Warszawa, 4 kwietnia 2012 r.

Sąd Okręgowy w Warszawie
II Wydział Cywilny
Al. Solidarności 127
00-898 Warszawa

Powód: **Bogdan Wróblewski**
ul. Czerska 8/10
00-732 Warszawa

Pozwany: **Skarb Państwa**
Reprezentowany przez Szefa Centralnego Biura Antykorupcyjnego
Al. Ujazdowskie 9
00-583 Warszawa

Sygn. II C 626/11

OPINIA „AMICUS CURIAE"

1. Wstęp

Fundacja PANOPTYKON zwraca się z prośbą o przyjęcie przez sąd opinii *amicus curiae* w sprawie o sygn. II C 626/11. Opinia „przyjaciela sądu" jest formą wyrażenia opinii przez organizację pozarządową. Celem opinii jest przedstawienie problemu, którego dotyczy sprawa, w szerszym, niekoniecznie znanym sądowi, świetle. Opinia nie wpływa na niezawisłość sędziowską, pozwala jedynie na przedstawienie argumentów, których nie przedstawiły strony.

Fundacja PANOPTYKON istnieje od 2009 r. Zajmujemy się problematyką ochrony praw człowieka w społeczeństwie nadzorowanym. Naszym zdaniem sprawa problem naruszenia dóbr osobistych poprzez zbieranie danych retencyjnych dotyczy ważnych społecznie standardów państwa demokratycznego, takich jak prawo do prywatności oraz wolność słowa.

2. Kwestie ogólne

Dane telekomunikacyjne to informacje nie dotyczące wprost treści przekazywanego komunikatu, pozwalające jednak ustalić wiele faktów „okołokomunikacyjnych". Wskazują one kto, kiedy, gdzie, z kim i w jaki sposób połączył się lub próbował się połączyć. Są to takie dane, jak numer telefonu (obu stron), czas połączenia, czy stacja przekaźnikowa, w zasięgu której znajdowały się telefony wykonującego i odbierającego połączenie. Dane telekomunikacyjne pozwalają na stworzenie szczegółowego obrazu życia prywatnego danej osoby, jej „telekomunikacyjnego profilu" zbudowanego z informacji na temat sieci jej kontaktów, mapy przemieszczania się i nawyków.

Obowiązek przechowywania danych telekomunikacyjnych nałożyła na państwa członkowskie Unii Europejskiej Dyrektywa Parlamentu Europejskiego i Rady z 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (dalej: **dyrektywa retencyjna**). Retencja, w wersji zaplanowanej przez dyrektywę, była pomyślana jako środek nadzwyczajny, który miał być wykorzystywany w przypadku najgroźniejszych przestępstw. Jednakże sposób wdrożenia dyrektywy retencyjnej przez ustawodawcę polskiego jest sprzeczny z tą ideą. W Polsce dostęp do danych telekomunikacyjnych możliwy jest nie tylko w przypadku poważnych przestępstw, ale również w wielu innych sytuacjach (w tym szeroko pojętych celach prewencyjnych) Służby mają w zasadzie nieograniczony i niekontrolowany dostęp do tych informacji. Co więcej operatorzy telekomunikacyjni zostali zobowiązani do przechowywania danych maksymalny dopuszczany przez dyrektywę retencyjną okres, czyli 24 miesięce (w innych krajach europejskich okres ten wynosi zazwyczaj od 6 do 12 miesięcy).

Z danych przedstawionych Fundacji PANOPTYKON przez Urząd Komunikacji Elektronicznej w trybie dostępu do informacji publicznej wynika, że w 2009 r. służby specjalne, policja, prokuratura i sądy sięgały po dane telekomunikacyjne ponad milion razy, w 2010 r. liczba ta sięgnęła prawie 1,4 mln, a w 2011 r. ponad 1,85 mln. Niestety brak odpowiednich obowiązków sprawozdawczych sprawia, że nie wiadomo, jakie dokładnie dane są pobierane i w jakich celach wykorzystywane.

Dane telekomunikacyjne, mimo że nie zawierają treści komunikacji, podlegają ochronie. Europejski Trybunał Praw Człowieka uznał już w 1984 r.[1], że rejestrowanie adresata i czasu rozmowy może naruszać art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności (dalej: **Konwencja**)[2]. Zbieranie przez władzę publiczną informacji na temat aktywności obywateli dotyka również konstytucyjnej zasady autonomii informacyjnej jednostki (art. 51) oraz ochrony tajemnicy komunikowania się (art. 49).

W ocenie Fundacji PANOPTYKON retencja danych telekomunikacyjnych w obecnym kształcie jest jednym z podstawowych zagrożeń dla praw człowieka w Polsce. Dlatego od dawna wskazujemy na konieczność zmian odpowiednich przepisów[3].

---

[1] Por. Malone v UK, 2 sierpnia 1984, skarga 8691/79, par. 83-85.

[2] Zgodnie z art. 8 ust. 1 Konwencji każdy ma prawo do poszanowania swojego życia prywatnego. Ust. 2 reguluje natomiast dopuszczalność ograniczenia tego prawa.

[3] Por. Raport „Internet a prawa podstawowe" autorstwa Katarzyny Szymielewicz oraz Anny Mazgal dostępny pod adresem: http://wolnyinternet.panoptykon.org/sites/default/files/raport_na_www.pdf.

3. Działalność Centralnego Biura Antykorupcyjnego wobec Powoda

W okresie od 1 stycznia do 17 maja 2007 r. oraz 7 maja – 17 maja 2007 r. Centralne Biuro Antykorupcyjne pozyskiwało dane telekomunikacyjne powoda[4] – Bogdana Wróblewskiego. Pobierane w tym okresie dane telekomunikacyjne pozwoliły ustalić, z kim i gdzie powód się kontaktował oraz z kim próbował nawiązać kontakt.

Fundacja PANOPTYKON chciałaby zwrócić uwagę na dwie kwestie, które podważają legalność działań strony pozwanej w tej sprawie.

Bezprawność działań CBA – arbitralny dostęp służby do danych retencyjnych

Centralne Biuro Antykorupcyjne powołane zostało jako służba specjalna do spraw zwalczania korupcji w życiu społecznym i gospodarczym. Zwalczanie korupcji, zdefiniowanej w ustawie, wyznacza zakres działania służby. Zwalczając korupcję CBA ma rozpoznawać, zapobiegać i wykrywać wymienione enumeratywnie w ustawie o CBA przestępstwa, np. przeciwko wymiarowi sprawiedliwości. Zakres działań CBA został więc w ustawie jednoznacznie określony. Tylko realizacja wymienionych w art. 2 ustawy o CBA zadań uzasadnia wykonywanie czynności operacyjno-rozpoznawczych. Innymi słowy, każde sięgnięcie po dane telekomunikacyjne musi pozostawać w związku z konkretnym zadaniem w zakresie zwalczania korupcji w życiu publicznym i działalności godzącej w interesy ekonomiczne państwa **[ograniczenie przedmiotowe]**.

Kontrola operacyjna – zgodnie z art. 17 ustawy o CBA – może być stosowana, gdy inne środki okazały się bezskuteczne (albo będą nieprzydatne). Oznacza to, że CBA może korzystać z tych środków tylko wtedy, gdy jest to **niezbędne**. Niezbędność ingerencji w prywatność jednostki ma swoje źródło w art. 51 Konstytucji. Ogranicza on możliwość pozyskiwania, gromadzenia i udostępniania przez władze publiczne informacji, jedynie do tych, które są **„niezbędne w demokratycznym państwie prawnym".** Ponadto ustawa wprowadza szereg innych ograniczeń w stosowaniu tych środków. Przede wszystkim jest to wymóg uzyskania zgody sądu. Wniosek o wyrażenie takiej zgody musi wskazywać konkretne przestępstwa, którego dotyczy sprawa. Kontrola danych telekomunikacyjnych została co prawda zwolniona z obowiązku uzyskania zgody sądu, jednakże dotyczą jej pozostałe ograniczenia wynikające z art. 17 ustawy o CBA – niezbędność i adekwatność **[ograniczenia jakościowe]** .

W ocenie Fundacji PANOPTYKON w przypadku Bogdana Wróblewskiego CBA sięgało po dane telekomunikacyjne przekraczając oba opisane powyżej ograniczenia. Z dokumentów przedstawionych w sprawie wynika, że zbieranie informacji na temat powoda nie było związane z żadną konkretną sprawą z zakresu ustawowych zadań CBA. Ponadto CBA nie wykazało, że wykorzystanie danych telekomunikacyjnych powoda było niezbędne. Oznacza to, że sięganie po te informacje odbywało się z przekroczeniem ograniczeń wynikających z ustawy o CBA, a tym samym – złamaniem zasady legalizmu.

4. Wątpliwości konstytucyjne

Prawo do prywatności czy autonomia informacyjna jednostki nie mają charakteru bezwzględnego. Ich ograniczenia muszą jednak spełniać określone wymogi. Zgodnie

[4] Wynika to z pisma Kierownika Sekcji Weryfikacji Systemowych – Dział Ustaleń Systemowych Polskiej Telefonii Cyfrowej sp. z o.o. z 4 marca 2011 r. oraz pisma do Prokuratora Andrzeja Pasiecznego z Prokuratury Okręgowej w Warszawie z 13 maja 2011 r.

z Konstytucją RP są to: wprowadzenie drogą ustawy, konieczność w demokratycznym państwie np. ze względu na jego bezpieczeństwo, a także nienaruszanie istoty wolności i praw. Natomiast w świetle Konwencji są to: wprowadzenie drogą ustawy oraz konieczność w społeczeństwie demokratycznym np. ze względu na bezpieczeństwo państwowe i publiczne oraz zapobieganie przestępstwom.

Wymóg ograniczenia w drodze ustawy oznacza nie tylko odpowiednią rangę aktu prawnego – powinien on również spełniać określone wymogi, które moglibyśmy nazwać „jakościowymi". Europejski Trybunał Praw Człowieka w wyroku z 28 czerwca 2007 r. w sprawie: *Stowarzyszenie integracji europejskiej i praw człowieka oraz Ekimdzhiev przeciwko Bułgarii*[5] wskazał na konieczność precyzyjności prawa ograniczającego prywatność obywatela. Zdaniem ETPC prawo krajowe powinno być na tyle precyzyjne, aby wskazywać obywatelom okoliczności i warunki, w jakich władze publiczne są upoważnione do dokonywania niejawnej i potencjalnie groźnej ingerencji w ich prawo do poszanowania życia prywatnego i korespondencji. ETPC zwrócił uwagę na fakt, że skoro stosowanie przez służby specjalne środków inwigilacji nie może być poddane kontroli opinii publicznej (co wynika z ich istoty) i ze względu na ryzyko nadużycia władzy, prawo krajowe powinno ustanawiać **odpowiednie i skuteczne gwarancje przeciwko nadużyciu**. W naszej ocenie w polskim porządku prawnym nie ma takich gwarancji.

Obecnie w Trybunale Konstytucyjnym znajdują się dwa wnioski Rzecznik Praw Obywatelskich[6] dotyczące zasad kontroli operacyjnej, w tym przepisów regulujących zasady dostępu CBA do danych telekomunikacyjnych. Rzecznik Praw Obywatelskich wskazała m.in. na:

(i) zbyt szeroki zakres spraw, w których możliwe jest sięganie po dane telekomunikacyjne;
(ii) brak zewnętrznych form kontroli nad korzystaniem z danych retencyjnych;
(iii) brak powszechnego obowiązku niszczenia zbędnych danych.

Ponadto – co wydaje się kluczowe w niniejszej sprawie – Rzecznik Praw Obywatelskich wskazała na brak jakichkolwiek gwarancji ochrony tajemnic zawodowych, m.in. tajemnicy dziennikarskiej. Tajemnica dziennikarska, regulowana w art. 15 ustawy – Prawo prasowe[7], stanowi o niezależności prasy i tym samym jest elementem konstytucyjnej wolności słowa. Jednym z kluczowych elementów tajemnicy dziennikarskiej jest zaś ochrona źródeł informacji. Nie budzi wątpliwości, że dane telekomunikacyjne zawierają dane umożliwiające identyfikację informatora dziennikarza, a zatem możliwość nieograniczonego wykorzystywania tych danych w pracy operacyjnej musi prowadzić do naruszenia tajemnicy dziennikarskiej.

5. Podsumowanie

W ocenie Fundacji PANOPTYKON Centralne Biuro Antykorupcyjne zbierając dane retencyjne dotyczące powoda przekroczyło swoje ustawowe uprawnienia. Jednocześnie istotne jest, że przepisy umożliwiające sięganie po te dane budzą daleko idące wątpliwości konstytucyjne. W naszej ocenie szczególnie istotny jest fakt, że powód jest dziennikarzem i jako taki powinien korzystać z ochrony swoich źródeł informacji.

---

[5] Wyrok z 28 czerwca 2007 r. w sprawie Stowarzyszenie integracji europejskiej i praw człowieka oraz Ekimdzhiev przeciwko Bułgarii, skarga nr 62540/00, dostępne pod adresem: http://cmiskp.echr.coe.int/tkp197/view.asp?item=1&portal=hbkm&action=html&highlight=Ekimdzhiev&sessionid=90049576&skin=hudoc-en.

[6] Sygnatury K 29/11 i K 23/11 połączone pod wspólną sygnaturą K 23/11.

[7] Ustawa z 26 stycznia 1984 r., Dz. U. nr 5, poz. 24.

W kontekście braku odpowiednich środków ochrony praw osoby, której prywatność została naruszona, niniejszy proces ma szczególnie istotne znaczenie. Powództwo o ochronę dóbr osobistych jest bowiem jedynym środkiem prawnym, jakim dysponował powód.

W imieniu Fundacji PANOPTYKON

Katarzyna Szymielewicz
Prezes Zarządu

Małgorzata Szumańska
Członkini Zarządu