Rozdział I. Dane telekomunikacyjne jako środek inwigilacji masowej w demokratycznym państwie prawa

Andrzej Adamski

„Fakt, że coś można robić, nie oznacza, że należy to robić. Ściganie przestępców mogło by być jeszcze bardziej efektywne niż w chwili obecnej, gdyby odciski linii papilarnych i próbki DNA pobierano od wszystkich obywateli" *Ian J. Loyd*

Wprowadzenie

Żyjemy w czasach fenomenalnego rozwoju technologii cyfrowych, które zwiększają komfort naszej egzystencji, lecz stanowią również zagrożenie dla praw podstawowych człowieka. Źródła tego zagrożenia są różnorodne i nie ograniczają się do cyberprzestępców wyspecjalizowanych w „kradzieży" cudzej tożsamości, czy firm internetowych zajmujących się profilowaniem konsumentów. Oprócz aktów bezprawia kryminalnego, obejmują także legalne działania organów państwowych powołanych do ochrony porządku i bezpieczeństwa publicznego, które zgodnie z prawem wykorzystują potencjał technologii informacyjno-komunikacyjnych (ICT) do swoich potrzeb. Sposób, w jaki funkcjonariusze aparatu kontroli społecznej i bezpieczeństwa państwa używają nowych technologii do gromadzenia i przetwarzania danych o obywatelach, budzi w wielu krajach zaniepokojenie opinii publicznej i jest kontestowany. Protestom pozarządowych organizacji obrońców praw i wolności obywatelskich przeciwko inwigilacji towarzyszą skargi rzeczników praw obywatelskich, parlamentarzystów i zwykłych obywateli kierowane do sądów krajowych i trybunałów międzynarodowych, w których kwestionuje się praworządność działań organów państwowych lub

zakres posiadanych przez nie uprawnień. Nie chodzi przy tym wyłącznie o sytuacje związane z gromadzeniem i wykorzystywaniem informacji przedstawiających wartość dowodową z punktu widzenia organów dochodzeniowo-śledczych, uprawnionych do wkraczania w sferę praw i wolności osób podejrzewanych o popełnienie przestępstw. Znacznie poważniejsze problemy prawne i polityczne wiążą się z wykorzystaniem najnowszych zdobyczy ICT do działań prewencyjnych, podejmowanych przez służby wywiadu (*intelligence service*) niektórych państw w ramach realizowanej tam proaktywnej strategii walki z terroryzmem i przestępczością zorganizowaną. Jak stwierdza jeden z dokumentów roboczych LIBE: „postęp techniczny jest jednym z czynników mających wpływ na zasadniczą zmianę modelu działania i praktyk służb specjalnych, które odeszły od tradycyjnej koncepcji ukierunkowanego nadzoru, stanowiącego konieczny i proporcjonalny środek zwalczania terroryzmu, i skierowały się ku systemom nadzoru prowadzonego na skalę masową”[1].

Model ten opiera się na założeniu, że ochrona bezpieczeństwa wewnętrznego, w szczególności przed terroryzmem, nie jest możliwa bez ingerencji w prawa człowieka i polega na inwigilacji nie tylko aktualnych lub potencjalnych przestępców (terrorystów), lecz także niewinnych obywateli, czyli osób, które nie są zaangażowane w działalność przestępczą lub kontakty z organizacjami terrorystycznymi. Szczegółowe implikacje tego założenia w przypadku działań prewencyjnych służb specjalnych mających na celu identyfikację na podstawie „profilu terrorysty” osób odpowiadających temu profilowi w populacji generalnej ilustrować może następujący przykład zaczerpnięty z literatury. Zakładając, że chodzi o profil terrorysty przebywającego w Holandii (16 mln mieszkańców), pochodzącego spoza Europy Zachodniej (1,7 mln mieszkańców), będącego wyznawcą Islamu (850 tys. mieszkańców) i należącego do drugiego pokolenia imigrantów (147 tys. mieszkańców), przyjmuje się, że jeden procent osób odpowiadających temu profilowi stanowią ekstremiści. Jeśli spośród tej grupy kolejne 10% osób może stanowić poważne zagrożenie dla reszty społeczeństwa, to na podstawie opracowanego profilu i przyjętych założeń 147 osób należy poddać inwigilacji. W praktyce oznacza to, że większość z nich, faktycznie bez powodu, zostanie pozbawiona części prywatności[2]. Problem inwigilacji masowej nie sprowadza się jednak tylko do „profilowania” w celu wyodrębnienia z populacji generalnej stosunkowo niewielkiej „grupy ryzyka”, którą poddaje się następnie konwencjonal-

[1] Dokument Roboczy Nr 1 w sprawie amerykańskich i unijnych programów nadzoru oraz ich wpływu na podstawowe prawa obywateli UE. Parlament Europejski, Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych, Sprawozdawca: *Claude Moraes*, 11.12.2013 r. (DT\1012434PL.doc), s. 2.

[2] *R. O'Harrow Jr.*, No Place to Hide, s. 139, cyt. za *B. van Loenen et al.*, Locating mobile devices, s. 87.

nym metodom obserwacji niejawnej. Obserwacją niejawną można dziś objąć większość mieszkańców danego kraju, nie informując ich o tym, że byli obiektem zainteresowania służb specjalnych.

Jeszcze w latach 70. XX w. możliwość inwigilowania populacji generalnej danego kraju w celu zapewnienia bezpieczeństwa jego mieszkańcom i ochrony struktur gospodarczych i państwowych przed zamachami terrorystycznymi stanowiła wizję literacką z gatunku *political fiction*. Rozwój technologii informacyjnych spowodował, że wizja ta stała się rzeczywistością przekraczającą wyobrażenia przeciętnego człowieka. W latach 90. XX w. tajny system globalnego podsłuchu telekomunikacyjnego ESCHELON przychwytywał w ciągu doby miliony przekazów informacji, które były filtrowane według słów „kluczy" przez komputery o dużej mocy obliczeniowej w poszukiwaniu potencjalnych i aktualnych zagrożeń bezpieczeństwa państw-beneficjentów tego systemu[3]. Tragiczne w skutkach wydarzenia z 11.9.2001 r. pokazały, że ESCHELON nie był w stanie im zapobiec. Jak to potwierdziły późniejsze oficjalne ustalenia, i w tym przypadku zawiodła nie technika, lecz ludzie. Najsłabszym ogniwem rozbudowanego systemu nasłuchu elektronicznego okazała się wymiana informacji pomiędzy amerykańskimi służbami specjalnymi, które nie zdołały odczytać docierających do nich sygnałów o przygotowaniach do zamachu[4]. Atak Al-Ka'idy na World Trade Center w Nowym Jorku i Pentagon w Waszyngtonie w istotnym stopniu wpłynął na zmianę strategii bezpieczeństwa narodowego wielu państw, przesuwając jej punkt ciężkości na zapobieganie zagrożeniom terrorystycznym. W latach 2001–2006 w Stanach Zjednoczonych mocą decyzji organów władzy wykonawczej, ustawodawczej i sądowniczej rozszerzono uprawnia FBI, CIA i NSA do gromadzenia i przetwarzania danych osobowych użytkowników telefonów komórko-

[3] European Parliament 1999–2004, Temporary Committee on the ECHELON Interception System Provisional, 18 May 2001 Draft Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system), Temporary Committee on the ECHELON Interception System Rapporteur: *Gerhard Schmid*, PR\439868EN.doc 1/113.

[4] Inquiry teams reviewing the prologue to 9/11 soon identified that poor exchange between the CIA, FBI and National Security Agency (NSA) contributed to the lack of warning (*R. Aldrich,* US–European Intelligence Co-operation on Counter-Terrorism: Low Politics and Compulsion, The British Journal of Politics and International Relations, 2009 vol. 11, s. 129); The largest fault noted by many sources on stopping the 9/11 attacks before they happened was the lack of communication between agencies (C. *Gingerich*, National Security Policy Responses to the 9/11 Attacks, Spring 2013, s. 24; https://spea.indiana.edu/doc/undergraduate/ugrd_thesis2013_mgmt_gingerich.pdf.

wych i Internetu, ograniczając jednocześnie zakres kontroli sądowej nad ingerencją państwa w sferę prywatności obywateli[5].

Kierując się kryteriami zbliżonymi do ustalania zakresu jurysdykcji w sprawach karnych, stworzono trzy oddzielne reżimy prawne monitorowania elektronicznych przekazów informacji prowadzone na skalę masową, w sposób zautomatyzowany z wykorzystaniem technologii *deep packet inspection*. Kontrola objęła informacje przesyłane na terytorium USA (*PATRIOT Act*) zagraniczne przekazy informacji kierowane do USA (*Foreign Intelligence Surveillance Act*), oraz wymianę danych prowadzoną poza granicami Stanów Zjednoczonych (*Executive Order 12333*)[6].

Nowe regulacje prawne, jakie przewidywało ustawodawstwo antyterrorystyczne, umożliwiły amerykańskim służbom specjalnym uruchomienie działań o charakterze wywiadowczym na niespotykaną wcześniej skalę. Świat dowiedział się o nich w czerwcu 2013 r. od *Edwarda Snowdena*, który w wywiadach udzielonych redakcji dziennika „The Guardian" ujawnił ściśle tajne szczegóły programów masowej inwigilacji (PRISM, MUSCULAR, XKeyscore, BULLRUN, Cotraveler i in.) realizowanych przez Agencję Bezpieczeństwa Narodowego (NSA) Stanów Zjednoczonych i służby wywiadu państw sojuszu „Pięciorga Oczu"[7].

Zapoczątkowany w 2007 r. ściśle tajny program PRISM, określany przez NSA mianem „źródła informacji wywiadowczej nr 1", zapewnił Agencji bezpośredni dostęp do centralnych serwerów dziewięciu wiodących amerykańskich dostawców usług internetowych (Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube i Apple) i przechowywanych tam plików audio, wideo, zawartości poczty elektronicznej, dokumentów i danych dotyczących logowania się na te serwery. Tego rodzaju praktykę dopuszczało prawo amerykańskie. Zgodnie z art. 702 amerykańskiej ustawy *Foreign Intelligence Surveillance Act of 1978*[8], korzystanie przez NSA z informacji przechowywanych w serwerach wskazanych firm nie wymaga uzyskania zezwolenia sądu lub innego organu judykacyjnego[9].

Na podobnej zasadzie funkcjonują programy TEMPORA i MUSCULAR, w ramach których służby wywiadowcze Wielkiej Brytanii (GCHQ) i USA przechwytują przekazy informacji przesyłane m.in. telekomunikacyjnymi kablami

[5] Timeline of NSA Domestic Spying, https://www.eff.org/nsa-spying/timeline; How the NSA's Domestic Spying Program Works https://www.eff.org/nsa-spying/how-it-works; Electronic surveillance under Presidents Bush and Obama http://apps.washingtonpost.com/g/page/national/electronic-surveillance-under-presidents-bush-and-obama/213/.

[6] *A. Arnbak*, *S. Goldberg*, Loopholes for Circumventing the Constitution.

[7] Tj. USA, Wielkiej Brytanii, Kanady, Australii i Nowej Zelandii – zob. np. *Ł. Wójcik*, Setki uszu pięciorga oczu.

[8] Dalej jako: FISA.

[9] *B. Gellman*, *L. Poitras*, U.S., British intelligence mining data.

podmorskimi oraz dane transmitowane między serwerami Yahoo, Google, Microsoft Hotmail i Windows Live Messenger. TEMPORA umożliwia wywiadowi brytyjskiemu (GCHQ) dostęp zarówno do metadanych, jak i treści korespondencji elektronicznej i informacji umieszczanych na Facebooku[10]. Do filtrowania strumienia informacji według indeksu rzeczowego GCHQ wykorzystuje 40 tys., a NSA – 31 tys. słów kluczowych[11]. Punkt dostępowy programu MUSCULAR jest usytuowany poza Stanami Zjednoczonymi, program podlega więc jurysdykcji ekstraterytorialnej sądu FISA, co pozwala na monitorowanie korespondencji obywateli amerykańskich[12].

Potężne narzędzie analityczne, jakim jest program XKEYSCORE, umożliwia personelowi NSA, przeszukiwanie – bez uprzedniego uzyskania autoryzacji – rozległych baz danych zawierających wiadomości przesyłane pocztą elektroniczną, treść rozmów prowadzonych za pośrednictwem czatów internetowych oraz historię wyszukiwania informacji w sieci przez miliony użytkowników, jak również metadanych na ich temat. System na bieżąco przeszukuje dane z ponad 700 serwerów zlokalizowanych w ok. 150 miejscach na świecie. Uznawany jest za najszerzej zakrojony system NSA do inwigilacji użytkowników Internetu. XKEYSCORE automatycznie sortuje dane według różnych kryteriów, umieszczając je w indeksowanej bazie danych, którą łatwo przeszukiwać na podstawie haseł. Posiada też funkcję inwigilacji w czasie rzeczywistym, która powala na bieżąco śledzić aktywność określonych „celów" w Internecie i prezentować rezultaty obserwacji analitykowi.

BULLRUN – program do deszyfrowania informacji jest rozwijany przez Agencję w celu złamania powszechnie stosowanych technologii kryptograficznych, które utrudniają NSA dostęp do treści przesyłanych lub udostępnianych przez miliony osób w transakcjach internetowych i korespondencji elektronicznej. Narodowa Agencja Bezpieczeństwa oficjalnie nie odniosła się do informacji ujawnionej przez *Snowdena* o istnieniu programu Bullrun. Z doniesień opublikowanych na łamach prasy brytyjskiej i amerykańskiej wynika, że przedstawiciele służb wywiadowczych zwrócili się o niepublikowanie artykułów na ten temat ze względu na bezpieczeństwo narodowe[13].

W ramach programu CO-TRAVELER Narodowa Agencja Bezpieczeństwa kontroluje dziennie ok. 5 mld rekordów danych lokalizacyjnych użytkow-

[10] *E. MacAskill*, *J. Borger*, *N. Hopkins*, *N. Davies*, *J. Ball*, GCHQ taps fibre-optic cables.

[11] *Tamże*.

[12] *A. Arnbak*, *S. Goldberg*, Loopholes for Circumventing the Constitution.

[13] Dokument Roboczy Nr 1 w sprawie amerykańskich i unijnych programów nadzoru, s. 3.

ników telefonów komórkowych na świecie[14]. Dane są przetwarzane w dwóch 27-terabajtowych bazach danych przez oprogramowanie umożliwiające ustalenie współrzędnych geograficznych użytkowników telefonów, śledzenie ich mobilności i tworzenie „map" kontaktów interpersonalnych w czasie i przestrzeni osób będących obiektem zainteresowania służb specjalnych. Odbywa się to przez korelowanie danych lokalizacyjnych „osób-celów" z danymi setek tysięcy innych użytkowników telefonów komórkowych w poszukiwaniu punktów, w których ich drogi krzyżują się ze sobą. Na tej podstawie analitycy Agencji ustalają relacje osobowe i tożsamość domniemanych współpracowników osób rozpracowywanych wywiadowczo[15].

Zasada działania programu Co-traveler stanowi znakomitą ilustrację jednego z głównych zastosowań modelu „nieograniczonej" inwigilacji, której obiektem są miliony osób nieświadomych tego, że ich dane są przetwarzane przez komputery i analityków służb specjalnych. Masowe przetwarzanie danych komunikacyjnych i lokalizacyjnych użytkowników telefonów komórkowych w połączeniu z danymi z innych źródeł informacji służy różnym celom. Głównie jednak identyfikacji osób stanowiących zagrożenie publiczne i określeniu ryzyka zachowań destrukcyjnych tych osób po to, by do nich nie dopuścić. Prewencyjnie zorientowane cele masowej inwigilacji opartej na analizie terabajtów danych cechuje odmienne podejście do roli informacji jako czynnika warunkującego skuteczność działań organów odpowiedzialnych za bezpieczeństwo państwa. Celem działania tych organów jest niedopuszczenie do zamachu terrorystycznego lub innego niepożądanego z punktu widzenia bezpieczeństwa publicznego zdarzenia. Priorytetem nie jest natomiast doprowadzenie do wykrycia i ukarania sprawcy zamachu, co jest zadaniem organów ścigania i wymaga od nich zgromadzenia i analizy informacji w celach dowodowych. Jak pisze David *Lyon*: „W przypadku masowej inwigilacji dane osobowe, takie jak metadane identyfikujące osoby, których dotyczą, nie są gromadzone w ograniczonych, określonych i przejrzystych celach, zgodnie z zasadami ochrony danych i poglądami obrońców prywatności. Następuje

[14] Z wyłączeniem Stanów Zjednoczonych, które zgodnie z ustawodawstwem federalnym (FISA) nie podlegają jurysdykcji NSA. Zob. *B. Gellman*, *A. Soltani*, NSA tracking cellphone locations worldwide.

[15] Należy zaznaczyć, że metadane mogą być źródłem bardziej istotnych informacji niż treść rozmów telefonicznych lub wiadomości przesyłane pocztą elektroniczną. Ze względu na ich format łatwiej je gromadzić i analizować. Zaawansowane narzędzia obliczeniowe umożliwiają analizę dużych zbiorów danych w celu uchwycenia ukrytych w nich wzorców i powiązań, w tym danych osobowych, przyzwyczajeń i zachowań. Nie odnosi się to do rozmów, które mogą odbywać się w dowolnej formie lub języku. Grupa Robocza Art. 29 819/14/PL WP 215, Opinia 04/2014 w sprawie inwigilacji komunikacji elektronicznej na potrzeby wywiadu i bezpieczeństwa narodowego, s. 5.

tu odwrócenie tradycyjnego porządku działań policyjnych i wywiadowczych. Ich celem nie są podejrzani lub inne osoby, na temat których organy te zbierają informacje. Tutaj dane pochodzące z różnych źródeł i zagregowane w pewien zbiór przed określeniem pełnego zakresu jego rzeczywistych i potencjalnych zastosowań są przetwarzane z wykorzystaniem różnych algorytmów i metod analizy nie tylko dla zrozumienia sekwencji minionych zdarzeń, ale także w celu przewidywania i reagowania na zachowania, zdarzenia i procesy, które mają dopiero nastąpić"[16].

Ideę masowej inwigilacji (Big Data) w bardziej dobitny sposób ujmuje tekst umieszczony na stronie internetowej Agencji Bezpieczeństwa Narodowego USA. W odpowiedzi na postawione tam pytanie: „Dlaczego gromadzimy Twoje dane?" posłużono się figurą retoryczną, która przeciwstawia „przeszłość" „teraźniejszości". *W* „przeszłości" organy ścigania przystępowały do gromadzenia informacji o podejrzanym po jego identyfikacji po to, by zebrać dowody działalności przestępczej tej osoby. „Obecnie" gromadzi się wszelkie dostępne dane na temat „wszystkich", po to, by zidentyfikować „nowe cele"[17]. Uzasadnienie działań podejmowanych w ramach inwigilacji masowej jest lakoniczne: „nie sposób z góry przewidzieć jakie informacje mogą mieć kluczowe znaczenie dla wykrycia spisku". Stąd też główna dyrektywa postępowania Krajowego Zarządu Inwigilacji NSA zajmującego się gromadzeniem, przetwarzaniem i przechowywaniem danych o obywatelach Stanów Zjednoczonych dla „dobra Narodu" brzmi: „zbieraj wszystkie dostępne informacje ze wszystkich dostępnych źródeł przez cały czas, przy każdej okazji, nieustannie"[18].

Agencja Bezpieczeństwa Narodowego USA od czasu ujawnienia części jej tajemnic przez *Edwarda Snowdena* nie kryje zakresu swoich zainteresowań rodzajem informacji, które gromadzi lub zamierza gromadzić na temat obywateli USA. Działając, jak sama to określa, „w duchu otwartości i przejrzystości", publikuje na stronie internetowej ich „przykładowy" wykaz, który obejmuje 25 pozycji[19].

---

[16] *D. Lyon*, Surveillance, Snowden, and Big Data, s. 4.

[17] Why We Collect Your Data; http://nsa.gov1.info/data/index.html#data.

[18] Tamże.

[19] In the spirit of openness and transparency, here is a partial list of current and planned future data collection targets: internet searches; websites visited; emails sent and received; social media activity (Facebook, Twitter, etc; blogging activity including posts read, written, and commented on; videos watched and/or uploaded online; photos viewed and/or uploaded online; mobile phone GPS-location data; mobile phone apps downloaded; phone call records; text messages sent and received; Skype video calls; online purchases and auction transactions; credit card/ debit card transactions; financial information; legal documents; travel documents; health records; cable television shows watched and recorded; commuter toll records; electronic bus and subway passes / Smartpasses; facial recognition data from surveillance cameras; educational records; arrest records; driver license information.

Rewelacje *Snowdena*, które obnażyły mechanizmy masowej inwigilacji „niewinnych" obywateli wywołały reakcję łańcuchową. Jej istotnym ogniwem były podmioty bezpośrednio zaangażowane w realizację wspomnianych wyżej programów. Zgodnie z zasadami demokracji, zostały one zobowiązane do zajęcia oficjalnego stanowiska w tej sprawie. Ujawnione przez *Snowdena* i opublikowane przez media tajne dokumenty przedstawiające metody działania NSA, nie pozostawiły Agencji wielkiego wyboru. W oświadczeniu opublikowanym w Internecie NSA potwierdziła ich autentyczność, a tym samym pośrednio prawdziwość doniesień swego byłego współpracownika. Jednocześnie zostały one uzupełnione o pewne szczegóły techniczne oraz charakterystyczny komentarz, opatrzony sentencją: „Jeśli nie masz niczego do ukrycia, to nie masz się czego obawiać", stanowiącą koronny argument przedstawicieli służb specjalnych na całym świecie w dyskusji z oponentami powołującymi się na prawo do prywatności[20].

Zakres danych osobowych użytkowników technologii informacyjnych gromadzonych na skalę masową w Europie prawdopodobnie nie jest aż tak szeroki, jak w USA. Sygnały radiowe telefonii mobilnej, satelitarnej i nadajników GPS przecinają przestrzeń powietrzną każdego państwa. W każdym z nich służby specjalne prowadzą „wywiad elektroniczny" (SIGINT), filtrując zawrotną liczbę danych przechodzących tranzytem przez ich terytorium. Problem ten nie dotyczy w takim samym stopniu wszystkich państw Unii Europejskiej[21]. Specyficzną formą inwigilacji masowej w Unii Europejskiej jest natomiast retencja danych telekomunikacyjnych. Wprowadzona dyrektywą 2006/24/WE[22] obejmuje kilkanaście rodzajów danych, które odpowiednio analizowane i interpretowane pozwalają uzyskać obraz aktywności życiowej nieomal każdego użytkownika telefonu komórkowego i Internetu w liczącej 550 mln mieszkańców Unii Europejskiej. Potencjał informacyjny, jaki tkwi w danych o połączeniach telekomunikacyjnych i lokalizacji urządzeń mobilnych używanych do komunikowania się jest ogromny i dzięki technologii informacyjnej może być wykorzystywany do różnych celów. Także w sposób, który narusza prawa podstawowe osób niemających żadnych związków z działalnością przestępczą. Zdaniem *Petera Hustinx'a* –

[20] Your data: If you have nothing to hide, you have nothing to fear, http://nsa.gov1.info/data/index.html#data. Nieporozumienie polega na tym, że argument „nie mam nic do ukrycia" opiera się na szczególnym sposobie pojmowania prywatności, jako rodzaju tajemnicy, swoistego prawa do ukrywania „złych" rzeczy. Por. *D. Solove*, "I've got Nothing to Hide" and other Misunderstandings of Privacy.

[21] *E. Fura*, *M. Klebmerg*, The Chilling Effect of Counter-Terrorism Measures.

[22] Dyrektywa Parlamentu Europejskiego i Rady 2006/24/WE z 15.3.2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz.Urz. WE L Nr 105, s. 54, dalej: dyrektywa 2006/24/WE).

Europejskiego Inspektora Ochrony Danych – „zatrzymywanie i przechowywanie danych o połączeniach telekomunikacyjnych i lokalizacji wszystkich osób w Unii Europejskiej, które używają telefonu lub Internetu, jest poważną ingerencją w ich prawo do prywatności i nie ulega wątpliwości, że dyrektywa retencyjna stanowi pod tym względem najbardziej inwazyjny instrument jaki kiedykolwiek został przyjęty w Unii Europejskiej, gdy chodzi o skalę i liczbę osób, które znalazły się w zasięgu jego oddziaływania"[23].

Na wszystkie te okoliczności zwracają uwagę dwa aktualne orzeczenia najwyższych na szczeblu Unii Europejskiej i Polski instancji judykacyjnych. Jest przy tym znamienne, że sentencje obu tych wyroków różnią się między sobą w zasadniczym stopniu. O ile Trybunał Sprawiedliwości Unii Europejskiej (TSUE) w wyroku z 8.4.2014 r.[24] unieważnił dyrektywę retencyjną UE ze względu na naruszenie praw podstawowych zagwarantowanych w art. 7 (prawo do ochrony życia prywatnego) i art. 8 (prawo do ochrony danych osobowych) Karty Praw Podstawowych UE z 7.12.2000 r.[25], to stanowisko TK prezentowane w wyroku z 30.7.2014 r. w przedmiocie gromadzenia i przechowywania przez okres 12 miesięcy danych telekomunikacyjnych[26] jest – generalnie rzecz biorąc przychylne utrzymaniu tej instytucji pod warunkiem poddania jej niezależnej kontroli zewnętrznej w zakresie udostępniania danych.

Retencja danych telekomunikacyjnych, w szczególności w kontekście niezbędnych zmian legislacyjnych wskazanych przez Trybunał Konstytucyjny we wspomnianym wyżej wyroku, jest głównym przedmiotem rozważań dalszej części tej pracy. Obejmują one kilka, ściśle ze sobą związanych, aspektów tej problematyki. Na wstępie przypomniane zostaną europejskie standardy prawne w dziedzinie przetwarzania danych osobowych i ochrony prywatności w sektorze telekomunikacyjnym[27] i sektorze łączności elektronicznej[28] poprzedzające wprowadzenie standardu retencyjnego[29]. Następnie scharakteryzowane zostaną

[23] *P. Hustinx*, Europejski Inspektor Ochrony Danych w wystąpieniu na konferencji „Taking on the Data Retention Directive", Bruksela, 3.12.2010 r.

[24] Sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland i Seitlinger i in.*

[25] Dalej jako: KPP.

[26] Wyr. TK z 30.7.2014 r., K 23/11, Dz.U. z 2014 r. poz. 1055; uzasadnienie: http://otk.trybunal.gov.pl/orzeczenia/ezd/sprawa_lista_plikow.asp?syg=K%2023/11.

[27] Dyrektywa Parlamentu Europejskiego i Rady 97/66/WE z 15.12.1997 r. w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze telekomunikacyjnym (Dz.Urz. WE L z 1998 r. Nr 24, s. 1), dalej jako: dyrektywa 97/66/WE.

[28] Dyrektywa Parlamentu Europejskiego i Rady 2002/58/WE z 12.7.2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.Urz. WE L Nr 201, s. 37, dalej jako: dyrektywa 2002/58/WE).

[29] Dyrektywa 2006/24/WE.

efekty implementacji dyrektywy 2006/24/WE w krajach członkowskich Unii Europejskiej w kontekście zasady proporcjonalności, tj. „ograniczenia celu" retencji danych w ustawodawstwie krajowym do ścigania „przestępstw poważnych" (*serious crime*) oraz prawnych mechanizmów kontroli dostępu podmiotów uprawnionych do danych zatrzymywanych i przechowywanych przez przedsiębiorców telekomunikacyjnych. Na tym tle omówione zostaną powody unieważnienia dyrektywy 2006/24/WE wyrokiem TSUE z 8.4.2014 r. i przedstawiona zostanie ocena wpływu tego wyroku na ustawodawstwo polskie. Krytyczna analiza polskich regulacji prawnych dotyczących retencji danych telekomunikacyjnych na tle standardów konstytucyjnych i konwencyjnych oraz sformułowanie postulatów *de lege ferenda* wychodzących naprzeciw stanowisku Trybunału Konstytucyjnego, zawartego w wyroku z 30.7.2014 r., stanowią finalne elementy niniejszego opracowania. W jego ramach prezentowane są również uwagi dotyczące problematyki kontroli operacyjnej z wykorzystaniem środków technicznych w środowisku sieci teleinformatycznych, które nawiązują do sentencji i uzasadnienia wspomnianego wyżej wyroku.

§ 1. Europejskie standardy prawne w dziedzinie przetwarzania danych osobowych i ochrony prywatności w sektorze telekomunikacyjnym i łączności elektronicznej

Retencja danych w telekomunikacji nie jest koncepcją nową. Niektórzy autorzy poszukują jej genezy w drugiej połowie XIX w., wskazując na pierwszy akt prawa międzynarodowego w dziedzinie telekomunikacji – Międzynarodową Konwencję Telegraficzną z 1865 r., która przewidywała 12-miesięczny okres przechowywania telegramów przez stacje telegrafu[30]. Obowiązek ten dotyczył ok. 300 mln wiadomości, jakie telegraficznie przesyłano na świecie w schyłku XIX w. Z dzisiejszej perspektywy jest to liczba symboliczna w porównaniu do 2,8 milionów wiadomości przesyłanych pocztą elektroniczną co sekundę przez mieszkańców Ziemi[31].

W drugiej połowie XX w. informacje o charakterze osobowym objęto w Europie ochroną prawną. Przyjęto zasady i procedury mające na celu wzmocnienie pozycji prawnej jednostki w warunkach automatycznego przetwarzania infor-

[30] *I. Lloyd*, Data Retention, s. 79 i n.
[31] *W. MacLean*, Is the Big Brother watching you?

macji na jej temat[32]. Podstawowe znaczenie miał w tym zakresie zakaz gromadzenia i przechowywania danych osobowych niezgodnie z celem utworzenia zbioru i dłużej niż to niezbędne ze względu na cel przetwarzania danych (zasada celowości). Zasada ta odnosiła się do wszelkich danych osobowych, w tym danych towarzyszących przekazom informacji generowanym automatycznie przez dostawców usług telekomunikacyjnych. Wynikające z niej ograniczenia prawne miały służyć ochronie prywatności użytkowników środków komunikowania się i nakazywały dostawcom usług usuwanie lub anonimizację wszelkich danych przetwarzanych w celu przekazywania komunikatów w sieci lub naliczania opłat za te usługi, gdy nie są one już potrzebne do celów transmisji komunikatu albo rozliczeń operatorskich z klientami. Pod koniec XX w., na skutek implementacji dyrektywy 97/66/WE, zasada ta znalazła odbicie w prawie telekomunikacyjnym państw Wspólnoty Europejskiej.

Zasada dopuszczała jednak wyjątki. Dyrektywa 97/66/WE zezwalała państwom członkowskim w określonych sytuacjach na odstępstwa od ustanowionych w niej norm prawnych chroniących prywatność użytkowników środków komunikowania się. Dotyczyło to również usuwania danych o połączeniach telekomunikacyjnych przez operatorów w okolicznościach, w których byłoby to konieczne m.in. ze względu na bezpieczeństwo państwa, ochronę porządku publicznego oraz zapobieganie i ściganie przestępstw[33]. Początkowo rządy państw członkowskich UE nie zamierzały korzystać z tych możliwości[34]. Nastawienie to zmieniło się po 11.9.2001 r. Standardy europejskie w dziedzinie ochrony prywatności użytkowników telekomunikacji spotkały się wówczas z krytyczną oceną władz amerykańskich, które apelowały do Komisji Europejskiej o rezygnację z „obowiązkowego niszczenia danych" (*mandatory data destruction regimes*), stanowiących „nieocenione źródło informacji dla organów ścigania i bezpieczeń-

[32] Por. Recommendation with Guidelines on the protection of privacy and transborder flows of personal data adopted by the Council of the Organisation for Economic Co-operation and Development on 23 September 1980; Council of Europe Convention No. 108 for the protection of individuals with regard to automatic processing of personal data, adopted 28 January 1981; Directive 95/46/EC of the European Parliament and of the Council of Europe of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (EU-Data Protection-Directive).

[33] Art. 14 ust. 1: „Państwa członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu obowiązków i praw określonych w artykułach 5, 6 i art. 8 ust. 1, ust. 2, ust. 3, i ust. 4, gdy takie ograniczenia stanowią środki niezbędne dla zabezpieczenia bezpieczeństwa narodowego, obrony, bezpieczeństwa publicznego oraz zapobiegania, prowadzenia dochodzeń, wykrywania i zaskarżania przestępstw kryminalnych (…)".

[34] Wyjątek stanowiły np. Włochy, które implementując dyrektywę 2006/24/WE, zastrzegły możliwość skorzystania z art. 14 ust. 1.

stwa publicznego w czasach zagrożenia terroryzmem i przestępczością zorganizowaną"[35].

Jeszcze przed zamachami z 11.9.2001 r. kilka państw członkowskich UE podjęło inicjatywę na rzecz rewizji standardów normatywnych chroniących prywatność w sektorze telekomunikacji. W maju 2001 r. Wielka Brytania, Francja i Belgia zgłosiły zastrzeżenia do projektu nowej dyrektywy na temat e-prywatności, domagając się pominięcia przepisu o usuwaniu i anonimizacji danych – w oparciu o argument, że regulacja ta nie uwzględnia potrzeb organów ścigania i realiów technologicznych związanych z komunikacją w Internecie[36]. Postulat ten początkowo napotkał na sprzeciw innych państw członkowskich i Komisji Europejskiej jednak po zamachach na WTC w Nowym Jorku i Pentagon w Waszyngtonie znalazł (w złagodzonej postaci) odbicie w nowej dyrektywie unijnej o e-prywatności, która zezwalała państwom członkowskim na stosowanie retencji danych, pod warunkiem przestrzegania zasad prawa wspólnotowego[37]. Z prawnego punktu widzenia przepis art. 15 ust. 1 dyrektywy 2002/58/WE był odstępstwem od jednej z fundamentalnych zasad ochrony danych osobowych. W praktyce sankcjonował fakty dokonane, w szczególności wprowadzenie przez niektóre państwa członkowskie (m.in. Francję i Wielką Brytanię) przepisów o retencji danych telekomunikacyjnych do ustawodawstwa wewnętrznego w 2001 r. Przede wszystkim jednak otwierał drogę do upowszechnienia tej instytucji w Unii Europejskiej i umożliwił rozpoczęcie prac nad nowym standardem prawnym – obowiązkowej

[35] Prepared statement of the United States of America Presented at EU Forum on Cybercrime Brussels, 27 November 2001, www.justice.gov/criminal/cybercrime/intl/MMR_Nov01_Forum.doc; The letter addressed to Mr. Romano Prodi, the President of the European Commission, from the US President Bush includes a demand that „data protection issues in the context of law enforcement and counter-terrorism imperatives" should be considered and that: „draft privacy directives that call for mandatory destruction to permit the retention of critical data for a reasonable period" should be revised, http://www.statewatch.org/news/2001/nov/06uslet.htm.

[36] Report of the Telecommunications Working Party to COREPER of 31 May 2001 on the proposed Eprivacy Directive, ECO 147 CODEC 492.

[37] Art. 15 ust. 1 dyrektywy 2002/58/WE: „Państwa Członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1–4, i art. 9 tej dyrektywy, gdy takie ograniczenia stanowią środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego (tj. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej, jak określono w art. 13 ust. 1 dyrektywy 95/46/WE. W tym celu, Państwa Członkowskie mogą, między innymi, uchwalić środki ustawodawcze przewidujące przechowywanie danych przez określony czas uzasadnione na podstawie zasad ustanowionych w niniejszym ustępie. Wszystkie środki określone w niniejszym ustępie są zgodne z ogólnymi zasadami prawa wspólnotowego, w tym zasadami określonymi w art. 6 ust. 1 i 2 TUE".

retencji danych w celu wzmocnienia bezpieczeństwa publicznego oraz bardziej efektywnego zapobiegania i zwalczania przestępczości.

Standard ten, po kilku latach sporów i dyskusji, zmaterializował się w postaci dyrektywy Parlamentu Europejskiego i Rady 2006/24/WE z 15.3.2006 r., która doszła do skutku głównie dzięki intensywnym zabiegom dyplomacji brytyjskiej, uwieńczonych sukcesem w okresie prezydencji Zjednoczonego Królestwa w UE w 2005 r.[38]

Z chwilą implementacji dyrektywy 2006/24/WE przez państwa członkowskie, debata na temat retencji danych przeniosła się na grunt narodowy. W niektórych krajach, w tym w Polsce, wejście w życie normatywnego standardu unijnego w tej dziedzinie wywołało krytykę regulacji ustawowych i publiczną dyskusję na temat zagrożeń dla praw i wolności obywatelskich. Sądy konstytucyjne Rumunii, Republiki Federalnej Niemiec i Republiki Czech uznały ustawodawstwo implementujące dyrektywę 2006/24/WE za niezgodne z ustawą zasadniczą tych państw i mocą wydanych orzeczeń uchyliły przepisy retencyjne.

Sentencje tych orzeczeń są nieomal jednobrzmiące i prowadzą do identycznych skutków prawnych w postaci utraty mocy obowiązującej zaskarżonych przepisów. Natomiast różnią się między sobą sposobem argumentacji prawniczej, a przede wszystkim motywami rozstrzygnięć stwierdzających niekonstytucyjność ustawodawstwa retencyjnego Rumunii, Niemiec i Czech[39].

Orzeczenie sądu konstytucyjnego Rumunii z 8.10.2009 r.[40] oraz orzeczenie sądu konstytucyjnego Czech z 22.3.2011 r.[41] są dalej idące niż wyrok sądu konstytucyjnego RFN z 2.3.2010 r.[42] Oba te orzeczenia uznają retencję danych *per se* (czyli gromadzenie i przechowywanie danych o życiu prywatnym użytkowników środków łączności elektronicznej na użytek organów ścigania i bezpieczeństwa publicznego) za instytucję niemożliwą do pogodzenia z konstytucyjnymi gwarancjami prawa do prywatności, ochrony tajemnicy korespondencji oraz autonomii informacyjnej jednostki. Stanowisko sądu konstytucyjnego Niemiec jest bardziej

[38] Szerzej na ten temat: *J. Rauhofer*, Just because you're paranoid, doesn't mean they're not after you.

[39] W przypadku tego ostatniego kraju – niezgodność z przepisami konstytucji oraz Karty Podstawowych Praw i Swobód Republiki Czech, zob. The Charter of Fundamental Rights and Basic Freedoms of the Czech Republic, http://www.psp.cz/cgi-bin/eng/docs/laws/1993/2.html.

[40] Constitutional Court Decision no 1258 from 8 October 2009, www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-dataretention.html.

[41] Ústavní soud zrušil část zákona o elektronických komunikacích, http://www.usoud.cz/clanek/5068.

[42] Federal Constitutional Court – Press office – Press release no. 11/2010 of 2 March 2010, Judgment of 2 March 2010, www.bundesverfassungsgericht.de/en/press/bvg10-011en.html.

umiarkowane. Wydane 2.3.2010 r. orzeczenie nie stwierdza, aby obowiązkowa retencja danych telekomunikacyjnych naruszała konstytucyjne gwarancje prawa do tajemnicy korespondencji. Wyraża natomiast pogląd, że instytucję tę wdrożono do ustawodawstwa RFN z naruszeniem zasady proporcjonalności, skutkiem czego zaskarżone przepisy nie gwarantują adekwatnego poziomu bezpieczeństwa danych, właściwej kontroli udostępniania danych podmiotom uprawnionym ani odpowiednich ograniczeń korzystania z danych przez te podmioty.

Kwestia kontroli dostępu do danych telekomunikacyjnych i ich wykorzystywania ma w tym kontekście znaczenie absolutnie podstawowe i w dużym stopniu niezależne od dalszych losów instytucji retencji danych i jej ostatecznego ukształtowania w prawie UE i państw członkowskich tej organizacji. Jest to problem szczególnie istotny w Polsce, w której dostęp tzw. podmiotów uprawnionych do danych gromadzonych i przechowywanych przez dostawców ogólnie dostępnych usług łączności elektronicznej oraz dostawców publicznych sieci łączności nie podlega podobnym ograniczeniom prawnym i mechanizmom kontrolnym do tych, jakie funkcjonują w większości państw Unii. Na potrzebę zmiany tego stanu rzeczy i konieczność zniwelowania dystansu, jaki dzieli Polskę pod tym względem od innych państw europejskich, wskazywano w polskiej literaturze przedmiotu wielokrotnie[43]. Ostatecznie postulat ten znalazł odbicie w wyroku Trybunału Konstytucyjnego z 30.7.2014 r.[44], który orzekł, że przepisy ustawy o Policji oraz siedmiu innych ustaw „policyjnych" są niezgodne z art. 47 i art. 49 w zw. z art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej z 2.4.1997 r.[45], ponieważ nie przewidują niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy z 16.7.2004 r. – Prawo telekomunikacyjne[46].

[43] Zob. *A. Adamski*, Obywatel bezpieczny, ale przezroczysty; *tenże*, Przestępczość w cyberprzestrzeni, s. 75 i 94; *tenże*, Retencja danych o ruchu telekomunikacyjnym; *tenże*, Implementacja dyrektywy retencyjnej w Polsce; zob. też *D. Adamski*, Retencja danych telekomunikacyjnych. Część prawnoporównawcza niniejszego opracowania (s. 10–66) jest poprawioną i zaktualizowaną wersją mojej pracy pt. Kontrola dostępu do danych telekomunikacyjnych podlegających obowiązkowi retencji na tle ustawodawstwa wybranych państw Unii Europejskiej, Warszawa 2012, wydanej przez Naczelną Radę Adwokacką w Warszawie.

[44] K 23/11, Dz.U. z 2014 r. poz. 1055.

[45] Dz.U. Nr 78, poz. 483 ze zm., dalej jako: Konstytucja RP.

[46] T.j. Dz.U. z 2014 r. poz. 243 ze zm., dalej jako: PrTelekom.

§ 2. Dyrektywa 2006/24/WE i ocena jej implementacji przez Komisję Europejską

I. Standard unijny

Dyrektywa 2006/24/WE zobowiązywała państwa członkowskie Unii Europejskiej do wprowadzenia standardu prawnego w zakresie retencji danych o ruchu telekomunikacyjnym dla potrzeb organów ścigania i wymiaru sprawiedliwości. Zgodnie z tym standardem, dostawcy ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności powinni zatrzymywać i przechowywać przez okres co najmniej 6 do 24 miesięcy określone kategorie danych, generowanych lub przetwarzanych w ramach prowadzonej działalności, by w ten sposób „zapewnić dostępność przedmiotowych danych do celu dochodzenia, wykrywania i ścigania poważnych przestępstw, określonych w ustawodawstwie każdego państwa członkowskiego”[47].

Zgodnie z art. 5 dyrektywy 2006/24/WE, zakres retencji obejmował sześć kategorii danych umożliwiających identyfikację:

1) źródła połączenia;
2) odbiorcy połączenia;
3) daty, godziny i czasu trwania połączenia;
4) rodzaju połączenia;
5) narzędzia komunikacji i
6) lokalizacji urządzenia komunikacji ruchomej, odnoszących się do pięciu rodzajów usług łączności elektronicznej:
   a) telefonii stacjonarnej;
   b) telefonii mobilnej;
   c) dostępu do Internetu;
   d) elektronicznej poczty internetowej oraz
   e) telefonii internetowej (VoIP).

Szczegółowa specyfikacja danych wynikająca z połączenia obu tych kryteriów liczy w sumie ok. 30 pozycji, w tym m.in. adres IP, nazwisko i adres abonenta, identyfikator użytkownika, numer telefonu, data i dokładny czas rozpoczęcia i zakończenia połączenia, data i godzina zalogowania i wylogowania z elektronicznej poczty internetowej, międzynarodowy numer tożsamości telefonicznej abonenta mobilnego (IMSI), międzynarodowy numer fabryczny mobilnego aparatu telefonicznego (IMEI) oraz dane pozwalające ustalić położenie geograficzne telefonów mobilnych.

[47] Art. 1 dyrektywy 2006/24/WE.

Danymi, do których zatrzymywania zobowiązani zostali – na podstawie art. 3 i 5 dyrektywy 2006/24/WE – dostawcy ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności, były przede wszystkim dane niezbędne do ustalenia źródła oraz odbiorcy połączenia, do określenia daty, godziny i czasu trwania połączenia oraz jego rodzaju, do określenia narzędzia komunikacji i do identyfikacji lokalizacji urządzenia komunikacji ruchomej, w tym m.in. nazwiska i adresu abonenta lub zarejestrowanego użytkownika, numeru nadawcy i odbiorcy połączenia, a także adresu IP w przypadku usług internetowych. Dane te są neutralne technologicznie, lecz pozwalają ustalić, z jaką osobą i za pomocą jakiego środka komunikował się abonent lub zarejestrowany użytkownik, a także – czas połączenia oraz miejsce, z którego zostało ono nawiązane. Dzięki nim można też ustalić częstotliwości komunikowania się abonenta lub zarejestrowanego użytkownika z określonymi osobami w danym okresie. Odpowiednio ze sobą zestawione i przetworzone przy użyciu specjalnie napisanych w tym celu programów, częściowo dostępnych w sieci jako oprogramowanie *open source*, pozwalają też na retrospektywną analizę aktywności życiowej i kontaktów społecznych nieomal wszystkich regularnych użytkowników telefonów mobilnych i Internetu[48].

Przedmiotem regulacji dyrektywy 2006/24/WE, jako instrument I filaru Unii Europejskiej (integracja gospodarcza), było głównie postępowanie dostawców usług łączności elektronicznej i określenie ich obowiązków związanych z zatrzymywaniem i przechowywaniem wymienionych rodzajów danych. Dyrektywa nie zawierała natomiast przepisów dotyczących organów powołanych do ścigania przestępstw. W tym zakresie dyrektywa 2006/24/WE odsyłała do ustawodawstwa wewnętrznego państw członkowskich, pozostawiając im względną swobodę kształtowania norm prawnych określających reguły dostępu i korzystania z danych o ruchu i lokalizacji przez policję i inne organy kontroli społecznej. Tym samym otwierała ona pole do monitorowania zachowań zarówno osób aktualnie podejrzanych o popełnienie przestępstwa (co nie mogło budzić zastrzeżeń), jak i „potencjalnych podejrzanych", co naruszało obowiązujące do tej pory w Europie standardy prawne służące utrzymaniu równowagi między poszanowaniem prywatności obywateli a zapewnieniem im bezpieczeństwa. O tym, która z tych alternatyw zostanie wybrana oraz kto, w jakim celu i jak długo będzie wykorzystywał dane stanowiące przedmiot retencji, zdecydować miały poszczególne państwa, stanowiąc odpowiednie regulacje prawne i kształtując politykę stosowania prawa[49].

[48] Zob. Malte Spitz data retention 2009, http://www.zeit.de/datenschutz/malte-spitz-data-retention.

[49] *A. Adamski*, Implementacja dyrektywy retencyjnej w Polsce, s. 7.

II. Ocena wdrożenia dyrektywy 2006/24/WE w krajach UE przez Komisję Europejską

1. Uwagi wstępne

W dniu 18.4.2011 r. opublikowane zostało sprawozdanie Komisji Europejskiej na temat implementacji dyrektywy 2006/24/WE przez kraje członkowskie UE, stanowiące wynik analizy porównawczej 25 raportów krajowych[50]. Jej przedmiotem były zasadnicze aspekty transpozycji tego instrumentu prawa unijnego do prawa krajowego państw członkowskich, stanowiące (zgodnie z art. 14 dyrektywy2006/24/WE) podstawę oceny wdrożenia dyrektywy retencyjnej oraz wniosków dotyczących ewentualnych zmian jej przepisów.

Według oceny Komisji Europejskiej, tzw. efekt harmonizacyjny dyrektywy nie został w pełni osiągnięty. Przede wszystkim z powodu niewdrożenia jej przez wszystkie kraje członkowskie UE, w tym Austrię i Szwecję, które nie dokonały transpozycji dyrektywy retencyjnej w ogóle, Belgię, która dokonała transpozycji częściowej, oraz Czechy, Niemcy i Rumunię, w których ustawy implementujące dyrektywę 2006/24/WE zostały na mocy wyroków sądów konstytucyjnych tych państw uchylone jako niezgodne z konstytucją.

Krytycznie oceniono również sposób wdrożenia dyrektywy 2006/24/WE przez te państwa członkowskie, które nie ograniczyły zakresu stosowania zatrzymania danych do kategorii „przestępstw poważnych" (*serious crime*) oraz nie uwzględniły w swoim ustawodawstwie mechanizmów kontroli dostępu podmiotów uprawnionych do danych.

2. Ograniczenie celu retencji danych

Dyrektywa wprowadziła dwa „ograniczenia celu" retencji danych:

1) nie przewidywała możliwości wykorzystywania danych w celu zapobiegania przestępstwom;
2) ograniczała możliwość korzystania przez podmioty uprawnione z danych o połączeniach, lokalizacji i subskrybentach usług telekomunikacyjnych do prowadzenia dochodzeń, wykrywania i ścigania przestępstw poważnych.

Oba te ograniczenia stanowiły wynik kompromisu politycznego między Komisją, Parlamentem Europejskim i Radą[51]. Na dodatek zostały one wprowadzone w sytuacji, w której część państw członkowskich miała już w swoim ustawo-

[50] European Commission, Report from the Commission to the Council and the European Parliament, Evaluation report on the Data Retention Directive (Directive 2006/24/EC), Brussels, 18.4.2011, COM(2011) 225 final.

[51] Por. *E. Kosta*, *P. Valcke*, Retaining the data retention directive, s. 371–373; *J. Rauhofer*, Just because you're paranoid, doesn't mean they're not after you, s. 344–348.

dawstwie przepisy retencyjne pozbawione podobnych ograniczeń. Nie dziwi więc stwierdzenie Komisji Europejskiej, że „stopień harmonizacji ustawodawstwa państw członkowskich jest w tej dziedzinie ograniczony”[52]. Według sprawozdania KE, dziesięć państw (Bułgaria, Estonia, Finlandia, Grecja, Hiszpania, Holandia, Irlandia, Litwa, Luksemburg, Węgry) uwzględniło kryterium „przestępstwa poważnego”, definiując je w różny sposób. Ustawodawstwo retencyjne czterech państw (Cypr, Malta, Portugalia, Wielka Brytania), ogólnie odwołuje się do kategorii „poważnych przestępstw” nie podając bliższej ich charakterystyki. System prawny ośmiu państw (Belgia, Dania, Francja, Łotwa, Polska, Słowacja, Słowenia, Włochy) nie uwzględnia ograniczeń dotyczących wagi przestępstw ani celu przetwarzania danych podlegających retencji, lecz zezwala podmiotom uprawnionym na ich wykorzystywanie do realizacji zadań związanych z zapobieganiem przestępczości oraz zapewnieniem bezpieczeństwa państwa i porządku publicznego.

Dane na ten temat w sprawozdaniu KE są mało precyzyjne i nie oddają złożoności sytuacji prawnej wynikającej z krzyżowania się przepisów będących efektem transpozycji dyrektywy 2006/24/WE z wcześniejszymi regulacjami, które wiele państw wprowadziło na podstawie art. 15 ust. 1 dyrektywy 2002/58/WE. Okoliczność ta może tłumaczyć niewielki wpływ dyrektywy retencyjnej na harmonizację ustawodawstwa państw członkowskich w omawianym aspekcie (tabela 1).

Tabela 1. „Ograniczenie celu” retencji danych w ustawodawstwie państw członkowskich UE

Ustawowa definicja poważnego przestępstwa i ograniczenie celu	Ustawowa definicja poważnego przestępstwa	Ograniczenie celu	Brak obu ograniczeń
Bułgaria	Irlandia[1)]	Belgia	Francja
Estonia	Malta[2)]	Włochy[3)]	Łotwa
Finlandia	Dania	Cypr	Polska
Grecja			Słowacja
Hiszpania			Słowenia
Holandia			Wielka Brytania
Litwa			
Luksemburg			
Węgry			
Portugalia[4)]			

[52] Sprawozdanie KE, s. 8.

1) Art. 1 *The Communications (Retention of Data) Act 2011* za „przestępstwo poważne" uznaje czyn zagrożony karą pozbawienia wolności nie niższą od lat 5 oraz dodatkowo – kilka typów przestępstw wymienionych w załączniku Nr 1. Art. 6 ustawy do celów retencji danych zalicza prewencję, wykrywanie, prowadzenie dochodzeń i ściganie poważnych przestępstw, ochronę bezpieczeństwa państwa oraz ratowanie życia ludzkiego.

2) Przestępstwa zagrożone karą pozbawienia wolności powyżej jednego roku, http://archive.maltatoday.com.mt/2008/09/10/t1.html.

3) Personal Data Protection Code, Legislative Decree no. 196 dated 30 June 2003; Decreto-legge 27 luglio 2005, n. 144, recante misure urgenti per il contrasto del terrorismo internazionale.

4) Portugalska ustawa 32/2008 z 17.7.2008 r. zawiera wykaz przestępstw, w sprawach których organy procesowe mogą uzyskać dostęp do danych.

Artykuł 15 ust. 1 dyrektywy 2002/58/WE nie został uchylony przez dyrektywę retencyjną[53], co miało określone implikacje prawne. Po pierwsze oznaczało, że wprowadzone przed 2006 r. przez część państw członkowskich UE na podstawie art. 15 ust. 1 dyrektywy 2002/58/WE przepisy umożliwiające retencję danych ze względu na inne cele (np. walkę z terroryzmem, zapewnienie bezpieczeństwa państwa, ochronę porządku publicznego) niż to przewiduje dyrektywa retencyjna, pozostają w mocy i nadal mogą być podstawą wykorzystywania danych telekomunikacyjnych np. w celu ścigania przestępstw drobnych albo zapobiegania przestępczości. Po drugie, pozwalało państwom członkowskim na warunkach określonych w art. 15 ust. 1 dyrektywy 2002/58/WE, w szczególności z poszanowaniem zasady konieczności i proporcjonalności, na ustanowienie reżimu retencyjnego w odniesieniu do innych rodzajów danych transmisyjnych albo innych celów niż te, które są przedmiotem dyrektywy 2006/24/WE[54]. Na tym tle kwestia charakteru prawnego dyrektywy retencyjnej jako standardu minimalnego, dotyczącego wyłącznie „dochodzenia, wykrywania i ścigania poważnych prze-

[53] Por. art. 11 dyrektywy 2006/24/WE („Zmiana dyrektywy 2002/58/WE"), na mocy którego uzupełniono art. 15 ust. 1 dyrektywy 2002/58/WE o nowy ust. 1a w następującym brzmieniu: „1a. Ustępu 1 nie stosuje się do danych, których zatrzymywanie jest wyraźnie wymagane na mocy dyrektywy 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania danych wygenerowanych lub przetworzonych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności dla celów określonych w art. 1 ust. 1 tej dyrektywy".

[54] Por. motyw 12 preambuły dyrektywy 2006/24/WE, zgodnie z którym: „Artykuł 15 ust. 1 dyrektywy 2002/58/WE powinien być stosowany w dalszym ciągu w odniesieniu do danych, w szczególności tych dotyczących nieudanych prób uzyskania połączenia, co do których nie istnieje szczególny wymóg zatrzymywania w świetle niniejszej dyrektywy i z tego względu nie zostały w niej ujęte, a także w odniesieniu do celów, które nie zostały uwzględnione w niniejszej dyrektywie".

stępstw" nie pozostawia wątpliwości[55]. Pojawiają się one natomiast w praktyce państw, w których występuje wspomniany dualizm podstaw prawnych retencji danych. Typowy w tych okolicznościach dylemat organów odpowiedzialnych za kontrolę dostępu do danych dotyczył dopuszczalności udostępniania danych gromadzonych zgodnie z dyrektywą retencyjną do celów w niej nieprzewidzianych[56].

3. Kontrola dostępu do danych

Dostęp podmiotów uprawnionych do danych telekomunikacyjnych będących przedmiotem retencji wymaga zgody sądu w większości państw członkowskich UE. Sprawozdanie KE stwierdza, że w jedenastu państwach wymóg ten ma charakter ogólny i obejmuje zapytania o wszelkie dane telekomunikacyjne podlegające zatrzymaniu. W trzech państwach sądowa kontrola dostępu do danych dotyczy większości danych (np. w Finlandii uzyskanie danych osobowych abonentów nie podlega kontroli sądu). W kolejnych czterech państwach zezwolenie na dostęp do danych wydaje nie sędzia lub prokurator, lecz wyższej rangi urzędnik państwowy. Prawo dwóch państw członkowskich nie przewiduje żadnej kontroli dostępu do danych, wystarczy pisemny lub ustny wniosek podmiotu uprawnionego do operatora (Polska, Łotwa).

Należy odnotować, że raport KE obejmuje 22 państwa członkowskie, pomija natomiast pięć (Austrię, Czechy, Niemcy, Rumunię, Szwecję), które nie dokonały transpozycji dyrektywy 2006/24/WE (w ogóle bądź na skutek uchylenia ustawy implementującej tę dyrektywę jako niezgodnej z konstytucją). Ponadto, nie wszystkie oceny dotyczące przedmiotowego zagadnienia, jakie zawiera raport KE, są trafne, nie wspominając o słabym ich udokumentowaniu.

Bardziej szczegółowa analiza tego zagadnienia, uwzględniająca (tam, gdzie było to możliwe) prawodawstwo poszczególnych państw, w tym niektórych krajów, które raport KE pomija, przynosi podobne rezultaty, aczkolwiek daje bardziej dokładny obraz „kontroli dostępu" do danych (tabela 2).

[55] Por. Sprawozdanie KE, s. 4.

[56] Reply of Finland to the Questionnaire issued by the Commission on 30 September 2009 to evaluate the application of Directive 2006/24/EC (Data Retention Directive), http://www.dataretention2010.net/files/Replies_in_to_the_evaluation_questionnaire_of_September_2009/Member_States/reply_fi_en.pdf.

Tabela 2. Organy sprawujące kontrolę nad dostępem do danych telekomunikacyjnych w państwach UE

Sąd	Sąd lub prokurator	Sędzia śledczy lub prokurator	Prokurator	Organ administracyjny	Brak kontroli uprzedniej	Brak organu kontroli zewnętrznej
Bułgaria Czechy[1)] Dania Finlandia Grecja Hiszpania Litwa Luksemburg Niemcy Portugalia Słowenia	Belgia Cypr[2)]	Estonia Holandia	Węgry Włochy[3)]	Francja[4)] Irlandia[5)] Malta[6)] Wielka Brytania	Irlandia Malta Wielka Brytania	Łotwa Polska Słowacja[7)]

1) Art. 88a kodeksu postępowania karnego przewiduje przekazywanie danych dotyczących zrealizowanych połączeń telekomunikacyjnych organom ścigania na podstawie nakazu sądowego w postępowaniu przygotowawczym.
2) *Law on Retention of Telecommunication Data*, L.183 (1)/2007.
3) *Personal Data Protection Code*, Legislative Decree no. 196 dated 30 June 2003.
4) *Code des postes et des communications électroniques* (CPCE).
5) *Communications (Retention of Data) Act 2011*.
6) Udostępnienie danych wymaga zgody sądu, gdy wniosek nie dotyczy konkretnej osoby lub określonej sprawy, zob. http://archive.maltatoday.com.mt/2008/09/10/t1.html.
7) *Act of 19 December 2007 amending the Act No 610/2003 Coll. on Electronic Communications and on Amendments to Certain Acts*.

Spośród 24 państw objętych powyższym zestawieniem, 14 wyłącznie lub częściowo stosuje sądową kontrolę podmiotów uprawnionych do korzystania z informacji o połączeniach telekomunikacyjnych i lokalizacji urządzeń mobilnych abonentów. W kolejnych ośmiu państwach kontrola taka jest sprawowana przez organy systemu wymiaru sprawiedliwości (prokuratorów, sędziów śledczych) albo organy administracyjne.

Wszystkie te rozwiązania są zgodne z europejskimi standardami ochrony praw i wolności obywatelskich[57]. W przypadku prawnie dozwolonej inwigilacji

[57] Por. wyr. ETPC z 2.8.1984 r., *Malone przeciwko Zjednoczonemu Królestwu*, Nr skargi 8691/79.

obywateli przez państwo, standardy te spełnia poddanie organów zaangażowanych w czynności operacyjne lub procesowe kontroli zewnętrznego i niezależnego od nich podmiotu[58]. Oczywiście nie zawsze i wszędzie będzie to równoznaczne z prawidłowym funkcjonowaniem organów kontroli i efektywnym wykonywaniem stawianych im zadań. A *priori* nie oznacza też większej skuteczności sądów niż organów administracyjnych[59]. Jest jednak warunkiem *sine qua non* uruchomienia mechanizmów kontrolnych, których w Polsce nie wprowadzono.

§ 3. Kontrola dostępu do danych telekomunikacyjnych w wybranych państwach Unii Europejskiej

I. Uwaga wstępna

Przedmiotem poniższej analizy jest ustawodawstwo czterech państw członkowskich UE – Francji, Włoch, Wielkiej Brytanii i Republiki Federalnej Niemiec. Państwa te reprezentują odmienne typy tradycji i kultury prawnej, pod wpływem których kształtowały się ich narodowe systemy prawa[60]. Jak się okazuje, czynniki te nie są obojętne dla pewnych rozwiązań prawnych związanych z tematem tego opracowania.

II. Francja

Retencja danych telekomunikacyjnych we Francji została wprowadzona na mocy ustawy o bezpieczeństwie codziennym (*Loi sur la sécurité quotidienne*) w listopadzie 2001 r.[61] Ustawa została uchwalona wkrótce po zamachach terrorystycznych w USA z 11 września i zobowiązywała dostawców dostępu do Internetu do przechowywania przez rok danych o aktywności w sieci swoich usługo-

[58] Por. wyroki ETPC: z 6.9.1978 r. *Klass i inni przeciwko Niemcom*, Nr skargi 5029/71; z 24.4.1990 r., *Huvig i Kruslin przeciwko Francji*, Nr skargi 11801/85; z 16.2.2000 r., *Amman przeciwko Szwajcarii*, Nr skargi 27798/95.

[59] W raporcie Komisji Weneckiej Rady Europy na temat demokratycznej kontroli służb specjalnych zwraca się uwagę na okoliczność, że warunkiem skutecznej kontroli tych służb przez organy sądowe jest odpowiednie przygotowanie merytoryczne sędziów, umożliwiające im wykonywanie zadań w kompetentny sposób. Zob. European Commission for Democracy Through Law (Venice Commission) Report on the democratic oversight of the security services, Strasbourg, 11 June 2007.

[60] Por. *A. Adamski*, *J. Bojarski*, *P. Chrzczonowicz*, *M. Filar*, *P. Girdwoyń*, Prawo karne.

[61] *Loi n°2001-1062 du 15 novembre 2001 relative ŕ la sécurité quotidienne.*

biorców. Ze względu na brak przepisów wykonawczych do ustawy, jej regulacje dotyczące retencji danych przez długi czas pozostawały martwą literą prawa. Dopiero wejście w życie rozporządzenia Ministra Sprawiedliwości z 24.3.2006 r. w sprawie przechowywania danych telekomunikacyjnych[62], którym implementowano do prawa francuskiego dyrektywę 2006/24/WE, radykalnie zmieniło sytuację, umożliwiając stosowanie przepisów retencyjnych zawartych w kilku ustawach.

Dotyczyło to przede wszystkim uchwalonej w styczniu 2006 r. nowej francuskiej ustawy antyterrorystycznej[63], która znacznie rozszerzyła pod względem podmiotowym obowiązek retencji danych, obarczając nim wszystkie podmioty świadczące usługę dostępu do Internetu, w tym właścicieli cyberkawiarni, hoteli i restauracji oraz dostawców sieci bezprzewodowych (WiFi), niezależnie od pobierania z tego tytułu opłat od użytkowników. Ustawa jednocześnie przyznała policji i służbom specjalnym prawo bezpośredniego dostępu do danych gromadzonych przez dostawców usług, bez potrzeby zwracania się w tym celu o zgodę do sądu. Uprawnienie to dotyczyło jednak tylko działań prewencyjnych, podejmowanych w celu zapobiegania terroryzmowi. Nie obejmowało natomiast czynności procesowych związanych z prowadzeniem dochodzeń i ściganiem sprawców przestępstw o charakterze terrorystycznym. W tym zakresie przepis art. 6 ustawy antyterrorystycznej z 23.1.2006 r.[64], który w pierwotnym brzmieniu zezwalał podmiotom uprawnionym na bezpośredni dostęp do danych także w związku z „karaniem aktów terroryzmu" został uznany przez Radę Konstytucyjną Republiki Francji za niezgodny z konstytucją i uchylony[65].

---

[62] *Décret n° 2006-358 du 24 mars 2006 d'application de la loi sur la sécurité quotidienne (LSQ), relatif ŕ la conservation des données de communication.*

[63] *LOI n° 2006-64 du 23 janvier 2006 relative ŕ la lutte contre le terrorisme et portant dispositions diverses relatives ŕ la sécurité et aux contrôles frontaliers, JORF n°20 du 24 janvier 2006 page 1129 texte n° 1.*

[64] Przepis ten został wprowadzony do CPCE jako art. L 34-1-1.

[65] Décision du Conseil constitutionnel n° 2005-532 DC du 19 janvier 2006, Act pertaining to the fight against terrorism and containing various provisions concerning security and border controls, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/2005532DC2005_532dcpdf.

W uzasadnieniu cyt. orzeczenia argumentowano, że poddanie procedurze administracyjnej kwestii wchodzących w zakres kompetencji organów sądowych stanowi naruszenie zasady trójpodziału władzy, jest więc sprzeczne z konstytucją. Źródłem zastrzeżeń był przepis, który kontrolę nad pozyskiwaniem danych od dostawców usług przez upoważnionych do tego funkcjonariuszy policji i żandarmerii powierzał urzędnikowi MSW. Pełnienie tej funkcji przez przedstawiciela władzy wykonawczej w odniesieniu do sfery działań prewencyjnych nie budziło zastrzeżeń na gruncie konstytucyjnym. Pojawiły się one natomiast w odniesieniu do nadzorowania przez niego czynności *de facto* procesowych, związanych z gromadzeniem materiału dowodowego na potrzeby wymiaru sprawiedliwości.

Wspomniana ustawa uregulowała także kwestie proceduralne związane z dostępem do danych przez funkcjonariuszy policji i organów bezpieczeństwa publicznego zajmujących się zwalczaniem terroryzmu.

Uzyskanie dostępu do danych jest kontrolowane jednoosobowo przez *personnalité qualifiée* – wykwalifikowanego urzędnika MSW, którego desygnuje w tym celu (na 3 lata) państwowa komisja kontroli legalności podsłuchów (CNCIS)[66]. Dokonuje ona przy tym wyboru jednego z trzech kandydatów zgłoszonych przez Ministra Spraw Wewnętrznych. Głównym zadaniem *personnalité qualifiée* jest rozpatrywanie wniosków o dostęp do danych składanych przez upoważnionych do tego funkcjonariuszy i podejmowanie stosownych decyzji w tych sprawach. Decyzje te wraz z ich pisemnym uzasadnieniem są przekazywane CNCIS, tam również trafia coroczny raport z działalności urzędnika kontrolującego dostęp do danych[67]. Zawarte w nim informacje, w tym dane statystyczne dotyczące liczby złożonych wniosków oraz sposobu ich załatwienia, są następnie publikowane w raportach z działalności CNCIS[68]. Dostępne dane statystyczne na ten temat przedstawia tabela 3.

Tabela 3. Liczba wniosków o udostępnienie danych telekomunikacyjnych złożonych przez służby specjalne do *personnalité qualifiée* i sposób ich załatwienia (2008–2012)

Rok	Liczba wniosków skierowanych do *personnalité qualifiée*	Wnioski uznane za prawidłowe	Wnioski załatwione odmownie	Wnioski zwrócone wnioskodawcy w celu uzyskania dodatkowych wyjaśnień
2008	38 306	34 911	93	3302
2009	43 559	39 070	30	4459
2010	45 716	38 566	90	–
2011	34 081	31 637	16	–
2012	29 322	26 569	23	–

[66] *Commission nationale de contrôle des interceptions de sécurité* (CNCIS). Komisja została powołana do życia przez ustawę Nr 91-646 z 10.7.1991 r., wkrótce po wydaniu przez ETPC wyroków z 24.4.1990 r., *Huvig i Kruslin przeciwko Francji*, Nr skargi 11801/85. Orzeczenia te były dla Francji niekorzystne w obu sprawach. Ze względu na wadliwą regulację prawną kontroli rozmów telefonicznych Trybunał stwierdził naruszenie art. 8 EKPC.

[67] Art. L 34-1-1 CPCE.

[68] Por. Commission nationale de contrôle des interceptions de sécurité – 18čme rapport d'activité – Année 2009, http://www.ladocumentationfrancaise.fr/rapports-publics/104000489/index.shtml.

W 2009 r. zdecydowana większość wniosków (76%) dotyczyła identyfikacji abonenta lub użytkownika usługi telekomunikacyjnej. Znacznie rzadziej (23%) pytano o połączenia telekomunikacyjne inwigilowanych osób. Znikoma była liczba zapytań o dane geolokacyjne (mniej niż 1% ogólnej liczby wniosków). W raportach CNCIS wskazuje się, że liczba wniosków jest znacznie wyższa od liczby osób, których wnioski te dotyczą (w pojedynczych przypadkach tej samej osoby może dotyczyć nawet 100 zapytań)[69].

Retencja danych telekomunikacyjnych, jako środek ułatwiający ściganie sprawców przestępstw i prowadzenie postępowań karnych przez powołane do tego w Francji organy, jest przedmiotem regulacji głównie przepisów prawa administracyjnego. Podstawowe znaczenie ma w tym zakresie art. L34-1 III wielokrotnie nowelizowanej ustawy – Kodeks pocztowy i komunikacji elektronicznej[70].

„Operatorzy telekomunikacyjni, w szczególności określeni w przepisach (…) powinni usuwać albo anonimizować wszelkie dane związane z przekazami informacji niezwłocznie po ich zakończeniu, zgodnie z przepisami (…)"[71].

„Osoby, które w ramach prowadzonej działalności, oferują publicznie dostępne usługi komunikacji elektronicznej związane z dostępem do sieci, także niezarobkowo, są zobowiązane do przestrzegania przepisów dotyczących operatorów usług komunikacji elektronicznej na zasadach określonych w tym przepisie"[72].

„Dla potrzeb ścigania przestępstw i prowadzenia postępowań karnych oraz w celu zapewnienia uprawnionym do tego organom dostępu do potrzebnych im informacji, określone rodzaje danych technicznych towarzyszących przekazom informacji nie powinny być usuwane lub anonimizowane wcześniej niż po upływie jednego roku od chwili ich powstania (…)"[73].

Przepisy ustaw karnych określających zakres uprawnień i obowiązków organów ścigania i wymiaru sprawiedliwości nie zawierają uregulowań *expressis verbis* odnoszących się do instytucji retencji danych telekomunikacyjnych. Tym niemniej w piśmiennictwie przedmiotu (oraz sprawozdaniu KE) wskazuje się w tym kontekście na art. 60-1 kodeksu postępowania karnego, który uprawnia funkcjonariusza policji sądowej, prokuratora publicznego (art. 77-1-1) oraz sędziego śledczego (art. 99-3) do zwrócenia się do osób fizycznych, w tym reprezentujących przedsiębiorstwa, instytucje albo organizacje prywatne lub publiczne, a tak-

[69] Commission nationale de contrôle des interceptions de sécurité, s. 31.

[70] *Code des postes et des communications électroniques*, dalej jako: CPCE.

[71] W brzmieniu określonym ustawą z 2001 r. o bezpieczeństwie codziennym.

[72] Przepis wprowadzony do art. L34-1 CPCE rozporządzeniem z 24.3.2006 r. w sprawie przechowywania danych telekomunikacyjnych.

[73] Przepis art. L32-3-1 (obecnie L34-1) wprowadzony do CPCE ustawą z 29.11.2001 r. o bezpieczeństwie codziennym.

że organy administracji publicznej z żądaniem wydania wszelkich dokumentów mających znaczenie dla toczącego się postępowania karnego, w tym „pochodzących z komputerów osobistych lub innych systemów przetwarzania danych". Przepis ten ma charakter ogólny i nie różnicuje kategorii danych lub systemów informatycznych, których dotyczy. Jest więc uważany za adekwatną podstawę prawną do żądania wydania danych wszelkiego rodzaju, w tym danych telekomunikacyjnych podlegających reżimowi retencji[74].

Elementy kontroli sądowej nad dostępem organów ścigania do danych informatycznych występują natomiast w przypadku zabezpieczenia dla celów postępowania karnego informacji udostępnianych w Internecie (np. na stronach webowych). Według art. 60-2 kodeksu postępowania karnego, funkcjonariusz policji sądowej, działając na podstawie postanowienia prokuratora rejonowego posiadającego stosowne upoważnienie sędziego wolności i detencji[75], może żądać od operatorów telekomunikacyjnych, w szczególności świadczących usługę dostępu do Internetu lub usługę hostingu, niezwłocznego podjęcia stosownych środków w celu zabezpieczenia – na okres nie dłuższy od roku – informacji dostępnych online, z których korzystają klienci dostawców tych usług. Konstrukcja tego przepisu przypomina jeden z europejskich standardów normatywnych w zakresie ścigania cyberprzestępstw, jakim jest „niezwłoczne zabezpieczenie danych przechowywanych w systemie informatycznym"[76]. Dotyczy bowiem danych, które aktualnie znajdują się w systemie i dzięki ich zabezpieczeniu mają zachować niezmienioną postać po to, by mogły być wykorzystane do celów dowodowych w toczącym się postępowaniu karnym. W odróżnienia od zabezpieczenia danych (ang. *preservation of data*), zatrzymanie danych (ang. *retention of data*) polega na gromadzeniu aktualnie generowanych przez użytkowników i dostawców sieci danych towarzyszących przekazom informacji w celu ich ewentualnego procesowego bądź pozaprocesowego wykorzystania w przyszłości.

Oprócz wymienionych aktów prawnych, retencję danych we Francji przewiduje również ustawa z 21.6.2004 r. o zaufaniu w gospodarce cyfrowej[77]. W tym wypadku chodzi o dane umożliwiające identyfikację dostawców informacji umieszczanych online. Obowiązek retencji tego rodzaju danych przez dostawców dostępu do Internetu oraz usługi hostingu przewiduje art. 6 LCEN, który

[74] *D. Chilstein*, Législation sur la cybercriminalité en France, s. 25.

[75] http://fr.wikipedia.org/wiki/Juge_des_libert%C3%A9s_et_de_la_d%C3%A9tention.

[76] Art. 16 konwencji Rady Europy o cyberprzestępczości – Council of Europe Convention on Cybercirme, Budapest, 21.11.2001 r. (ETS No.185), http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.

[77] *Loi n° 2004-475 du 21 juin 2004 pour la confiance dans l'économie numérique* (JORF, 22 juin 2004), dalej jako: LCEN.

został uzupełniony obszernym rozporządzeniem wykonawczym z 25.2.2011 r.[78] Zawiera ono szczegółowy katalog danych podlegających retencji oraz wyjaśnia pojęcie „*contribution ŕ une création de contenu*", jakim posługuje się ustawa w odniesieniu do czynności internautów określanych jako „udział w kreowaniu treści". Określa też tryb uzyskania dostępu do danych przez funkcjonariuszy policji i poddaje ich postępowanie kontroli administracyjnej na zasadach analogicznych do tych, jakie przewiduje art. L 34-1-1 CPCE (zob. wyżej). Innowacja, jaką przewiduje rozporządzenie z 25.2.2011 r., polega na przeniesieniu obiegu dokumentów (zapytań, zezwoleń, odpowiedzi na zapytania) na platformę elektroniczną Ministerstwa Spraw Wewnętrznych, o której w sensacyjnym tonie pisze francuska prasa[79].

Uprawnienia służb specjalnych do korzystania z danych telekomunikacyjnych zdefiniowano na nowo w 2013 r. Nastąpiło to w drodze nowelizacji przepisów ustawy z 12.3.2012 r. – Kodeks Bezpieczeństwa Wewnętrznego[80] w pozornie niezwiązanym z tą ustawą akcie prawnym[81], na podstawie którego ustanowiono dostęp do danych, dokumentów i informacji „przetwarzanych lub przechowywanych" w sieciach dostawców usług komunikacji elektronicznej. Przepisy KBW[82] wymienią w tym kontekście zarówno „dane techniczne" umożliwiające identyfikację subskrybentów usług, realizowanych połączeń oraz lokalizacji używanych przez nich urządzeń końcowych, jak i „dokumenty i informacje" związane z zakresem kompetencji trzech ministerstw: bezpieczeństwa wewnętrznego, obrony narodowej oraz gospodarki i finansów. W aspekcie przedmiotowym udostępniane dane, informacje i dokumenty powinny mieć znaczenie dla „zapobiegania terroryzmowi oraz przestępczości, w tym zorganizowanej", a także „potencjału naukowego i gospodarczego Francji". Funkcjonariusze służby bezpieczeństwa, którzy posiadają stosowne pełnomocnictwa wspomnianych wyżej ministerstw, mogą żądać w trybie administracyjnym od dostawców usług komunikacji elektronicznej udostępnienia danych, informacji lub dokumentów wskazanych w ustawie. Pisemny wniosek o udostępnienie danych wraz z uzasadnieniem podlega kontroli *personnalité qualifiée* według opisanej wyżej procedury. Natomiast

[78] *Décret n° 2011-219 du 25 février 2011 relatif ŕ la conservation et ŕ la communication des données permettant d'identifier toute personne ayant contribué ŕ la création d'un contenu mis en ligne (JORF n°0050 du 1 mars 2011 page 3643 texte n° 32)*.

[79] LeFigaro, La nouvelle plate-forme d'interception des services de renseignement devrait gérer 20 000 requętes par an. http://www.lefigaro.fr/france/20070528.WWW000000165_lantiterrorisme_espionne_aussi_mails_et_textos.html.

[80] *Code de la Sécurité Intérieure*, dalej jako: KBW, http://www.legifrance.gouv.fr/Droit-francais/Codification/Tables-de-concordance/Code-de-la-securite-interieure.

[81] Ustawa z 18.12.2013 r. o programowaniu wojskowym (*La loi de programmation militaire*).

[82] Por. art. L246-1 do art. L246-3.

gromadzenie informacji i dokumentów w czasie rzeczywistym wymaga pisemnego, merytorycznie uzasadnionego wniosku właściwego rzeczowo ministerstwa i kontrasygnaty premiera rządu. Decyzja premiera jest ważna przez 30 dni i może zostać przedłużona w tym samym trybie o kolejne 30 dni. O wydaniu decyzji zezwalającej na przechwytywanie informacji i dokumentów w czasie rzeczywistym ustawa nakazuje zawiadomić w ciągu 48 godzin przewodniczącego państwowej komisji kontroli legalności podsłuchów (CNCIS). Jeśli Komisja stwierdzi, że decyzja została wydana z naruszeniem przepisów ustawy, powinna zwrócić się do premiera z wnioskiem o jej uchylenie, zawiadamiając o tym jednocześnie ministra-wnioskodawcę oraz ministra odpowiedzialnego za komunikację elektroniczną. Dodatkowym zabezpieczeniem jest możliwość kontrolowania przez CNCIS w czasie rzeczywistym legalności stosowanych przez oficerów służb specjalnych środków inwigilacji. Przepisy KBW przewidują stały dostęp Komisji do urządzeń gromadzących informacje z sieci w ramach omawianej procedury. Ustawa zobowiązuje również Komisję do zgłaszania swoich zastrzeżeń premierowi i wyznacza mu 15-dniowy termin na wprowadzenie odpowiednich środków zaradczych. Omawiane regulacje prawne weszły w życie w dniu 1.1.2015 r.

Wykorzystywanie danych lokalizacyjnych generowanych w czasie rzeczywistym przez telefony komórkowe i nadajniki GPS do celów procesowych w sprawach karnych zostało uregulowane ustawowo. Władza ustawodawcza została do tego zobligowana przez Sąd Kasacyjny, który w dwóch wyrokach wydanych w październiku 2013 r. uznał za absolutnie konieczne w świetle art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności z 4.11.1950 r.[83] wprowadzenie uprzedniej kontroli sądowej wniosków policji o dostęp do danych umożliwiających lokalizację w czasie rzeczywistym użytkowników telefonów komórkowych[84].

Ostatnia ze wskazanych zmian ustawodawczych jest związana z nowelizacją kodeksu postępowania karnego, który w 2014 r. został uzupełniony o rozdział zatytułowany „Geolokacja"[85]. Definicja legalna stosowanego w tym zakresie środka inwigilacji („każde urządzenie techniczne służące do lokalizowania w czasie rzeczywistym na terytorium całego kraju osoby bez jej wiedzy albo pojazdu lub innego przedmiotu bez zgody jego właściciela lub posiadacza" – art. 230-32 kodeksu) obejmuje m.in. telefon komórkowy. Przesłanki wykorzystania funkcji lokalizacyjnych telefonu mobilnego w celu ustalenia aktualnego miejsca po-

[83] Dz.U. z 1993 r. Nr 61, poz. 284 ze zm., dalej jako: EKPC.

[84] Cour de cassation chambre criminelle, Audience publique du mardi 22 octobre 2013, N° de pourvoi: 13-81949, http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000028116556.

[85] Article 1 of the Law supplements section IV of book I of the Code of Criminal Procedure with a chapter V entitled „Geolocation", including Articles 230-32 to 230-44.

bytu jego właściciela lub posiadacza określone zostały w sposób rygorystyczny. Funkcjonariusz policji sądowej, który prowadzi dochodzenie lub śledztwo, może z nich skorzystać, jeżeli spełniony jest warunek „konieczności" i to w odniesieniu do ograniczonej grupy przestępstw. Zaliczono do nich czyny zagrożone karą pozbawienia wolności nie niższą od lat trzech w przypadku przestępstw przeciwko osobie oraz czyny o charakterze terrorystycznym, ponadto czyny zagrożone karą pozbawienia wolności nie niższą od lat pięciu w przypadku śledztw lub dochodzeń mających na celu ustalenie przyczyny śmierci, powodów zaginięcia osoby lub poszukiwania zbiegów – art. 230-33 kodeksu. W zależności od rodzaju przestępstwa, do wyrażenia zgody na stosowanie geolokacji i ewentualne przedłużenie okresu stosowania tego środka może być uprawniony prokurator, sędzia śledczy lub sędzia „wolności i detencji" (juge des libertés et de la détention). Jednorazowo okres poddania tej formie inwigilacji podejrzanego nie może przekraczać 15 dni, jeżeli decyduje o tym prokurator. Nie może być dłuższy od czterech miesięcy, gdy postanowienie w tej sprawie wydaje sędzia „wolności i detencji".

Reasumując powyższe spostrzeżenia i uwagi, należy stwierdzić, że prawo francuskie:

1) nie przewiduje sądowej kontroli dostępu do danych telekomunikacyjnych, o których mowa w art. L 34-1 CPCE, tj. będących przedmiotem retencji zgodnie z przepisami rozporządzenia z 24.3.2006 r. w sprawie przechowywania danych telekomunikacyjnych i dyrektywy 2006/24/WE;
2) przewiduje możliwość procesowego wykorzystania danych telekomunikacyjnych na podstawie art. 60-1 kodeksu postępowania karnego, który funkcjonariuszom policji sądowej, prokuratorom i sędziom śledczym pozwala na uzyskanie danych bezpośrednio od dostawców usług łączności elektronicznej;
3) przewiduje kontrolę uprzednią dostępu do danych w trybie administracyjnym, gdy są one wykorzystywane przez funkcjonariuszy policji i służb specjalnych w ramach czynności operacyjnych związanych z zapobieganiem przestępstwom, w szczególności o charakterze terrorystycznym, a ostatnio również w celu ochrony przed szpiegostwem przemysłowym i gospodarczym;
4) przewiduje szerszy pod względem przedmiotowym i podmiotowym zakres retencji danych transmisyjnych w porównaniu z dyrektywą 2006/24/WE, która w odróżnieniu od ustawodawstwa francuskiego (art. 6 LCEN) nie obejmuje usługi hostingu i danych generowanych przez jej klientów;
5) zostało również wyposażone w mechanizm sądowej kontroli udostępniania danych telekomunikacyjnych umożliwiających policji lokalizację w czasie rzeczywistym osób podejrzanych o popełnienie poważnych przestępstw[86].

[86] Projekt zmian francuskiej procedury karnej w tym zakresie został pozytywnie oceniony przez Radę Konstytucyjną decyzją Nr 2014-693 DC z 25.3.2014 r. Zob. *C. Fonteix*, Le régime