



dr hab. Michał Balcerzak, prof. US

dr Ewa Michałkiewicz-Kądziela

**Wyrok Europejskiego Trybunału Praw Człowieka w sprawie Pietrzak, Bychawska-Siniarska i inni
przeciwko Polsce z 28 maja 2024 r.**

**(nieadekwatność zabezpieczeń prawnych przed arbitralnością i nadużyciami w odniesieniu do
niejawnego nadzoru – inwigilacji)**

Dnia 28 maja 2024 r. Europejski Trybunał Praw Człowieka (Trybunał) wydał wyrok w sprawie Pietrzak, Bychawska-Siniarska i inni p. Polsce (skargi nr 72038/17 i 25237/18), który dotyczył ustawodawstwa regulującego kwestie związane z możliwością inwigilacji obywateli. Skarżący zarzucili stronie polskiej naruszenie art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności (Konwencja) gwarantującego każdemu prawo do prywatności.

Skarżącymi byli obywatele polscy: Mikołaj Pietrzak – adwokat i były dziekan Okręgowej Rady Adwokackiej w Warszawie, a także Dominika Bychawska-Siniarska, Barbara Grabowska-Moroz, Wojciech Klicki i Katarzyna Szymielewicz – osoby związane z organizacjami pozarządowymi zajmującymi się ochroną praw człowieka i prawem do prywatności. Wszyscy skarżący wykonywali działalność zawodową i publiczną, która narażała ich na potencjalne ryzyko objęcia tajną inwigilacją ze strony służb państwowych.

Tłem sprawy była nowelizacja ustawy o Policji z 15 stycznia 2016 r. oraz uchwalenie ustawy o działaniach antyterrorystycznych z 10 czerwca 2016 r., które znacząco rozszerzyły uprawnienia operacyjne służb. Przewidywały one m.in. szeroką retencję danych telekomunikacyjnych i elektronicznych, możliwość ich uzyskiwania przez służby w trybie uproszczonym oraz stosowanie środków operacyjnych bez obowiązku informowania osób nimi objętych, nawet po zakończeniu działań. Regulacje te zostały skrytykowane przez Rzecznika Praw Obywatelskich, Generalnego Inspektora Ochrony Danych Osobowych, Krajową Radę Sądownictwa, Naczelną Radę Adwokacką



oraz liczne organizacje społeczne, a także przez Komisję Wenecką, jako niezgodne ze standardami praw człowieka.

Część skarżących podjęła próby uzyskania informacji, czy byli objęci inwigilacją. W marcu 2016 r. Wojciech Klicki i Katarzyna Szymielewicz zwrócili się do szefa ABW o udzielenie informacji, czy w okresie 2012–2016 byli objęci nadzorem operacyjnym. Wnioski te zostały odrzucone, a ABW wskazała, że dane tego rodzaju mają charakter niejawnny i nie mogą być ujawniane osobom zainteresowanym. Podobnie potraktowano kolejne odwołania i ponowne wnioski. W 2017 r. wszyscy skarżący wnieśli skargi do Prezesa Rady Ministrów oraz szefów właściwych służb, powołując się na art. 227 Kodeksu postępowania administracyjnego. Wskazywali, że przepisy o inwigilacji uniemożliwiają im ustalenie, czy byli inwigilowani, a także pozbawiają ich jakiegokolwiek środka prawnego, który pozwalałby zakwestionować legalność ewentualnych działań służb. Organy te w odpowiedziach podkreślały poufny charakter danych oraz wskazywały, że informacje o stosowaniu środków nadzoru mogą być ujawnione jedynie sądom i prokuraturze.

Skarżący argumentowali, że ze względu na zakres i charakter zaskarżonych przepisów istnieje realne prawdopodobieństwo, iż zostali lub mogą zostać objęci inwigilacją, a brak obowiązku powiadamiania ich o zastosowanych środkach oraz brak dostępu do skutecznych środków prawnych uniemożliwia im ochronę swoich praw. Po wyczerpaniu ścieżki krajowej, skarżący zdecydowali się złożyć skargi do Trybunału, zarzucając naruszenie art. 8 Konwencji poprzez zezwolenie na funkcjonowanie w państwie systemu niejawnego nadzoru (monitorowanie operacyjne i zatrzymywanie danych telefonicznych, pocztowych i dotyczących łączności elektronicznej) bez możliwości poddania go kontroli sądowej ze względu na brak w prawie krajowym środka prawnego, który umożliwiłby inwigilowanym osobom złożenie skargi oraz zakwestionowanie legalności prowadzonych przez służby działań monitorujących.

Trybunał odniósł się nie tylko do przepisów prawa polskiego, ale do regulacji Unii Europejskiej oraz prawa i praktyki wewnętrznej 35 państw-stron Konwencji. W ten sposób Trybunał ustalił standard kontroli sądowej nad niejawnym nadzorem stosowanym przez służby państwowe. Trybunał odnotował, że w większości badanych porządków prawnych występuje kontrola uprzednia, jednakże aż 15 państw wprowadziło także kontrolę *a posteriori*. W większości państw



objętych analizą osoba fizyczna posiada uprawnienie, by odwołać się od decyzji nakładającej nadzór niejawny lub też zbadać legalność decyzji nakładającej taki środek. Ponadto aż 21 państw nałożyło na podmioty stosujące nadzór do celów zwalczania przestępczości obowiązek poinformowania o tym fakcie osoby poddanej nadzorowi, po zakończeniu prowadzonych w stosunku do niej działań monitorujących. Co więcej, wiele państw wprowadziło także dodatkowe zabezpieczenia, które mają przyczynić się do ochrony osoby podlegającej nadzorowi przed nadużyciami ze strony władz państwowych (m.in. wykaz przestępstw, w związku z którymi można zastosować nadzór niejawny, pisemny obowiązek uzasadnienia decyzji o objęciu osoby nadzorem, ograniczenie możliwości wydłużenia czasu nadzoru).

Trybunał zdecydował się dokonać kontroli zaskarżonych przepisów *in abstracto*, bez konieczności dowiedzenia przez skarżących, że zostali oni rzeczywiście poddani inwigilacji przez służby państwowe. Trybunał doszedł do wniosku, że już samo istnienie w krajowym porządku prawnym przepisów, które pozbawiają osoby fizyczne odpowiedniej ochrony wynikającej z art. 8 Konwencji, jest wystarczającą podstawą do rozpoznania sprawy.

Trybunał przypomniał, że art. 8 Konwencji obejmuje wszelką korespondencję prywatną, ale wymiana informacji między profesjonalnymi pełnomocnikami prawnymi a ich klientami korzysta ze szczególnego poziomu ochrony. Pełnomocnik profesjonalny nie może należycie wykonywać swojej misji, jeżeli nie jest w stanie zapewnić klientowi poufności komunikacji.

Rozpoznając sprawę Trybunał wskazał, że nadrzędnym wymogiem dla prawidłowo skonstruowanego systemu nadzoru niejawnego jest istnienie odpowiednich narzędzi, które będą te działania inwigilacyjne monitorowały oraz skutecznie kontrolowały, co pozwoli na ochronę jednostki przed nadużyciami ze strony władzy oraz nieuprawnioną ingerencję w prawo do prywatności obywateli. Nawet jeżeli w ustawodawstwie krajowym prawodawca przewidział przepisy ograniczające zakres uprawnień służb policyjnych i wywiadowczych często nie jest to wystarczające do zapewnienia odpowiedniej ochrony przed nadużyciami, których mogą dopuścić się służby państwowe. Trybunał zasugerował, że konieczne jest wprowadzenie przez państwa-strony Konwencji precyzyjnych rozwiązań, które określą „mechanizm monitorowania operacji niejawnego



nadzoru i będą opierać się na niezależnym organie monitorującym, działającym z własnej inicjatywy i posiadającym niezbędne instrumenty prawnego do wykrywania i zwalczania nadużyć¹.

Trybunał podkreślił, że system kontroli operacyjnej przewidziany w ustawie o Policji cechował się nadmiernym zakresem i brakiem dostatecznych zabezpieczeń przed arbitralnością. Katalog przestępstw, w których można stosować nadzór, był szeroki, a procedury zatwierdzania i nadzoru sądowego – niewystarczające. W konsekwencji, niemal każda osoba korzystająca z usług telekomunikacyjnych mogła zostać objęta inwigilacją bez realnej możliwości obrony swoich praw.

W odniesieniu do retencji danych komunikacyjnych Trybunał wskazał, że przepisy nakładały na dostawców usług obowiązek ogólnego i masowego przechowywania danych o wszystkich użytkownikach, niezależnie od jakiegokolwiek powiązania z przestępstwem. Dane te mogły być przechowywane przez 12 miesięcy i udostępniane służbom w bardzo szerokim zakresie. Zdaniem Trybunału takie rozwiązanie stanowiło ingerencję „o szczególnie poważnym i szerokim charakterze” w prawo do prywatności i nie spełniało wymogu proporcjonalności.

Trybunał zwrócił uwagę, że choć formalnie przewidziano pewne mechanizmy kontroli sądowej, nie zapewniały one rzeczywistej ochrony przed nadużyciami. Brakowało m.in. obowiązku informowania osób o objęciu ich nadzorem, co czyniło niemożliwym dochodzenie roszczeń po zakończeniu inwigilacji. Taki system, zdaniem Trybunału, budził w społeczeństwie uzasadnione poczucie bezbronności wobec działań służb.

W związku z powyższym Trybunał stwierdził, że przepisy krajowe dotyczące tajnego nadzoru zawarte zakwestionowanym ustawodawstwie nie spełniają wymogów art. 8 Konwencji w odniesieniu do skargi dotyczącej kontroli operacyjnej; w odniesieniu do zatrzymywania danych dotyczących komunikacji do celów ewentualnego dostępu do nich przez organy krajowe, a także w odniesieniu do skargi dotyczącej systemu niejawnego nadzoru w działaniach antyterrorystycznych.

¹ Zob. § 193 wyroku z 28 maja 2024 r. ETPC w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce, skargi nr 72038/17 i 25237/18.