STUDIA PRAWA PUBLICZNEGO
2022 • NR 4 (40) ISSN 2300-3936
DOI: 10.14746/spp.2022.4.40.6

Marcin Rojszczak*

Nieukierunkowana inwigilacja elektroniczna w świetle aktualnego orzecznictwa Europejskiego Trybunału Praw Człowieka

Wprowadzenie**

Trwający od kilkunastu lat dialog sądów europejskich na temat standardów stosowanych w inwigilacji elektronicznej w ostatnim czasie nabrał dynamiki. Stało się tak zarówno na skutek kolejnych, precedensowych rozstrzygnięć Trybunału Sprawiedliwości UE (TSUE) – zwłaszcza dotyczących dopuszczalności stosowania nieukierunkowanych środków retencji danych telekomunikacyjnych[1], jak i kolejnych wyroków Europejskiego Trybunału Praw Człowieka (ETPC) dotyczących oceny proporcjonalności różnych aspektów krajowych przepisów inwigilacyjnych. Nie mniej istotne były również wnioski płynące ze spraw zawisłych przed krajowymi sądami konstytucyjnymi – pozwalające z jednej strony

* Marcin Rojszczak, dr, Politechnika Warszawska, e-mail: marcin.rojszczak@pw.edu.pl, https://orcid.org/0000-0003-2037-4301.

** Autor pragnie pogratulować Pani Prof. Krystynie Wojtczak stworzenia z SPP przyjaznego miejsca publikacji wyników pracy badawczej, które w trwały sposób wpisało się w mapę najciekawszych polskich czasopism prawniczych. Przede wszystkim jednak dziękuję za otwartość i życzliwość, z którą zawsze będę wspominał współpracę z Panią Profesor. Szczerze gratuluję zarówno jubileuszu pracy zawodowej Pani Profesor, jak i 10. rocznicy czasopisma SPP. Niniejszy artykuł powstał jako mój wyraz uhonorowania obu jubileuszy.

[1] E. Celeste, *The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios*, „European Constitutional Law Review" 2019, nr 15(1), s. 134–157; V. Mitsilegas, E. Guild, E. Kuskonmaz, N. Vavoula, *Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks*, „European Law Journal" 2022, s. 1–36.

SPP 3(39), 2022: 111–141. © The Author(s), Adam Mickiewicz University Press, 2022.
Open Access article, distributed under the terms of the CC licence (BY-NC-ND, https://creativecommons.org/licenses/by-nc-nd/4.0/).

ocenić recepcję wyroków sądów europejskich w prawodawstwie krajowym, a z drugiej – wyznaczyć kierunek dalszej ewolucji standardu prawnej regulacji inwigilacji elektronicznej, zwłaszcza w obszarach, które dotychczas znajdowały się poza głównym nurtem analizy[2].

Jednym z dyskutowanych zagadnień jest kwestia dopuszczalności stosowania nieukierunkowanych środków inwigilacyjnych przez organy władzy publicznej. Wdrażanie środków tego typu tradycyjnie łączone jest z realizacją celów bezpieczeństwa narodowego, a więc z działalnością podejmowaną przez służby wywiadu krajowego i zagranicznego[3]. W ten sposób inwigilacja nieukierunkowana niejako utożsamiana jest z hurtowym monitorowaniem łączności elektronicznej i definiowana jako mechanizm, którego stosowanie jest potrzebne (niezbędne) do identyfikowania poważnych zagrożeń dla podstawowych interesów państwa.

Jednak w rzeczywistości, zarówno wiązanie inwigilacji nieukierunkowanej jedynie z monitorowaniem łączności elektronicznej, jak i postrzeganie jej wyłącznie jako środka wykorzystywanego w obszarze bezpieczeństwa narodowego to istotne uproszczenie, którego bezkrytyczne przyjęcie może prowadzić do nadmiernego zawężenia dalszej analizy. Rozwój nowoczesnych form przetwarzania danych umożliwił bowiem opracowanie wielu rozbudowanych systemów algorytmicznych, które dzięki przetwarzaniu olbrzymich baz danych pozwalają na dostarczanie szczegółowych analiz dotyczących jednostki. Nie wykorzystują one w tym celu danych telekomunikacyjnych, jak również nie służą realizacji zadań z obszaru bezpieczeństwa państwa. Mogą natomiast być wykorzystane do analizy danych finansowych i na tej podstawie wykrywania potencjalnych nadużyć podatkowych czy – dzięki analizie materiałów opublikowanych online – wykrywać (i raportować organom ścigania) przypadki dystrybucji treści bezprawnych. Współcześnie systemy posiadające potencjał do masowej inwigilacji nie należą do rozwiązań niszowych, stosowanych w wąskim zakresie przez wysoce wyspecjalizowane agendy, ale znajdują coraz szersze zastosowanie w instrumentarium organów publicznych – także państw demokratycznych.

---

[2] Szerzej na ten temat: *European constitutional courts towards data retention laws*, pod red. M. Zubika, J. Podkowika, R. Rybskiego, Cham 2021.

[3] W tym kontekście pod pojęciem „służba wywiadu zagranicznego" należy rozumieć organ państwa uprawniony do prowadzenia zadań wywiadowczych poza granicami państwa macierzystego; terminu tego nie należy zatem mylić ze służbami obcego wywiadu.

W efekcie rozstrzygnięcie wątpliwości dotyczących konieczności i proporcjonalności stosowania tego typu środków to kluczowe zagadnienie, wyznaczające oś dalszej dyskusji na temat celów, które mogą uzasadniać ich stosowanie, oraz koniecznych zabezpieczeń prawnych, które należy wprowadzić w celu minimalizacji ryzyka nadużycia władzy[4].

ETPC w swoim orzecznictwie wielokrotnie zajmował się problemem zgodności krajowych programów inwigilacyjnych z Konwencją o ochronie praw człowieka i podstawowych wolności (EKPC)[5]. W tym zakresie wypracował także własny test, wykorzystywany przez lata do oceny badanych regulacji krajowych. W rzeczywistości jednak zdecydowana większość spraw, zawisłych przed Trybunałem do końca pierwszej dekady XXI wieku dotyczyła przypadków inwigilacji ukierunkowanej, związanych głównie z działaniami podejmowanymi w obszarze walki z przestępczością. Trybunał w swoim orzecznictwie bardzo szczątkowo odnosił się do przypadków stosowania inwigilacji nieukierunkowanej, a nawet gdy to robił – nie wprowadzał szczegółowych kryteriów pozwalających na wypracowanie bardziej ogólnego standardu kontroli tego typu programów.

Dopiero dynamiczny rozwój zdolności inwigilacyjnych państw, który z jednej strony można łączyć ze wzrostem zagrożeń terrorystycznych, a z drugiej z upowszechnieniem się nowych środków technicznych pozwalających na masowe i hurtowe przetwarzanie danych, skutkował wniesieniem do ETPC skarg wprost zmierzających do zakwestionowania legalności prawnych podstaw prowadzenia programów masowej inwigilacji. Pierwsza z tego typu spraw, w której skarżącymi było dziesięć organizacji pozarządowych, koncentrowała się w dużej mierze na programie TEMPORA, prowadzonym od lat przez brytyjską służbę

[4] Stąd też w piśmiennictwie coraz częściej dyskutowane są nowe propozycje w zakresie oceny proporcjonalności środków inwigilacyjnych – zob. np. J. Milaj, *Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance*, „International Review of Law, Computers & Technology" 2016, nr 30(3), s. 115–130.

[5] Należy pamiętać, że Trybunał obecnie bada także skargi dotyczące polskich przepisów inwigilacyjnych – w których skarżący kwestionują zbyt szerokie uprawnienia organów publicznych, mogące również prowadzić do rejestrowania łączności objętej tajemnicą zawodową. Jak wskazują skarżący, osoby wobec których zastosowano rozbudowane środki inwigilacyjne, pozbawione są przy tym skutecznych narzędzi sądowej ochrony swoich praw. Zob. *Pietrzak v. Polska* (72038/17) oraz *Bychawska-Siniarska i in. v. Polska* (25237/18).

wywiadu elektronicznego – Government Communications Headquarters (GCHQ)[6]. Z kolei w postępowaniu zainicjowanym przez Centrum för rättvisa Trybunał ocenił szwedzkie ramy inwigilacyjne, wykorzystywane przez wojskową agencję wywiadu elektronicznego – Försvarets radioanstalt (FRA)[7]. Chociaż obie sprawy łączyło szereg podobieństw, to jednak były one także istotnie różne. Przyczyną było zarówno odmienne podejście prawodawcy krajowego do limitowania uprawnień inwigilacyjnych służb wywiadowczych, jak i różne cele, dla których stosowano (w rzeczywistości podobne) środki inwigilacyjne.

W obu sprawach – finalnie rozstrzygniętych przez Wielką Izbę – Trybunał wprost odniósł się do kwestii dopuszczalności i granic stosowania nieukierunkowanych form inwigilacji. Uwzględniając pozycję prawną Konwencji w europejskim modelu ochrony praw człowieka, a także jej wpływ na prawo unijne, należy oczekiwać, że w następnych latach tezy przedstawione w obu wyrokach będą wyznaczały kierunek interpretacyjny dla krajowych sądów konstytucyjnych.

W tle wyroków *Big Brother Watch* oraz *Centrum för rättvisa* ETPC rozstrzygnął inną, nie mniej ciekawą sprawę – dotyczącą wprost zgodności z Konwencją uogólnionych form retencji danych telekomunikacyjnych. Zagadnienie to, jako blisko związane z prawem UE, było wcześniej przedmiotem bardzo szczegółowego orzecznictwa ze strony TSUE[8]. Wydanym w 2022 r. wyrokiem w sprawie *Ekimdzhiev i in. v. Bułgaria*[9] ETPC kompleksowo odniósł się do tego zagadnienia, niejako przy okazji potwierdzając swoje wcześniejsze stanowisko dotyczące stosowania środków inwigilacji elektronicznej.

Celem niniejszego artykułu jest przybliżenie ewolucji standardu ETPC dotyczącego inwigilacji elektronicznej, w szczególności jej

---

[6] Wyrok ETPC (Wielka Izba) z 25 V 2021 r. w sprawie *Big Brother Watch i in. v. Wielka Brytania*, 58170/13, 62322/14 i 24960/15. W niniejszym artykule omawiane są obydwa wyroki zapadłe w tej sprawie – wydane zarówno przez Izbę, jak i Wielką Izbę. Aby uniknąć niejednoznaczności, wszelkie odniesienia do wyroku Izby będą zawsze zawierały odpowiednią wzmiankę. W pozostałych przypadkach przypisy będą kierowały do wyroku Wielkiej Izby.

[7] Wyrok ETPC (Wielka Izba) z 25 V 2021 r. w sprawie *Centrum för rättvisa v. Szwecja*, 35252/08, pkt 365.

[8] Zob. np. B. Grabowska-Moroz, *Ochrona gromadzonych danych telekomunikacyjnych i zasady ich udostępniania na tle Konstytucji RP i prawa Unii Europejskiej*, „Europejski Przegląd Sądowy" 2016, nr 1, s. 31–36; A. Grzelak, *Trybunał Sprawiedliwości ponownie o relacji między koniecznością zwalczania przestępczości a prawem do prywatności*, „Europejski Przegląd Sądowy" 2017, nr 3, s. 31–36.

[9] Wyrok ETPC z 11 I 2022 r. w sprawie *Ekimdzhiev i in. v. Bułgaria*, 70078/12.

nieukierunkowanych form. W tym zakresie przedstawiany tekst należy traktować jako kontynuację – niejako *post scriptum* – wcześniejszej publikacji, przedstawionej ponad pięć lat temu także na łamach „Studiów Prawa Publicznego"[10]. Obecny artykuł ma jednak nie tylko zrekapitulować tezy, przedstawione w najnowszym orzecznictwie, lecz również sprowokować dalszą dyskusję na temat trafności stanowiska Trybunału przedstawionego w odniesieniu do najważniejszych zagadnień prawnych dotyczących stosowania masowej inwigilacji. W zamierzeniu autora w ten sposób możliwe będzie przybliżenie odpowiedzi na pytanie, czy obecny standard wyznaczony przez ETPC można uznać za wystarczający dla ochrony przed zagrożeniami związanymi z upowszechnianiem nowoczesnych środków inwigilacyjnych i ich coraz szerszym stosowaniem przez organy władzy publicznej.

1. Ewolucja standardu orzeczniczego

Wyznaczenie granic dopuszczalnej ingerencji w prawa jednostki za pomocą środków inwigilacyjnych to zagadnienie nierozerwalnie związane z europejskim modelem ochrony praw człowieka[11]. W istocie jednym z celów jego ustanowienia była właśnie ochrona przed nadużyciami ze strony organów władzy publicznej, które w dalszej perspektywie mogłyby prowadzić do powstania niedemokratycznych form rządów. W tym zakresie ochrona prywatności – rozumiana także jako zakaz swobodnego gromadzenia danych nadmiarowych przez państwo jest jednym z filarów porządku konstytucyjnego państw europejskich, ale i gwarancją *explicite* wynikającą z EKPC.

Nie dziwi zatem, że do ETPC stosunkowo szybko zaczęły być kierowane skargi, w których kwestionowano dopuszczalność stosowania krajowych przepisów inwigilacyjnych. Jednym z fundamentalnych orzeczeń, zapadłych jeszcze przed upowszechnieniem się możliwości prowadzenia inwigilacji elektronicznej na dużą skalę, była sprawa *Klass i in. v. Niemcy*[12]. Sprawa ta dotyczyła przypadków inwigilacji prowadzonej w ramach procedury karnej. Jej wyjaśnienie w pierwszej kolejności

[10] M. Rojszczak, *Prawne podstawy prowadzenia masowej inwigilacji obywateli opartej na hurtowym i nieukierunkowanym przechwytywaniu danych w UE z uwzględnieniem dorobku orzeczniczego TSUE i ETPC*, „Studia Prawa Publicznego" 2017, nr 2(18), s. 159–187.

[11] P. Bernal, *Data gathering, surveillance and human rights: recasting the debate*, „Journal of Cyber Policy" 2016, nr 1(2), s. 243–264.

[12] Wyrok ETPC z 6 IX 1978 r. w sprawie *Klass i in. v. Niemcy*, 5029/71.

wymagało potwierdzenia istnienia interesu prawnego skarżących w sytuacji braku możliwości wykazania przez nich objęcia ich kwestionowanymi środkami inwigilacyjnymi. W badanej sprawie niemiecki rząd federalny złożył oświadczenie, że wobec żadnego z wnioskujących nigdy nie wdrożono działań na podstawie skarżonej ustawy, określającej zasady stosowania środków inwigilacyjnych. Na tej podstawie władze dowodziły, że nie można mówić o naruszeniu praw, a więc skarga powinna być oddalona z uwagi na brak interesu prawnego w jej wniesieniu. Zaakceptowanie takiego stanowiska prowadziłoby zatem do uniemożliwienia sądowej ochrony praw tylko z tego powodu, że osoby pokrzywdzone nie mogłyby wykazać faktycznego zakresu niejawnych działań podejmowanych przez organy państwa. Trybunał sprzeciwił się takiej wykładni, wskazując, że jeżeli krajowe prawodawstwo tworzące ramy dla stosowania inwigilacji nie będzie zgodne z gwarancjami wynikającymi z Konwencji, to – co oczywiste – stosowanie tych przepisów (prowadzące do objęcia inwigilacją konkretnych osób) także będzie obarczone tą samą wadą.

W ten sposób w wyroku *Klass i in. v. Niemcy* Trybunał przesądził, że w zakresie jego kognicji (wynikającej z art. 34 EKPC) znajduje się badanie skarg wnoszonych na krajowe przepisy inwigilacyjne, jeżeli tylko skarżący są objęci zakresem ich stosowania – a więc potencjalnie mogą być podmiotami inwigilacji prowadzonej na ich podstawie. Ta teza była wielokrotnie powtarzana w późniejszym orzecznictwie[13], w tym także w sprawach dotyczących stosowania środków nieukierunkowanych[14]. W praktyce ten – wydany w 1978 r. – wyrok istotnie wpłynął na dalszą ewolucję europejskiego modelu prawnej regulacji działań inwigilacyjnych, potwierdzając możliwość sądowej kontroli działań państwa także w obszarach tradycyjnie łączonych z bezpieczeństwem narodowym. Dość powiedzieć, że brak analogicznej wykładni ze strony amerykańskich sądów federalnych – włączając w to Sąd Najwyższy – jest do dzisiaj istotną przeszkodą dla zbadania konstytucyjności prowadzonych przez tamtejsze służby rozbudowanych programów inwigilacyjnych.

[13] Zob. także omówienie ewolucji stanowiska sądu dotyczącego możliwości skarżenia przepisów *in abstracto* przedstawione w wyroku ETPC z 6 IX 1978 r. w sprawie *Roman Zakharov v. Rosja*, 47143/06, pkt 166–169.

[14] Zob. np. wyrok ETPC z 18 V 2010 r. w sprawie *Kennedy i in. v. Wielka Brytania*, 26839/05.

Jednak pierwszym wyrokiem, w którym ETPC wprost został skonfrontowany z potrzebą oceny dopuszczalności działań prowadzonych w ramach inwigilacji nieukierunkowanej, była rozstrzygana dopiero trzydzieści lat później sprawa *Weber i Saravia v. Niemcy*[15]. Jej kanwą był tzw. program kontroli strategicznej (ang. *strategic monitoring*)[16], polegający na przechwytywaniu (podsłuchiwaniu) łączności telekomunikacyjnej realizowanej pomiędzy abonentami z Niemiec a abonentami z wybranych krajów trzecich. Chociaż program ten – także dzisiaj – kwalifikowany jest jako typ inwigilacji nieukierunkowanej, to w praktyce łączył cechy inwigilacji masowej oraz ukierunkowanej. Kontrola strategiczna była środkiem pośrednim pomiędzy tradycyjnymi programami wywiadowczymi, prowadzonymi w czasach zimnowojennych a powstałymi później programami służącymi identyfikacji zagrożeń zewnętrznych. Okoliczność ta jest często pomijana w dyskusjach nad trafnością zapadłego przed Trybunałem rozstrzygnięcia, co prowadzi do utraty z pola widzenia istotnego kontekstu badanej sprawy. Inwigilacja strategiczna nie mogła służyć do monitorowania ruchu wyłącznie krajowego, a także komunikacji niezwiązanej z konkretnym, określonym państwem trzecim. Należy o tym pamiętać, badając kluczową tezę wyroku *Weber i Saravia*, w której Trybunał nie zakwestionował dopuszczalności prowadzenia hurtowego monitorowania łączności, wskazując przy tym na niezbędność tego środka dla identyfikacji niektórych szczególnie poważnych zagrożeń dla bezpieczeństwa publicznego (w tym handlu bronią)[17]. Stanowisko Trybunału wyrażone w tej sprawie przez wiele lat było wskazywane przez zwolenników stosowania środków nieukierunkowanych jako dowód na zgodność tego typu działań z konwencyjnym modelem ochrony praw podstawowych.

Oceniając niemieckie prawodawstwo, Trybunał zrekapitulował także swój – zdefiniowany po raz pierwszy w sprawie *Huvig*[18] – standard zabezpieczeń prawnych, których ustanowienie powinno towarzyszyć stosowaniu niejawnych programów inwigilacyjnych. W szczególności w ocenie Trybunału przepisy ustawowe powinny: (i) zawierać wskazanie

[15] Postanowienie ETPC z 29 VI 2006 r. w sprawie *Weber i Saravia v. Niemcy*, 54934/00.

[16] Terminu tego nie należy mylić z pojęciem „wywiadu strategicznego" (ang. *strategic intelligence*), także stosowanego w naukach o bezpieczeństwie. Zob. A. Barnea, *Strategic intelligence: a concentrated and diffused intelligence model*, „Intelligence and National Security" 2020, nr 35(5), s. 701–716.

[17] *Weber i Saravia*, pkt 109.

[18] Wyrok ETPC z 24 IV 1990 r. w sprawie *Huvig v. Francja*, 11105/84.

typów przestępstw, które mogą wiązać się z zastosowaniem środków inwigilacyjnych; (ii) definiować kategorię osób, które mogą być poddane inwigilacji; (iii) wskazywać czas trwania monitorowania łączności; (iv) określać zasady stosowane przy analizie, przechowywaniu i dalszym wykorzystywaniu zgromadzonych informacji; (v) wprowadzać środki ostrożności, jakie należy podjąć przy przekazywaniu danych innym stronom; oraz (vi) warunki, po spełnieniu których przechwycone dane należy zniszczyć[19].

Co ciekawe, początkowo Trybunał uznawał, że standard ten nie musi być stosowany we wszystkich przypadkach, a jedynie tych, w których zastosowane środki prowadzą do szczególnej dotkliwości dla jednostki. Z tego powodu w sprawie *Uzun* Trybunał uznał że monitorowanie geolokalizacji jednostki nie prowadzi do naruszenia prywatności w stopniu porównywalnym do przechwytywania łączności, stąd też zaakceptował stan, w którym prawo krajowe nie uwzględnia wszystkich opisanych wcześniej zabezpieczeń prawnych[20]. W konsekwencji, po wydaniu wyroku *Uzun* w dorobku prawnym ETPC funkcjonowały *de facto* dwa standardy zabezpieczeń prawnych, stosowane w zakresie inwigilacji elektronicznej – w wersji pełnej (*Huvig*, później *Weber*) oraz uproszczonej (*Uzun*)[21].

Chociaż standard *Huvig* wydawał się wystarczający dla regulacji programów inwigilacji ukierunkowanej, w szczególności realizowanych w ramach procedury karnej, to wraz z rozwojem możliwości technicznych jasne stało się, że nie jest on adekwatny do ograniczenia ryzyka związanego ze stosowaniem nowoczesnych środków nieukierunkowanych. Co więcej, sam Trybunał w sprawie *Mustafa Sezgin Tanrıkulu* dostrzegł zagrożenia związane z wykorzystaniem niewystarczająco precyzyjnych uprawnień ustawowych, które stworzone dla realizacji kontroli ukierunkowanej mogą być wykorzystane do przeprowadzonej inwigilacji masowej[22]. W tym wypadku bardziej trafnym terminem byłaby jednak *inwigilacja blankietowa* – a więc taka, w której ustawodawca stworzył bardzo ogólne ramy pozostawiające

[19] *Weber i Saravia*, pkt 95.

[20] Wyrok ETPC z 2 IX 2010 r. w sprawie *Uzun v. Niemcy*, 35623/05, pkt 52.

[21] G. Malgieri, P. De Hert, *European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards „Good Enough" Oversight, Preferably but Not Necessarily by Judges*, w: *The Cambridge Handbook of Surveillance Law*, pod red. D.C. Graya, S.E. Hendersona, Cambridge 2017, s. 509–532.

[22] Wyrok ETPC z 18 VII 2017 r. w sprawie *Mustafa Sezgin Tanrıkulu v. Turcja*, 27473/06, pkt 51–60.

zbyt szeroki margines uznania w stosowaniu inwigilacji organom władzy publicznej.

Dostrzegając zagrożenia związane z programami nieukierunkowanymi, Trybunał w najnowszym orzecznictwie rozszerzył klasyczny test *Weber*, wskazując na potrzebę zredefiniowania niektórych wymagań oraz wprowadzenia dodatkowych – zapewniających adekwatną ochronę jednostki. W ten sposób w wyroku *Big Brother Watch* ETPC uznał, że prawodawstwo krajowe tworzące ramy dla wykorzystania środków nieukierunkowanych powinno – poza wymaganiami wskazanymi w sprawie *Weber* – dodatkowo wskazywać procedury autoryzacji środków nieukierunkowanych oraz zasady sprawowania nadzoru przez niezależny organ, pozwalające na zapewnienie zgodności z prawem prowadzonych działań inwigilacyjnych oraz skuteczne reagowanie w przypadku zidentyfikowania nadużyć[23]. Co więcej, Trybunał podkreślił również potrzebę ustanowienia mechanizmów kontroli *ex post*, ukierunkowanych na potwierdzanie, że niezależny nadzór funkcjonuje prawidłowo i prowadzi do podejmowania skutecznych działań w przypadku wykrytych nadużyć.

O ile zatem klasyczny test *Huvig* koncentrował się na ograniczaniu ryzyk związanych z prowadzeniem inwigilacji ukierunkowanej, o tyle standard przedstawiony w sprawie *Big Brother Watch* wprost odnosi się do programów nieukierunkowanych. Co warte podkreślenia, zasadnicza zmiana uwzględniona przez Trybunał nie dotyczy zabezpieczeń związanych z zakresem czy dopuszczalnymi formami gromadzenia danych, ale z kompleksowym charakterem ustanowionych mechanizmów nadzorczych – mających zapobiegać nadużyciom związanym z arbitralnością podejmowanych decyzji. Trybunał tym samym potwierdził, że co do zasady inwigilacja nieukierunkowana nie wykracza poza to, co można uznać za niezbędne dla ochrony celów działania państwa demokratycznego[24]. Jednocześnie jednak zdefiniował szczegółową listę zabezpieczeń, których uwzględnienie może stanowić wyzwanie, jeśli weźmie się pod uwagę specyfikę programów nieukierunkowanych[25].

---

[23] Wyrok ETPC (Wielka Izba) z 25 V 2021 r. w sprawie *Big Brother Watch i in. v. Wielka Brytania*, 58170/13, 62322/14 i 24960/15, pkt 361.

[24] *Big Brother Watch*, pkt 347.

[25] M. Zalnieriute, *Procedural Fetishism and Mass Surveillance under the ECHR*, „Verfassungsblog" (2 VI 2021), https://verfassungsblog.de/big-b-v-uk/ (dostęp: 7 IX 2022).

2. Otwarte problemy prawne

2.1. Cele stosowania środków nieukierunkowanych

Już we wczesnym orzecznictwie ETPC potwierdził możliwość stosowania przez organy publiczne środków tajnej obserwacji dla realizacji prawnie usprawiedliwionych celów wskazanych w Artykule 8(2) Konwencji. Nie ulegało wątpliwości, że niejawne gromadzenie danych może być środkiem nie tylko potrzebnym, lecz także koniecznym do walki z poważną przestępczością[26]. Trybunał wskazywał przy tym, że zakres wdrażanych środków powinien zależeć zarówno od celu ich stosowania, jak i charakteru ingerencji, z jaką wiąże się ich użycie. Ten klasyczny element testu proporcjonalności został jednak istotnie doprecyzowany w przypadku realizacji celów bezpieczeństwa narodowego. W takim bowiem przypadku, jak wskazano już w sprawie *Klass i in. v. Niemcy*, państwa posiadają szczególnie szeroki margines uznania (ang. *fairly wide margin of appreciation*[27]), prowadzący do możliwości wdrożenia potrzebnych w ocenie rządzących środków służących ochronie najważniejszych funkcji państwa. Trybunał w ten sposób odniósł się zatem wyłącznie do możliwości wykorzystania inwigilacji nieukierunkowanej dla realizacji celów bezpieczeństwa narodowego.

Ścisły związek z bezpieczeństwem narodowym był dostrzegalny we wszystkich sprawach, w których Trybunał podejmował kwestię oceny dopuszczalności stosowania programów nieukierunkowanych. Korzystając z argumentacji przedstawionej w sprawie *Weber* (zob. wcześniejsze uwagi na temat monitoringu strategicznego), w wyroku *Liberty i inni v. Wielka Brytania*, uznał, że ocena wynikającego z treści Konwencji testu „zgodności z prawem" wdrażanych środków nieukierunkowanych, w szczególności ich dostępności oraz przewidywalności, powinna bazować na tych samych kryteriach, które zostały wcześniej zdefiniowane dla programów ukierunkowanych[28]. Opierając się na tej obserwacji, wskazał, że programy nieukierunkowane muszą być prowadzone na podstawie czytelnych przepisów ustawowych, według kryteriów i zasad podlegających zewnętrznej ocenie (zapewniającej przewidywalność) oraz ochronę przed ryzykiem nadużyć. Przewidywalność (ang. *foreseeability*) w tym kontekście nie oznacza oczywiście wiedzy osób

[26] Wyrok ETPC z 2 VIII 1984 r. w sprawie *Malone v. Wielka Brytania*, 8691/79, pkt 81.
[27] *Klass i in. v. Niemcy*, pkt 49.
[28] Wyrok ETPC z 1 VII 2008 r. w sprawie *Liberty i in. v. Wielka Brytania*, 58243/00, pkt 63.

inwigilowanych o fakcie prowadzenia obserwacji, a możliwości zrozumienia przez jednostkę konsekwencji, jakie mogą wiązać się z podejmowaniem przez nią określonych aktywności[29]. Sprawa *Liberty* to także pierwszy przypadek, w którym Trybunał wskazał na niedopuszczalność stosowania uogólnionych form inwigilacji i to z uwagi na ich blankietowy charakter – utrudniający (lub uniemożliwiający) powiązanie podejmowanych działań z faktycznymi potrzebami w obszarze bezpieczeństwa narodowego[30].

Również w najnowszym orzecznictwie Trybunał potwierdził, że stosowanie środków nieukierunkowanych *per se* nie prowadzi do naruszenia Konwencji. Jednocześnie jednak, jak się wydaje, nieco zniuansował swoje wcześniejsze stanowisko, wskazując na zmiany społeczne i gospodarcze, jakie miały miejsce od czasu rozstrzygnięcia spraw *Weber* i *Liberty*. W szczególności podkreślił znaczenie dynamicznego wzrostu aktywności online podejmowanych przez użytkowników oraz olbrzymi zakres informacji, jaki może być w związku z tym gromadzony na ich temat. Na tej podstawie uznał, że stosowanie środków nieukierunkowanych może prowadzić do zagrożeń dla praw jednostek daleko wykraczających poza niebezpieczeństwa dostrzegane dekadę wcześniej.

Powyższe nie doprowadziło jednak do zakwestionowania możliwości stosowania tego typu środków dla realizacji celów bezpieczeństwa państwa. Co więcej, w wyroku *Centrum för rättvisa* Trybunału uznał masową inwigilację jako środek mający kluczowe znaczenie w identyfikacji zagrożeń dla bezpieczeństwa narodowego[31]. Idąc dalej, wskazał również, że „[o]becnie, nie istnieje żaden alternatywny środek […] który mógłby zastąpić masowe przechwytywanie łączności".

Abstrahując od źródeł przekonania Trybunału na temat skuteczności masowej inwigilacji[32], przedstawione tezy wymagają szerszego omówienia. Po pierwsze, zarówno w sprawach *Big Brother Watch*, jak i *Centrum för rättvisa* Trybunał *explicite* odnosił się do uprawnień służb wywiadowczych dotyczących hurtowego (ang. *bulk*) podsłuchiwania (i przetwarzania) łączności elektronicznej. Nie kwestionowano przy tym, że wykorzystanie tych uprawnień służy realizacji celów bezpieczeństwa państwa: zarówno GCHQ jak i FRA realizują działania wprost związane

[29] Wyrok ETPC z 26 III 1987 r. w sprawie *Leander v. Szwecja*, 9248/81, pkt 81.

[30] *Liberty i in. v. Wielka Brytania*, pkt 69.

[31] Wyrok ETPC (Wielka Izba) z 25 V 2021 r. w sprawie *Centrum för rättvisa v. Szwecja*, 35252/08, pkt 365.

[32] Ibidem. Por. także zbliżoną argumentację w wyroku *Big Brother Watch*, pkt 386.

z obronnością. Obie agencje historycznie powstały w strukturach sił zbrojnych, nie posiadają uprawnień śledczych oraz nie prowadzą postępowań karnych.

Obserwacja ta prowadzi do pytania: czy stanowisko Trybunału, akceptujące możliwość korzystania ze środków nieograniczonych w obszarze bezpieczeństwa państwa, należy interpretować w sposób ścisły? Zatem, czy w ocenie Trybunału dopuszczalność wykorzystania tego typu środków wynika wyłącznie ze szczególnego (szerokiego) marginesu uznania, z którego korzystają państwa w obszarze bezpieczeństwa narodowego, czy może decyzja o wdrożeniu nieograniczonych form inwigilacji może być podjęta w odniesieniu do każdego uznanego celu działalności państwa wskazanego w art. 8(2) EKPC? W rzeczywistości jest to pytanie o dopuszczalność skorzystania ze środków nieukierunkowanych w zakresie walki z przestępczością. Od lat zwolennicy stosowania tego typu programów dowodzili ich przydatności (czy wręcz: niezbędności) dla potrzeb identyfikacji poważnych przestępstw kryminalnych. Trybunał dotąd nie zajął jednak czytelnego stanowiska w tym zakresie. Ograniczył się do wskazania, że „Konwencja nie zabrania stosowania masowego przechwytywania w celu ochrony bezpieczeństwa narodowego i innych podstawowych interesów narodowych przed poważnymi zagrożeniami zewnętrznymi"[33]. Odniesienie do *zagrożeń zewnętrznych* przemawia za wąską interpretacją dopuszczalnego celu stosowania nieukierunkowanej inwigilacji. Taka wykładnia byłaby również zgodna z najnowszym orzecznictwem TSUE, zgodnie z którym realizacja celów bezpieczeństwa państwa wykracza poza pozostałe prawnie uzasadnione obszary działania władz publicznych i w efekcie może uzasadniać stosowanie środków bardziej ingerujących w prawa jednostki[34].

Pośrednie potwierdzenie trafności powyższych rozważań można odnaleźć w niedawnym wyroku wydanym w sprawie *Ekimdzhiev i in. v. Bułgaria*, w którym Trybunał wskazał na wadliwość bułgarskich przepisów inwigilacyjnych między innymi z uwagi na użycie w nich nieprecyzyjnej definicji „obiektu" inwigilacji. Termin ten wykorzystywany był do określenia zakresu inwigilacji w przypadkach, gdy tożsamość osób, które miały zostać poddane kontroli, pozostawała nieznana. Trybunał zwrócił jednak uwagę, że zbyt dowolne definiowanie „obiektu" inwigilacji może prowadzić do nadużycia uprawnień poprzez zbudowanie

[33] *Big Brother Watch*, pkt 347.

[34] Wyrok TSUE z 6 X 2020 r. w sprawie *La Quadrature du Net*, C-511/18, C-512/18 i C-520/18, pkt 137.

w oparciu o model inwigilacji ukierunkowanej mechanizmu pozwalającego na masowe gromadzenie danych.

Wydaje się, że powyższa argumentacja to jednak za mało dla potwierdzenia hipotezy o dopuszczalności stosowania nieukierunkowanych środków, ale tylko w zakresie realizacji celów bezpieczeństwa narodowego. Co więcej, nie pozwala ona także rozstrzygnąć szeregu dalszych wątpliwości. Przede wszystkim nie jest jasne, dlaczego Trybunał odniósł się *explicite* tylko do zagrożeń zewnętrznych. W naukach o bezpieczeństwie podział na zagrożenia zewnętrzne i wewnętrzne jest coraz trudniej definiowalny. Terroryzm jest przykładem poważnego zagrożenia dla bezpieczeństwa publicznego, które chociaż jest często inspirowane zewnętrznie, w większości przypadków posiada także wyraźny łącznik wewnętrzny. Idąc dalej, kryterium rozstrzygającym dla klasyfikacji zagrożeń na zewnętrzne i wewnętrzne nie może być lokalizacja komunikujących się użytkowników. O ile zapoczątkowany kilkadziesiąt lat temu niemiecki program kontroli strategicznej mógł bazować na tym selektorze dla wyboru zakresu przechwytywanej łączności (monitorowano wyłącznie łączność międzynarodową nawiązywaną z wybranymi krajami trzecimi), o tyle doświadczenia z prowadzonych dekadę później amerykańskich programów wywiadowczych wskazywały, że nawet przechwytując wyłącznie komunikację zawierającą łącznik zagraniczny, gromadzona jest także zauważalna ilość komunikacji *stricte* krajowej[35]. Problem gromadzenia tzw. przypadkowo gromadzonych danych (ang. *about collection*) – polegający na pośrednim rejestrowaniu dużej ilości komunikacji krajowej – był bardzo szeroko dyskutowany po ujawnieniu przez E. Snowdena szczegółów amerykańskich programów inwigilacyjnych i *de facto* prowadził do wniosku o braku możliwości ograniczenia zakresu gromadzonych danych wyłącznie na podstawie kryteriów geograficznych[36]. Powyższe wskazuje, że wprowadzone kryterium „zagrożeń zewnętrznych" nie pozwala na skuteczne ograniczenie zakresu danych gromadzonych przez służby specjalne w ramach programów nieukierunkowanych[37].

[35] N.S. Guliani, *The Government Is 'Incidentally' Sucking Up Tens of Millions of Americans' Communications a Year, and It's a Privacy Nightmare*, American Civil Liberties Union (23 III 2017), https://cli.re/xabKxA (dostęp: 7 IX 2022).

[36] W.C. Banks, *Next Generation Foreign Intelligence Surveillance Law: Renewing 702*, „University of Richmond Law Review" 2017, nr 51(3), s. 671–703.

[37] Ponieważ w Stanach Zjednoczonych programy nieukierunkowane prowadzone są bez uprzedniej zgody sądu karnego, w praktyce powstaje problem dotyczący możliwości przedstawienia zgromadzonych w ten sposób dowodów w sprawach karnych. Co do

W szerszym ujęciu należy pamiętać, że Trybunał, mówiąc o możliwości stosowania masowej inwigilacji, w istocie nie ustanawia *a priori* zakazu jej stosowania. Nie przesądza także, że każda jej forma będzie finalnie uznana za dopuszczalną. Dość powiedzieć, że zarówno w sprawie *Big Brother Watch*, jak i *Centrum för rättvisa* Trybunał uznał naruszenie gwarancji konwencyjnych. Oznacza to, że chociaż pogląd Trybunału o przydatności masowej inwigilacji nie zmienił się na przestrzeni lat, to istotnej zmianie uległ standard zabezpieczeń prawnych, jaki powinien towarzyszyć decyzji o zastosowaniu tego typu środków. Wynika z tego, że w przypadku standardu ETPC wnioskowanie na temat dopuszczalności stosowania nieograniczonej inwigilacji musi uwzględniać kontekst badanych przepisów, a próby budowania ogólnych wniosków o zgodności tej formy nadzoru z EKPC mają charakter wysoce spekulatywny.

Brak jasnej wykładni ze strony Trybunału niestety uniemożliwia ustalenie, czy poszanowanie gwarancji wynikających z Konwencji stoi na przeszkodzie stosowaniu przez organy publiczne nieograniczonych form inwigilacji także dla realizacji innych zadań, niezwiązanych z bezpieczeństwem narodowym. Nie jest także jasne, czy dopuszczalne jest stosowanie środków zakładających niezróżnicowane i hurtowe gromadzenie informacji w celu monitorowania zdarzeń o czysto wewnętrznym charakterze. Istnieje cała mozaika zastosowań środków posiadających potencjał inwigilacyjnych, których nie sposób w efekcie ocenić pod kątem zgodności z Konwencją z uwagi na zbyt kazuistyczny standard ETPC, koncentrujący się niemal wyłącznie na obszarze bezpieczeństwa państwa.

2.2. Dopuszczalny zakres przetwarzania danych

Ewolucja stanowiska ETPC w obszarze nieukierunkowanych form inwigilacji jest najpełniej widoczna w przypadku sprawy szwedzkich przepisów inwigilacyjnych – które początkowo zostały uznane za zgodne z Konwencją (zob. wyrok Izby z 19 lipca 2018 r.). Dopiero Wielka

zasady, inwigilacja stosowana w ramach procedury karnej i względem osób podlegających jurysdykcji USA, musi być prowadzona w oparciu o uprzednio wydany nakaz sądowy (ang. *warrant*) zgodnie z wymaganiami Czwartej Poprawki. Problem szerzej omawia E. Goitein, *Another Bite Out Of Katz: Foreign Intelligence Surveillance And The "Incidental Overhear" Doctrine*, „American Criminal Law Review" 2020, nr 55(1), s. 105–125.

Izba, ponownie rozpoznając sprawę, podjęła odmienną decyzję. Był to efekt wprowadzenia nowej, zaktualizowanej względem zastosowanej w sprawie *Weber*, listy minimalnych zabezpieczeń, jakie powinny być wprowadzone w krajowym prawodawstwie, aby spełnić wymaganie konieczności i zgodności z prawem, wynikające z art. 8(2) EKPC.

Co oczywiste, modernizacja standardu zabezpieczeń prawnych dokonana przez Wielką Izbę wywiera skutek także dla oceny dopuszczalności stosowania innych programów, opartych na niezróżnicowanych i hurtowym przechwytywaniu danych. Przykładem mogą być przepisy niemieckie, które w 2006 r. zostały uznane przez ETPC za zgodne z postanowieniami Konwencji. Przez lata wyrok ten budził uzasadnione wątpliwości w zakresie trafności przedstawionych wniosków, między innymi z uwagi na brak dostrzeżenia przez Trybunał zagrożeń wynikających z braku adekwatnego nadzoru i niezależnej kontroli nad stosowaniem inwigilacji[38]. W rzeczywistości te same niedoskonałości, które Wielka Izba wskazała w 2021 r., badając regulacje szwedzkie, charakteryzowały również badane dekadę wcześniej przepisy niemieckie. Stąd wniosek, że gdyby w sprawie *Weber i Saravia v. Niemcy* zastosować standard stosowany przez ETPC obecnie, praktyka niemiecka musiałaby również zostać uznana za naruszającą gwarancje wynikające z Konwencji. Przykład ten dowodzi, że odmiennie niż uważa wielu komentatorów[39], Trybunał w ostatnich latach znacząco zaostrzył stosowane przez siebie kryteria badania przepisów inwigilacyjnych – a wniosek ten dotyczy również programów nieukierunkowanych.

Jednocześnie jednak nie należy tracić z pola widzenia szeregu problemów szczegółowych, które ujawniają się w trakcie uważnej lektury najnowszych orzeczeń Trybunału. Dotyczą one kluczowych elementów stosowania środków nieukierunkowanych – w szczególności sposobu gromadzenia danych, ich dalszego przetwarzania oraz późniejszej retencji.

Środki wykorzystujące niezróżnicowane i hurtowe gromadzenie danych bazują na stosowaniu selektorów w celu wstępnego filtrowania danych, które następnie mają zostać poddane dalszej analizie. Dobór selektorów (kryteriów wyszukiwania) to kluczowy etap, warunkujący

[38] C. Schaller, *Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden*, „German Law Journal" 2018, nr 19(4), s. 941–980.

[39] Na tym tle porównaj inspirującą analizę przedstawioną w: B. van der Sloot, *Big Brother Watch and others v. the United Kingdom & Centrum för Rättvisa v. Sweden: Does the Grand Chamber Set Back the Clock in Mass Surveillance Cases?*, „European Data Protection Law Review" 2021, nr 7(2), s. 319–326.

przydatność całego systemu do realizacji zadań, dla których został opracowany. Zbyt mała liczba filtrów spowoduje, że system będzie gromadził olbrzymie ilości niepotrzebnych informacji. Z jednej strony może to negatywnie wpłynąć na jego efektywność (opracowanie analiz będzie angażowało większe zasoby, zarówno osobowe, jak i techniczne), z drugiej – na dokładność (większa liczba błędów, tzw. *false positive*). Z kolei zastosowanie zbyt szczegółowych kryteriów może prowadzić do pominięcia ważnych informacji, kluczowych dla rozpoznania nowego – nieznanego wcześniej – wektora zagrożenia.

Na powyższy problem można spojrzeć także inaczej – poprzez sposób definiowania selektorów. Mogą się one bazować na opisie trendów, zjawisk czy zdarzeń, które znajdują się w zainteresowaniu służb. Alternatywnie mogą koncentrować się na opisaniu konkretnych osób (lub ich grup), które w takim zainteresowaniu pozostają. W takim przypadku użycie ogólnych selektorów będzie prowadziło do gromadzenia większej ilości informacji, a użycie bardzo konkretnych selektorów (nazywanych także silnymi selektorami – np. danych osobowych, numerów telefonów) zmieni system analizy prewencyjnej w środek inwigilacji ukierunkowanej[40].

Jest oczywiste, że dowolność doboru kryteriów wyszukiwania zwiększa ryzyko nadużycia władzy. Najprostszym przykładem jest omówione wyżej wykorzystanie systemu w sposób ukierunkowany, przeciwko konkretnym osobom. W większości modeli prawnych wprowadzono dedykowane procedury, które powinny zostać zastosowane w przypadku inwigilacji ukierunkowanej – obejmujące w szczególności uprzednią kontrolę sądową oraz rozbudowane środki nadzoru, stosowane także *ex post*. Ponieważ środki nieukierunkowane zazwyczaj wykorzystywane są poza ramami procedury karnej (są stosowane przez służby specjalne w obszarze bezpieczeństwa państwa), nadzór nad doborem selektorów to pierwszy (i – niestety – często jedyny) sposób sprawowania niezależnego nadzoru nad zakresem gromadzonych danych.

Przegląd różnych modeli prawnych ujawnia jednak fundamentalne różnice w zakresie implementacji tego zabezpieczenia: w niektórych przypadkach, *de facto*, nie jest ono w ogóle stosowane (Niemcy, Wielka Brytania), w innych jest realizowane częściowo (Stany Zjednoczone), podczas gdy w jeszcze innych ustawodawca szczegółowo określił

[40] Warto podkreślić, że ryzyko to zostało także dostrzeżone przez Wielką Izbę ETPC w wyroku *Big Brother Watch* (zob. pkt 346 wyroku).

kryteria definiowania i zatwierdzania selektorów (Szwecja). Model amerykański można uznać za pośredni – bazuje on nie tyle na zatwierdzaniu konkretnych selektorów, a na sądowej kontroli procedur stosowanych w ramach filtrowania danych[41].

W tym zakresie prawodawstwo szwedzkie można natomiast uznać za niemal wzorcowe. Najważniejsze zasady dotyczące doboru selektorów wynikają z przepisów rangi ustawowej (w tym np. ograniczenia w zakresie stosowania silnych selektorów), a ponadto ich stosowanie podlega uprzedniej kontroli sądowej. Trybunał, oceniając szwedzką regulację, wskazał jednak na istnienie obszarów doskonalenia – w tym związanych z brakiem możliwości weryfikacji przez sąd niektórych typów selektorów (takich jak rozbudowane ciągi alfanumeryczne czy wyrażenia regularne) lub wnioskowaniem o zatwierdzenie kategorii selektorów zamiast konkretnych wyrażeń, które będą wyszukiwane.

Wstępne filtrowanie ogranicza zakres gromadzonych danych, jednak stanowi dopiero etap poprzedzający właściwe przetwarzanie – którego celem jest ujawnienie zdarzeń istotnych z punktu widzenia uprawnionych organów. W świetle wcześniejszego orzecznictwa ETPC nie ulega wątpliwości, że sama czynność gromadzenia danych stanowi ingerencję w prawo do prywatności[42], a w przypadku stosowania tajnych środków inwigilacyjnych zgromadzone dane powinny być przechowywane wyłącznie przez czas niezbędny do realizacji celów, dla których zostały zgromadzone[43]. W praktyce przez lata trwały jednak dyskusje, jak zinterpretować to wymaganie w odniesieniu do środków nieukierunkowanych – które z definicji wymagają przechwytywania danych nadmiarowych, co do których nie wiadomo, czy i kiedy będą potrzebne do realizacji jakichkolwiek prawnie uzasadnionych celów. Immamentną cechą inwigilacji prewencyjnej jest próba identyfikacji nieznanych wcześniej zdarzeń, co z kolei wymaga gromadzenia danych także względem osób, znajdujących się poza zakresem zainteresowania uprawnionych organów. Okoliczność ta wydaje się co najmniej trudna

[41] Mechanizm ten wynika z art. 702 ustawy o nadzorze nad wywiadem obcym (Foreign Intelligence Surveillance Act of 1978). Bazuje on na sądowej kontroli tzw. procedur minimalizacji. Sąd nie dokonuje jednak oceny zasadności inwigilacji konkretnych osób, jego kognicja ogranicza się do weryfikacji zasad (procedur), według których analitycy uprawnionych organów typują cele inwigilacji. Szerzej w: M. Rojszczak, *Prywatność w epoce Wielkiego Brata: podstawy prowadzenia programów masowej inwigilacji w systemie prawnym Stanów Zjednoczonych*, „Ius Novum" 2019, nr 1, s. 235–265.

[42] Wyrok ETPC z 26 III 1987 r. w sprawie *Leander v. Szwecja*, 9248/81, pkt 48.

[43] Wyrok ETPC z 16 II 2000 r. w sprawie *Amann v. Szwajcaria*, 27798/95, pkt 78–79.

do pogodzenia z obowiązkiem przetwarzania danych wyłącznie przez czas niezbędny dla realizacji zadań publicznych[44].

Dane gromadzone w systemach masowej inwigilacji można w ogólności podzielić na dwie kategorie: dane nieprzetworzone (które nie zostały poddane dalszej analizie) i dane przetworzone. W przypadku tych drugich rozsądne jest postulowanie, aby wyłącznie dane mające wartość dla organów publicznych były dalej przechowywane. Powstaje jednak kłopot z wyznaczeniem zasad, jakie powinny dotyczyć pierwszej kategorii informacji – a więc danych nieprzetworzonych. Brak jakichkolwiek ograniczeń w tym zakresie mógłby powodować, że będą one przechowywane bezterminowo[45]. Co więcej, nie wiadomo, według jakiego kryterium rozgraniczyć dane przetworzone od nieprzetworzonych.

Trybunał w sprawie *Centrum för rättvisa* zaakceptował fakt przechowywania danych nieprzetworzonych maksymalnie przez okres jednego roku, pod warunkiem że wcześniej nie zostały „poddane ręcznej analizie"[46]. Z kolei dane przetworzone mogą być przechowywane tak długo, jak to jest niezbędne do osiągnięcia celów ich zgromadzenia.

Zasady te pozornie wydają się ustanawiać czytelne ograniczenie, którego przestrzeganie można dodatkowo łatwo skontrolować. W rzeczywistości jednak, uwzględniając specyfikę systemów nieukierunkowanych, tak sformułowane warunki pozostawiają duży potencjał do nadużyć. W systemach bazujących na hurtowym gromadzeniu danych zdecydowana większość analiz prowadzona jest automatycznie – bez angażowania analityków/inżynierów. Coraz powszechniej w tego typu produktach wykorzystywane są również mechanizmy uczenia maszynowego, w których dane są przetwarzane nie tylko w poszukiwaniu określonych wzorców, ale również w celu trenowania wykorzystywanego modelu analitycznego[47]. Tego typu systemy potencjalnie nie potrzebują

[44] Na tym tle porównaj także stanowisko ETPC wyrażone w wyroku z 4 XII 2008 r. w sprawie *S. and Marper v. Wielka Brytania*, pkt 125.

[45] Tak było między innymi w programach prowadzonych przez amerykańską agencję wywiadu elektronicznego (*National Security Agency*, NSA). Zob. np. odtajnione zasady minimalizacji danych, zgodnie z którymi zagraniczna komunikacja dotycząca obywateli USA mogła być przechowywana przez czas „wymagany ze względów utrzymaniowych lub technologicznych" – *Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence information pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended*, 8 I 2007, Art. 6(a)(1), https://cli.re/EmJaMn (dostęp: 7 IX 2022).

[46] *Centrum för rättvisa v. Szwecja*, pkt 338–339.

[47] M.H. Murphy, *Algorithmic surveillance: the collection conundrum*, „International Review of Law, Computers & Technology" 2017, nr 31(2), s. 225–242.

selektorów, aby móc samodzielnie identyfikować istotne powiązania pomiędzy danymi. W ich przypadku dane mogą być *de facto* przechowywane bezterminowo i to bez naruszania wymagań ustanowionych przez Trybunał.

Wydaje się, że dokładnie taki sposób działania charakteryzuje systemy administrowane przez szwedzką FRA. Wskazuje na to możliwość bezterminowego przechowywania danych nieosobowych[48]. Niestety z uwagi na brak bardziej szczegółowego podjęcia tego wątku w postępowaniu przed Trybunałem, nie sposób ocenić, czy faktycznie dane nieprzedstawiające wartości dla służb w każdym przypadku podlegają retencji po upływie maksymalnie 12 miesięcy, czy może są wykorzystywane jako dane treningowe – a w takim wypadku zasady retencji ich już nie dotyczą.

Dlatego należy oczekiwać, że w przyszłości Trybunał uzupełni swój standard o bardziej szczegółowe odniesienie się także do zasad postępowania z danymi zgromadzonymi w programach nieukierunkowanych – zwłaszcza w zakresie przyspieszonej retencji danych wrażliwych czy obowiązkowej anonimizacji danych testowych (treningowych).

2.3. Transgraniczna inwigilacja

Odrębnym zagadnieniem, od lat dyskutowanym na tle standardu strasburskiego, jest odniesienie gwarancji konwencyjnych do transgranicznych aspektów stosowania technik inwigilacyjnych. Problem ten dotyczy zarówno międzynarodowej współpracy uprawnionych organów (służb specjalnych oraz organów ścigania), jak i ograniczeń, jakie powinny być stosowane w przypadku prowadzenia inwigilacji zagranicznej, w szczególności ukierunkowanej na teren innego państwa – strony Konwencji.

W pierwszej kolejności należy odnieść się do kwestii przekazywania (udostępniania) danych zgromadzonych w jednym państwie służbom specjalnym innego państwa. Przykładem współpracy tego typu jest porozumienie Pięciorga Oczu (*Five Eyes Agreement*, FVEY), tworzące ramy współpracy pomiędzy służbami wywiadu elektronicznego Stanów Zjednoczonych, Wielkiej Brytanii, Australii, Nowej Zelandii oraz Kanady[49]. Jej istotnym elementem jest wzajemne udostępnianie

[48] *Centrum för rättvisa v. Szwecja*, pkt 341.

[49] C. Pfluke, *A history of the Five Eyes Alliance: Possibility for reform and additions*, „Comparative Strategy" 2019, nr 38(4), s. 302–315.

zgromadzonych informacji, w tym także pozyskanych z zastosowaniem środków nieukierunkowanych. W niektórych przypadkach obejmuje ona także umożliwienie partnerom zagranicznym bezpośredniego dostępu do własnych baz danych[50].

Współpraca tego typu znacząco zwiększa możliwości poszczególnych służb, jednocześnie tworząc szereg nowych wyzwań w zakresie zapewnienia zgodności z prawem[51]. Dane, które są przekazywane pomiędzy poszczególnymi państwami, pierwotnie są gromadzone z wykorzystaniem krajowych programów inwigilacyjnych, realizowanych z poszanowaniem praw i zabezpieczeń ustanowionych w prawie krajowym. O ile w przypadku państw europejskich (w szczególności państw członkowskich EU) można mówić o wspólnych elementach standardu stosowania inwigilacji, o tyle w przypadku współpracy z państwami trzecimi różnice mogą obejmować nawet podstawowe zagadnienia. Dość powiedzieć, że w Stanach Zjednoczonych agencja wywiadu elektronicznego (NSA) realizuje programy nieukierunkowane na podstawie dwóch różnych ram prawnych – federalnej ustawy FISA oraz rozporządzenia wykonawczego nr 12333[52]. Programy prowadzone na podstawie rozporządzenia wykonawczego cechuje duża swoboda działań podejmowanych przez NSA i praktycznie brak zabezpieczeń prawnych, zbliżonych do istniejących w omówionym wcześniej standardzie ETPC[53].

W efekcie współpraca organów publicznych państw – stron Konwencji z ich odpowiednikami w państwach trzecich prowadzi do pytań o skutki tej praktyki dla ochrony praw jednostek. Zagadnienie to dotyczy zarówno przypadków przekazywania danych zagranicę (do państwa trzeciego), jak i pozyskiwania danych z państwa trzeciego, a następnie wykorzystywania ich na potrzeby realizacji zadań publicznych w państwie odbierającym.

Trybunał odniósł się do tego problemu dopiero w sprawie *Big Brother Watch*. W istocie kwestia współpracy brytyjskiego GCHQ z amerykańską

[50] S. Kim, P. Perlin, *Newly Disclosed NSA Documents Shed Further Light on Five Eyes Alliance*, „Lawfare" (25 III 2019).

[51] Privacy International, *Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards*, 24 IV 2018, https://cli.re/VpZZnX (dostęp: 7 IX 2022).

[52] Szerzej: M. Rojszczak, *Prywatność w epoce Wielkiego Brata…*

[53] Stąd też od lat organizacje pozarządowe domagają się uchylenia lub przeprowadzenia głębokiej reformy rozporządzenia 12333. Zob. np. J. Laperruque, *Executive Order 12333: The Spy Power Too Big for Any Legal Limits*, „Project on Government Oversight" 24 III 2022, https://cli.re/eqD3Zk (dostęp: 7 IX 2022).

NSA była jednym z głównych zarzutów podnoszonych przez skarżących w tej sprawie. Dowodzili oni, że dane przekazywane do USA przestają być chronione zgodnie z gwarancjami wynikającymi z Konwencji, a z uwagi na brak tożsamych zabezpieczeń obecnych w prawie federalnym – *de facto* zostają oni pozbawieni swoich praw. W szczególności prawo amerykańskie nie limituje czasu przechowywania informacji pozyskanych z inwigilacji, nie ogranicza zakresu ich późniejszego wykorzystania, jak również nie wiąże zakresu przetwarzanych danych z kryterium niezbędności czy proporcjonalności[54]. Ryzyko erozji zabezpieczeń konwencyjnych było tym bardziej prawdopodobne, że w przeszłości informowano o przypadkach celowego zlecenia inwigilacji służbom państwa trzeciego, a następnie uzyskiwania dostępu do zgromadzonych w ten sposób danych z pomięciem ograniczeń wynikających z prawa krajowego[55]. Działania takie podejmowały zarówno służby amerykańskie, jak i służby państw europejskich (w tym niemieckie)[56].

Chociaż Trybunał już w sprawie *Weber i Saravia v. Niemcy* wskazywał, że prawo krajowe powinno określać zasady udostępniania danych pozyskanych z inwigilacji podmiotom trzecim (innym organom publicznym oraz partnerom zagranicznym), to wymaganiu temu nie towarzyszyły żadne szczegółowe wytyczne, pozwalające na ocenę spełnienia tego kryterium. Dopiero w sprawie *Big Brother Watch* Trybunał wskazał, że państwo przekazujące powinno zapewnić, aby udostępniane dane były przetwarzane i przechowywane w sposób zgodny z wymaganiami wynikającymi z Konwencji[57]. W tym zakresie doprecyzowano, że zasady dotyczące transferu danych powinny wynikać z przepisów prawa, co tym samym wyklucza możliwość stosowania blankietowych zgód czy pozostawienia zbyt dużej swobody decyzyjnej uprawnionym organom. Trybunał dodatkowo wyjaśnił, że państwo odbierające musi zapewnić, aby przekazane dane były zabezpieczone w sposób chroniący przed

[54] Szerzej: L.K. Donohue, *The future of foreign intelligence: privacy and surveillance in a digital age*, New York 2016.

[55] Zob. np. C. Johnson, *German loophole allows BND spy agency to snoop on own people*, „The Guardian" 29 XI 2014, https://cli.re/47ejk3 (dostęp: 7 IX 2022).

[56] Na tym tle należy również pamiętać, że FVEY to nie jedyne porozumienie wywiadowcze, tworzące ramy dla współpracy w obszarze inwigilacji elektronicznej. Innym przykładem jest Maximator – program, w ramach którego współpracę prowadziły służby pięciu państw europejskich (Dania, Szwecja, Niemcy, Holandia i Francja) – zob. B. Jacobs, *Maximator: European signals intelligence cooperation, from a Dutch perspective*, „Intelligence and National Security" 2020, nr 35(5), s. 659–668.

[57] *Big Brother Watch i in. v. Wielka Brytania*, pkt 362.

nieproporcjonalną ingerencją w prawa jednostki. Wymaganie to obejmuje również obowiązek uregulowania zasad dalszego udostępniania danych przez organy państwa otrzymującego.

W tym względzie kluczowe dla stanowiska ETPC jest wyjaśnienie sposobu oceny modelu zabezpieczeń prawnych stosowanego w państwie trzecim. Należy pamiętać, że Trybunał Sprawiedliwości podczas badania dopuszczalności unijnych ram transferu danych komercyjnych do Stanów Zjednoczonych uznał amerykański model prawny za niezapewniający adekwatnego poziomu ochrony do wynikającego z prawa UE[58]. Na tej podstawie uznał nieważność decyzji Komisji, co miało poważne skutki dla swobodnej wymiany danych z USA[59].

Gdyby zatem ETPC – w ślad za TSUE – zastosował koncepcję adekwatności (równorzędności) zabezpieczeń, skutkiem mogłoby być zablokowanie jakiekolwiek współpracy z państwami trzecimi (nie tylko ze Stanami Zjednoczonymi) w zakresie przekazywania danych pochodzących z inwigilacji elektronicznej. Trybunał uznał jednak, że zapewnienie kompatybilności modeli ochrony nie wymaga, aby państwo odbierające wdrożyło porównywalne zabezpieczenia do istniejących w państwie przekazującym[60]. Co więcej, chociaż w ocenie Trybunału państwo przekazujące powinno zapewnić, aby transfer danych do zagranicznej służby wywiadowczej podlegał niezależnej kontroli, to jednocześnie z wymagania tego nie należy odczytywać potrzeby wydawania uprzedniej zgody poprzedzającej każdy z transferów.

W konsekwencji ETPC przyjął mało rygorystyczny schemat zabezpieczeń stosowany dla transgranicznej wymiany danych pochodzących z inwigilacji. Wprowadzona koncepcja „kompatybilności" zabezpieczeń jest nieprecyzyjna i daleko mniej jednoznaczna niż adekwatność zabezpieczeń stosowana w orzecznictwie TSUE. Nie ulega wątpliwości, że to celowy zabieg ETPC, który chciał uniknąć zarzutów o eksterytorialne stosowanie własnych standardów. Na tym tle należy przypomnieć o od lat powtarzanych zarzutach, jakoby koncepcja adekwatności zabezpieczeń promowana przez TSUE w istocie zmierzała do budowy – opierając się na prawie UE – globalnych standardów w dziedzinie ochrony danych

[58] Wyrok TSUE z 16 VI 2020 r. w sprawie *Facebook Ireland i Schrems (Schrems II)*, C-311/18.

[59] J.X. Dhont, *Schrems II. The EU adequacy regime in existential crisis?*, „Maastricht Journal of European and Comparative Law" 2019, nr 26(5), s. 597–601.

[60] *Big Brother Watch i in. v. Wielka Brytania*, pkt 362.

(efekt brukselski)[61]. Jednocześnie jednak stanowisko ETPC, zgodnie z którym państwo otrzymujące nie musi zapewniać porównywalnej ochrony (ang. *comparable protection*) do funkcjonującej w państwie przekazującym, prowadzi do pytań o skuteczność stosowania standardu strasburskiego w świecie zglobalizowanych usług cyfrowych. Trybunał, akceptując możliwość stosowania masowej inwigilacji przy pozostawieniu znacznej swobody w udostępnianiu tych danych służbom państw trzecich, podważył sens budowania europejskiego modelu ochrony danych. Jest to szczególnie duży problem dla państw członkowskich UE – funkcjonujących w ramach otwartego rynku wewnętrznego, którego elementem jest także sektor usług telekomunikacyjnych. Skoro każde państwo może bez przeszkód monitorować całą łączność elektroniczną (uzasadniając to celami bezpieczeństwa narodowego), a następnie przekazywać ją do państw trzecich, to w ten sposób możliwe jest łatwe (i jak widać – skuteczne) pominięcie większości zabezpieczeń wynikających ze standardu ustalonego w sprawie *Big Brother Watch*. W szczególności znika problem obowiązkowej retencji danych, ograniczenia przechwytywania danych wrażliwych, obowiązku przetwarzania danych wyłącznie dla celów, dla których zostały zgromadzone itp. Wszystkie te zabezpieczenia mogą być pominięte dzięki przekazaniu danych do partnera zagranicznego, który następnie może je zwrotnie udostępniać służbom państwa przekazującego.

Obecne stanowisko ETPC nie zawiera także czytelnego stanowiska w zakresie zasad, jakie powinny znaleźć zastosowanie przy imporcie danych z państw trzecich. W takim wypadku państwo otrzymujące może nie posiadać informacji na temat okoliczności pozyskania danych czy zastosowanego reżimu prawnego. Standard strasburski w istocie nie odnosi się do przypadków, gdy dane są pozyskane przez stronę trzecią, a dopiero później importowane do państwa – strony Konwencji. Należy pamiętać, że stroną trzecią nie musi być organ publiczny, ale np. podmiot prywatny (multinarodowy koncern technologiczny). Wydaje się, że w takim wypadku poszanowanie gwarancji wynikających z Konwencji wymaga, aby dane pochodzące z inwigilacji mogły być pozyskiwane wyłącznie od państw stosujących porównywalny model ochrony praw podstawowych. Dlatego nie sposób zaakceptować

[61] A. Bradford, *The Brussels effect: how the European Union rules the world*, New York 2020; C. Ryngaert, M. Taylor, *The GDPR as Global Data Protection Regulation?*, „AJIL Unbound" 2020, nr 114, s. 5–9.

poglądu przedstawionego zarówno w wyroku Izby[62], jak i Wielkiej Izby[63], zgodnie z którymi także przypadki stosowania inwigilacji przez zagraniczne służby wywiadowcze – działające na zlecenie państwa – strony Konwencji – znajdują się poza zakresem stosowania EKPC, a więc nie mogą być oceniane pod kątem naruszeń praw i gwarancji z niej wynikających także w państwie odbierającym.

Odrębnym, równie doniosłym, problemem jest odniesienie Konwencji – a w konsekwencji i standardu wypracowanego przez ETPC – do inwigilacji o czysto zagranicznym charakterze. Terminem tym określa się typ inwigilacji, w przypadku której łącznik krajowy w ogóle nie występuje. W ogólności dotyczy zatem działań prowadzonych przez organy państwa wymierzonych w przechwytywanie łączności realizowanej przez obcokrajowców przebywających poza obszarem własnej jurysdykcji. Istotą tego problemu jest wyjaśnienie, czy działania takie objęte są zakresem stosowania Konwencji. W tym zakresie Trybunał dotychczas stosował dwie ważne doktryny – efektywnej kontroli oraz zachowania przestrzeni prawnej. Zgodnie z pierwszą, państwo posiada obowiązki wynikające z Konwencji wyłącznie względem osób podlegających jego jurysdykcji (bezpośrednio lub pośrednio)[64]. Z kolei obowiązek zachowania przestrzeni prawnej dotyczy sytuacji, gdy w wyniku podjętych działań jedno z państw przejmuje kontrolę nad częścią terytorium innego państwa – strony Konwencji. W takim wypadku, zgodnie z wykładnią Trybunału, ochrona jednostek przed pozostawieniem ich w „próżni prawnej" wymaga, aby państwo, które przejęło kontrolę, również stało się odpowiedzialne za zagwarantowanie i ochronę praw wynikających z Konwencji[65].

Zasada efektywnej kontroli wydaje się nie mieć zastosowania do przypadków inwigilacji o czysto zagranicznym charakterze – gromadzenie informacji o obcokrajowcu i to z wykorzystaniem narzędzi informatycznych na odległość nie wystarcza do uznania, że osoby poddane tym środkom znajdują się pod władczą kontrolą organów państwa

[62] Wyrok ETPC (Izba) z 13 IX 2018 r. w sprawie *Big Brother Watch i in. v. Wielka Brytania*, 58170/13, 62322/14 and 24960/15, pkt 420.

[63] *Big Brother Watch i in. v. Wielka Brytania*, pkt 495.

[64] Zob. Także: European Court of Human Rights, *Guide on Article 1 of the European Convention on Human Rights*, 2020, https://cli.re/JpwmZW (dostęp: 7 IX 2022); C. Ryngaert, *Clarifying the Extraterritorial Application of the European Convention on Human Rights (Al-Skeini v the United Kingdom)*, „Utrecht Journal of International and European Law" 2012, nr 28(74), s. 57.

[65] Wyrok ETPC z 10 V 2001 r. w sprawie *Cypr v. Turcja*, 25781/94, pkt 78.

stosującego inwigilację. Jednocześnie Trybunał wielokrotnie w swoim orzecznictwie podkreślał, że celem Konwencji jest stworzenie przez umawiające się strony wspólnej przestrzeni ochrony praw podstawowych[66]. Przestrzeń ta co do zasady nie rozciąga się jednak na obszar znajdujący się pod jurysdykcją państw trzecich[67].

Ciekawe wnioski płyną natomiast z odniesienia doktryny zachowania przestrzeni prawnej do inwigilacji o czysto zagranicznym charakterze. Otóż, jeżeli zarówno państwo stosujące środki inwigilacyjne, jak i państwo, pod jurysdykcję którego podlega osoba poddana takim środkom, są stronami EKPC, to zgodnie z wykładnią przedstawioną w sprawie *Cypr v Turcja*[68], tego typu ingerencja powinna być oceniana pod kątem zgodności z gwarancjami wynikającymi z Konwencji.

Niestety, ani w sprawie *Big Brother Watch*, ani w *Centrum för rättvisa* ETPC nie odniósł się szczegółowo do tego problemu. W wyroku Izby zapadłym w pierwszej z tych spraw – z uwagi na brak podniesienia przez rząd zarzutu orzekania poza zakresem stosowania Konwencji – Trybunał uznał, że w rozpatrywanej sprawie nie występuje spór dotyczący terytorialnej jurysdykcji[69]. W ten sposób, zamiast rozstrzygnąć dyskutowany od lat problem, Trybunał skoncentrował się na wyjaśnieniu, dlaczego tym aspektem sprawy się nie zajmie[70].

Podsumowanie

Nieukierunkowane formy inwigilacji to środek, który w rękach zdeterminowanego rządu jest narzędziem o olbrzymim potencjale ingerencji

[66] Postanowienie ETPC z 12 XII 2001 r. w sprawie *Banković i in. v. Belgia i in.*, 52207/99, pkt 80.

[67] Tak: Postanowienie ETPC z 11 XII 2006 r. w sprawie *Mohammed Ben El Mahi i in. v. Dania*, 5853/06.

[68] Zob. przypis 57. Szerzej: L. Hammer, *Re-examining the extraterritorial application of the ECHR to northern Cyprus: the need for a measured approach*, „The International Journal of Human Rights" 2011, nr 15(6), s. 858–872.

[69] Wyrok ETPC (Izba) z 13 IX 2018 r. w sprawie *Big Brother Watch i in. v. Wielka Brytania*, 58170/13, 62322/14 and 24960/15, pkt 271. Wniosek ten został także potwierdzony w trakcie postępowania przez Wielką Izbą, gdy rząd potwierdził że przynajmniej niektórzy skarżący w okresie badanym w postępowaniu znajdowali się pod jurysdykcją brytyjską (*Big Brother Watch i in. v. Wielka Brytania*, pkt 272).

[70] Szersze omówienie wyroku Izby w: B. van der Sloot, E. Kosta, *Big Brother Watch and Others v UK: Lessons from the Latest Strasbourg Ruling on Bulk Surveillance*, „European Data Protection Law Review" 2019, nr 5(2), s. 252–261.

w prawa i wolności osobiste. Abstrahując od trwającej dyskusji, czy stosowanie tego typu środków można uznać za konieczne w warunkach działania państwa demokratycznego, zapewnienie ochrony przed możliwymi nadużyciami wymaga ustanowienia kompleksowego katalogu zabezpieczeń prawnych.

Bez wątpienia wykładnia przedstawiona przez Trybunał w najnowszym orzecznictwie – w szczególności w sprawie *Big Brother Watch* – przyczynia się do realizacji tego celu. Sąd nie tylko rozstrzygnął niektóre z pojawiających się wcześniej wątpliwości, ale przede wszystkim dostosował standard orzeczniczy, uwzględniając wprost ryzyka wynikające z prowadzenia zaawansowanych programów inwigilacyjnych. Jednocześnie jednak zaprezentowana argumentacja w wielu obszarach wydaje się aż nadto zachowawcza, przez co nie prowadzi do ustanowienia spójnych zasad, kompleksowo opisujących wymagania względem współczesnych sposobów gromadzenia i przetwarzania danych.

Trybunał niezmiennie wskazuje, że realizacja celów bezpieczeństwa narodowego może uzasadniać podjęcie decyzji o stosowaniu środków inwigilacyjnych opartych na niezróżnicowanym i hurtowym przechwytywania łączności. Nie wyjaśnia jednak, czy realizacja innych ważnych zadań organów publicznych może być również uznana za wystarczającą dla zastosowania środków nieukierunkowanych. Trudno to pominięcie zrozumieć, zwłaszcza w sytuacji gdy istnieje wiele dowodów na wdrażanie przez państwa nowych platform analitycznych posiadających oczywisty potencjał do stosowania nieukierunkowanej inwigilacji i to w dziedzinach niezwiązanych z bezpieczeństwem narodowym. Masowa inwigilacja to dzisiaj nie tylko środki stosowane przez agencje wywiadowcze wyłącznie w odniesieniu do łączności elektronicznej.

Trybunał stoi na stanowisku, że stosowanie masowej inwigilacji można pogodzić z zasadami funkcjonowania państwa demokratycznego. Środkiem do osiągnięcia tego celu ma być standard zabezpieczeń prawnych, pierwotnie dedykowany programom inwigilacji ukierunkowanej, a w sprawie *Big Brother Watch* rozszerzony w sposób *explicite* uwzględniający zagrożenia związane z programami nieukierunkowanymi. Chociaż wprowadzone zmiany należy ocenić pozytywnie, to w stanowisku Trybunału brakuje refleksji nad przyczynami, dlaczego dotychczasowy standard orzeczniczy okazał się nieskuteczny. Sprawa *Weber* była rozstrzygana w roku 2006, a więc ponad 15 lat temu. Od tego czasu ujawniono bogactwo informacji na temat masowych programów

inwigilacyjnych, prowadzonych także przez państwa europejskie. Czy zatem należy uznać, że to prawodawcy i rządy poszczególnych państw błędnie interpretowały istniejący wówczas standard orzeczniczy ETPC i akceptowały używanie środków go naruszających, czy jednak to sam standard był na tyle nieprecyzyjny oraz niespójny, że jego efektywność była niewielka? Na tym tle symptomatycznie wygląda ocena szwedzkich przepisów inwigilacyjnych dokonana w sprawie *Centrum för rättvisa* – gdy najpierw Izba (bazując m.in. na standardzie wprowadzonym w sprawie *Weber*) nie stwierdziła naruszenia, a następnie Wielka Izba doprecyzowała standard oceny i na tej podstawie uznała, że szwedzkie przepisy jednak naruszają Konwencję.

Stanowisko ETPC warto skontrastować także z wykładnią TSUE. W istocie standard luksemburski w zakresie programów nieukierunkowanych (w tym wypadku: ogólnej retencji danych) można zrekapitulować w kilku punktach: (1) niezróżnicowane formy inwigilacji zakładające hurtowe gromadzenie danych co do zasady prowadzą do nieproporcjonalnej ingerencji w prawa jednostki, wobec czego są niezgodne z prawem UE; (2) z uwagi na szczególne znaczenie realizacji celów bezpieczeństwa narodowego, państwa mogą stosować niezróżnicowane formy inwigilacji w przypadkach, gdy jest to konieczne dla osiągnięcia rzeczywistych potrzeb w zakresie bezpieczeństwa państwa; (3) w każdym przypadku dane pozyskane w ten sposób nie mogą być przechowywane poza UE[71]. Z czytelnego stanowiska, przedstawionego w punkach 1 i 2 wynika niedopuszczalność stosowania masowej inwigilacji dla realizacji innych celów niż bezpieczeństwa narodowego. Z kolei z tezy 3 wynika niedopuszczalność stosowania takich środków z zamiarem przekazania pozyskanych w ten sposób danych do zagranicznych partnerów. Standard strasburski nie zawiera prostej odpowiedzi na żadne z tych zagadnień. Co więcej, ETPC do tej pory nie odpowiedział nawet jasno, czy gwarancje wynikające z Konwencji w ogóle mają zastosowanie do niektórych rodzajów inwigilacji (jak na przykład inwigilacji o czysto zagranicznym charakterze).

Oczywiście analizując stanowisko TSUE, należy zawsze pamiętać o zakresie stosowania prawa UE, co w tym wypadku oznacza, że standard unijny nie może być wprost odniesiony do wielu programów

[71] M. Rojszczak, *National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts*, „European Constitutional Law Review" 2021, nr 17(4), s. 607–635.

inwigilacyjnych, których badanie znajduje się w kognicji ETPC[72]. Nie zmienia to jednak faktu, że TSUE – stosując przekonującą i spójną argumentację – wypracował w ostatnich latach kompleksową wykładnię Karty praw podstawowych, w sposób realny chroniący przed nieuprawnioną inwigilacją elektroniczną. Niestety nie można tego samego powiedzieć o zawiłej i pełnej niejednoznaczności wykładni ETPC.

Podobne wnioski przedstawione zostały także w zdaniach odrębnych dołączonych do wyroku *Big Brother Watch*. Uwagę zwraca stanowisko sędziów P. Lemmensa, F. Vehabovića oraz M. Bošnjaka, w którym wskazali na brak ustanowienia w wyroku jasnych i czytelnych wymagań minimalnych. W tym zakresie trafnie zauważyli, że standard ETPC „[w]ymaga jasnej definicji poszczególnych zabezpieczeń w prawie krajowym, ale sam nie ustanawia żadnych minimalnych zabezpieczeń"[73]. Przekonuje również przedstawiona przez nich argumentacja dotycząca łatwości, z jaką – poprzez wykorzystanie odpowiednio dobranych selektorów – możliwe jest wykorzystanie programów nieukierunkowanych do prowadzenia inwigilacji ukierunkowanej, przy jednoczesnym ominięciu szczegółowych zabezpieczeń ustanowionych dla przypadków inwigilacji celowanej. W tym zakresie trudno nie przyznać także racji sędziemu Pinto de Albuquerque, który uznał stanowisko Trybunału za „niedopuszczalne niejasne" – w konsekwencji prowadzące „nie tylko do osłabienia autorytetu Trybunału, ale także wartości tego wyroku"[74].

Uzasadnienie wyroku Wielkiej Izby w sprawie *Big Brother Watch* zawiera ponad 500 paragrafów. Oczywiście objętość tekstu nie mówi nic o jego jakości, a wniosek ten bez wyjątku dotyczy także orzeczeń sądowych. Pamiętając jednak, że kwestia stosowania nieukierunkowanej inwigilacji od lat znajduje się w centrum zainteresowania zarówno prawodawców, opinii publicznej, jak i judykatury, można było oczekiwać, że Wielka Izba, tak szczegółowo odnosząc się do przedłożonej jej sprawy, rozstrzygnie także rzeczywiste problemy związane z tolerowaniem nieukierunkowanych form inwigilacji w europejskiej przestrzeni prawnej. Tym bardziej, że szereg z istniejących obecnie niejasności wynika z niejednoznacznego stanowiska, jakie Trybunał podejmował w przeszłości.

---

[72] I. Buono, A. Taylor, *Mass Surveillance in the CJEU: Forging a European Consensus*, „The Cambridge Law Journal" 2017, nr 76(2), s. 250–253.

[73] Zob. zdanie odrębne sędziów P. Lemmensa, F. Vehabovića oraz M. Bošnjaka do wyroku *Big Brother Watch i in v. Wielka Brytania*, pkt 14(b).

[74] Zob. zdanie odrębne sędziego Pinto de Albuquerque do wyroku *Big Brother Watch i in v. Wielka Brytania*, pkt 2.

Dlatego wydaje się, że Trybunał nie w pełni wykorzystał możliwość, aby swoją wykładnią wpłynąć na praktykę państw dotyczącą coraz szerszego stosowania nieograniczonych form inwigilacji. Uwagę zwraca także dostrzegalny brak spójności pomiędzy kierunkiem orzecznictwa ETPC a standardem stosowanym przez TSUE. Chociaż nie jest to pierwszy przypadek, gdy Trybunał Sprawiedliwości ustanawia wyższy poziom ochrony, niż wynikający z orzecznictwa EPKC, to z perspektywy wyznaczania szerszych, regionalnych standardów – nieograniczonych tylko do państw członkowskich EU – taka sytuacja musi niepokoić.

BULK ELECTRONIC SURVEILLANCE IN THE LIGHT OF CURRENT EUROPEAN COURT OF HUMAN RIGHTS CASE LAW

Summary

In 2016, while testifying before a UK parliamentary committee, William Binney, former technical director of the US National Security Agency, stated that by implementing bulk surveillance programmes, "your government and my government has permitted what terrorists have wanted all along but could never achieve. That is to cause us to restrict our freedoms while also tripping up our efforts to stop them".

Despite the passage of years, controversy about the proportionality of the use of surveillance programmes involving indiscriminate and bulk data collection continues unabated. There are numerous arguments that such measures should not be used in democratic states. Despite the recurring reports of abuse and questionable usefulness of such solutions, there is also no shortage of arguments put forward by proponents of the use of untargeted measures proving the need (or even necessity) for their use for public security purposes.

The issue presented here is also the subject of ongoing interest on the part of legislators and the judiciary. The article aims to provide an overview of the evolution of the ECtHR's position on the use of electronic surveillance, in particular its untargeted forms. However, the article is intended not only to recapitulate the reasoning as set out in recent case law – including the 2021 judgments of the Grand Chamber in *Big Brother Watch et al. v. United Kingdom* and *Centrum för rättvisa v Sweden* – but also to prompt further discussion on the relevance of the Court's position as set out in relation to the most important legal issues relating to mass surveillance. It is the author's intention that in this way it will be possible to answer the question of whether the current standard set by the ECtHR can be considered sufficient to protect against the risk associated with the spread of modern surveillance measures and their increasing use by public authorities.

Keywords: electronic surveillance – bulk surveillance – personal data protection – right to privacy.

LITERATURA

Banks W.C., *Next Generation Foreign Intelligence Surveillance Law: Renewing 702*, „University of Richmond Law Review" 2017, nr 51(3).

Barnea A., *Strategic intelligence: a concentrated and diffused intelligence model*, „Intelligence and National Security" 2020, nr 35(5).

Bernal P., *Data gathering, surveillance and human rights: recasting the debate*, „Journal of Cyber Policy" 2016, nr 1(2).

Bradford A., *The Brussels effect: how the European Union rules the world*, New York 2020.

Buono I., Taylor A., *Mass Surveillance in the CJEU: Forging a European Consensus*, „The Cambridge Law Journal" 2017, nr 76(2).

Celeste E., *The Court of Justice and the Ban on Bulk Data Retention: Expansive Potential and Future Scenarios*, „European Constitutional Law Review" 2019, nr 15(1).

Dhont J.X., *Schrems II. The EU adequacy regime in existential crisis?*, „Maastricht Journal of European and Comparative Law" 2019, nr 26(5).

Donohue L.K., *The future of foreign intelligence: privacy and surveillance in a digital age*, New York 2016.

European constitutional courts towards data retention laws, pod red. M. Zubika, J. Podkowika, R. Rybskiego, Cham 2021.

Goitein E., *Another Bite Out Of Katz: Foreign Intelligence Surveillance And The "Incidental Overhear" Doctrine*, „American Criminal Law Review" 2020, nr 55(1).

Grabowska-Moroz B., *Ochrona gromadzonych danych telekomunikacyjnych i zasady ich udostępniania na tle Konstytucji RP i prawa Unii Europejskiej*, „Europejski Przegląd Sądowy" 2016, nr 1.

Grzelak A., *Trybunał Sprawiedliwości ponownie o relacji między koniecznością zwalczania przestępczości a prawem do prywatności*, „Europejski Przegląd Sądowy" 2017, nr 3.

Guliani N.S., *The Government Is 'Incidentally' Sucking Up Tens of Millions of Americans' Communications a Year, and It's a Privacy Nightmare*, American Civil Liberties Union (23 III 2017), https://cli.re/xabKxA (dostęp: 7 IX 2022).

Hammer L., *Re-examining the extraterritorial application of the ECHR to northern Cyprus: the need for a measured approach*, „The International Journal of Human Rights" 2011, nr 15(6).

Jacobs B., *Maximator: European signals intelligence cooperation, from a Dutch perspective*, „Intelligence and National Security" 2020, nr 35(5).

Johnson C., *German loophole allows BND spy agency to snoop on own people*, „The Guardian" 29 XI 2014, https://cli.re/47ejk3 (dostęp: 7 IX 2022).

Kim S., Perlin P., *Newly Disclosed NSA Documents Shed Further Light on Five Eyes Alliance*, „Lawfare" (25 III 2019).

Laperruque J., *Executive Order 12333: The Spy Power Too Big for Any Legal Limits*, „Project on Government Oversight" 24 III 2022, https://cli.re/eqD3Zk (dostęp: 7 IX 2022).

Malgieri G., De Hert P., *European Human Rights, Criminal Surveillance, and Intelligence Surveillance: Towards „Good Enough" Oversight, Preferably but Not Necessarily by Judges*, w: *The Cambridge Handbook of Surveillance Law*, pod red. D.C. Graya, S.E. Hendersona, Cambridge 2017.

Milaj J., *Privacy, surveillance, and the proportionality principle: The need for a method of assessing privacy implications of technologies used for surveillance*, „International Review of Law, Computers & Technology" 2016, nr 30(3).

Mitsilegas V., Guild E., Kuskonmaz E., Vavoula N., *Data retention and the future of large-scale surveillance: The evolution and contestation of judicial benchmarks*, „European Law Journal" 2022.

Murphy M.H., *Algorithmic surveillance: the collection conundrum*, „International Review of Law, Computers & Technology" 2017, nr 31(2).

Pfluke C., *A history of the Five Eyes Alliance: Possibility for reform and additions*, „Comparative Strategy" 2019, nr 38(4).

Privacy International, *Secret Global Surveillance Networks: Intelligence Sharing Between Governments and the Need for Safeguards*, 24 IV 2018, https://cli.re/VpZZnX (dostęp: 7 IX 2022).

Rojszczak M., *National Security and Retention of Telecommunications Data in Light of Recent Case Law of the European Courts*, „European Constitutional Law Review" 2021, nr 17(4).

Rojszczak M., *Prawne podstawy prowadzenia masowej inwigilacji obywateli opartej na hurtowym i nieukierunkowanym przechwytywaniu danych w UE z uwzględnieniem dorobku orzeczniczego TSUE i ETPC*, „Studia Prawa Publicznego" 2017, nr 2(18).

Rojszczak M., *Prywatność w epoce Wielkiego Brata: podstawy prowadzenia programów masowej inwigilacji w systemie prawnym Stanów Zjednoczonych*, „Ius Novum" 2019, nr 1.

Ryngaert C., *Clarifying the Extraterritorial Application of the European Convention on Human Rights (Al-Skeini v the United Kingdom)*, „Utrecht Journal of International and European Law" 2012, nr 28(74).

Ryngaert C., Taylor M., *The GDPR as Global Data Protection Regulation?*, „AJIL Unbound" 2020, nr 114.

Schaller C., *Strategic Surveillance and Extraterritorial Basic Rights Protection: German Intelligence Law After Snowden*, „German Law Journal" 2018, nr 19(4).

van der Sloot B., *Big Brother Watch and others v. the United Kingdom & Centrum för Rättvisa v. Sweden: Does the Grand Chamber Set Back the Clock in Mass Surveillance Cases?*, „European Data Protection Law Review" 2021, nr 7(2).

van der Sloot B., Kosta E., *Big Brother Watch and Others v UK: Lessons from the Latest Strasbourg Ruling on Bulk Surveillance*, „European Data Protection Law Review" 2019, nr 5(2).

Zalnieriute M., *Procedural Fetishism and Mass Surveillance under the ECHR*, „Verfassungsblog" (2 VI 2021), https://verfassungsblog.de/big-b-v-uk/ (dostęp: 7 IX 2022).