujawnienie krępujących lub intymnych faktów odnoszących się do życia prywatnego jednostki; f) przywłaszczenie sobie cudzego nazwiska, pseudonimu, osiągnięcia; g) nieuzasadnione niepokojenie innej osoby poprzez śledzenie, inwigilowanie, narzucanie swojego towarzystwa lub też w inny sposób; h) naruszenie korespondencji oraz rozpowszechnianie cudzego wizerunku bez zezwolenia osoby zainteresowanej; i) nadużywanie informacji uzyskanych prywatnie (ochrona wypowiedzi); j) ujawnienie informacji uzyskanej od zainteresowanego w warunkach poufności. Z punktu widzenia prezentowanej koncepcji niezwykle istotną rzeczą jest właściwe nakreślenie poszczególnych sfer życia osobistego, do których podmiot uprawniony ma prawo wyrażenia „zakazu wstępu" dla osób postronnych, w szczególności wobec dziennikarzy. Zaaprobować należy pogląd zakładający, iż wydzielić można trzy takie sfery. Po pierwsze, chodzi tu o sferę intymności obejmującą taki zakres faktów dotyczących jednostki i jej przeżyć, którymi nie dzieli się nawet z najbliższymi osobami, i których ujawnienie wywołuje uczucie wstydu i zakłopotania, a nawet udręki. Wymienić tu należy takie dobra jak: swoboda przeżyć zmysłowych dostępnych jedynie dla jego partnera, wolność przekonań i praktyk religijnych, pamięci po osobach najbliższych, cześć i honor, stosunki rodzinne w obrębie najbliższej rodziny (Sut, 1995: 49–57). Po drugie, wyróżnić można sferę prywatności, która obejmuje także sferę życia społecznego. Tradycyjnie przyjmuje się, iż w tym obszarze prawnie chronionym mieszczą się takie dobra osobiste jak życie rodzinne i sąsiedzkie, stosunki przyjacielskie i koleżeńskie. Wreszcie wymienić należy w tym katalogu sferę powszechnej dostępności. Granica pomiędzy tymi dwoma obszarami jest płynna i trudna do jednoznacznego wyznaczenia. Zaryzykować można jednak stwierdzenie, iż przebiega ona nie tam gdzie życie prywatne rozgrywa się publicznie, lecz tam, gdzie zaczyna ono dotyczyć innych osób.

Jak już wyżej sygnalizowano, ochrona prywatności gwarantowana jest w systemie prawnym Rady Europy, a mianowicie w art. 8 ust. 1 *Konwencji o ochronie praw człowieka i podstawowych wolności* z 4 listopada 1950 r. Zgodnie z tym przepisem każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. W ust. 2 tego przepisu niedopuszczalna jest ingerencja władzy publicznej w korzystanie z prawa wyrażonego w art. 8 ust. 1, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób (Garlicki, 2010: 491). Jak wielokrotnie podkreślał w swym orzecznictwie Europejski Trybunał Praw Człowieka (dalej: ETPCz) termin „życie prywatne", nie może być odnoszony wy-

łącznie do spraw ściśle osobistych i wewnętrznych człowieka, ale obejmuje również sferę działalności społecznej, rozumianej jako możność rozwijania kontaktów z innymi i interakcji ze światem zewnętrznym. Z kolei, zgodnie z wytycznymi ETPCz, termin „korespondencja" obejmuje przekazywanie informacji rozmaitymi kanałami, w tym za pomocą poczty elektronicznej czy innych kanałów transmisji danych w ramach sieci internetowej. Odnosząc się do głównego tematu niniejszego opracowania, warte zaznaczenia jest, że ETPCz dostrzegał konflikt takich wartości jak z jednej strony sfera prywatności jednostek, a z drugiej konieczność zapewnienia instrumentów pozwalających organom państwa stojących na straży bezpieczeństwa obywateli i sugerował konieczność stworzenia odpowiedniego balansu pomiędzy tymi dwoma wartościami chronionymi prawnie. Dlatego Trybunał dopuszcza możliwość pozyskiwania i retencji określonych danych przez organy państwa oraz zapewnienia odpowiednich i skutecznych środków służących zapewnieniu bezpieczeństwa państwa (Orzeczenie ETPCz, 1978; Orzeczenie ETPCz, 1990; Orzeczenie ETPCz, 2006a; Orzeczenie ETPCz, 2007a; Orzeczenie ETPCz, 2007b; Orzeczenie ETPCz, 2007c; Orzeczenie ETPCz, 2009a; Orzeczenie ETPCz, 2012c; Orzeczenie ETPCz, 2012b), zwłaszcza w przypadkach uzasadnionych walką z przestępczością oraz koniecznością zwalczania terroryzmu czy też szpiegostwa (Orzeczenie ETPCz, 1978). Każda jednak taka ingerencja w obszar chronionej prywatności, musi być należycie uzasadniona standardami dopuszczalnymi w społeczeństwach demokratycznych oraz służyć w istocie ochronie wartości, o których mowa w art. 8 ust. 2 Konwencji. ETPCz wyraźnie wskazuje, że przypadkami naruszającymi tę sferę są z pewnością wypadki stosowania środków inwigilacji (ang. *secret surveillance measures*), polegające zwykle na różnego typu postaciach podsłuchów telefonicznych, traktując takie przypadki co do zasady jako nieuprawnioną ingerencję w sferę prywatności chronionej na podstawie art. 8 Konwencji (Orzeczenie ETPCz, 1978; Orzeczenie ETPCz, 2000; Orzeczenie ETPCz, 2009a; Orzeczenie ETPCz, 2012a; Orzeczenie ETPCz, 2013). W orzecznictwie strasburskim podkreślano, że ochrona obejmuje treść różnorodnych form komunikacji, a więc nie tylko rozmowy telefoniczne, ale także pocztę, w tym elektroniczną, a nadto daty i długość rozmów, zestawienie wykonanych prób komunikacji, co stanowi tzw. integralny element komunikacji telefonicznej (ang. *integral element in the communications made by telephone*) (Orzeczenie ETPCz, 1984; Orzeczenie ETPCz, 2001b; Orzeczenie ETPCz, 2007d). Powyższe jednak nie oznacza, że krajowe regulacje nie mogą przyznawać organom państwa odpowiednich środków do monitorowania przestrzeni publicznej, w tym cyberprzestrzeni, w celu zapewnienia bezpieczeństwa państwa i obywateli. Regulacje takie muszą być jednak przewidywalne dla obywateli (Orzeczenie ETPCz, 2006a). Stąd też ETPCz wypracował określony standard regulacji w tym obszarze. Wskazywano, że po pierwsze, konieczne jest wskazanie rodzajów czynów zabronionych w przypadkach podejrzenia, o które dopuszczalne jest podejmowanie takich kroków przez organy państwa. Przy czym owe wskazanie musi być odpowiednio precyzyjne, nie wystarczy zatem posłużenie się ogólnymi zapisami, np. iż chodzi o tzw. przestępstwa poważne. Po drugie, stosowana dana technika inwigilacji musi być wyraźnie przewidziana i dopuszczona przez obowiązujące prawo w momencie jego zastosowania. Po trzecie, należy wskazać w krajowych regulacjach kategorie podmiotów, w stosunku do których mogą być pozyskiwane w sposób niejawny informacje. Należy

także określić maksymalny czas stosowania takich środków. Ponadto przyjęta w danym kraju procedura wyrażania zgody na zastosowanie środka niejawnego pozyskiwania informacji, musi mieć charakter uprzedni i pisemny, i nie może sprowadzać się jedynie do oceny zasadności stosowania takich technik tylko w aspekcie formalnym. Dodatkowo organ, który podejmuje taką decyzję musi mieć odpowiednie umocowanie prawne i umiejscowienie w strukturze organów państwa. Chodzi o to, aby był to podmiot niezależny i zewnętrzny wobec organów władzy wykonawczej (Orzeczenie ETPCz, 2007e). Następnie należy zapewnić odpowiednie procedury kontroli stosowanych środków inwigilacji. Wreszcie trzeba zagwarantować konieczność poinformowania następczego osoby podlegającej takiej kontroli oraz wskazać ewentualne wszelkie wyjątki od tej reguły.

Należy tu także wspomnieć o regulacjach prawnych Unii Europejskiej dotykających tego problemu. Otóż chodzi w szczególności o dyrektywę 2006/24/WE Parlamentu Europejskiego i Rady z 15 marca 2006 r. *w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE* (Dyrektywa 2006/24/WE). Warto tu przypomnieć, że zgodnie z art. 1 tego aktu normatywnego, celem tej regulacji było zbliżenie przepisów państw członkowskich w zakresie obowiązków dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności w zakresie zatrzymywania pewnych danych przez nie generowanych lub przetwarzanych, aby zapewnić dostępność przedmiotowych danych do celu dochodzenia, wykrywania i ścigania poważnych przestępstw, określonych w ustawodawstwie każdego państwa członkowskiego. Jak wyjaśniono w ust. 2 tego przepisu postanowienia, zamieszczone w tym dokumencie stosuje się do danych o ruchu i lokalizacji, dotyczących zarówno osób fizycznych, jak i prawnych, oraz do powiązanych z nimi danych niezbędnych do identyfikacji abonenta lub zarejestrowanego użytkownika, natomiast nie odnoszą się one do samej treści komunikatów elektronicznych, w tym informacji uzyskiwanych przy użyciu sieci łączności elektronicznej. W myśl postanowień artykułu 4 tej dyrektywy państwa członkowskie zobowiązały się zagwarantować, że dane zatrzymywane w myśl niniejszej dyrektywy były udostępniane jedynie właściwym organom krajowym, w szczególnych przypadkach i zgodnie z krajowym ustawodawstwem. Proces oraz warunki uzyskiwania dostępu do zatrzymanych danych, w przypadkach gdy został spełniony wymóg konieczności oraz proporcjonalności, powinny być określone w prawie krajowym każdego państwa członkowskiego, podlegając odpowiednim przepisom prawa Unii Europejskiej lub międzynarodowego prawa publicznego, w szczególności EKOPC, zgodnie z interpretacją Europejskiego Trybunału Praw Człowieka. W art. 5 wymieniono katalog danych podlegających ewentualnej retencji. Dyrektywa stanowi nadto, że okres retencji takich danych będzie trwać nie krócej niż 6 miesięcy oraz nie dłużej niż dwa lata od daty połączenia. Dyrektywa nakłada nadto na państwa członkowskie obowiązek powołania organów sprawujących odpowiedni nadzór nad takimi praktykami. Co jednak istotne, Trybunał Sprawiedliwości UE w wyroku z 8 kwietnia 2014 r. w połączonych sprawach High Court of Ireland i Verfassungsgerichtshof z Austrii (sygn. C-293/12), stwierdził o nieważności całej dyrektywy z uwagi na naruszenie praw podstawowych zagwarantowanych w art. 7 (prawo

do ochrony życia prywatnego) i art. 8 (prawo do ochrony danych osobowych) *Karty praw podstawowych Unii Europejskiej* (*Karta*, 2007).

Na gruncie polskiego porządku prawnego, na szczególną uwagę zasługuje stanowisko wyrażone w wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. (*Wyrok TK*, 2014). Przesądzono tu o niezgodności z Konstytucją Rzeczypospolitej Polskiej, wybranych, zaskarżonych przepisów wielu aktów normatywnych dających podstawy wykonywania przez organy ścigania kontroli operacyjnej[5]. W uzasadnieniu wyroku Trybunał przedstawił bardzo wnikliwe spostrzeżenia na opisywany problem. Taka decyzja wypływała w przekonania, że ustrojodawca stoi na stanowisku zapewnienia możliwie jak najszerszej prawnej ochrony wolności człowieka, będącej naturalnym atrybutem prawnego statusu jednostki, co wywodzi się z treści normy z art. 31 ust. 1 Konstytucji. Przypomnijmy, że zgodnie z tym przepisem wolność człowieka podlega ochronie prawnej. W ust. 2 tego przepisu stanowi się, iż każdy jest obowiązany szanować wolności i prawa innych i nikogo nie wolno zmuszać do czynienia tego, czego prawo mu nie nakazuje. Jednocześnie w ust. 3 tego przepisu postanowiono, iż ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla zapewnienia jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Co jednak ważne, ograniczenia takie nie mogą jednak naruszać istoty wolności i praw jednostek. Jak podkreślał wielokrotnie w swym orzecznictwie TK, wolność człowieka chroniona jest zarówno w jej aspekcie pozytywnym, jak i negatywnym. Trybunał zdefiniował przy tym, że „aspekt pozytywny wolności polega na tym, że jednostka może swobodnie kształtować swoje zachowania w danej sferze, wybierając takie formy aktywności, które jej samej najbardziej odpowiadają, lub powstrzymywać się od podejmowania jakiejkolwiek działalności. Aspekt negatywny [...] polega na prawnym obowiązku powstrzymania się – kogokolwiek – od ingerencji w sferę zastrzeżoną dla jednostki. Obowiązek taki ciąży na państwie i na innych podmiotach – nie wyłączając samorządów zawodowych zawodów zaufania publicznego. Odstąpienie od respektowania «aspektu negatywnego» wolności konstytucyjnych jest możliwe tylko na zasadach, w zakresie i w formie przewidzianej w art. 31 ust. 3 Konstytucji, ze względu na wymienione tam – enumeratywnie – wartości i przy spełnieniu wymogu proporcjonalności ograniczeń" (*Wyrok TK*, 2004; *Wyrok TK*, 2014).

Jak już wyżej sygnalizowano, zgodnie z art. 47 ustawy zasadniczej, gwarantuje się ochronę prawną życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Trzeba też tu wspomnieć o art. 51 ust. 1 Konstytucji,

---

[5] Chodzi o wybrane przepisy: ustawy z 6 kwietnia 1990 r. *o Policji* (Dz. U. 2015, poz. 355 z późn. zm.), ustawy z 12 października 1990 r. *o Straży Granicznej* (Dz. U. 2014, poz. 1402 z późn. zm.), ustawy z 28 września 1991 r. *o kontroli skarbowej* (Dz. U. 2015, poz. 553 z późn. zm.), ustawy z 24 sierpnia 2001 r. *o Żandarmerii Wojskowej i wojskowych organach porządkowych* (Dz. U. 2013, poz. 568 z późn. zm.), ustawy z 24 maja 2002 r. *o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz. U. 2015, poz. 1929 z późn. zm.), ustawy z 9 czerwca 2006 r. *o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (Dz. U. 2014, poz. 253 z późn. zm.), ustawy z 9 czerwca 2006 r. *o Centralnym Biurze Antykorupcyjnym* (Dz. U. 2014, poz. 1411 z późn. zm.) oraz ustawy z 27 sierpnia 2009 r. *o Służbie Celnej* (Dz. U. 2015, poz. 990 z późn. zm.).

stojącym na straży tzw. autonomii informacyjnej. W myśl postanowień tego ostatniego przepisu, nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. Z kolei ust. 2 tego przepisu stanowi, iż władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. Trybunał w komentowanym wyroku zaznaczył przy tym, iż ochrona prywatności i autonomii informacyjnej, jest konsekwencją ochrony przyrodzonej i niezbywalnej godności człowieka, co z kolei gwarantowane jest art. 30 Konstytucji. Stąd też TK sformułował pogląd, iż „zachowanie przez człowieka godności wymaga poszanowania jego czysto osobistej sfery, w której nie jest narażony na konieczność 'bycia z innymi' czy 'dzielenia się z innymi swoimi przeżyciami czy doznaniami' " (*Wyrok TK*, 2005; *Wyrok TK*, 2009; *Wyrok TK*, 2014). Zgodzić należy się nadto z tezą, że art. 47 i art. 51 Konstytucji chronią tę samą wartość konstytucyjną, a mianowicie sferę prywatności, bowiem tzw. autonomia informacyjna jest istotnym elementem prawa do prywatności. Jak zdefiniował TK, autonomia informacyjna „polega na samodzielnym decydowaniu o ujawnianiu innym podmiotom informacji dotyczących własnej osoby, a także na sprawowaniu kontroli nad tymi informacjami, nawet jeśli znajdują się w posiadaniu innych osób" (*Wyrok TK*, 2002; *Wyrok TK*, 2002a; *Wyrok TK*, 2011). Dodatkowo TK zauważył, iż z ochroną prywatności i autonomii informacyjnej współgra prawo do ochrony tajemnicy komunikowania się gwarantowane w art. 49 ustawy zasadniczej. Przypomnieć należy, że zgodnie z tym przepisem gwarantuje się wolność i ochronę tajemnicy komunikowania się. Przepis ten stanowi jednocześnie, że ograniczenia w tym obszarze mogą nastąpić jedynie w przypadkach określonych w akcie rangi ustawowej. Podkreśla się przy tym, iż w tym przypadku chodzi o wolność komunikowania za pomocą wszelkich środków przekazu (Sarnecki, 2007: 3). Warto odnotować także pogląd TK wyrażony w wyroku z 20 czerwca 2005 r. (sygn. K 4/04), iż „przejawem prawa do prywatności jest również wolność komunikowania się, która obejmuje nie tylko tajemnicę korespondencji, ale i wszelkiego rodzaju kontakty międzyosobowe" (*Wyrok TK*, 2005; *Wyrok TK*, 2014). Zważywszy na powyższe TK stwierdził, iż „konstytucyjną ochroną wynikającą z art. 47, art. 49 i art. 51 ust. 1 Konstytucji objęte są 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 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 czy 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 znaczenia, czy wymiana informacji dotyczy życia ściśle prywatnego, czy też prowadzonej działalności zawodowej, w tym działalności gospodarczej. Nie ma bowiem takiej sfery życia osobistego człowieka, co do której konstytucyjna ochrona byłaby wyłączona bądź samoistnie ograniczona. W każdej z tych sfer jednostka ma więc konstytucyjnie gwarantowaną

wolność przekazywania i pozyskiwania informacji, w tym „udostępniania informacji o sobie samej" (*Wyrok TK*, 2014). Dodatkowo Trybunał Konstytucyjny zwrócił uwagę, że powyższe reguły można i należy odnosić do cyberprzestrzeni, mimo, że w ustawie zasadniczej ustrojodawca nie odnosi się wprost do tej sfery. Dostrzeżono, że internet jest jedynie kanałem informacyjnym, w którym spotyka się różne techniki i technologie porozumiewania się na odległość, część z nich jest podobna do tych postaci znanych ze świata analogowego (np. e-mail należy traktować identycznie jak korespondencję pocztową, a VOIP, ang. *voice over internet protocol*, jak zwykłe rozmowy telefoniczne). Stąd też TK podkreślił, iż „Internet powinien być postrzegany tym samym jako jedno z narzędzi umożliwiających korzystanie z wolności i praw podmiotowych, a nie jako sfera odrębna czy wymykająca się konstytucyjnej ochronie. W tym stanie rzeczy ocena przepisów umożliwiających ingerencję w wolności i prawa podmiotowe, odnoszące się do korzystania przez jednostki m.in. z Internetu, powinna być przeprowadzana z uwzględnieniem treści normatywnej właściwych w danym wypadku przepisów Konstytucji gwarantujących ochronę praw podstawowych" (*Wyrok TK*, 2014).

Jednocześnie TK dostrzegł zagrożenia wynikające z wykorzystywania nowych technologii komunikacyjnych, które stały się przecież narzędziem do popełniania groźnych przestępstw, w tym działań o charakterze terrorystycznym. Stąd też Trybunał zgodził się, iż istnieje konieczność zapewnienia służbom policyjnym i ochrony państwa szczególnych uprawnień do monitorowania tej przestrzeni wirtualnej, celem możliwości zapobiegania i wykrywania przestępstw. Jest to o tyle ważne, że istota sieci światowej, jaką jest *World Wide Web*, rodzi dodatkowe zagrożenia, zwłaszcza w sferze egzekucji prawa poza lub ponad granicami kraju. Podkreślono wręcz, że pozbawienie służb policyjnych możliwości monitorowania tej sfery działalności społeczeństwa, mogłoby być traktowane jako zaniechanie wywiązywania się państwa z jego konstytucyjnego obowiązku, o którym mowa w art. 5 ustawy zasadniczej, a mianowicie strzeżenia niepodległości i nienaruszalności terytorium Rzeczypospolitej Polskiej, a także zapewnienia bezpieczeństwa obywateli. Nadto takie zaniechania ze strony państwa mogłyby prowadzić do naruszeń prawa międzynarodowego i zobowiązań państwa w zakresie zwalczania przestępczości. Podnosi się jeszcze jeden argument przemawiający za koniecznością ingerencji państwa w taki obszar prywatności. Rezygnacja z takich uprawnień po stronie organów państwa, mogłaby wręcz podważać zasadę sprawności działania instytucji publicznych, o której mowa we wstępie do Konstytucji. Trybunał dostrzegł również okoliczność, iż zagwarantowanie odpowiednim służbom pozyskiwania określonych informacji o działaniach określonych osób, ingerujące w ich sferę prywatności ma jeszcze jeden istotny wymiar. Otóż w istocie jest to realizowanie przez państwo powinności zapewnienia wolności pozostałych obywateli. Arsenał środków jest w tym zakresie bogaty, ale w szczególności chodzi o czynności operacyjno-rozpoznawcze, na które składają się m.in. kontrola operacyjna komunikowania także przy użyciu sieci internetowych oraz gromadzenie i przetwarzanie danych telekomunikacyjnych. Jak widać takie możliwości mogą ingerować w sferę prywatności niezwykle dotkliwie. Dają one możliwości nieustannego wręcz inwigilowania jednostek, bez możliwości dowiedzenia się o takich działaniach przez obywateli. Formułując taką konkluzję TK odwołał się do stanowiska wyrażonego w wyroku Trybunału Sprawiedliwości UE z 8 kwietnia 2014 r., sygn. C-293/12, pkt 27 (*Wyrok TSUE*,

2014), iż wyżej wskazane dane nie pozwalają jeszcze same w sobie odtworzyć całej aktywności jednostki, to jednak po odpowiednim zestawieniu, istnieje możliwość rekonstrukcji całego profilu osobowego, łącznie z ustaleniem wszelkiego zaangażowania np. o charakterze politycznym, społecznym. Trzeba też uwzględniać okoliczność, że zdarzały się przypadki ujawnienia danych gromadzonych w takich rejestrach, poprzez złamanie zabezpieczeń technicznych, co też z pewnością stanowi pogwałcenie sfery prywatności. Trzeba oczywiście uwzględniać także okoliczność, że nowe technologie są niekiedy źródłem i narzędziem popełniania czynów zabronionych, czyli tzw. cyberprzestępczości. Udostępnienie służbom policyjnym stosownych możliwości rodzi kolizję z prawem do ochrony prywatności, tajemnicy komunikowania się, autonomii informacyjnej (*Wyrok TK*, 2014).

Dlatego w ocenie TK konieczne jest stworzenie odpowiedniego, zróżnicowanego podejścia do takich możliwości, przy uwzględnieniu zasady proporcjonalności i znalezienie „złotego środka" pomiędzy, z jednej strony, koniecznością zagwarantowania konstytucyjnie chronionych praw i wolności jednostki a możliwościami wyposażenia służb państwowych w uprawnienia, które mają zapobiegać przestępczości, a więc działaniom członków społeczeństwa, którzy naruszają w sposób niezgodny z prawem wolności innych obywateli. Stąd też TK sformułował dyrektywę o konieczności uwzględnienia zasady proporcjonalności w zakresie dostępu do takich danych. W komentowanym wyroku sprecyzowano warunki ustawowej regulacji tej sfery. I tak po pierwsze, ustawa musi dostatecznie precyzować przesłanki dopuszczalności takich działań (w zakresie gromadzenie, przechowywanie oraz przetwarzanie danych dotyczących jednostek) po stronie państwa. Po drugie, konieczne jest wyraźne określenie sposobów i form niejawnej ingerencji w sferę prywatności, które tworzą zamknięty katalog organów państwa upoważnionych do dostępu do takich danych. Jak podkreślił TK ustawa musi precyzować dokładnie przesłanki niejawnego pozyskiwania informacji o osobach (precyzując kategorie podmiotów, wobec których mogą być podejmowane takie czynności), do których można zaliczyć konieczność wykrywania i ściganie wyłącznie poważnych przestępstw (wskazując precyzyjnie o jakie kategorie przestępstw chodzi), ewentualnie podejmowanie próby zapobiegania im. Pożądane jest także stworzenie w ustawie enumeratywnego wyliczenia rodzajów środków niejawnego pozyskiwania informacji, a także możliwych typów informacji pozyskiwanych za pomocą poszczególnych środków. Przy czym czynności operacyjno-rozpoznawcze należy zawsze traktować wyłącznie jako subsydiarny środek i to tylko wtedy, gdy nie ma możliwości ich uzyskania w inny, mniej dolegliwy dla nich sposób. Trzecim warunkiem jest wskazanie maksymalnych ram czasowych stosowania takich środków (przy czym nie mogą one przekraczać ram koniecznych w demokratycznym państwie prawa). Po czwarte, konieczne jest wskazanie aktem rangi ustawowej odpowiedniej procedury zarządzania takich czynności. Jak podkreślił TK: „niezbędne jest precyzyjne unormowanie w ustawie procedury zarządzenia czynności operacyjno-rozpoznawczych, obejmującej w szczególności wymóg uzyskania zgody niezależnego organu na niejawne pozyskiwanie informacji. Precyzyjne określenie w ustawie zasad postępowania z materiałami zgromadzonymi w toku czynności operacyjno-rozpoznawczych, zwłaszcza zasad ich wykorzystania oraz niszczenia danych zbędnych i niedopuszczalnych, zagwarantowanie bezpieczeństwa zgromadzonych danych przed nieuprawnionym dostę-

pem 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" (*Wyrok TK*, 2014). Kolejnym warunkiem możliwości stosowania tego typu technik inwigilacji wskazanym przez TK, jest konieczność uregulowania zakresu wykorzystania pozyskiwanych w taki sposób danych. Trybunał zauważył, że należy wymagać od ustawodawcy „zagwarantowania 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. 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" (*Wyrok TK*, 2014).

Ustawa z 15 stycznia 2016 r. *o zmianie ustawy o Policji oraz niektórych innych ustaw* miała w intencji projektodawców stanowić wypełnienie dyrektyw Trybunału Konstytucyjnego. Przedmiot tej regulacji zasługuje z pewnością na odrębne opracowanie. Warto tylko zaznaczyć, że wobec tej regulacji zgłaszano poważne zastrzeżenia co do jej zgodności z Konstytucją. W tym gronie należy wymienić opinię Rzecznika Praw Obywatelskich (*Opinia RPO*, 2015), a także Komisji Weneckiej z czerwca 2016 r.

BIBLIOGRAFIA

Banaszak B. (2009), *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa.

Bodzian A. (2006), *Tajemnica przedsiębiorstwa a dostęp do informacji o działalności przedsiębiorców*, w: *Prawo do informacji*, (red.) W. Góralczyk jun., Warszawa.

Dyrektywa Parlamentu Europejskiego i Rady nr 2003/98/WE z 17 listopada 2003 r. *w sprawie ponownego wykorzystywania informacji sektora publicznego*, Dz. U. UE L 345 z 31.12.2003.

Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z 15 marca 2006 r. *w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE*, Dz. U. UE L 105 z 15.03.2006.

Jabłoński M., Wygoda K. (2002), *Dostęp do informacji i jego granice*, Wrocław.

Jaskowska M. (2002), *Dostęp do informacji publicznej w świetle orzecznictwa Naczelnego Sądu Administracyjnego*, Toruń.

Kamińska I., Rozbicka-Ostrowska M. (2007), *Dostęp do informacji publicznej. Orzecznictwo sądów administracyjnych*, Warszawa.

Karta praw podstawowych Unii Europejskiej (2007), Dz. U. UE C 303 z 14.12.2007.

Konstytucja III RP w tezach orzeczniczych Trybunału Konstytucyjnego i wybranych sądów (2008), Warszawa.

Konstytucja Rzeczypospolitej Polskiej z 2 kwietnia 1997 (1997), Dz. U. 1997, Nr 78, poz. 483 z późn. zm.

Konwencja o ochronie praw człowieka i podstawowych wolności (2010), t. I, *Komentarz*, (red.) L. Garlicki, Warszawa.

Konwencja o ochronie praw człowieka i podstawowych wolności (1950), Dz. U. 1993, Nr 61, poz. 284.

Kopff A. (1982), *Ochrona sfery życia prywatnego jednostki w świetle doktryny i orzecznictwa*, „ZNUJ Prace Prawnicze", z. 100.

Kopff A. (1972), *Koncepcja praw do intymności i prywatności życia osobistego (zagadnienia konstrukcyjne)*, „Studia Cywilistyczne", t. XX.

Kordasiewicz B. (1991), *Jednostka wobec środków masowego przekazu*, Wrocław–Warszawa–Kraków.

Kubiński K. W. (1993), *Ochrona życia prywatnego człowieka*, „RPSiE", z. 1.

Mednis A. (2006), *Prawo do prywatności a interes publiczny*, Kraków.

Międzynarodowy Pakt Praw Obywatelskich i Politycznych z 19 grudnia 1966 (1966), Dz. U. 1977, Nr 38, poz. 167.

Nowicki M. A. (1999), *Europejska Konwencja Praw Człowieka. Wybór orzecznictwa*, wyd. 2, Warszawa.

Nowicki M. A. (2005), *Nowy Europejski Trybunał Praw Człowieka. Wybór orzeczeń 1999–2004*, Kraków.

Obywatelskie prawo do informacji (2008), (red.) T. Gardocka, Warszawa.

Opinia RPO Rzecznika Praw Obywatelskich z 28 grudnia 2015 (2015), https://www.rpo.gov.pl/sites/default/files/Do_Marszalka_Sejmu.pdf (20.06.2016).

Orzeczenie ETPCz z 6 września 1978 r. w sprawie Klass i inni przeciwko Niemcom (1978), skarga nr 5029/71.

Orzeczenie ETPCz z 2 sierpnia 1984 r. w sprawie Malone przeciwko Wielkiej Brytanii (1984), skarga nr 8691/79.

Orzeczenie ETPCz z 24 kwietnia 1990 r. w sprawie Kruslin przeciwko Francji (1990), skarga nr 11801/85.

Orzeczenie ETPCz z 16 lutego 2000 r. w sprawie Amann przeciwko Szwajcarii (2000), skarga nr 27798/95.

Orzeczenie ETPCz z 1 marca 2007 r. w sprawie Heglas przeciwko Czechom (2001a), skarga nr 17362/03.

Orzeczenie ETPCz z 25 września 2001 r. w sprawie P. G. i J. H. przeciwko Wielkiej Brytanii (2001b), skarga nr 44787/98.

Orzeczenie ETPCz z 29 czerwca 2006 r. w sprawie Weber i Saravia przeciwko Niemcom (2006a), skarga nr 54934/00.

Orzeczenie ETPCz z 28 czerwca 2007 r. w sprawie Association for European Integration and Human Rights and Ekimdzhiev przeciwko Bułgarii (2007a), skarga nr 62540/00.

Orzeczenie ETPCz z 3 kwietnia 2007 r. w sprawie Copland przeciwko Wielkiej Brytanii (2007b), skarga nr 62617/00.

Orzeczenie ETPCz z 1 lipca 2007 r. w sprawie Liberty i inni przeciwko Wielkiej Brytanii (2007c), skarga nr 58243/00.

Orzeczenie ETPCz z 3 kwietnia 2007 r. w sprawie Copland przeciwko Wielkiej Brytanii (2007d), skarga nr 62617/00.

Orzeczenie ETPCz z 26 kwietnia 2007 r. w sprawie Dumitru Popescu przeciwko Rumunii (2007e), skarga nr 71525/01.

Orzeczenie ETPCz z 10 lutego 2009 r. w sprawie Iordachi i inni przeciwko Mołdawii (2009a), skarga nr 25198/02.

Orzeczenie ETPCz z 27 października 2012 r. w sprawie Savovi przeciwko Bułgarii (2012a), skarga nr 7222/05.

Orzeczenie ETPCz z 4 grudnia 2012 r. w sprawie Lenev przeciwko Bułgarii (2012b), skarga nr 41452/07.

Orzeczenie ETPCz z 23 października 2012 r. w sprawie Hadzhiev przeciwko Bułgarii (2012c), skarga nr 22373/04.

Orzeczenie ETPCz z 25 czerwca 2013 r. w sprawie Valentino Acatrinei przeciwko Rumunii (2013), skarga nr 18540/04.

Sarnecki P. (2007), *Uwaga 3 do art. 49*, w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz do art. 49, teza 3*, (red.) L. Garlicki, t. III, Warszawa.

Sobczak J. (2008), *Prawo prasowe. Komentarz*, Warszawa.

Sut P. (1995), *Czy sfera intymności jest dobrem osobistym chronionym w prawie polskim?*, „Palestra", nr 7–8.

Tarnacka K. (2009), *Prawo do informacji w polskim prawie konstytucyjnym*, (red.) M. Zubik, Warszawa.

Ustawa z 15 stycznia 2016 r. *o zmianie ustawy o Policji oraz niektórych innych ustaw*, Dz. U. 2016, poz. 147.

Wyrok TK z 20 czerwca 2005 (2005), sygn. K 4/04, OTK ZU nr 6/A/2005, poz. 64.

Wyrok TK z 18 lutego 2004 (2004), sygn. P 21/02, OTK ZU nr 2/A/2004, poz. 9.

Wyrok TK z 19 lutego 2002 (2002), sygn. U 3/01, OTK ZU nr 1/A/2002, poz. 3.

Wyrok TK z 23 czerwca 2009 (2009), sygn. K 54/07, OTK ZU nr 6/A/2009, poz. 86.

Wyrok TK z 20 listopada 2002 (2002a), sygn. K 41/02, OTK ZU nr 6/A/2002, poz. 83.

Wyrok TK z 13 grudnia 2011 (2011), sygn. K 33/08, OTK ZU nr 10/A/2011, poz. 116.

Wyrok TK z 12 grudnia 2005 (2005), sygn. K 32/04, OTK ZU nr 11/A/2005, poz. 132.

Wyrok TK z 6 sierpnia 2014 (2014), Dz. U. 2014, poz. 1055, uzasadnienie: http://otkzu.trybunal.gov.pl/2014/7A/80 (20.06.2016).

Wyrok TSUE Trybunału Sprawiedliwości UE z 8 kwietnia 2014 (2014), sygn. C-293/12.

Zaremba M. (2009), *Prawo dostępu do informacji publicznej. Zagadnienia praktyczne*, Warszawa.

STRESZCZENIE

Przedmiotem niniejszego opracowania jest próba ukazania konfliktu pomiędzy wartościami chronionymi w demokratycznych państwach, a mianowicie z jednej strony sferą prywatności jednostki a koniecznością zapewnienia przez państwo bezpieczeństwa swoich obywateli, m.in. poprzez możliwość zapewnienia dostępu odpowiednim organom ściągania do danych internetowych. Stąd też konieczne jest poszukiwanie odpowiedniego balansu pomiędzy tymi dwoma normami chronionymi prawnie. Jako materiał badawczy posłużyło orzecznictwo Trybunału Konstytucyjnego oraz regulacje prawne Rady Europy i Unii Europejskiej.

Słowa kluczowe: prawo do prywatności, dostęp organów ścigania do danych internetowych

NATIONAL SECURITY AND SECRET SURVEILLANCE MEASURES IN THE CONTEXT OF THE RIGHTS TO PROTECT PRIVACY IN THE JUDICATURES OF THE CONSTITUTIONAL COURT IN POLAND

ABSTRACT

This paper shows the conflict between two values protected in every democratic country by constitutional law. On the one hand, the right to privacy and on the other hand the competencies of the State to ensure the security of its citizens eg. by using secret surveillance measures. Therefore, it is necessary to seek an appropriate balance between these two standards protected by law based on selected judicatures of the Constitutional Tribunal in Poland, and the regulations of the Council of Europe and the European Union.

Key words: the right to privacy, law enforcement, access to Internet data, the security of the State