



KRAJOWA IZBA
RADCÓW PRAWNYCH

00-540 Warszawa, Aleje Ujazdowskie 41 lok. 2
tel/fax: 022 622 05 88, 622 84 28;33 • e-mail: kirp@kirp.pl • NIP: 526-10-43-011

L.dz. 12511 /OBSiL/2015

Warszawa, dnia 30 grudnia 2015 r.

SEKRETARIAT Z-CY SZEFA KS

L. dz.

Data wpływu 30. 12. 2015

Pan

Adam Podgórski

Zastępca Szefa Kancelarii Sejmu RP

Szanowny Panie Ministrze,

Dziękuję za skierowanie do mnie, przy Pana piśmie znak GMS-WP-173-293/15 datowanym na 28 grudnia br., w trybie art. 60 pkt. 2 ustawy o radcach prawnych, poselskiego projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw celem zaopiniowania tego projektu.

Pańskie pismo, które otrzymałem w dniu 29 grudnia br., nie określało terminu, w którym opinia winna być sporządzona, co w zaistniałych okolicznościach związanych z trwającym posiedzeniem Sejmu potraktowałem jako oczekiwanie na niezwłoczne opiniowanie projektu ustawy.

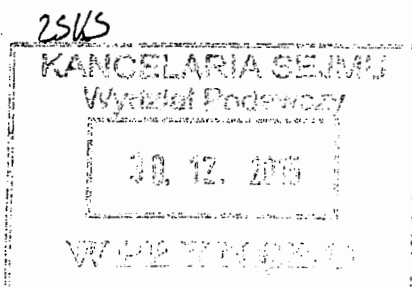
Wypełniając to oczekiwanie, niniejszym przekazuję stanowisko w przedmiocie projektu wspomnianej ustawy, sporządzone przez ekspertów Ośrodka Badań, Studiów i Legislacji Krajowej Rady Radców Prawnych z prośbą o pilne udostępnienie posłom. Informuję jednocześnie, że przekazane Sejmowi stanowisko zostaje umieszczone równocześnie na stronie www.kirp.pl prowadzonej przez Krajową Radę Radców Prawnych.

Pozostaję z wyrazami szacunku

Prezes

Krajowej Rady Radców Prawnych

r.pr. Dariusz Sałajewski



Warszawa, 30 grudnia 2015 r.

Stanowisko
Ośrodka Badań, Studiów i Legislacji Krajowej Rady Radców Prawnych
dotyczące
poselskiego projektu ustawy o zmianie ustawy o Policji
oraz niektórych innych ustaw
(druk sejmowy Nr 154)

I

W dniu 23 grudnia 2015 r. grupa posłów zainicjowała postępowanie legislacyjne w sprawie projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk sejmowy Nr 154).

Zgodnie z intencją autorów projektu, wyrażoną w uzasadnieniu, ma on na celu dostosowanie systemu prawa do wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. (sygn. akt K 23/11). W postępowaniu, stanowiącym kanwę przywołanego wyroku, na wniosek Rzecznika Praw Obywatelskich oraz Prokuratora Generalnego, Trybunał Konstytucyjny dokonał kontroli konstytucyjności wybranych przepisów ustawy z 6 kwietnia 1990 r. o Policji (Dz. U. z 2015 r., poz. 355 i 529), ustawy z 12 października 1990 r. o Straży Granicznej (Dz. U. z 2014 r., poz. 1402, ze zm.), ustawy z 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2011 r., Nr 41, poz. 214, ze zm.), ustawy z 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2013 r., poz. 568, ze zm.), ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2010 r., Nr 29, poz. 154, ze zm.), ustawy z 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U. z 2014 r., poz. 1411 i 1822), a także ustawy z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2014 r., poz. 253, ze zm.).

Trybunał badał zgodność z Konstytucją Rzeczypospolitej przepisów wyżej wymienionych ustaw, zawierających regulacje dotyczące kontroli operacyjnej, pozyskiwania danych telekomunikacyjnych, ochrony tajemnicy zawodowej w toku kontroli operacyjnej oraz niszczenia zbędnych danych telekomunikacyjnych. W wyroku orzekł m. in. o niezgodności z Konstytucją określonych przepisów wskazanych ustaw

instytucjonalnych, przez to, że nie przewidują niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy z 16 lipca 2004r. – Prawo telekomunikacyjne (Dz. U. z 2014 r., poz. 243), jak również stwierdził niekonstytucyjność określonych przepisów tych ustaw 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.

W kontekście oceny przedmiotowego projektu ustawy, na obecnym etapie jego procedowania, szczególnie warte przypomnienia jest to, iż **w uzasadnieniu wyroku z 30 lipca 2014 r. Trybunał Konstytucyjny zwrócił uwagę na potrzebę wprowadzenia koniecznych i pożądaných zmian w regulacjach prawnych, dotyczących kontroli operacyjnej, tak, by odpowiadały one w pełni standardom demokratycznego państwa prawnego.**

Po pierwsze, wskazane wyżej regulacje ustawowe powinny precyzować przedmiotowe przesłanki zarządzenia czynności operacyjnych. Ustawodawca nie może bowiem, w ważnej z punktu widzenia wolności i praw jednostki materii, posługiwać się zwrotami niedookreślonymi, ale zobowiązany jest zdefiniować zamknięty i możliwie wąski katalog poważnych przestępstw, uzasadniających stosowanie środków, tak poważnie ingerujących w sferę statusu jednostki.

Po drugie, ustawy powinny sprecyzować zamknięty rodzajowo katalog środków i metod działania, za pomocą których Policja i służby specjalne mogą w sposób niejawný gromadzić informacje o jednostkach. Określenie sposobów i metod ingerencji w konstytucyjnie chronioną sferę prywatności jednostki nie może być przedmiotem arbitralnej decyzji organów państwa.

Po trzecie, ustawy powinny precyzować maksymalny czas prowadzenia niejawných czynności, po upływie którego dalsze ich stosowanie jest niedopuszczalne. Tak określone terminy muszą przy tym uwzględniać potrzebę zapewnienia efektywności prac operacyjno – rozpoznawczych.

Po czwarte, ustawy powinny regulować procedurę zarządzania czynności operacyjno – rozpoznawczych, a także badania ich legalności, przez zewnętrzny i niezależny od organów władzy wykonawczej podmiot, najlepiej sąd. Regulacją ustawową muszą być objęte zasady wykorzystywania zgromadzonych materiałów oraz przesłanki i tryb ich niszczenia.

Po piąte, wskazane ustawy instytucjonalne muszą precyzyjnie regulować zakres wykorzystywania danych pozyskanych w toku czynności operacyjno – rozpoznawczych, a zwłaszcza wykorzystywanie ich w procesie karnym jako materiał dowodowy. Muszą również określać tryb postępowania z materiałami, które podlegają niezwłocznemu, protokolarnemu, komisijnemu zniszczeniu, z uwagi na ich zbędność lub nieprzydatność.

Podkreślenia wymaga, iż większość rozwiązań normatywnych, zawartych w opiniowanym projekcie ustawy jest zbieżna z propozycjami, przedłożonymi przez Senat poprzedniej kadencji w projekcie ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk sejmowy Nr 3765). Projekt ów jedynie połowicznie wykonywał wyrok Trybunału Konstytucyjnego, zwłaszcza w odniesieniu do konkretnych rozwiązań normatywnych, sygnalizowanych w uzasadnieniu orzeczenia i jako taki oceniony został krytycznie – zarówno w stanowisku Krajowej Rady Radców Prawnych, przesłanym Sejmowi 27 lipca 2015 r., jak również w wystąpieniu jej przedstawiciela na posiedzeniu sejmowej komisji Obrony Narodowej, 9 września br. Równie krytyczne uwagi pod adresem ówczesnego projektu zgłaszali obecni na posiedzeniu posłowie.

Tym większe zdumienie budzi fakt, iż obecny projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw nie dość, że powieliła błędne rozwiązania projektu poprzedniego, to jeszcze zawiera nowe propozycje, które bezsprzecznie pogłębiają stan niezgodności zarówno z Konstytucją z 2 kwietnia 1997 r., jak również budzą poważne wątpliwości co do zgodności z prawem unijnym, w świetle orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej. Analiza proponowanych w projekcie rozwiązań nie pozostawia wątpliwości, iż godzą one w szereg konstytucyjnie chronionych wolności i praw jednostki, zwłaszcza zaś w prawo do prywatności, tajemnicę korespondencji, jak również w prawo do obrony. **Wbrew deklaracji, wyrażonej przez wnioskodawców w uzasadnieniu projektu, ujęte w nim konstrukcje normatywne nie czynią zadość zasadzie subsydiarności, albowiem w odniesieniu do przesłanek wdrożenia przez Policję oraz inne organy uprawnione środków kontroli operacyjnej projekt nie odwołuje się ani razu do klauzuli stosowania ich wyłącznie wówczas, gdy inne środki okażą się bezskuteczne albo mogą być nieprzydatne. W praktyce oznacza to możliwość wykorzystywania środków kontroli operacyjnej na dowolnych zasadach, bez istnienia uzasadnionych podstaw, umożliwiając jednocześnie niczym nieograniczoną, a w szczególności pozbawioną kontroli inwigilację obywateli i**

instytucji. Tym samym, rozwiązania przyjęte w projekcie, dotyczące możliwości stosowania środków operacyjnych, budzą poważne wątpliwości pod kątem ich zgodności z zasadą proporcjonalności, wyrażoną w art. 31 ust. 3 Konstytucji Rzeczypospolitej Polskiej.

W świetle powyższych konstatacji, zastrzeżenia Ośrodka Badań, Studiów i Legislacji Krajowej Rady Radców Prawnych, zgłoszone wobec senackiego projektu z poprzedniej kadencji pozostają w pełni aktualne.

II

W odniesieniu do wymogu precyzyjnego określenia przedmiotowych przesłanek stosowania czynności operacyjno - rozpoznawczych, poprzez wskazanie w ustawie zamkniętego i możliwie wąskiego katalogu poważnych przestępstw, uzasadniających zarządzanie ich wdrożenia, autorzy projektu - wbrew jednoznacznej sygnalizacji Trybunału Konstytucyjnego zawartej w powołanym wyżej orzeczeniu - **powielili mankamenty dotychczas obowiązujących regulacji.** W art. 19 ust. 1 ustawy o Policji proponuje się bowiem stosowanie owych czynności w odniesieniu do przestępstw umyślnych, ściganych z oskarżenia publicznego. Tak więc projektodawca ponownie posługuje się w tym przypadku zwrotem niedookreślonym, miast wskazania wąskiego katalogu przestępstw, stosując tym samym kategoryzację rodzajową, obejmującą bardzo szeroki katalog czynów zabronionych określonych w ustawach karnych. Formuła ta nie spełnia wymogu pożądanej precyzji, zwłaszcza z punktu widzenia interesów jednostki. W stosunku do człowieka i obywatela ustawa powinna nie tylko jednoznacznie definiować zachowania narażające go na odpowiedzialność karną, ale również takie, w przypadku których dopuszczalna jest głęboka ingerencja państwa w sferę jego prywatności poprzez prowadzenie czynności operacyjno - rozpoznawczych, albowiem prowadzą one do ingerencji w szczególnie chronioną konstytucyjnie sferę praw i wolności. Biorąc pod uwagę szczególny - z punktu widzenia statusu jednostki - charakter projektowanej materii, ujęcie przedmiotowego zakresu stosowania kontroli operacyjnej w taki sposób, jak ma to miejsce w obecnej wersji projektu, niezależnie od zastrzeżenia w nim jej subsydiarnego charakteru, stoi w sprzeczności z regułą pewności prawa i godzi w zasadę zaufania obywatela do państwa oraz zasadę przyzwoitej legislacji. **Biorąc to pod uwagę należy jednoznacznie**

stwierdzić, iż kwestia ta wymaga zdecydowanej modyfikacji w toku dalszych prac nad projektem.

Natomiast, co się tyczy wymogu doprecyzowania w ustawie zamkniętego rodzajowo katalogu środków i metod działania w ramach owych czynności, projekt ustawy nowelizującej reguluje tę kwestię w sposób satysfakcjonujący. Podobnie pozytywnie ocenić należy ujętą w projekcie propozycję precyzyjnego określenia maksymalnego czasu prowadzenia kontroli operacyjnej, przez okres do 18 miesięcy, choć rozważenia wymaga kwestia ewentualnego skrócenia go maksymalnie do 12 miesięcy.

W tym kontekście zdziwienie budzi z kolei brak zastosowania precyzyjnego kryterium czasowego w odniesieniu do okresu jaki może obejmować pozyskiwanie przez służby danych telekomunikacyjnych, pocztowych i internetowych. Brak analogicznego ograniczenia temporalnego w odniesieniu do powyżej wskazanych danych przesądza o możliwości ich pozyskiwania z okresu bliżej nieokreślonej przeszłości.

III

Negatywnie ocenić należy przyjęty w projektowanej nowelizacji model zupełnie nieefektywnej kontroli legalności czynności operacyjno – rozpoznawczych. Brak stworzenia skutecznego mechanizmu badania zgodności z prawem stosowania szerokiego katalogu środków kontroli operacyjnej (które przewiduje projekt nowelizacji) przez zewnętrznego i niezależnego od organów władzy wykonawczej podmiot, prowadzi do naruszenia konstytucyjnych gwarancji ochrony wolności i praw jednostki, a także zasad demokratycznego państwa prawnego. Trybunał Konstytucyjny w przywołanym wyroku jednoznacznie uznał, że rozwiązaniem optymalnym w tym zakresie powinna być sądowa kontrola stosowania czynności operacyjno – rozpoznawczych. Tymczasem projektowane rozwiązania redukują relacje pomiędzy sądami, a służbami stosującymi kontrolę operacyjną w zasadzie do działań o charakterze sprawozdawczym, które w żadnej mierze nie stanowią instytucjonalnej gwarancji mogącej zapobiegać powstałym w toku czynności operacyjnych naruszeniom praw i wolności. Przewidziane w projektowanej ustawie obowiązki natury sprawozdawczej z pewnością nie stanowią efektywnego mechanizmu kontroli legalności, celowości i zasadności podejmowania czynności operacyjno – rozpoznawczych wobec obywateli, a mają jedynie walor statystyczny. Przewidziany w ustawie sposób wykonywania obowiązków sprawozdawczych (z zachowaniem wymogów ustawy z dnia

5 sierpnia 2010r. o ochronie informacji niejawnych) zakłada uniemożliwienie ewentualnym osobom zainteresowanym dostępem do informacji, czy w ich przypadku doszło do ingerencji w ich konstytucyjne prawa i wolności.

Z tych względów osoba, wobec której zastosowano środki kontroli operacyjnej, pozbawiona jest jakichkolwiek prawnych możliwości zakwestionowania zgodności z prawem zastosowania środków operacyjnych na drodze sądowej, choćby nawet miało to nastąpić *ex post*. Na niewątpliwą potrzebę wprowadzenia takich rozwiązań wprost wskazywał Trybunał Konstytucyjny, niemniej jednak nie znajduje to jakiegokolwiek odzwierciedlenia w projektowanej nowelizacji ustawy. Zaniechanie stworzenia realnych mechanizmów bieżącej kontroli sądowej nad czynnościami operacyjno – rozpoznawczymi prowadzi do sytuacji, w której osoba im poddana pozbawiona będzie skutecznej ochrony podstawowych konstytucyjnych praw i wolności.

Na uwagę zasługuje, iż zawarta w projekcie fasadowa regulacja sądowej kontroli legalności, przewidziana w art. 19 ust. 15h -15j ustawy o Policji (analogicznie w stosunku do innych służb) wobec materiałów zgromadzonych w ramach czynności operacyjno – rozpoznawczych, a dotycząca dopuszczalności ich wykorzystania w postępowaniu karnym, nie znajduje już zastosowania w odniesieniu do pozyskiwania danych telekomunikacyjnych, pocztowych i internetowych.

IV

Wzorem przedłożenia senackiego z poprzedniej kadencji, opiniowany projekt poselski zakłada, że kontrolą operacyjną objęte mają być również osoby, zobowiązane do ochrony tajemnicy obrończej, w rozumieniu art. 178 kodeksu postępowania karnego, jak również osoby, których działalność objęta jest tajemnicą zawodową (między innymi tajemnicą radcy prawnego i tajemnicą adwokacką), w rozumieniu art. 180 § 2 kodeksu postępowania karnego. Proponowana regulacja budzi istotne zastrzeżenia, zwłaszcza z punktu widzenia wyrażonego w art. 42 ust. 2 Konstytucji prawa do obrony i związanych z nim materialnych i procesowych gwarancji.

Zdecydowany sprzeciw budzi zwłaszcza procedura, proponowana w art. 19 ust. 15f ustawy o Policji i w odpowiednich przepisach pozostałych ustaw instytucjonalnych. Wskazany przepis projektu stanowi, iż w przypadku, gdy zachodzi przypuszczenie, że materiały, uzyskane w toku kontroli operacyjnej mogą zawierać informacje objęte

tajemnicą obrończą lub stanowiące tajemnice związane z wykonywaniem zawodu lub funkcji, o których mowa w art. 180 § 2 Kodeksu postępowania karnego (m. in. tajemnica radcy prawnego i tajemnica adwokacka), właściwy organ Policji przekazuje prokuratorowi te materiały. Tak sformułowany przepis zobowiązuje i uprawnia jednocześnie funkcjonariuszy Policji i odpowiednio innych uprawnionych formacji do dokonywania wstępnej selekcji materiałów, uzyskanych w toku kontroli operacyjnej i – w zasadzie – dyskrejonalnego decydowania o udostępnianiu ich prokuratorowi, a pośrednio sądowi, w trybie art. 19 ust. 15g projektu. W nawiązaniu do powyższych krytycznych uwag, odnoszących się do przyjętej w projekcie nieefektywnej formuły sądowej kontroli czynności operacyjno – rozpoznawczych, należy jednoznacznie stwierdzić, że rozwiązanie proponowane w art. 19 ust. 15f projektu i w odpowiednich przepisach pozostałych ustaw instytucjonalnych czyni tę kontrolę wręcz iluzoryczną. Zwraca także uwagę brak możliwości złożenia zażalenia przez osobę zobowiązaną do zachowania tajemnicy zawodowej (a więc i radcy prawnego), na postanowienie sądu o wykorzystaniu w postępowaniu karnym materiałów objętych tą tajemnicą. Ponadto, projektowana procedura wstępnego selekcjonowania materiałów operacyjnych przez organy uprawnionych formacji kłóci się również z logiką procesu karnego w fazie postępowania przygotowawczego, w której to prokurator jest gospodarzem postępowania. Rozwiązaniem o wiele bardziej racjonalnym byłoby zatem wprowadzenie regulacji, która obligowałaby organy uprawnionych formacji do przekazywania prokuratorowi wszystkich zgromadzonych materiałów operacyjnych, celem dokonania przezeń ich kwalifikacji, pod kątem tego, czy zawierają informacje, stanowiące tajemnicę adwokacką lub tajemnicę radcy prawnego. Za takim rozwiązaniem przemawia również fakt, iż prokurator, ustawowo zobowiązany do strzeżenia praworządności, zatem również legalności procesu karnego, daje rękojmię obiektywnego przeprowadzenia tej czynności, w o wiele większym stopniu niż funkcjonariusz, zainteresowany zgromadzeniem wszelkich możliwych dowodów, dających podstawę do wszczęcia i prowadzenia postępowania karnego, zwłaszcza w jego obecnej, kontradiktoryjnej formule. Nie ulega wątpliwości, że najlepszym rozwiązaniem jest jednak wprowadzenie zewnętrznego (co nie wyklucza jego połączenia organizacyjnego ze strukturą prokuratury) i niezależnego organu, do którego właściwości można przekazać te czynności.

Ponadto, w odniesieniu do standardów ochrony tajemnicy zawodowej radcy prawnego i adwokata, opiniowany projekt poselski stanowi wręcz regres względem

senackiego projektu z lipca br. Dotyczy to kwestii pozyskiwania danych telekomunikacyjnych, określonych w art. 180c i art. 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r., poz. 243, 827 i 1198), danych pocztowych, określonych w art. 82 ust. 1 pkt 1 ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe, oraz dodanych opiniowaną nowelizacją danych internetowych (co stanowi novum względem poprzedniego przedłożenia senackiego), określonych w art. 18 ust. 1-5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2013 r., poz. 1422, ze zm.). Obecny projekt nie przewiduje bowiem procedury, ujętej w art. 20ca projektu senackiego. Przewidywała ona, iż dane telekomunikacyjne i pocztowe, zawierające informacje dotyczące bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 kodeksu postępowania karnego, Komendant Główny Policji, Komendant Centralnego Biura Śledczego Policji albo komendant wojewódzki Policji powinien niezwłocznie przekazać prokuratorowi, który następnie powinien niezwłocznie skierować je do właściwego sądu okręgowego z wnioskiem o wyrażenie zgody na ich wykorzystanie w postępowaniu karnym. W art. 20cb ust. 1 ówczesny projekt stanowił również, że jeżeli z materiałów sprawy wynika, iż konieczne jest pozyskanie danych telekomunikacyjnych lub pocztowych zawierających informacje dotyczące bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 § 2 kodeksu postępowania karnego, Komendant Główny Policji, Komendant Centralnego Biura Śledczego Policji albo komendant wojewódzki Policji występują do właściwego sądu okręgowego z pisemnym wnioskiem o wyrażenie - w drodze postanowienia - zgody na pozyskanie tych danych i wykorzystanie ich w postępowaniu karnym. Opiniowany projekt poselski nie zawiera w tym względzie żadnej regulacji. **Co więcej, postępowanie w zakresie pozyskiwania danych, o których mowa w art. 20c projektu, pozbawione jest jakiejkolwiek kontroli sądowej, albowiem w świetle ust. 6 proponowanego artykułu dane telekomunikacyjne, pocztowe i internetowe, mające znaczenie dla postępowania karnego, odpowiedni funkcjonariusze Policji przekazują prokuratorowi właściwemu miejscowo lub rzeczowo, który podejmuje decyzję o zakresie i sposobie wykorzystania przekazanych danych.**

V

Konkludując powyższe rozważania należy stwierdzić, iż analiza przepisów, zawartych w poselskim projekcie ustawy o zmianie ustawy o Policji oraz niektórych

innych ustaw (druk sejmowy Nr 154) prowadzi do jednoznacznego wniosku, iż proponowana regulacja nie tylko nie przystaje do demokratycznych standardów, wyznaczonych w wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r. (sygn. akt K 23/11), ale dodatkowo poszerza zakres rozwiązań niezgodnych z Konstytucją Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. Jest również co najmniej wątpliwa z punktu widzenia prawa unijnego oraz orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej. Z powyższych względów, Krajowa Rada Radców Prawnych opiniuje negatywnie projekt w dotychczasowym brzmieniu.

Jednocześnie, rozumiejąc potrzebę uchwalenia stosownej ustawy przed datą wejścia w życie wyroku Trybunału Konstytucyjnego, postulujemy przeprowadzenie na dalszych etapach postępowania ustawodawczego gruntownych zmian treści projektu, zmierzających do dostosowania przyszłej ustawy do wymogów demokratycznego państwa prawnego, które projekt w obecnym kształcie narusza.

dr hab. Arkadiusz Bereza, prof. nadzw.

(-)

radca prawny

dr Przemysław Mijał

(-)

radca prawny

dr hab. Sławomir Patyra, prof. nadzw.

(-)

radca prawny

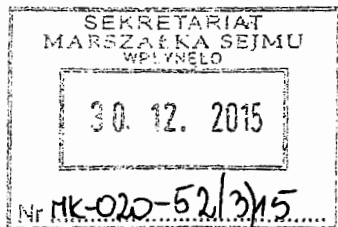


NACZELNA RADA ADWOKACKA

ul. Świętojerska 16, 00-202 Warszawa
tel. 22 505 25 00, 22 505 25 01, fax 22 505 25 08
e-mail: nra@nra.pl www.nra.pl

Warszawa, dnia 29 grudnia 2015 r.

NRA.12-SM-1.242.2015



Szanowny Pan

Marek Kuchciński

Marszałek Sejmu RP

OPINIA

**do poselskiego projektu ustawy o zmianie ustawy o Policji
oraz niektórych innych ustaw (druk sejmowy nr 154)**

Adwokatura jest ustawowo powołana do współdziałania w ochronie praw i wolności obywatelskich oraz w kształtowaniu i stosowaniu prawa (art. 1 ust. 1 ustawy z dnia 26 maja 1982 r. Prawo o adwokaturze, Dz. U. z 2015 r. poz. 615, z późn. zm.). Z tego powodu, w obszarze szczególnego zainteresowania Naczelnej Rady Adwokackiej, której zadaniem jest m.in. wydawanie opinii o projektach aktów prawodawczych oraz przedstawianie wniosków i postulatów w zakresie tworzenia i stosowania prawa, znajdują się projekty dotyczące gwarancji i ograniczeń w korzystaniu przez jednostki z praw i wolności konstytucyjnych.

Zaproponowane w poselskim projekcie ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw, druk sejmowy nr 154 (dalej: **Projekt**) rozwiązania będą prowadzić do poważnych ograniczeń w zakresie korzystania przez jednostki z ich praw i wolności konstytucyjnych, w szczególności z prawa do prywatności, tajemnicy korespondencji oraz zasady autonomii informacyjnej. Ponadto Naczelna Rada Adwokacka nie może zgodzić się ze stwierdzeniem zawartym w uzasadnieniu opiniowanego Projektu, iż ma on na celu dostosowanie stanu

prawnego do wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r., wydanego w sprawie pod sygn. akt K 23/11. Projekt ten bowiem tylko w niektórych aspektach odnosi się do ww. orzeczenia Trybunału Konstytucyjnego. W tym zakresie w zasadzie stanowi powtórzenie propozycji przedstawionych w *senackim projekcie ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw, druk sejmowy nr 3765* (dalej: **projekt senacki**), procedowanym przez Parlament poprzedniej kadencji, krytycznie opiniowanym przez Naczelną Radę Adwokacką¹. Projekt wprowadza też nowe rozwiązania w stosunku do senackiego projektu, które zdaniem Naczelnej Rady Adwokackiej ograniczają standardy ochrony praw i wolności obywatelskich, a nie wynikają z konieczności wykonania wyroku Trybunału Konstytucyjnego, wydanego w sprawie pod sygn. akt K 23/11.

W związku z przedłożeniem Projektu, a także wniesieniem – po zakończeniu prac legislacyjnych nad projektem senackim – wniosku do Trybunału Konstytucyjnego przez Rzecznika Praw Obywatelskich w dniu 4 grudnia 2015 r., zarejestrowanego pod sygnaturą akt K 41/15, a dotyczącego przepisów regulujących stosowanie kontroli operacyjnej, Naczelna Rada Adwokacka przedstawia kilka uwag dotyczących projektowanych rozwiązań. Ze względu na niezwykle szybkie tempo prac legislacyjnych (Projekt wypłynął do Sejmu RP w dniu 23 grudnia 2015 r., zaś jego pierwsze czytanie ma odbyć się w dniu 29 grudnia 2015 r.), Naczelna Rada Adwokacka przedstawia swoje uwagi w sposób skrótowy.

1. Na mocy przepisów zawartych w opiniowanym Projekcie, w znacznej mierze tożsamych z propozycjami senackiego projektu, adwokaci będą mogli być poddawani najbardziej ingerencyjnym środkom pracy operacyjnej – kontroli operacyjnej i pozyskiwaniu danych telekomunikacyjnych. Rozwiązanie takie godzi w prawa i wolności konstytucyjne, w szczególności w prawo do obrony, z którym nierozzerwalnie związane jest istnienie zaufania pomiędzy adwokatem świadczącym pomoc prawną a jego Mocodawcą. W Projekcie proponuje się wprowadzenie mechanizmu zakładającego, że to funkcjonariusze Policji lub innych służb będą decydować o tym, czy informacje uzyskane w trakcie działań operacyjnych zawierają tajemnicę obrończą lub adwokacką, i podejmować w tym zakresie dalsze działania związane z wykorzystaniem tych materiałów na potrzeby procesowe. Rozwiązanie takie stanowi poważne zagrożenie dla ochrony tych tajemnic i dla praw i wolności, ochronie których tajemnica ta służy.

¹ Kalendarium prac i aktywności NRA w zakresie senackiego projektu ustawy o Policji oraz niektórych innych ustaw dostępne jest pod adresem: <http://www.adwokatura.pl/z-zycia-nra/kalendarium-dzialan-nra-dotyczacych-projektu-ustawy-o-policji/>.

2. W ślad za stanowiskami przedstawianym w toku prac legislacyjnych nad projektem senackim w 2015 r., Naczelna Rada Adwokacka raz jeszcze podkreśla, że 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.
3. Podobnie, jak miało to miejsce w projekcie senackim, Projekt wprost wskazuje, że w ramach kontroli operacyjnej może dochodzić do utrwalania treści chronionych jako tajemnica zawodowa – adwokacka, obrończa oraz dziennikarska. Z treści Projektu wynika, że osoby obowiązane do ochrony tajemnicy obrończej i adwokackiej, nie są wykluczone spod działania przepisów o kontroli operacyjnej. Projekt, w ślad za projektem senackim, 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 chronionych jako tajemnica adwokacka, funkcjonariusz ma obowiązek 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.
4. W ocenie Naczelnej Rady Adwokackiej 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 przedprocesowy charakter czynności operacyjno – rozpoznawczych, do których zalicza się kontrola operacyjna – materiał dotyczący każdego poufnego kontaktu adwokata z osobą, niebędącą 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.

5. Naczelna Rada Adwokacka ponownie krytycznie odnosi także do proponowanego mechanizmu zwalniania z tajemnicy. Projektowany mechanizm 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. Zastrzeżenia Naczelnej Rady Adwokackiej 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 zobowiązany będzie je przekazać prokuratorowi. Niezrozumiała jest rola prokuratora, którego zadaniem ma być jedynie wnioskowanie do sądu o podjęcie decyzji w przedmiocie tych danych. Procedura w tym kształcie powoduje, że 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.² nie określają jakichkolwiek przesłanek, którymi kierować powinien się sąd podejmując decyzję o wykorzystaniu informacji, co stwarza ryzyko decyzji arbitralnych w tym zakresie.
6. W ślad za dotychczasowymi stanowiskami, dotyczących projektu senackiego, Naczelna Rada Adwokacka krytycznie ocenia też okoliczność, że projektowane rozwiązania nie przewidują, by postanowienie o wyrażeniu zgody na wykorzystanie materiałów zawierających tajemnicę prawnie chronioną, miało zawierać uzasadnienie. Stanowiące wzór dla tej instytucji, postanowienie wydane na podstawie art. 180 § 2 k.p.k. uzasadnienie takie natomiast zawiera.

² 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.

7. Naczelna Rada Adwokacka zwraca wreszcie uwagę, że Projekt, podobnie jak procedowany wcześniej projekt senacki, nie przewiduje możliwości złożenia zażalenia przez osobę obowiązaną do ochrony tajemnicy obrończej i adwokackiej, na postanowienie o wykorzystaniu w postępowaniu karnym materiałów zawierających tę tajemnicę.
8. 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 niejawną kontrolę 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.
9. Projekt ponadto nie wprowadza jakichkolwiek mechanizmów, mających na celu zagwarantowanie osobie, wobec której zastosowano środki kontroli operacyjnej, możliwości zakwestionowania, chociażby *ex post*, legalności zastosowania środków operacyjnych na drodze sądowej. Na potrzebę wprowadzenia takich regulacji zwracał uwagę Trybunał Konstytucyjny już w wyroku z 12 grudnia 2005 r., sygn. akt K 32/04 oraz w będącym jego następstwem postanowieniu sygnalizacyjnym z dnia 25 stycznia 2006 r., sygn. akt S 2/06. W ostatnim czasie na potrzebę taką wskazał także Rzecznik Praw Obywatelskich we wniosku z 4 grudnia 2015 r. sygn. akt K 41/15. Brak możliwości zakwestionowania legalności środków operacyjnych przez osobę, wobec której były one stosowane nie zapewnia skutecznej ochrony tajemnicy korespondencji oraz autonomii informacyjnej, gwarantowanych przepisami Konstytucji RP.
10. Twórcy Projektu wykraczają znacznie ponad cel wprowadzenia projektowanych rozwiązań, to jest wykonanie wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014

r., wydanego w sprawie pod sygn. akt K 23/11, w zakresie wprowadzenia rozwiązania polegającego na umożliwieniu Policji i innym służbom dostępu do tzw. „danych internetowych”. W szczególności za pole do olbrzymich nadużyć uznać należy przyznanie ww. podmiotom możliwości sięgania po te dane, bez jakiegokolwiek uprzedniej, zewnętrznej, merytorycznej kontroli. Wątpliwe jest również wprowadzenie w Projekcie pojęcia „dane internetowe” z odesłaniem do przepisu art. 18 ust. 1 – 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, skoro przedmiotowa regulacja takim pojęciem w żadnym miejscu się nie posługuje. Zarówno brak definicji legalnej pojęcia „dane internetowe”, jak i zróżnicowanie poziomu ich ochrony w stosunku do danych telekomunikacyjnych, stanowią w ocenie Naczelnej Rady Adwokackiej wadliwe rozwiązania.

11. Projekt przewiduje ponadto utrzymanie bardzo ogólnej podstawy prawnej do pozyskiwania przez Policję i inne służby danych telekomunikacyjnych. Pozyskiwanie tych danych będzie w zasadzie możliwe w ramach „wykonywania zadań” przez te podmioty, przy czym Centralne Biuro Antykorupcyjne uprawnione będzie także do pozyskiwania danych telekomunikacyjnych w celach analitycznych. Zdaniem Naczelnej Rady Adwokackiej projektowane rozwiązania utrwalają jedynie istniejący aktualnie stan, nadal pozostając w sprzeczności z celami, jakie przyświecały wprowadzeniu tzw. retencji danych, to jest wprowadzeniu mechanizmów pozwalających na efektywniejsze ściganie szczególnie poważnych przestępstw. Proponowany standard pozyskiwania danych telekomunikacyjnych jest nie do pogodzenia z tym wskazanym w wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r., sygn. akt K 23/11, a także w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej (wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 8 kwietnia 2014 r. w połączonych sprawach C-293/12 i C-594/12).

12. Projekt nie wprowadza skutecznych mechanizmów weryfikacji pozyskiwania przez Policję i inne służby danych telekomunikacyjnych, w tym także danych internetowych i pocztowych. Za skuteczną procedurę nie można uznać bowiem procedury przewidującej składanie przez Policję i inne służby półrocznych sprawozdań właściwemu sądowi okręgowemu. Składanie sprawozdań nie służy kontroli legalności, celowości i zasadności pozyskiwania w konkretnym przypadku danych telekomunikacyjnych, a jedynie oddaniu obrazu statystycznego, związanego z pozyskiwaniem danych obywateli. Ponadto, procedura związana ze składaniem sprawozdań nie będzie miała charakteru uprzedniego, a co najwyżej – z uwagi na jej fakultatywny charakter – następczy. Zdaniem

Naczelnej Rady Adwokackiej procedury kontroli nad uzyskiwaniem danych telekomunikacyjnych, pocztowych lub internetowych, sprawowanej następnie przez sąd okręgowy nie można uznać za skuteczną. Projektowane rozwiązania nie precyzują ponadto, co miałyby być przedmiotem „kontroli nad uzyskiwaniem przez Policję [i inne służby] danych telekomunikacyjnych, pocztowych lub internetowych, a także jakie – poza poinformowaniem organu Policji lub innej służby o jej wyniku – miałyby być jej efekty. Dodatkowo, Projekt – odmiennie niż projekt senacki – nie wprowadza obowiązku niezwłocznego usunięcia uzyskanych danych telekomunikacyjnych, pocztowych lub internetowych pozyskanych przez Policję lub inną służbę po stwierdzeniu przez sąd okręgowy braku podstaw do ich uzyskania.

13. Naczelna Rada Adwokacka zwraca także uwagę na sprzeczność pomiędzy proponowanymi rozwiązaniami dotyczącymi składania sprawozdań właściwym sądom okręgowym przez Policję i służby w zakresie pozyskiwania danych telekomunikacyjnych, pocztowych lub internetowych, a przepisami regulującymi podstawy sięgania po ww. dane. W Projekcie wskazuje się, że dane telekomunikacyjne, internetowe lub pocztowe będą mogły być pozyskiwane w związku z „realizacją zadań”, do których w przypadku Policji i innych służb należy m.in. ściganie przestępstw. Tymczasem w sprawozdaniu kierowanym do właściwego sądu okręgowego organy Policji i innych służb obowiązane będą wskazywać kwalifikacje prawne czynów, w związku z których zaistnieniem doszło do pozyskania ww. danych. Z analizy projektowanych rozwiązań wynika, że sądy okręgowe nie będą informowane o wszelkich przypadkach pozyskania danych telekomunikacyjnych, pocztowych i internetowych przez Policję i inne służby, skoro pozyskiwanie takich danych może odbywać się także w ramach realizacji przez te podmioty zadań innych niż ściganie przestępstw.

14. Za wątpliwą z perspektywy ochrony praw i wolności konstytucyjnych uznać należy także regulację Projektu przewidującą, że sprawozdanie dla sądów okręgowych będzie przygotowywane przez organy Policji i innych służb z zachowaniem wymogów ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych. Zdaniem Naczelnej Rady Adwokackiej rozwiązanie takie spowoduje, że osoba, której dane zostały pobrane nigdy zapewne nie poweźmie informacji, iż doszło do ingerencji w jej prawa i wolności konstytucyjne z uwagi na rygor ochrony informacji niejawnych. Procedura kontroli

dokonywanej przez sąd okręgowy nie przewiduje też jakiegokolwiek w niej udziału osoby, której dane zostały pobrane.

15. Projekt nie przewiduje też realizacji postulatu wprowadzenia zewnętrznego, eksperckiego ciała, które miałyby kontrolować działania Policji i innych służb w zakresie stosowania czynności operacyjno – rozpoznawczych.

16. Wreszcie wskazać należy, że wbrew deklarowanym intencjom wykonania wyroku Trybunału Konstytucyjnego z 30 lipca 2014 r., sygn. akt K 23/11, Projekt przewiduje wprowadzenie zmian, które w żaden sposób nie wynikają z tego wyroku. Takim rozwiązaniem jest przykładowo dodanie w art. 17 ust. 1 ustawy o CBA, przestępstwa z art. 305 k.k., które będzie można ścigać przy użyciu kontroli operacyjnej. W tym zakresie wskazać należy, że w uzasadnieniu Projektu nigdzie nie wskazano na konieczność wprowadzenia tej zmiany. Po wtóre, podkreślić należy, że przestępstwo z art. 305 k.k. w sytuacji, gdy pokrzywdzonym nie jest Skarb Państwa podlega ściganiu na wniosek, a zatem brak takiego oświadczenia pokrzywdzonego, niweczyć będzie efekty prowadzonej kontroli operacyjnej. Nie można też nie odnotować, że Projekt w istotny sposób rozbudowuje katalog przestępstw, które przy użyciu kontroli operacyjnej może ścigać Żandarmeria Wojskowa. Projekt proponuje tu dodanie kilkunastu czynów. Co ciekawe, tak szerokiego katalogu przestępstw nie przewidują przepisy dotyczące zadań Policji. Dla przykładu, w myśl projektu Żandarmeria Wojskowa będzie mogła prowadzić kontrolę operacyjną w zakresie takich czynów jak: nielegalne organizowanie adopcji (art. 211a k.k.), czy też skierowanych przeciwko wolności seksualnej i obyczajności, a zatem przestępstw nietypowych dla zakresu jej działania. Zdaniem Naczelnej Rady Adwokackiej wprowadzenie nowych typów czynów, których ściganie będzie możliwe przy użyciu kontroli operacyjnej powinno być każdorazowo szczegółowo i przekonująco uzasadnione oraz spełniać kryterium proporcjonalności regulacji.

Adw. Mikołaj Piętrzak

Przewodniczący Komisji
Praw Człowieka przy NRA

**Prezes
Naczelnej Rady Adwokackiej**

adw. Andrzej Ziara



**GENERALNY INSPEKTOR
OCHRONY DANYCH
OSOBOWYCH**

dr Edyta Blalak-Jomaa

Warszawa, dnia 30 grudnia 2015 r.

DOLiS – 033 – 640/15/BG

Pan

Marek Kuchciński

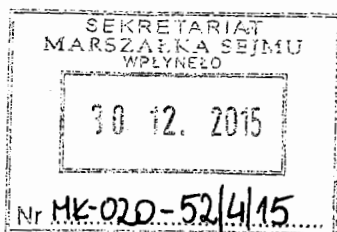
Marszałek Sejmu

Rzeczypospolitej Polskiej

Sejm Rzeczypospolitej Polskiej

ul. Wiejska 4/6/8

00-902 Warszawa



Szanowny Panie Marszałku,

w związku z wniesieniem do Sejmu projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw (druk nr 154), Generalny Inspektor Ochrony Danych Osobowych pragnie wyrazić swoje zastrzeżenia do proponowanych regulacji.

Trybunał Konstytucyjny w wyroku z dnia 30 lipca 2014 r. (sygn. akt K 23/11) za niezgodne z art. 47 i art. 49 w związku z art. 31 ust. 3 Konstytucji uznał przepisy art. 20c ust. 1 ustawy o Policji, art. 10b ust. 1 ustawy o Straży Granicznej, art. 36b ust. 1 pkt 1 ustawy o kontroli skarbowej, art. 30 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych, art. 28 ust. 1 pkt 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 32 ust. 1 pkt 1 ustawy o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego, art. 18 ust. 1 pkt 1 ustawy o Centralnym Biurze Antykorupcyjnym, art. 75d ust. 1 ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej, w zakresie, w jakim nie przewidują one niezależnej kontroli udostępniania danych telekomunikacyjnych, o których mowa w art. 180c i art. 180d ustawy Prawo telekomunikacyjne.

W opiniowanym projekcie ustawy zaproponowano, aby podmiotem wyznaczonym do kontroli nad uzyskiwaniem danych telekomunikacyjnych, pocztowych lub internetowych został: sąd okręgowy właściwy dla siedziby podmiotu, któremu udostępniono dane – w odniesieniu do Policji,

Straży Granicznej i Służby Celnej, wojskowy sąd okręgowy właściwy dla siedziby organu Żandarmerii Wojskowej, Sąd Okręgowy w Warszawie – w odniesieniu do kontroli skarbowej, Agencji Bezpieczeństwa Wewnętrznego i Centralnego Biura Antykorupcyjnego oraz Wojskowy Sąd Okręgowy w Warszawie – w odniesieniu do Służby Kontrwywiadu Wojskowego.

Zdaniem Generalnego Inspektora **zapropozowana forma kontroli jest niewystarczająca** – przepisy nie nakładają bowiem na Policję i służby innych nowych obowiązków poza przekazywaniem sądom raz na 6 miesięcy sprawozdań obejmujących liczbę przypadków pozyskania w okresie sprawozdawczym danych telekomunikacyjnych, pocztowych lub internetowych oraz rodzaj tych danych, a także kwalifikacje prawne czynów, w związku z zaistnieniem których wystąpiono o dane telekomunikacyjne, pocztowe lub internetowe albo informacje o pozyskaniu danych w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych.

W ramach kontroli sąd **może** zapoznać się z materiałami uzasadniającymi udostępnianie danych – sądom nie przyznano przy tym kompetencji do oceny zasadności pozyskania danych w określonej sytuacji oraz nie przewidziano procedury niszczenia danych w przypadku stwierdzenia braku podstaw do ich pozyskania (a zatem pozyskanych niezgodnie z prawem). Spod jakiegokolwiek kontroli wyłączono m. in. pozyskiwanie danych określonych w art. 161 ustawy Prawo telekomunikacyjne oraz danych z wykazu, o którym mowa w art. 179 ust. 9 tej ustawy.

Proponowany w projekcie model przewiduje jedynie fakultatywną kontrolę następczą pozyskiwania danych telekomunikacyjnych, pocztowych i internetowych (zachodzi zatem podstawowa obawa, że w praktyce sądy nie będą z tego uprawnienia korzystać), co nie może zostać uznane za należyte wykonanie wyroku Trybunału Konstytucyjnego.

Przypomnieć należy, iż Trybunał uznał za konieczne wprowadzenie proceduralnego wymogu, którym jest **kontrola nad niejawnym pozyskiwaniem informacji o osobach przez niezależny od rządu organ państwa**. Status ustrojowy i zakres ustawowych kompetencji takiego organu ma gwarantować efektywną, niezależną i profesjonalną kontrolę nad służbami policyjnymi i ochrony państwa. Konieczne jest, by był to organ niezależny od rządu i niepozostający z funkcjonariuszami pozyskującymi dane w bezpośredniej lub pośredniej relacji zwierzchności. Wymaganie to uznać należy za ugruntowane w dotychczasowym orzecznictwie Trybunału Konstytucyjnego, a także Europejskiego Trybunału Praw Człowieka i Trybunału Sprawiedliwości Unii Europejskiej (jak wskazane zostało w cz. III, pkt 2 i 3 uzasadnienia wyroku – np. wyrok TK z 12 grudnia 2005 r., sygn. K 32/04; orzeczenia ETPC z: 29 czerwca 2006 r. w sprawie Weber i Saravia przeciwko Niemcom, skarga 54934/00; 2 września 2010 r. w sprawie Uzun przeciwko Niemcom, skarga nr 35623/05).

Trybunał nie przesądził jak dokładnie ma wyglądać procedura dostępu do danych, a w szczególności, czy konieczne ma być w odniesieniu do każdego rodzaju zatrzymywanych danych, o których mowa w art. 180c i art. 180d prawa telekomunikacyjnego, uzyskanie zgody na ich udostępnienie. Zdaniem Trybunału, nie jest wobec tego wykluczone – w odniesieniu do udostępniania danych telekomunikacyjnych w toku czynności operacyjno-rozpoznawczych – wprowadzenie, jako zasady, kontroli następczej. Jak wskazano w wyroku, „regulując ten mechanizm, ustawodawca powinien uwzględnić m.in. specyfikę działania i ustawowy zakres zadań poszczególnych rodzajów służb, sytuacje niecierpiące zwłoki, w których szybkie pozyskanie danych telekomunikacyjnych może być niezbędne dla zapobieżenia popełnieniu przestępstwa lub jego wykrycia. **Trybunał dostrzega jednak argumenty za wprowadzeniem kontroli uprzedniej w pewnych wypadkach. W szczególności chodzić może o dostęp do danych telekomunikacyjnych osób wykonujących zawody zaufania publicznego lub jeśli nie ma konieczności pilnego działania służb**”. Z powyższego wynika, że w sytuacjach, kiedy nie potrzeba pilnego działania służb nie zachodzi, kontrola powinna mieć charakter uprzedni. Dzięki temu przypadki sięgania po dane mogłyby podlegać ocenie pod względem spełniania kryteriów adekwatności, niezbędności i celowości. Tymczasem, projektowane przepisy w żadnej sytuacji nie przewidują przeprowadzania kontroli uprzedniej – nawet, gdy miałyby zostać pozyskane dane dotyczące bezpośrednio osoby wykonującej zawód lub funkcję, o których mowa w art. 180 §2 Kodeksu postępowania karnego.

Jak wynika z informacji przygotowanej przez Urząd Komunikacji Elektronicznej, w 2014 r. służby, sądy i prokuratury złożyły łącznie 2 177 916 zapytań o dane telekomunikacyjne. Większa kontrola nad tym procesem pomogłaby zapobiec przypadkom sięgania po dane w sposób automatyczny i tym samym ograniczyć skalę zjawiska. Skoro bowiem pozyskiwanie danych dokonuje się w sposób niejawnny, bez wiedzy i woli podmiotów, o których informacje są gromadzone, **brak niezależnej kontroli organów państwa nad tym procesem stwarza ryzyko nadużyć**. Może to nie tylko przyczyniać się do nieuzasadnionej ingerencji w wolności lub prawa człowieka, ale i stanowić zagrożenie demokratycznych mechanizmów sprawowania władzy. Wymóg unormowania w ustawie proceduralnych mechanizmów przeciwdziałających arbitralności podczas pozyskiwania danych telekomunikacyjnych jest tym silniejszy, im szerszy jest zakres kompetencji organów państwa do niejawnego pozyskiwania informacji.

Nie można uznać za wystarczający modelu kontroli zaproponowanego przez projektodawcę, który nie przewiduje jako zasady **każdorazowej, obowiązkowej oceny adekwatności, niezbędności i celowości udostępniania danych telekomunikacyjnych, pocztowych i internetowych**. Nadal nie istnieje zatem gwarancja odpowiedniego poziomu ochrony prywatności i tajemnicy komunikowania się osób, których dane są pozyskiwane przez Policję i służby. Nie

przesądzać jakie konkretnie organy miałyby zajmować się taką kontrolą. Generalny Inspektor stoi na stanowisku, iż projektowane przepisy powinny szczegółowo określać mechanizmy kontroli. Wskazać również należy, iż **kontrola następcza powinna być traktowana jako wyjątek i stosowana jedynie w sprawach niecierpiących zwłoki**. W każdym jednak przypadku niezależny organ powinien ocenić czy pozyskanie danych jest w konkretnej sytuacji rzeczywiście niezbędne i należycie uzasadnione oraz czy cel, w którym dane są udostępniane nie mogłyby zostać zrealizowany przy użyciu innych, mniej ingerujących w prywatność jednostki środków.

Zapowiedzi uregulowania w przepisach zewnętrznej kontroli przez niezależny autonomiczny organ, znalazły się już w opracowanym w 2011 r. *Raporcie dotyczącym retencji danych telekomunikacyjnych. Propozycje wprowadzenia nowych regulacji ograniczających ingerencję organów państwowych w prywatność obywateli oraz wzmacniających mechanizmy kontroli nad służbami specjalnymi w kontekście prac nad zmianą przepisów dotyczących dostępu do danych telekomunikacyjnych*. Przedmiotowy raport podkreślał ograniczone możliwości takiej kontroli wobec służb specjalnych realizujących swoje kompetencje w zakresie wykonywania czynności operacyjno – rozpoznawczych i jako remedium proponował model niezależnego, powoływanego przez parlament, organu kontrolnego, którego celem byłaby **kontrola przestrzegania przez służby specjalne Konstytucji Rzeczypospolitej Polskiej oraz innych przepisów prawa, szczególnie w zakresie praw i wolności obywatelskich**. W dokumencie tym dość kompleksowo odniesiono się do przedmiotowej instytucji, omawiając tak istotne z punktu widzenia jego działania zagadnienia, jak powoływanie i skład, zadania, kompetencje oraz wyniki pracy organu kontrolnego.

Ponadto należy przypomnieć, że w informacji o wynikach kontroli *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*, Najwyższa Izba Kontroli wskazała, iż „sięganie po dane retencyjne stanowi istotną ingerencję w prawa i wolności obywatelskie, w szczególności prawo do prywatności. (...) W obecnym stanie prawnym nie istnieje żaden podmiot, który mógłby sprawować rzeczywistą kontrolę nad wykorzystaniem tego środka przez uprawnione organy, służby i formacje. **Sytuacja ta jest wyjątkowa w zestawieniu ze standardami przyjętymi w większości państw Unii Europejskiej. W 24 państwach taką kontrolę sprawuje sąd lub prokuratura albo niezależny organ administracyjny**”.

Zgodnie z opublikowanym w 2011 r. *sprawozdaniem Komisji Europejskiej na temat implementacji dyrektywy 2006/24/WE przez kraje członkowskie Unii Europejskiej* (stanowiącym wynik analizy porównawczej 25 raportów krajowych) **tylko w trzech państwach – w Irlandii, na Malcie i w Wielkiej Brytanii – nie była sprawowana kontrola uprzednia nad udostępnianiem**

danych telekomunikacyjnych, a w trzech kolejnych – w Polsce, na Łotwie i Słowacji – brak było jakiegokolwiek organu kontroli zewnętrznej.

Z uwagi na powyższe, Generalny Inspektor wskazuje, iż projektowane przepisy przewidywać powinny **każdorazową, obowiązkową kontrolę przez niezależny organ adekwatności, niezbędności i celowości udostępniania danych telekomunikacyjnych, pocztowych i internetowych**. W tym miejscu należy również zauważyć, iż **projekt nie zakłada stosowania zasady subsydiarności**, tj. ograniczenia możliwości sięgania po dane do sytuacji, gdy inne środki okazały się bezskuteczne albo mogą być nieprzydatne. Sądy nie mogłyby zatem ocenić, na ile sięgnięcie w określonej sytuacji po dane było rzeczywiście niezbędne i należycie uzasadnione, co dodatkowo osłabia poziom ochrony prywatności jednostek.

Odnosząc się do innych zmian wprowadzonych przez projekt, za niedostateczną realizację wyroku Trybunału Konstytucyjnego należy uznać przepisy ograniczające czas przeprowadzania kontroli operacyjnej przez Agencję Bezpieczeństwa Wewnętrznego i Agencję Wywiadu oraz Służbę Kontrwywiadu Wojskowego. Zgodnie ze stanowiskiem Trybunału, „ustawa ma precyzować maksymalny czas prowadzenia niejawnych czynności, po upływie którego dalsze ich prowadzenie jest już niedopuszczalne. (...) Ustawodawca musi mieć także na uwadze, że w **demokratycznym państwie prawa nie jest dopuszczalne – nawet za zgodą sądu i w sytuacji podejrzenia popełnienia nawet poważnych przestępstw – prowadzenie czynności operacyjno-rozpoznawczych bezterminowo, choćby miało się to wiązać z bezpowrotną utratą dowodów**”. Tymczasem, w przypadku wyżej wymienionych służb, dopuszczalne byłoby przedłużenie kontroli operacyjnej na następujące po sobie okresy, z których żaden nie może trwać dłużej niż 12 miesięcy (podczas gdy w przypadku innych podmiotów uprawnionych do prowadzenia kontroli operacyjnej łączna długość okresów nie może przekraczać 12 miesięcy). W praktyce, proponowane rozwiązanie stwarzałoby zatem możliwość bezterminowego prowadzenia czynności operacyjno-rozpoznawczych, co stoi w sprzeczności ze standardami konstytucyjnymi i intencją Trybunału.

Projekt przewiduje ponadto prowadzenie rejestrów postanowień, pisemnych zgód, wniosków i zarządzeń dot. kontroli operacyjnej. Nie został przy tym określony sposób prowadzenia tych rejestrów oraz wzory dokumentów wchodzących w ich zakres, co – jeżeli w rejestrach takich miałyby być przetwarzane również dane osobowe – nie może zyskać akceptacji Generalnego Inspektora Ochrony Danych Osobowych. **Przepisy rangi ustawowej powinny bowiem regulować zasadnicze kwestie dotyczące prowadzenia rejestru, w szczególności zaś katalog danych znajdujących się w rejestrze, okres przechowywania tych danych, zasady udostępniania informacji z rejestru, krąg podmiotów mających dostęp do danych**.

Kolejną kwestią, która budzi zastrzeżenia Generalnego Inspektora jest brak określenia w projekcie okresu, przez który uprawnione podmioty mogą przetwarzać pozyskane dane

telekomunikacyjne, pocztowe i internetowe. Stoi to w sprzeczności z wyrażoną w art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych zasadą ograniczenia czasowego, zgodnie z którą **dane mogą być przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.** Projekt przewiduje jedynie, iż dane, które nie mają znaczenia dla postępowania karnego, podlegają niezwłocznemu komisijnemu i protokolarnemu zniszczeniu. Nie został natomiast uregulowany sposób postępowania z danymi wykorzystanymi w postępowaniu, w tym kwestia weryfikacji potrzeby ich dalszego przetwarzania. **W praktyce może prowadzić to do nieuzasadnionego, bezterminowego przechowywania danych.** Okres przetwarzania danych telekomunikacyjnych, pocztowych i internetowych powinien zatem być określony w sposób precyzyjny, tak, aby wyeliminować ryzyko nadużyć (istniejące obecnie wobec faktu, iż nie przewidziano zewnętrznej kontroli niezbędności dalszego przetwarzania danych do realizacji ustawowych zadań).

W uzasadnieniu do wyroku Trybunał Konstytucyjny podkreślił również, że niejawnie pozyskiwanie przez organy władzy publicznej informacji o jednostce wymaga zachowania daleko idących gwarancji proceduralnych – przede wszystkim **ma istnieć obowiązek poinformowania jednostki o podjętych wobec niej działaniach operacyjno-rozpoznawczych oraz pozyskaniu informacji na jej temat** (bez względu na to, czy były to osoby podejrzane o naruszenie prawa, czy osoby postronne, które przypadkowo stały się obiektem kontroli). W opinii Trybunału, ustawodawca powinien zagwarantować późniejsze poinformowanie o tym fakcie (gdyż powiadomienie jednostki na etapie wykonywania działań operacyjno-rozpoznawczych i gromadzenia informacji narażałoby te działania na nieskuteczność). Na konieczność ustanowienia takiego obowiązku informacyjnego zwracał już uwagę TK w postanowieniu z 25 stycznia 2006 r., sygn. S 2/06). Zapewnienie informacji jest przesłanką skorzystania przez jednostki z wynikającego z art. 51 ust. 3 Konstytucji prawa dostępu do urzędowych dokumentów i zbiorów danych. Jak zauważył Trybunał, **zaniechanie poinformowania o zebraniu o jednostkach informacji przez władze publiczne samo w sobie stanowi naruszenie art. 51 ust. 3 i 4 Konstytucji.** Skoro jednostka nie wie o zebraniu na jej temat określonych informacji – ponieważ dokonało się to w sposób niejawny, bez jej wiedzy i zgody – nie dysponuje możliwością uzyskania dostępu do nich i nie może żądać ich sprostowania lub usunięcia na warunkach określonych w art. 51 ust. 4 Konstytucji. Z uwagi na powyższe, Generalny Inspektor wskazuje na konieczność uzupełnienia projektu o obowiązek informacyjny wobec osób, których dane zostały pozyskane przez Policję i służby.

Należy ponadto dodać, iż **kwestia sięgania przez Policję i służby po dane telekomunikacyjne nie może zostać uregulowana w sposób prawidłowy bez odniesienia się do wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 8 kwietnia 2014 r.,**

stwierdzającego nieważność dyrektywy 2006/24 w sprawie zatrzymywania danych w połączonych sprawach C-293/12 i C-594/12 *Digital Rights Ireland*. TSUE uznał nieważność dyrektywy ze względu na naruszenie art. 7 (poszanowanie życia prywatnego i rodzinnego) i 8 (ochrona danych osobowych) w zw. z art. 52 ust. 1 Karty Praw Podstawowych Unii Europejskiej. Jako przyczynę nieważności dyrektywy Trybunał wskazał brak proporcjonalności zawartych w niej rozwiązań, które, mimo iż adekwatne do celu, który ma zostać za ich pomocą osiągnięty, ingerują zbyt głęboko w prawa podstawowe. TSUE uznał, że ten sam cel (zwalczanie poważnej przestępczości oraz zapewnienie bezpieczeństwa publicznego) można było osiągnąć środkami, które w mniejszym stopniu ingerują w prawa obywateli. W odniesieniu do szczegółowych regulacji, Trybunał zauważył między innymi następujące uchybienia:

- w dyrektywie nie przewidziano jakiegokolwiek zróżnicowania, ograniczenia lub wyjątku w zależności od celu dotyczącego zwalczania poważnych przestępstw,
- dyrektywa nie przewiduje żadnego obiektywnego kryterium, które pozwoliłoby zagwarantować, że właściwe organy krajowe będą miały dostęp do danych i będą mogły je wykorzystywać wyłącznie w celu zapobiegania, wykrywania i ścigania przestępstw, które z uwagi na zakres i wagę ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty, można uznać za wystarczająco poważne, by taką ingerencję uzasadnić,
- dyrektywa nie określa żadnych materialnych i proceduralnych przesłanek, w przypadku zaistnienia których właściwe organy krajowe będą mogły uzyskać dostęp do danych i następnie je wykorzystać,
- dyrektywa nie zawiera jasnych i precyzyjnych reguł określających zakres ingerencji w prawa podstawowe ustanowione w art. 7 i 8 karty.

Mimo iż wyrok w sprawie *Digital Rights Ireland* nie powoduje automatycznie nieważności aktów prawa krajowego implementujących dyrektywę 2006/24, to konieczne jest uwzględnienie go w pracach legislacyjnych nad projektem ustawy, który dotyczy tej samej materii. Tymczasem, zaproponowanych w projekcie rozwiązań nie można uznać za zgodne z wytycznymi Trybunału Sprawiedliwości Unii Europejskiej.

Przykładowo, zaproponowany art. 20c ust. 1 ustawy o Policji przewiduje możliwość pozyskiwania przez Policję danych telekomunikacyjnych, pocztowych i internetowych m.in. w celu rozpoznawania, zapobiegania, zwalczania, wykrywania albo uzyskania i utrwalenia dowodów przestępstw – bez ograniczenia tego uprawnienia do sytuacji związanych z przestępstwami poważnymi. Zachodzi zatem potrzeba ponownego przeglądu katalogu sytuacji, w których dopuszczalne jest sięganie po dane przez Policję i służby.

Podsumowując, w opinii Generalnego Inspektora Ochrony Danych Osobowych, zaproponowana nowelizacja ustawy o Policji i innych ustaw nie stwarza wystarczających gwarancji ochrony prywatności i tajemnicy komunikowania się obywateli, a tym samym nie stanowi pełnej realizacji wyroku Trybunału Konstytucyjnego z dnia 30 lipca 2014 r. (sygn. akt K 23/11).

Z wyrazami szacunku

GENERALNY INSPEKTOR
OCHRONY DANYCH OSOBOWYCH

[Podpis]
dr Edyta Bielak-Jomaa

