PANOPTYKON
F U N D A C J A

Zarząd: Katarzyna Szymielewicz, Małgorzata Szumańska
Rada programowa: Adam Bodnar, Ewa Charkiewicz, Dominika Dörre-Nowak, Józef Halbersztadt, Joanna Kamiol, Monika Płatek, Maciej Ślusarek, Piotr Waglowski, Roman Wieruszewski

Warszawa, 13 czerwca 2012 r.

Szanowny Pan
Jacek Cichocki
Minister Spraw Wewnętrznych

Fundacja PANOPTYKON dziękuje za zaproszenie do przedstawienia swoich uwag do opublikowanych 28 maja 2012 r. „Założeń projektu ustawy o zmianie niektórych ustaw, w związku z pozyskiwaniem i wykorzystywaniem danych telekomunikacyjnych" (dalej: „Założenia"). Niestety w naszej ocenie przedstawiony dokument nie zbliża nas do rozwiązania złożonego problemu gromadzenia danych telekomunikacyjnych na potrzeby bezpieczeństwa oraz dostępu Policji i służb specjalnych do danych podlegających obowiązkowej retencji.

Założenia są dokumentem mało konkretnym i w rzeczywistości powtarzają pojawiające się od wielu miesięcy, bardzo ogólne postulaty reformy. Zakłada się w nich zmianę 15 ustaw – przede wszystkim tzw. ustaw kompetencyjnych regulujących działania Policji i innych służb[1], ale również ustaw o ustroju sądów powszechnych[2] i sądów wojskowych[3] oraz procedur cywilnej (dalej: „Kpc") i karnej (dalej: „Kpk"). Z założeń nie wynika nawet kierunek zmian przewidywanych w Kpc, Kpk oraz ustroju sądów powszechnych i wojskowych. Z drugiej strony planowane zmiany w ustawach kompetencyjnych również nie odnoszą się w sposób

[1] Jako ustawy kompetencyjne określamy: ustawę z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U z 2010 r. nr 29 poz. 154 j.t. z późn. zm.), ustawę z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (Dz. U. z 2006 r. nr 104 poz. 709 z późn. zm.), ustawę z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz. U z 2006 nr 104 poz. 708 z późn. zm.), ustawę z dnia 6 kwietnia 1990 r. o Policji (Dz. U z 2007 r. nr 43 poz. 277 j.t. z późn. zm.), ustawę z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. z 2011 r. nr 116 poz. 675 j.t. z późn. zm.), ustawę z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych. (Dz. U. z 2001 r. nr 123 poz. 1353 z późn. zm.), ustawę z dnia 28 września 1991 r. o kontroli skarbowej (Dz. U. z 2011 r. nr 41 poz. 214 j.t.) oraz ustawę z dnia 27 sierpnia 2009 r. o Służbie Celnej (Dz. U. z 2009 r. nr 168 poz. 1323 z późn. zm.).

[2] Ustawa z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych (Dz. U. z 2001 r. nr 98 poz. 1070 z późn. zm.)

[3] Ustawa z dnia 21 sierpnia 1997 r. Prawo o ustroju sądów wojskowych (Dz. U. z 1997 nr 117 poz. 753 z późn. zm.).

szczegółowy i wyczerpujący do wszystkich problemów zidentyfikowanych w tym obszarze[4]. Zaskakujące jest, że – pomimo wielu miesięcy prac[5] – rządowi nie udało się przedstawić kompleksowego projektu ustawy zmieniającej wskazane przepisy lub przynajmniej konkretniejszych założeń takiej ustawy. Byłoby to zgodne z wielokrotnymi deklaracjami Ministra Jacka Cichockiego, który publicznie zobowiązywał się do przedstawienia do końca maja 2012 r. projektu kompleksowej zmiany przepisów dotyczących retencji danych telekomunikacyjnych[6]. Co więcej, w ocenie Fundacji PANOPTYKON przedstawione założenia nie są zgodne z zasadami prawidłowej legislacji, bowiem nie zawierają oceny przewidywanych skutków (kosztów i korzyści) społeczno-gospodarczych regulacji. Obowiązek przedstawienia takiej oceny wynika z § 9 Regulaminu pracy Rady Ministrów[7].

Jednocześnie pragniemy podkreślić, że Fundacja PANOPTYKON z dużym entuzjazmem przyjmuje deklarowane cele i kierunki zmian. W Założeniach czytamy, że „celem projektowanej ustawy będzie ograniczenie ingerencji organów państwowych w prywatność poszczególnych osób oraz wzmocnienie mechanizmów kontroli nad pozyskiwaniem i wykorzystywanie danych telekomunikacyjnych przez uprawnione służby i organy". Szczegółowa analiza Założeń prowadzi jednak do wniosku, że zdecydowanie różnimy się w wizji metod i środków, które miałyby służyć realizacji tego celu.

1. Przedmiotowa dopuszczalność retencji danych

Obecnie obowiązujące przepisy pozwalają na bardzo szeroki dostęp Policji oraz służb do danych telekomunikacyjnych. Przedstawia to poniższa tabela:

Służba	Cel sięgania po dane	Typ przestępstw
POLICJA (art. 20 c ustawy o policji)	▪ Zapobieganie ▪ Wykrywanie	Wszystkie przestępstwa
KONTROLA SKARBOWA (art. 36b ustawy o kontroli skarbowej)	▪ Zapobieganie ▪ Wykrywanie	Przestępstwa skarbowe
SŁUŻBA CELNA (art. 75d ustawy o Służbie Celnej)	▪ Zapobieganie ▪ Wykrywanie	Przestępstwa skarbowe
STRAŻ GRANICZNA (art. 10b ustawy o Straży	▪ Zapobieganie ▪ Wykrywanie	Wszystkie przestępstwa

[4] W „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" wskazano m.in. na konieczność powołania niezależnego organu, powoływanego przez Sejm, którego zadaniem byłoby kontrolowanie praktyki sięgania po dane telekomunikacyjne przez policję i służby specjalne. Tymczasem opiniowane Założenia nie odnoszą się do konieczność istnienia niezależnego organu kontrolnego.

[5] Jeszcze w październiku 2011 r. Minister Jacek Cichocki w wypowiedział prasowych deklarował, że są już przygotowane szczegółowe propozycje dotyczące nowelizacji 14 ustaw, mające na celu ograniczenie okresu retencji przechowywania danych telekomunikacyjnych do jednego roku, ograniczenie zakresu ich wykorzystywania przez uprawnione organy do ścigania poważnych przestępstw oraz zwiększenie kontroli nad wykorzystywaniem tych danych, por.
http://wiadomosci.gazeta.pl/wiadomosci/1,114873,10441264,Cichocki__Propozycja_ograniczenia_dostepu_sluzb_do.html

[7] Uchwała nr 49 Rady Ministrów z dnia 19 marca 2002 r. Regulamin pracy Rady Ministrów (M.P. z 5 kwietnia 2002 r.).

Granicznej)		
ŻANDARMERIA WOJSKOWA (art. 30 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych)	▪ Zapobieganie ▪ Wykrywanie	Wszystkie przestępstwa oraz przestępstwa skarbowe
AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO (art. 28 i 5 ust.1 ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu)	W celu realizacji zadań ustawowych: ▪ zapobieganie ▪ rozpoznawanie ▪ wykrywanie Ponadto m.in.: ▪ realizowanie zadań związanych z ochroną informacji niejawnych ▪ uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego	Przestępstwa o szczególnym charakterze (np. szpiegostwo, terroryzm)
CENTRALNE BIURO ANTYKORUPCYJNE (art. 18 ustawy o CBA)	▪ rozpoznawanie ▪ zapobieganie ▪ wykrywanie Ponadto m.in.: ujawnianie i przeciwdziałanie nieprzestrzeganiu ustawy o ograniczeniu prowadzenia działalności gospodarczej przez osoby pełniące funkcje publiczne	Przestępstwa o szczególnym charakterze (np. przeciwko wymiarowi sprawiedliwości) o charakterze korupcyjnym
SŁUŻBA KONTRWYWIADU WOJSKOWEGO (art. 32 i 5 ustawy o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego)	M.in.: ▪ rozpoznawanie ▪ zapobieganie ▪ wykrywanie	Przestępstwa popełniane przez żołnierzy pełniących czynną służbę wojskową

Zgodnie z Dyrektywą 2006/24/WE[8] (dalej: „Dyrektywa retencyjna", „Dyrektywa") dostęp do danych możliwy jest w celu **„dochodzenia, wykrywania i ścigania poważnych przestępstw"**.

[8] Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z 15 marca 2006 r., pkt 21.

W naszej ocenie przepis ten wciąż wymaga prawidłowego wdrożenia do polskiego porządku prawnego zarówno na poziomie **dopuszczalnych celów sięgania po dane**, jak i **kategorii przestępstw**, w związku z którymi jest to dopuszczalne. W ocenie Fundacji PANOPTYKON cytowany przepis został błędnie wdrożony do polskiego prawa, które pozwala na wykorzystywanie retencjonowanych danych także w celach prewencyjnych, a zatem dopuszcza dalej idącą ingerencję w prywatność, niż zakładała to Dyrektywa.

Zgodnie z opiniowanymi Założeniami dane telekomunikacyjne będą mogły być pozyskiwane i wykorzystywane dla potrzeb postępowań dotyczących przestępstw zagrożonych karą pozbawienia wolności, której **górna granica** wynosi co najmniej 3 lata. Wyjątkiem od tej zasady mają być postępowania o ściganie przestępstw popełnionych przy użyciu środków komunikacji elektronicznej, a także przestępstw celnych.

Oczywiście ograniczenie możliwości sięgania po dane tylko do przestępstw zagrożonych karą powyżej 3 lat pozbawienia wolności jest krokiem w dobrym kierunku, jednak daleko niewystarczającym. Naszym zdaniem zapewnienie zgodności z Dyrektywą retencyjną wymaga bowiem szerszych zmian. Są one niezbędne nie tylko do prawidłowego wdrożenia Dyrektywy, ale również zapewnienia obywatelom odpowiedniego poziomu ochrony prywatności.

W naszej ocenie, by prawidłowo zrealizować założenia Dyrektywy w zakresie dopuszczalności wykorzystywania retencji danych, niezbędne są następujące zmiany w polskim porządku prawnym:

i. <u>Ograniczenie możliwości sięgania po dane jedynie do poważnych przestępstw, którymi na gruncie polskiego systemu prawnego są zbrodnie</u>

Jak wynika z przedstawionej tabeli, Policja oraz cztery rodzaje służb (kontrola skarbowa, Służba Celna, Straż Graniczna i Żandarmeria Wojskowa) mają dostęp do danych telekomunikacyjnych w celu ścigania wszystkich rodzajów przestępstw lub przestępstw skarbowych.

W ocenie Fundacji PANOPTYKON takie rozwiązanie jest nie tylko niezgodne z Dyrektywą retencyjną, ale również nadmiernie ingeruje w konstytucyjną zasadę ochrony prywatności. Należy bowiem pamiętać, że ujawnianie Policji oraz innym służbom danych retencyjnych stanowi ingerencję w wynikającą z art. 47 i 51 ust. 3 Konstytucji oraz art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności ochronę prywatności[9]. Oczywiście taka ingerencja bywa dopuszczalna w demokratycznym państwie prawa, ale pod warunkiem spełnienia wymogu proporcjonalności. Sięganie po dane telekomunikacyjne w drobnych sprawach tego warunku nie spełnia. Proponowane w Założeniach ograniczenie do przestępstw zagrożonych karą pozbawienia wolności, której **górna granica** wynosi co najmniej 3 lata pozwala na sięganie po dane telekomunikacyjne w sprawach przestępstw, które w naszej ocenie nie mają „poważnego charakteru", np. określone w art. 290 Kodeksu karnego przestępstwo wyrębu drzewa w lesie.

Ponadto, zgodnie z Założeniami, nawet zaproponowane ograniczenie (na podstawie kryterium wysokości kary) nie ma być stosowane w sposób konsekwentny. Dopuszczalne ma być sięganie po dane telekomunikacyjne także w związku z przestępstwami popełnionymi przy użyciu środków komunikacji elektronicznej, a także przestępstwami celnymi – bez względu na wysokość grożącej kary. Stanowi to wyjątek poszerzający, i tak już szeroki, katalog przestępstw

[9] Por. wyrok Europejskiego Trybunału Praw Człowieka z dnia 2 sierpnia 1984 r. w sprawie Malone przeciwko Wielkiej Brytanii, skarga nr 8691/79, a także wyrok Trybunału Konstytucyjnego z dnia 20 czerwca 2005 r. o sygn. K 4/04, w których oba Trybunały uznały, że sięganie po dane telekomunikacyjne stanowi ingerencję w prywatność jednostki.

uzasadniających sięganie po dane telekomunikacyjne.

Postulujemy zatem zastąpienie zaproponowanego w Założeniach kryterium granicy zagrożenia karą pozbawienia wolności powyżej trzech lat możliwością sięgania po dane jedynie w sprawach dotyczących **zbrodni**[10], a ewentualne wyjątki od tej zasady powinny być szczególnie uzasadnione i wyraźnie wskazane przez ustawę.

ii. Zmiana warunków, w których Policja i służby mogą sięgać po dane telekomunikacyjne

Dyrektywa dopuszcza dostęp do danych jedynie w celu **„dochodzenia, wykrywania i ścigania** poważnych przestępstw". Poza zawężeniem dostępu jedynie do poważnych przestępstw, konieczne jest zatem usunięcie przepisów umożliwiających dostęp do danych w przypadku innych czynności, niż wskazane w Dyrektywie. Naszym zdaniem w tym katalogu nie mieści się (wskazane we wszystkich ustawach kompetencyjnych) **zapobieganie** przestępstwom. W Dyrektywie retencja danych została pomyślana jako narzędzie pomagające w wykrywaniu przestępstw. Wprowadzenie dodatkowej kategorii „zapobiegania" – ze względu na swoją nieprecyzyjność – otwiera niezwykle szerokie możliwości sięgania po dane, a tym samym wypacza sens i cele Dyrektywy.

2. Kontrola zewnętrzna

Obecnie obowiązujące przepisy nie przewidują **jakiejkolwiek kontroli** zewnętrznej nad sięganiem przez Policję oraz inne służby po dane telekomunikacyjne. Sytuacja ta jest wyjątkowa w zestawieniu ze standardami przyjętymi w większości państw Unii Europejskiej. W 24 państwach taką kontrolę sprawują sądy i prokuratura[11] albo niezależne organy administracyjne[12].

Na konieczność wprowadzenia kontroli zewnętrznej zwróciła uwagę Rzecznik Praw Obywatelskich we wniosku do Trybunału Konstytucyjnego[13], w którym zakwestionowała zgodność przepisów ustaw kompetencyjnych z art. 8 Konwencji oraz art. 49 w związku z art. 31 ust. 3 Konstytucji. Jednym z głównych argumentów Rzecznik był brak zewnętrznej kontroli nad sięganiem po dane telekomunikacyjne. We wniosku czytamy: „standardy zawarte w art. 49 Konstytucji oraz w art. 8 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności nie są respektowane, gdyż ustawodawca nie zapewnił zewnętrznych form kontroli korzystania przez poszczególne służby z przyznanych im szerokich uprawnień w zakresie dostępu do danych objętych tajemnicą telekomunikacyjną".

Opiniowane Założenia nie proponują w tym zakresie oczekiwanych, gruntownych zmian. Mimo krytyki ze strony różnych środowisk, powraca propozycja powołania wewnętrznych pełnomocników ds. ochrony danych osobowych i telekomunikacyjnych. Jesteśmy przekonani, że wewnętrzny pełnomocnik nie jest w stanie skutecznie i obiektywnie kontrolować działań własnej instytucji, nawet jeśli chronią go gwarancje nieusuwalności z pracy i z pełnionej funkcji bez zgody organu nadzorującego. Dlatego konieczne jest nadanie odpowiednich uprawnień kontrolnych niezależnej instytucji – sądom lub np. Generalnemu Inspektorowi Ochrony Danych

[10] Zgodnie z Kodeksem karnym zbrodnią jest przestępstwo zagrożone karą pozbawienia wolności nie krótszą od 3 lat.

[11] Sądy: Bułgaria, Czechy, Dania, Finlandia, Grecja, Hiszpania, Litwa, Luksemburg, Niemcy, Portugalia, Słowenia, sąd lub prokurator: Belgia, Cypr, sędzia śledczy lub prokurator: Estonia, Holandia, prokurator: Węgry i Włochy.

[12] Model kontroli administracyjnej zastosowany został we Francji, Irlandii, na Malcie oraz w Zjednoczonym Królestwie.

[13] Wniosek Rzecznik Praw Obywatelskich z 1 sierpnia 2011 r., zarejestrowany pod sygn. K 23/11, czeka na rozpoznanie.

Osobowych.

Projekt przewiduje również zwiększenie nadzoru prokuratury nad działaniami Policji i służb. Miałby się on realizować w następczej kontroli materiału zebranego na potrzeby konkretnego postępowania karnego. Naszym zdaniem ta propozycja również nie rozwiązuje problemu braku zewnętrznej kontroli nad pozyskiwaniem danych telekomunikacyjnych i nie ograniczy możliwych nadużyć na etapie pracy operacyjnej. Tak ukształtowana kontrola prokuratora byłaby przecież ograniczona wyłącznie do tych sytuacji, w których Policja lub służby same zdecydowały się skierować materiał do prokuratora, by ten wniósł akt oskarżenia. W naszej opinii zaproponowane w Założeniach kompetencje kontrolne prokuratora są zatem zdecydowanie niewystarczające, a wręcz mogą być uznane za iluzoryczne.

3. Sprawozdawczość

Projekt Założeń zawiera istotną propozycję, dotyczącą nałożenia obowiązków sprawozdawczych na wszystkie podmioty uprawnione do pobierania danych telekomunikacyjnych. Obecnie bardzo ogólne statystyki gromadzone są jedynie przez operatorów telekomunikacyjnych, co utrudnia poznanie praktyki służb i rzeczową dyskusję o problemie. Zgodnie z Założeniami każdego roku mają być upubliczniane m.in. dane na temat liczby numerów telefonów i IP, w przypadku których dokonywano sprawdzeń – w rozbiciu na zapytania abonenckie, informacje o połączeniach i dane geolokalizacyjne.

To ważne wskaźniki, jednak naszym zdaniem wciąż niewystarczające i niepozwalające na pełną analizę praktyki korzystania z danych telekomunikacyjnych. Warto zastanowić się na objęciem obowiązkiem sprawozdawczym w szczególności informacji dotyczących liczby i rodzajów spraw – co mogłoby rzucić nowe światło na to, jak często dane telekomunikacyjne są wykorzystywane do walki z poważną przestępczością, a jak często w bardziej drobnych sprawach, oraz czasu, jakiego dotyczy dane zapytanie. Z drugiej strony warto również zwrócić uwagę, że zbieranie danych o liczbie osób, których dane były pobierane – jak przewidziano w Założeniach – może być w praktyce bardzo trudne i stwarzać ryzyko tworzenia niewiarygodnych statystyk.

4. Niszczenie danych

Pozytywnie oceniamy propozycję wprowadzenia obowiązku niezwłocznego niszczenia danych, „które nie zawierają dowodów pozwalających na wszczęcie postępowania karnego, informacji mających znaczenie dla postępowania lub informacji istotnych dla bezpieczeństwa państwa". Obecnie w przypadku niektórych służb brakuje przepisów, które wprowadzałyby obowiązek niszczenia zbędnych danych. Na tę niebezpieczną lukę wielokrotnie zwracano już uwagę[14].

5. Problemy nieporuszone w Założeniach

Opiniowane Założenia mają nie tylko bardzo ogólny charakter, ale pomijają również inne istotne zagadnienia, które w naszej ocenie wymagają regulacji. Postulujemy:

[14] Problem ten podniosła m.in. Rzecznik Praw Obywatelskich w cytowanym wyżej wniosku do Trybunału Konstytucyjnego (sygn. K 23/11, czeka na rozpoznanie).

i. Wprowadzenie mechanizmu informowania o sięganiu po dane telekomunikacyjne analogicznego do obowiązku wskazanego w art. 239 Kodeksu postępowania karnego[15]

W ocenie Fundacji PANOPTYKON niezbędne jest wprowadzenie obowiązku informacyjnego na wzór rozwiązań zastosowanych w Kodeksie postępowania karnego w sytuacji kontroli i utrwalania treści rozmów. Zgodnie z tymi przepisami, ogłoszenie postanowienia o kontroli i utrwalaniu rozmów telefonicznych osobie, której ono dotyczy, może być odroczone na czas niezbędny ze względu na dobro sprawy[16].

Naszym zdaniem następcze informowanie o fakcie sięgania po dane telekomunikacyjne pozwoli na ograniczenie skali tego zjawiska, wywoła bowiem efekt „samoograniczania się" przez uprawnione podmioty. W uzasadnionych przypadkach taka informacja umożliwi również samym obywatelom kwestionowanie legalności i prawidłowości czynności podejmowanych przez Policję i służby oraz dalsze interwencje prawne (np. dochodzenie roszczeń z tytułu naruszenia dóbr osobistych na drodze cywilnej).

ii. Wprowadzenie mechanizmu gwarantującego ochronę tajemnic zawodowych, takich jak dziennikarska czy adwokacka

Doświadczenie z praktycznym wykorzystywaniem dostępu do danych telekomunikacyjnych przez polskie służby, a w szczególności nagłośnione nadużycia na tym polu, wskazuje na potrzebę zagwarantowania szczególnej ochrony danym stanowiącym tajemnicę zawodową. W obecnym stanie prawnym brakuje takiego mechanizmu, co sprawia, że nawet świadome gromadzenie informacji stanowiących tajemnicę zawodową w ramach działań operacyjnych mieści się w granicach formalnych kompetencji służb.

W opinii Fundacji PANOPTYKON zasady wykorzystywania danych stanowiących tajemnicę zawodową wymaga odrębnego uregulowania. Przyjmując, że nie jest możliwe odróżnienie danych telekomunikacyjnych stanowiących tajemnicę zawodową na etapie kierowania zapytania o dane do operatora, a tym samym zapobieżenie pobieraniu tych danych przez Policję lub inne służby, pewne gwarancje ochrony tego typu danych mogłyby zostać wprowadzone w ramach proponowanej przez nas instytucji kontroli zewnętrznej nad wykorzystywaniem retencji danych.

Kolejnym instrumentem, który pośrednio mógłby się przyczynić do wzmocnienia ochrony tajemnic zawodowych oraz ograniczyć możliwe nadużycia na tym polu, jest omówiony powyżej mechanizm informowania samych obywateli o sięganiu po ich dane telekomunikacyjne. W oparciu o uzyskiwane na tej podstawie informacje lekarze, adwokaci czy dziennikarze mogliby skuteczniej dochodzić roszczeń z tytułu nieuprawnionego naruszenia tajemnicy ich zawodu, a tym samym wywołać efekt „samoograniczania się" przez uprawnione podmioty.

* * *

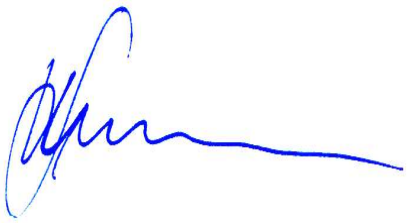
Dziękując za możliwość odniesienia się do Założeń, wyrażamy nadzieję, że powyższe uwagi zostaną przez Ministerstwo Spraw Wewnętrznych uwzględnione lub przynajmniej poważnie

[15] Zgodnie z art. 239 Kpk (§ 1) Ogłoszenie postanowienia o kontroli i utrwalaniu rozmów telefonicznych osobie, której ono dotyczy, może być odroczone na czas niezbędny ze względu na dobro sprawy (§ 2) Ogłoszenie postanowienia, o którym mowa w § 1, w postępowaniu przygotowawczym może być odroczone nie później niż do czasu zakończenia tego postępowania.

[16] Należy wprowadzić wyjątki od obowiązku informowania o sięganiu po dane telekomunikacyjne w absolutnie szczególnych sytuacjach w związku z najpoważniejszymi przestępstwami.

rozpatrzone w toku dalszych prac nad projektem zmian prawnych w zakresie obowiązkowej retencji danych oraz związanych z tym instrumentem uprawnień Policji i innych służb. Jednocześnie wyrażamy gotowość do udziału w konsultacjach społecznych, jakie będą towarzyszyć publikacji zapowiadanego projektu ustawy.

W imieniu Fundacji PANOPTYKON



Katarzyna Szymielewicz
Prezes Zarządu

Małgorzata Szumańska
Członkini Zarządu