

**OPINIA NACZELNEJ RADY ADWOKACKIEJ DO
SENACKIEGO PROJEKTU USTAWY O ZMIANIE USTAWY O POLICJI
ORAZ NIEKTÓRYCH INNYCH USTAW (DRUK SENACKI NR 967)**

I. Uwagi ogólne

Opiniowany senacki projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk senacki nr 967)(dalej: Projekt) jak wskazuje się w jego uzasadnieniu, ma na celu dostosowanie systemu prawa do wyroku Trybunału Konstytucyjnego z 30 lipca 2015 r. sygn. K 23/11. Dostosowanie to ma polegać na wprowadzeniu zmian w obowiązujących przepisach, których niekonstytucyjność orzekł Trybunał Konstytucyjny, ale i w zakresie tych regulacji, gdzie mimo niestwierdzenia niezgodności z Konstytucją RP, dostrzeżone zostały pewne problemy interpretacyjne i praktyczne.

Przykładem jest tu proponowana w Projekcie zmiana brzmienia przepisów regulujących zakres środków możliwych do stosowania w ramach kontroli operacyjnej. Trybunał Konstytucyjny orzekł tu, że przepisy art. 19 ust. 6 pkt 3 ustawy o Policji, art. 9e ust. 7 pkt 3 ustawy o Straży Granicznej, art. 36c ust. 4 pkt 3 ustawy o kontroli skarbowej, art. 31 ust. 7 pkt 3 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ust. 6 pkt 3 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 31 ust. 4 pkt 3 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, art. 17 ust. 5 pkt 3 ustawy o Centralnym Biurze Antykorupcyjnym rozumiane w ten sposób, że właściwy organ zarządzający kontrolę operacyjną wskazuje określony w prawie rodzaj środka technicznego uzyskiwania informacji i dowodów oraz ich utrwalania stosowany w indywidualnej sprawie, są zgodne z art. 2 i art. 47 w związku z art. 31 ust. 3 Konstytucji RP. Wątpliwości budzić musi proponowany sposób określenia katalogu tych środków jako: podsłuch rozmów prowadzonych przy użyciu środków technicznych; podsłuch i podgląd pomieszczeń i osób poza miejscami publicznymi; kontrola treści korespondencji; nadzór elektroniczny osób, miejsc i przedmiotów oraz środków transportu¹. Wydaje się, że katalog

¹ Obecnie w ramach kontroli operacyjnej możliwe jest stosowanie: kontroli treści korespondencji; kontroli zawartości przesyłek; stosowanie środków technicznych umożliwiających uzyskiwanie w sposób niejawną

ten jest niezbyt precyzyjnie określony², zwłaszcza w kontekście ostatnich doniesień³ na temat stosowania przez CBA narzędzia „Remote Control System”. Ma ono umożliwiać monitorowanie komputerów i telefonów, pozyskiwanie danych przechowywanych na tych urządzeniach, nawet w sytuacji gdy użytkownik nie jest podłączony do Internetu oraz śledzenie korespondencji w Internecie. Rodzi się wątpliwość, czy projektowana definicja środków możliwych do stosowania kontroli operacyjnej, umożliwić będzie korzystanie z tego typu narzędzi.

Należy jednocześnie podkreślić, że Projekt w ogóle nie wykonuje postanowienia sygnalizacyjnego Trybunału Konstytucyjnego z dnia 25 stycznia 2006 r. sygn. S 2/06, wydanego w następstwie wyroku z 12 grudnia 2005 r. sygn. K 32/04. Trybunał Konstytucyjny wskazał tu na potrzebę uregulowania obowiązku informowania osób objętych kontrolą operacyjną o fakcie jej prowadzenia. W uzasadnieniu Projektu (s. 5) twórcy projektu wskazują, że Trybunał Konstytucyjny dostrzega problem braku w obowiązujących przepisach obowiązku po stronie Policji i służb obowiązku poinformowania po zakończeniu czynności operacyjno – rozpoznawczych osoby, która tego typu czynnościom została poddana. Jednakże ich zdaniem, wprowadzenie tego typu regulacji w przepisach ww. ustaw policyjnych, stanowiłoby naruszenie reguł, na podstawie których działają służby i mogłoby osłabić ich skuteczność, jak i kłóciłoby się z ustawowym obowiązkiem ochrony form i metod ich działania. Wobec jasnego stanowiska przedstawionego przez Trybunał Konstytucyjny zarówno w wyroku z 12 grudnia 2005 r. oraz postanowieniu sygnalizacyjnym z 25 stycznia 2006 r. i okoliczności, że obowiązek takiego informowania ma silną konstytucyjną podstawę

informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych, a także w przypadku niektórych służb rejestrowanie obrazu.

² W piśmiennictwie można spotkać bardziej precyzyjne określenie katalogu tych środków. A. Biernaczyk wskazuje, że do tego katalogu środków należą: podsłuchu w pomieszczeniu (PP), podsłuchu telefonu stacjonarnego (PT), podsłuchu telefonu komórkowego (PTK), podsłuchu faksu (PTFax), podglądu przy wykorzystaniu urządzeń do rejestracji obrazu i dźwięku (PDF), kontrolowania korespondencji w sieci internetowej (KKI), kontrolowania treści korespondencji pisemnej (KK), kontrolowania zawartości przesyłek (KZP). Zob. A. Biernaczyk, *Zarys problematyki czynności operacyjnych realizowanych w trybie art. 19, 19a i 19b ustawy z dnia 6 kwietnia 1990 r. o Policji (w:) Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu Nowoczesne technologie i praca operacyjna*, red. L. Paprzycki, Z. Rau, Warszawa 2009, s. 116. O wiele bardziej precyzyjna była też propozycja przedstawiona w poselskim projekcie ustawy o czynnościach operacyjno – rozpoznawczych (Sejm VI kadencji, druk sejmowy nr 353).

³ http://www.tokfm.pl/blogi/panoptykon/2015/07/legalne_ale_tajne_analiza_kontrowersji_wokol_rcs/1.

w art. 51 ust. 4 Konstytucji RP, takie stanowisko twórców Projektu musi spotkać się z dezaprobatą⁴.

Ponadto krytycznie należy ocenić brak w Projekcie propozycji powołania zewnętrznego, eksperckiego organu, który odpowiadał by za kontrolę działalności służb z perspektywy respektowania praw i wolności konstytucyjnych⁵.

II. Uwagi szczegółowe

Kontrola operacyjna a ochrona tajemnic prawnie chronionych

W wyroku z 30 lipca 2014 r. Trybunał Konstytucyjny orzekł, że art. 19 ustawy o Policji, art. 9e ustawy o Straży Granicznej, art. 36c ustawy o kontroli skarbowej, art. 31 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 27 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 31 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, art. 17 ustawy o Centralnym Biurze Antykorupcyjnym **w zakresie, w jakim nie przewidują gwarancji niezwłocznego, komisyjnego i protokolarnego zniszczenia materiałów zawierających informacje objęte zakazami dowodowymi, co do których sąd nie uchylił tajemnicy zawodowej bądź uchylenie było niedopuszczalne**, są niezgodne z art. 42 ust. 2, art. 47, art. 49, art. 51 ust. 2 i art. 54 ust. 1 w związku z art. 31 ust. 3 Konstytucji RP.

Wykonując to rozstrzygnięcie Projekt wprost wskazuje, że w ramach kontroli operacyjnej może dochodzić do utrwalania treści zawierających chronione jako tajemnica zawodowa, w tym tak adwokacka, jak i obrończa. Z Projektu wynika bowiem w sposób oczywisty, że osoby obowiązane do ochrony tajemnicy obrończej i adwokackiej, nie są wykluczone spod działania

⁴ Należy zauważyć, że podobny postulat dotyczący przekazania informacji o pozyskaniu danych telekomunikacyjnych, zainteresowanemu abonentowi, został wyrażony przez Najwyższą Izbę Kontroli przy okazji kontroli pt. „Uzyskiwanie i przetwarzanie przez uprawnione podmioty danych z bilingów, informacji o lokalizacji oraz innych danych, o których mowa w art. 180 c i d ustawy Prawo telekomunikacyjne”.

⁵ Taki postulat poruszany jest w dyskusji nad problematyką kontroli nad działalnością służb specjalnych. Por. sprawozdanie z konferencji „Jak daleko sięgnie państwo? Retencja danych, bilingi, inwigilacja a gwarancje praw i wolności obywatelskich” w dniu 10 grudnia 2014 r. organizowanej przez Naczelną Radę Adwokacką oraz Krajową Radę Radców Prawnych dostępne na stronie: <http://www.adwokatura.pl/z-zycia-nra/polsce-potrzebny-jest-niezalezny-organ-kontroli-retencji-danych/>.

przepisów o kontroli operacyjnej. Projekt zakłada natomiast obowiązek dokonywania przez funkcjonariuszy prowadzących kontrolę operacyjną oceny, czy materiały w jej ramach zgromadzone zawierają dane objęte tajemnicą, o której mowa w art. 178 k.p.k. czy też tajemnicą, o której mowa w art. 180 § 2 k.p.k. W przypadku stwierdzenia, że chodzi o tajemnicę obrończą aktualizuje się obowiązek zniszczenia zgromadzonych danych. W przypadku zaś danych chronione jako tajemnica adwokacka, funkcjonariusz ma przekazać je prokuratorowi, a ten niezwłocznie będzie musiał wystąpić do sądu, celem wydania: 1) postanowienia o wyrażeniu zgody na wykorzystanie ich w postępowaniu karnym, albo 2) zarządzenia o niezwłocznym, komisyjnym i protokolarnym ich zniszczeniu.

Rozwiązanie, w którym to funkcjonariusz danej służby – zainteresowany wszczęciem i prowadzeniem postępowania karnego o przestępstwo, na którego okoliczność prowadzona jest kontrola operacyjna - ma ocenić czy zgromadzony materiał zawiera treści chronione jako tajemnica obrończa lub adwokacka należy ocenić krytycznie. Przede wszystkim, istnieje ryzyko, że z uwagi na wczesny – zazwyczaj przed procesowy charakter czynności operacyjno – rozpoznawczych, do których zalicza się kontrola operacyjna - materiał dotyczący każdego poufnego kontaktu adwokata z „figurantem”, niebędącym formalnie jeszcze podejrzanym, uznawany będzie za niezawierający informacji chronionych, tudzież zawierający informacje objęte tajemnicą, o której mowa w art. 180 § 2 k.p.k. Taka praktyka w oczywisty sposób naruszać będzie prawo do obrony, które aktualizuje się z chwilą zgłoszenia się klienta do adwokata, nie zaś formalnego przedstawienia zarzutów. Ponadto w sytuacji, gdy kontrola operacyjna prowadzona będzie wobec osoby nieoznaczonej „NN”, nie będzie możliwe ustalenie, czy zgromadzone materiały chronione są jako jedna z tajemnic zawodowych.

Krytycznie odnieść się należy także do proponowanego mechanizmu zwalniania z tajemnicy. Tryb ten zakłada poinformowanie aż dwóch podmiotów (prokuratora i sądu) o fakcie zarejestrowania w ramach kontroli operacyjnej materiałów chronionych jako tajemnica, o której mowa w art. 180 § 2 k.p.k. Zastrzeżenie budzi okoliczność, że funkcjonariusz nie będzie mógł sam zarządzić zniszczenia materiałów, zawierających dane objęte ochroną tajemnicy z art. 180 § 2 k.p.k. jak i wystąpić do sądu o podjęcie decyzji w sprawie zniszczenia lub wykorzystania tych materiałów, tylko musi je przekazać prokuratorowi. Niezrozumiała jest rola prokuratora, który wnioskuje jedynie do sądu o podjęcie decyzji w przedmiocie tych

danych. Procedura w tym kształcie powoduje, że taka chroniona na podstawie art. 180 § 2 k.p.k. treść stanie się znana różnym podmiotom. Ponadto proponowane regulacje w przeciwieństwie do art. 180 § 2 k.p.k.⁶ nie przewidują jakichkolwiek przesłanek, którymi kierować powinien się sąd podejmując decyzję o wykorzystaniu informacji, co stwarza ryzyko decyzji arbitralnych w tym zakresie.

Krytycznie należy ocenić też sytuację, że projekt nigdzie nie przewiduje, by postanowienie o wyrażeniu zgody na wykorzystanie materiałów zawierających tajemnicę prawnie chronioną, miało by zawierać uzasadnienie. Stanowiące wzór dla tej instytucji, postanowienie wydane na podstawie art. 180 § 2 k.p.k. uzasadnienie takie natomiast zawiera.

Wreszcie Projekt nie przewiduje możliwości złożenia zażalenia przez osobę obowiązującą do ochrony tajemnicy obrończej i adwokackiej, na postanowienie o wykorzystaniu w postępowaniu karnym materiałów zawierających tę tajemnicę.

Trybunał Konstytucyjny w wyroku z 30 lipca 2014 r. odnosząc się do kwestii ochrony tajemnic prawnie chronionych i braku regulacji nakazujących niszczenie materiałów tę tajemnicę zawierających, wskazał, że zbliżone w swej istocie rozwiązania legislacyjne (do art. 180 § 2 k.p.k.) powinny dotyczyć również ochrony tajemnicy zawodowej w trakcie czynności operacyjno-rozpoznawczych, w tym kontroli operacyjnej. Zdaniem Trybunału Konstytucyjnego nie ma żadnych uzasadnionych podstaw, by na tym etapie postępowania stosować łagodniejsze standardy niż przewidziane w postępowaniu karnym, wręcz przeciwnie, standardy te – z uwagi na niejawnosć kontroli oraz jej ponadprocesowy charakter – powinny być co najmniej zbieżne ze standardami w postępowaniu karnym. W ocenie Naczelnej Rady Adwokackiej, wykonanie wyroku Trybunału Konstytucyjnego, w proponowanym kształcie tego wskazania Trybunału Konstytucyjnego nie realizuje, gdyż proponowany standard ochronny jest niższy niż obowiązujący na gruncie art. 180 § 2 k.p.k.

Pozyskiwanie danych telekomunikacyjnych a ochrona tajemnic zawodowych

⁶ W art. 180 § 2 k.p.k. przesłankami zwolnienia z tajemnicy jest niezbędność dla dobra wymiaru sprawiedliwości oraz niemożliwość ustalenia danej okoliczności na podstawie innego dowodu.

Projekt wprowadza zmiany w przepisach ww. ustaw policyjnych, zasad pozyskiwania danych telekomunikacyjnych, o których mowa w art. 180c i 180d Prawo telekomunikacyjne. Jednakże mimo, że w uzasadnieniu wskazuje się, iż propozycja stanowi doprecyzowanie tychże zasad, to trudno nie oprzeć się wrażeniu, że proponowane ramy ustawowe będą stwarzać niezwykle szeroką możliwość pozyskania przedmiotowych danych. Jest to szczególnie widoczne w przypadku Policji, gdzie pozyskiwanie danych może dotyczyć ogólnie „przestępstw ściganych z oskarżenia publicznego”. Oznacza to zaprzeczenie, celów jakim służyło wprowadzenie możliwości pozyskiwania danych telekomunikacyjnych, tj. zwalczanie szczególnie poważnych przestępstw i zagrożeń terrorystycznych. Twórcy projektu zrezygnowali przy tym ze wskazania w przepisach, że do pozyskania danych telekomunikacyjnych będzie dochodzić w warunkach subsydiarności, czyli tylko wtedy, gdy inne środki okazały się nieskuteczne.

Projektowane przepisy sankcjonują przy tym sytuację, gdy w ramach pozyskania danych telekomunikacyjnych, dochodzi do zebrania informacji o osobach, zobowiązanych na podstawie art. 180 § 2 k.p.k. do ochrony tajemnicy zawodowej. Projekt przewiduje, że w przypadku danych już zebranych, na wniosek prokuratora, któremu będą one przekazywane, sąd będzie rozstrzygać o możliwości ich wykorzystania lub konieczności ich zniszczenia. W sytuacji zaś, gdy dane mają zostać dopiero zebrane, sąd ma zdecydować o zgodzie na ich pozyskanie, chyba, że zajdzie przypadek „niecierpiący zwłoki”, kiedy to funkcjonariusz będzie jednocześnie występował do operatora o przekazanie danych i występował do sądu o zgodę na ich wykorzystanie.

Kształt projektowanych przepisów musi niepokoić. Twórcy projektu z jednej strony przyjęli, że pozyskanie danych telekomunikacyjnych może naruszać co najwyżej tajemnicę z art. 180 § 2 k.p.k. Nie zauważają przy tym jednej istotnej okoliczności, iż zakres możliwych do pozyskania danych telekomunikacyjnych, jest tak szeroki, że na jego podstawie możliwe jest bieżące monitorowanie działalności osoby odpowiedzialnej do ochrony tajemnicy zawodowej, w szczególności tego, gdzie, z kim, w jakich godzinach, jak często, nawiązuje ona relacje z klientem.

Nie jest jasne przy tym, jak należy rozumieć użyte w Projekcie sformułowanie, iż dane mają „bezpośrednio dotyczyć osoby wykonującej zawód lub funkcję, o której mowa w art. 180 § 2 k.p.k.” Literalnie wykładając ten przepis dojść należy do wniosku, że jego dyspozycja jest spełniona, gdy wniosek o pozyskanie danych dotyczy numeru abonenckiego, którego użytkownikiem jest osoba obowiązana do zachowania tajemnicy. Co jednak w sytuacji, gdy przy okazji, na zasadzie ekscesu zebrane zostaną dane dotyczące takiej osoby. Wydaje się, że także i w takiej sytuacji takie dane telekomunikacyjne podlegają ochronie jako tajemnica zawodowa.

Krytycznie odnieść należy się też do przyznania w Projekcie możliwości złożenia zażalenia na postanowienie sądu o braku zgody na pozyskanie danych telekomunikacyjnych osoby zobowiązanej do ochrony tajemnicy zawodowej organowi, który wystąpił o wyrażenie zgody i braku takiego środka odwoławczego dla osoby, której te dane dotyczą w przypadku wydania przez sąd postanowienia o możliwości wykorzystania lub przyszłego pozyskania tych danych.

Generalnie też krytycznie należy ocenić propozycję by pozyskiwanie danych telekomunikacyjnych tak jak dotychczas nie podlegało żadnej uprzedniej, zewnętrznej kontroli. Skutecznym mechanizmem kontroli nie będzie na pewno, projektowane wprowadzenie obowiązku sprawozdawczego wobec sądów. Powziąć należy w szczególności wątpliwość co do tego, czy na podstawie przekazanego sprawozdania – w takim kształcie jak proponowane w Projekcie – sąd będzie miał możliwość skontrolowania prawidłowości pozyskania danych do konkretnej sprawy.

III. Konkluzje

Projekt nie realizuje postulatów płynących z wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. w stopniu wystarczającym. Projektowane regulacje przede wszystkim nie wprowadzają efektywnych mechanizmów nadzoru i kontroli nad stosowaniem kontroli operacyjnej oraz pozyskiwaniem danych telekomunikacyjnych przez służby.

W szczególności świadczą o tym propozycje stworzenia mechanizmu weryfikacji, czy zgromadzone dane dotyczą okoliczności chronionych jako tajemnica zawodowa. Przewidują one bowiem, że decyzja co do zakresu ochrony tych informacji, podejmowana ma być arbitralnie i nie będzie podlegać kontroli przez osoby obowiązane do zachowania tajemnicy zawodowej.