



Inwigilacja w Polsce A.D. 2018

[Arkadiusz Nyzio](#)

Na początku kalendarzowego lata publikowane są trzy rodzaje informacji obrazujących skalę inwigilacji w Polsce w roku poprzednim. Warto przyjrzeć się statystykom dotyczącym bilingów, podsłuchów, kontroli korespondencji i danych użytkowników, którymi w 2018 r. interesowały się organy i instytucje polskiego państwa. Jak zawsze w przypadku prowadzonych przez nie niejawnych działań, informacje są skąpe, a w ślad za każdą niepełną odpowiedzią podąża szereg pytań i wątpliwości.

1. Kontrola operacyjna i procesowa

1.1. Najważniejsze pojęcia, podstawa prawna i procedura

Pierwszym z typów inwigilacji, którym należy się przyjrzeć, jest kontrola operacyjna i procesowa. Najczęściej łączy się ją z podsłuchami, obejmuje ona jednak także inne czynności, np. kontrolę zawartości przesyłek czy treści korespondencji mailowej.

Kontrolę stosuje się zarówno pozaprocesowo, w ramach czynności operacyjno-rozpoznawczych (kontrola operacyjna), jak i na gruncie Kodeksu postępowania karnego, czyli po wszczęciu postępowania (kontrola i utrwalanie rozmów, częściej po prostu kontrola procesowa).

Kontrola operacyjna, jako rozwiązanie szczególnie dotkliwe dla praw i wolności jednostki, od 2001 r. objęta jest w Polsce uprzednią kontrolą sądową (kontrola *ex ante*). Oznacza to, że posiadające uprawnienia do jej prowadzenia instytucje muszą składać do sądów okręgowych uzasadnione wnioski o jej zarządzenie. Mogą one dotyczyć wyłącznie sytuacji, w których stosowanie innych, mniej dotkliwych dla jednostki, metod jest bezskuteczne lub nieprzydatne (zasada subsydiarności). Dodatkowe ograniczenie dotyczy rodzaju

przestępstw, które mogą być w ten sposób zwalczane. Kontrola operacyjna może być stosowana tylko w przypadku tzw. przestępstw katalogowych, czyli enumeratywnie wymienionych w ustawach kompetencyjnych przestępstw umyślnych ściganych z oskarżenia publicznego (z urzędu). To ważne z punktu widzenia zasady proporcjonalności, wskazującej, że przedsięwzięte środki powinny być adekwatne do charakteru popełnionego czynu zabronionego. Tak więc, przykładowo, Policja nie może podsłuchiwać nikogo w związku z kradzieżą czy kradzieżą z włamaniem, ale w związku z rozbojem – już tak. Stosowanie kontroli operacyjnej i procesowej w związku z wykroczeniami jest niedopuszczalne.

W Polsce o zarządzenie kontroli operacyjnej wnioskować mogą służby policyjne, czyli Policja, Straż Graniczna (SG), Służba Ochrony Państwa (SOP), Żandarmeria Wojskowa (ŻW) i Służba Celno-Skarbowa (SCS) działająca w ramach Krajowej Administracji Skarbowej (KAS) oraz służby specjalne: Centralne Biuro Antykorupcyjne (CBA), Agencja Bezpieczeństwa Wewnętrznego (ABW) i Służba Kontrwywiadu Wojskowego (SKW). Ponadto, kompetencję tę posiada Biuro Nadzoru Wewnętrznego (BNW), będące jednostką organizacyjną Ministerstwa Spraw Wewnętrznych i Administracji. Przed złożeniem wniosku do sądu, zainteresowane zarządzeniem kontroli operacyjnej instytucje muszą jeszcze uzyskać zgodę właściwego prokuratora okręgowego lub prokuratora generalnego. Zamieszczona poniżej tabela przedstawia organy decyzyjne w zakresie kontroli operacyjnej.

Tabela 1. Właściwe organy w zakresie wnioskowania o zarządzenie kontroli operacyjnej, wyrażania zgody na zarządzenie kontroli operacyjnej i zarządzania kontroli operacyjnej.

Wnioskodawca		Prokurator – instytucja wyrażająca zgodę na zarządzenie kontroli operacyjnej	Sąd – instytucja zarządzająca kontrolę operacyjną
Instytucja	Organ wnioskujący		
Policja	komendant główny, komendanci Centralnego Biura Śledczego Policji i Biura Spraw Wewnętrznych Policji, komendanci wojewódzcy (po upoważnieniu – także ich zastępcy)	generalny lub okręgowy – w przypadku wniosków komendantów wojewódzkich lub ich zastępców	okręgowy
Straż Graniczna	komendant główny, komendant Biura Spraw Wewnętrznych SG, komendant oddziału (po upoważnieniu – także ich zastępcy)	generalny lub okręgowy – w przypadku wniosków komendantów oddziałów lub ich zastępców	okręgowy
Służba Ochrony Państwa	komendant (po upoważnieniu – także jego zastępcę)	generalny	okręgowy w Warszawie

Krajowa Administracja Skarbowa	szef (po upoważnieniu – także jego zastępca)	generalny	okręgowy w Warszawie
Centralne Biuro Antykorupcyjne	szef (po upoważnieniu – także jego zastępca)	generalny	okręgowy w Warszawie
Agencja Bezpieczeństwa Wewnętrznego	szef (po upoważnieniu – także jego zastępca)	generalny	okręgowy w Warszawie
Biuro Nadzoru Wewnętrznego	inspektor nadzoru wewnętrznego (po upoważnieniu – także jego zastępca)	generalny	okręgowy w Warszawie
Żandarmeria Wojskowa	komendant główny, komendant oddziału – za zgodą komendanta głównego (po upoważnieniu – także ich zastępcy)	generalny lub zastępca prokuratora okręgowego do spraw wojskowych – w przypadku wniosków komendantów oddziałów lub ich zastępców	wojskowy okręgowy
Służba Kontrwywiadu Wojskowego	szef (po upoważnieniu – także jego zastępca)	generalny	wojskowy okręgowy w Warszawie

Istnieje jeszcze tryb specjalny, dotyczący przypadków „niecierpiących zwłoki”, czyli takich, w których występuje ryzyko utraty informacji oraz zatarcia lub zniszczenia dowodów. W takich sytuacjach kontrola operacyjna może być zarządzona po uzyskaniu zgody właściwego prokuratora, bez udziału sądu. Organ uprawniony do prowadzenia kontroli jest zobligowany, aby jednocześnie zwrócić się do właściwego sądu z wnioskiem o wydanie postanowienia w tej sprawie. Jeśli w przeciągu pięciu dni od zarządzenia kontroli operacyjnej sąd takiego postanowienia nie wyda, kontrola operacyjna musi zostać przerwana, a zebrane w jej toku materiały – zniszczone.

Tajnością o szczególnej skali objęte są czynności operacyjno-rozpoznawcze prowadzone przez instytucje wywiadowcze – Agencję Wywiadu i Służbę Wywiadu Wojskowego. O ich działaniach zewnętrznych oficjalnie nie wiadomo dosłownie nic. Natomiast prowadzenie przez nie niektórych działań inwigilacyjnych, w tym kontroli operacyjnej, na terenie Polski jest dopuszczalne wyłącznie w związku z ich „działalnością poza granicami państwa” i jedynie za pośrednictwem instytucji kontrwywiadowczych.

Jeśli zaś chodzi o kontrolę procesową, to zarządza ją sąd na wniosek prokuratora. Także ta forma kontroli dotyczy zamkniętego katalogu najpoważniejszych przestępstw, który jest ujęty w [art. 237](#) Kodeksu postępowania karnego.

1.2. „Jawna roczna informacja”

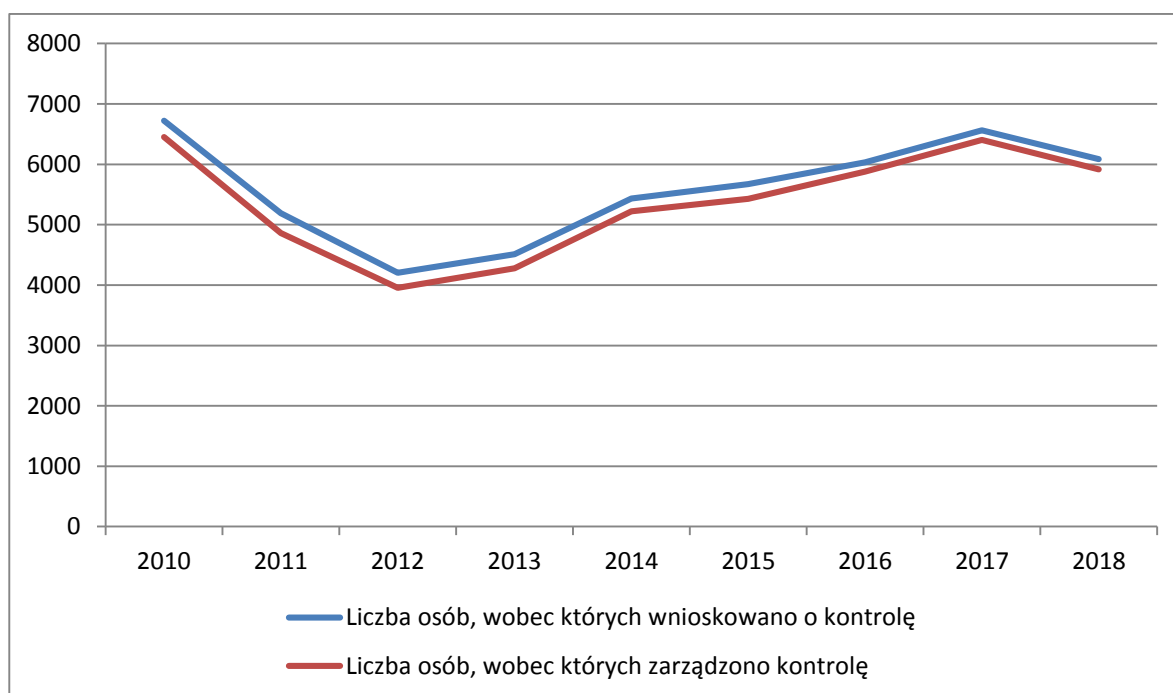
W 2011 r. do polskiego prawa wprowadzono obowiązek przedstawiania przez prokuratora generalnego (wówczas organu odrębnego od ministra sprawiedliwości) parlamentowi jawnej rocznej informacji w zakresie kontroli operacyjnej i procesowej. Przepis znalazł się w ustawie o prokuraturze z 1985 r., a później przeniesiono go do ustawy [Prawo o prokuraturze](#) z 2016 r.

„Jawna roczna informacja” obejmuje zarówno liczbę osób, co do których właściwy sąd wydał postanowienie o zarządzeniu kontroli, jak i osób, w kontekście których wydał postanowienie odmowne. Zawiera także liczbę osób, w kontekście których wnioski o zarządzenie kontroli operacyjnej nie uzyskał zgody prokuratora. Dotycząca roku ubiegłego informacja powinna być przedstawiona parlamentowi do 30 czerwca roku następnego.

Datowana na 6 czerwca 2019 r. „jawna roczna informacja” obejmująca 2018 r. została opublikowana 25 czerwca. Poniższy wykres przedstawia najważniejsze ujęte w niej dane, czyli liczbę osób, których dotyczyły złożone wnioski i osób objętych kontrolą, osadzone na szerszym tle historycznym.

Warto podkreślić, że w „jawnych rocznych informacjach” jest mowa o liczbie osób, których dotyczyły wnioski, a nie o liczbie wniosków. Dla uproszczenia wywodu będę zatem posługiwał się akronimem OW, oznaczającym całościową liczbę osób, których dotyczyły wnioski („osobowniosek”).

Wykres. 1. Kontrola operacyjna i procesowa w latach 2010–2018 – liczba OW i osób, wobec których zarządzono kontrolę.



W 2018 r. zarządzono kontrolę operacyjną lub procesową wobec 6 tys. osób, przy 6,5 tys. osób w roku poprzednim. Mogłoby się wydawać, że, przedstawiając sprawę obrazowo, w każdej polskiej gminie w 2018 r. znajdowały się „niecałe” trzy osoby, wobec których stosowano ten środek, byłby to jednak wniosek nieuprawniony. Liczby te dotyczą bowiem osób, wobec których w ubiegłym roku zarządzono kontrolę, a nie liczby osób, które w ubiegłym roku były objęte kontrolą. Osób tych mogło być więcej, jako że w 2018 r. mogły jeszcze trwać kontrole zarządzane w 2017 r. lub wcześniej.

Maksymalny okres stosowania kontroli operacyjnej przez zdecydowaną większość instytucji bezpieczeństwa wynosi w Polsce 18 miesięcy, ale realizuje się go fazami. Pierwsza, domyślna faza nie może być dłuższa niż trzy miesiące, a każda kolejna realizowana jest w trybie przedłużenia. Pierwsze przedłużenie nie może być dłuższe niż trzy miesiące, a łączna długość wszystkich kolejnych przedłużeń nie może przekroczyć roku. Każde przedłużenie, czyli uruchomienie kolejnej fazy kontroli, wymaga odpowiedniego uzasadnienia i odbywa się w trybie analogicznym do zarządzenia kontroli – postanawia o tym sąd, działając na wniosek właściwej instytucji, po uzyskaniu zgody prokuratora.

Instytucje kontrwywiadowcze (ABW, SKW) są z tego górnego limitu wyłączone. Przykładowo, w ramach rozpoznawania, zapobiegania i wykrywania przestępstw szpiegostwa czy terroryzmu ABW może w uzasadnionych przypadkach stosować podsłuch przez dowolny, nawet wieloletni, okres. Postanowienie w tej sprawie również wydaje sąd, w procedurze analogicznej do przedstawionej powyżej. Tak jak w przypadku pozostałych instytucji, kontrola realizowana jest fazami, a żadna z dwóch pierwszych faz nie może być dłuższa niż trzy miesiące. Kolejne przedłużenia mogą obejmować dłuższe okresy, żaden z nich nie może jednak trwać dłużej niż rok.

Kontrola procesowa jest pod tym względem uregulowana bardziej restrykcyjnie. Zgodnie z art. 238 Kodeksu postępowania karnego może być ona prowadzona maksymalnie przez trzy miesiące, z możliwością jednego przedłużenia, musi to jednak dotyczyć „szczególnie uzasadnionego wypadku”. Także faza przedłużenia nie może trwać dłużej niż trzy miesiące. Od zapisanego w kodeksie limitu sześciu miesięcy nie ma wyjątków, co bywa krytykowane w doktrynie jako rozwiązanie [zbyt sztywne](#).

Tak więc, przykładowo, od sierpnia 2016 r. mógł być prowadzony podsłuch operacyjny, zarządzony na wniosek Policji, w związku z chęcią uzyskania i utrwalenia dowodów w zakresie przestępstwa płatnej protekcji. Jeśli przyczyny zarządzenia kontroli nie ustawały, a w jej trakcie pojawiły się nowe okoliczności, podsłuch mógł być stosowany jeszcze na początku 2018 r., przy czym ostatnią fazę przedłużenia zarządzono jeszcze w 2017 r.

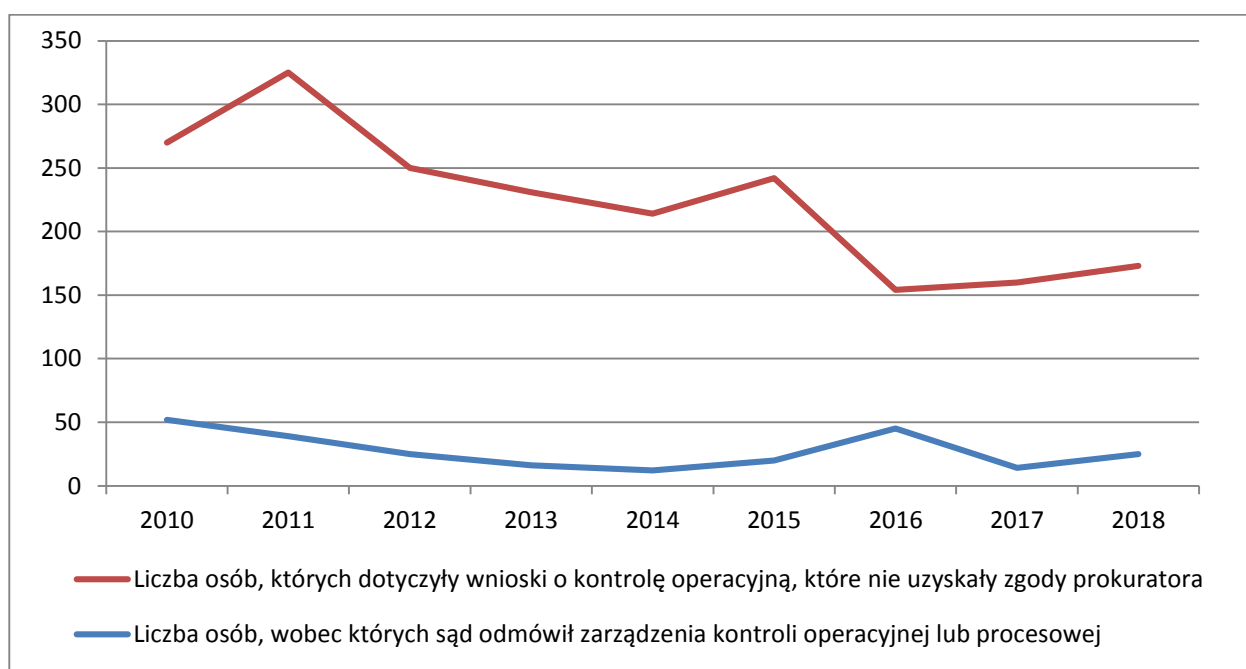
Nie wiadomo więc, jaka jest suma osób objętych kontrolą operacyjną lub procesową, nie są też dostępne dane dotyczące średniej długości trwania kontroli ani liczby przypadków,

w których trwała (trwa) ona dłużej niż 18 miesięcy. Nie wspominając już o danych dotyczących rodzaju przestępstwa, w związku z którym była lub jest prowadzona.

W stosunku do 2017 r. liczba OW zmniejszyła się o 7%. Tym samym zatrzymany został zapoczątkowany w 2012 r. trend wzrostowy. Utrzymuje się natomiast trend polegający na tym, że niemal wszystkie osoby, których dotyczą wnioski, stają się przedmiotem kontroli. Od 2016 r. wskaźnik ten przekracza 97%. Jeśli instytucje wnioskują o objęcie kogoś kontrolą, jest niemal pewne, że będzie miała ona miejsce.

Kolejny wykres przedstawia liczbę OW, na które nie zgodzili się prokuratorzy lub w przypadku których postanowienia odmowne wydali sędziowie.

Wykres. 2. Kontrola operacyjna i procesowa w latach 2010–2018 – liczba OW, które nie uzyskały zgody prokuratora i wobec których sędziowie wydali postanowienia odmowne.



O tym, że kontrola nie zostaje zarządzona, częściej decydują prokuratorzy niż sędziowie, nie należy jednak wyciągać z tego wniosku, że kontrola sądowa jest bardziej „liberalna”. Przyczyna tej dysproporcji tkwi w procedurze. Tryb ustanawiania kontroli operacyjnej jest, w odróżnieniu od kontroli procesowej, dwustopniowy – najpierw właściwa instytucja (np. Policja) składa wniosek do prokuratora, a dopiero po wydaniu przez niego zgody trafia on do sędziego, który postanawia o zarządzeniu lub niezarządzeniu kontroli. Oznacza to, że rozpatrywane przez sądy wnioski dotyczące kontroli operacyjnej są już „przefiltrowane” przez prokuratorów.

Odwrotna proporcja byłaby bardzo niepokojącym sygnałem, świadczącym o tym, że niezawisli sędziowie muszą korygować zbyt pobłażliwe podejście prokuratury. Tymczasem od 2010 r. ani razu nie zdarzyło się, aby liczba osób, w przypadku których sąd odmówił zarządzenia kontroli, przekroczyła 0,8% wszystkich OW.

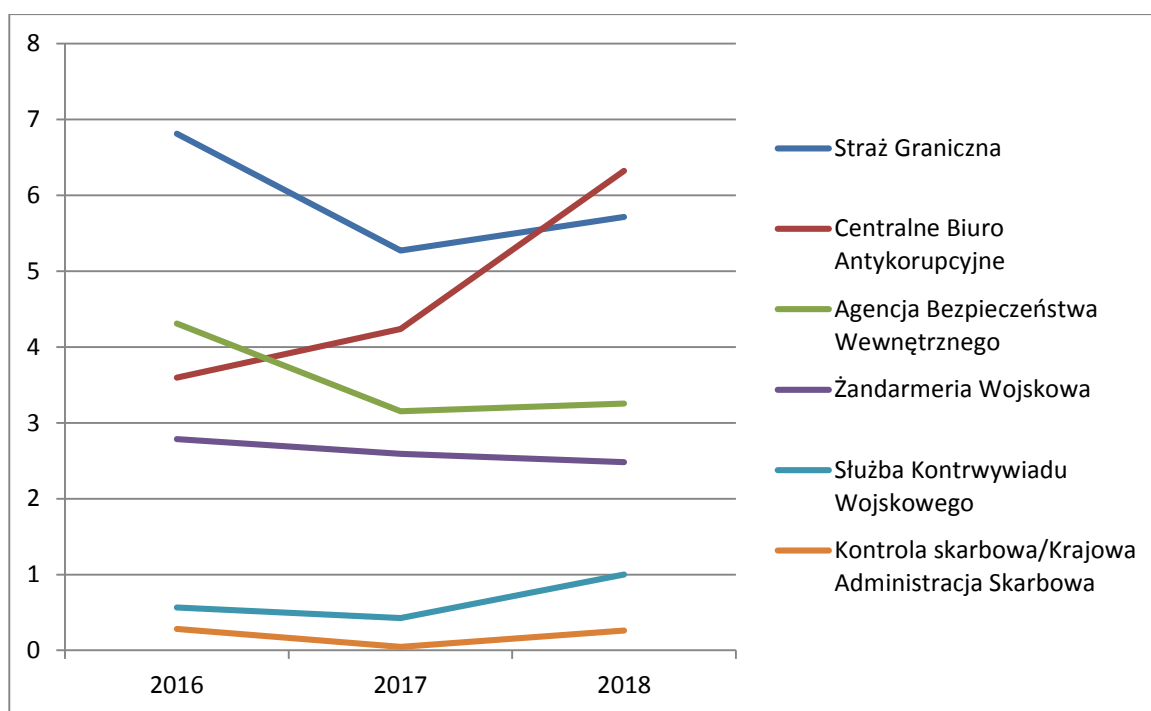
Wniosek, który trafia do sędziego, zawiera zarówno opis przestępstwa i inne podstawowe informacje, jak i uzasadnienie potwierdzające, że zasada subsydiarności została zastosowana. Sąd podejmuje decyzję jednoosobowo, bazując wyłącznie na materiałach, które otrzymał.

Jakie są powody niewyrażenia zgody lub niezarządzenia kontroli – nie wiadomo. Żadna, nawet najbardziej ogólna, statystyka w tym zakresie nie jest upubliczniana.

Przedstawiane przez prokuratora generalnego Andrzeja Seremeta (pełnił tę funkcję w latach 2010–2016) „jawne roczne informacje” były tak lakoniczne, jak to tylko możliwe. Jednostronicowe dokumenty zawierały jedynie podstawowe liczby i informacje o udziale Policji we wnioskach. Zbigniew Ziobro, od 2015 r. minister sprawiedliwości, a od 2016 r. także prokurator generalny, przedstawia więcej informacji dotyczących wnioskodawców. Dzięki temu możliwe było przygotowanie zamieszczonego poniżej wykresu, który uszczegóławia dane dotyczące liczby osób objętych kontrolą.

Z wykresu wyłączyłem Policję, w innym wypadku byłby on zupełnie nieczytelny. Instytucja ta odpowiada bowiem za około 80% ogólnej liczby OW (2016 – 79,9%, 2017 – 81,8%, 2018 – 79,1%). Przepaść oddzielająca Policję, która w 2018 r. wygenerowała wnioski dotyczące 4,8 tys. osób, od pozostałych instytucji, jest ogromna i taka z pewnością pozostanie. Decyduje o tym szeroki zakres zadań tej instytucji. Trzeba przy tym zauważyć, że od 2010 r. procentowy udział Policji w OW nie był tak niski, jak w 2018 r.

Wykres. 3. Kontrola operacyjna w latach 2016–2018 – procentowy udział poszczególnych instytucji bezpieczeństwa (poza Policją) w ogólnej liczbie OW.



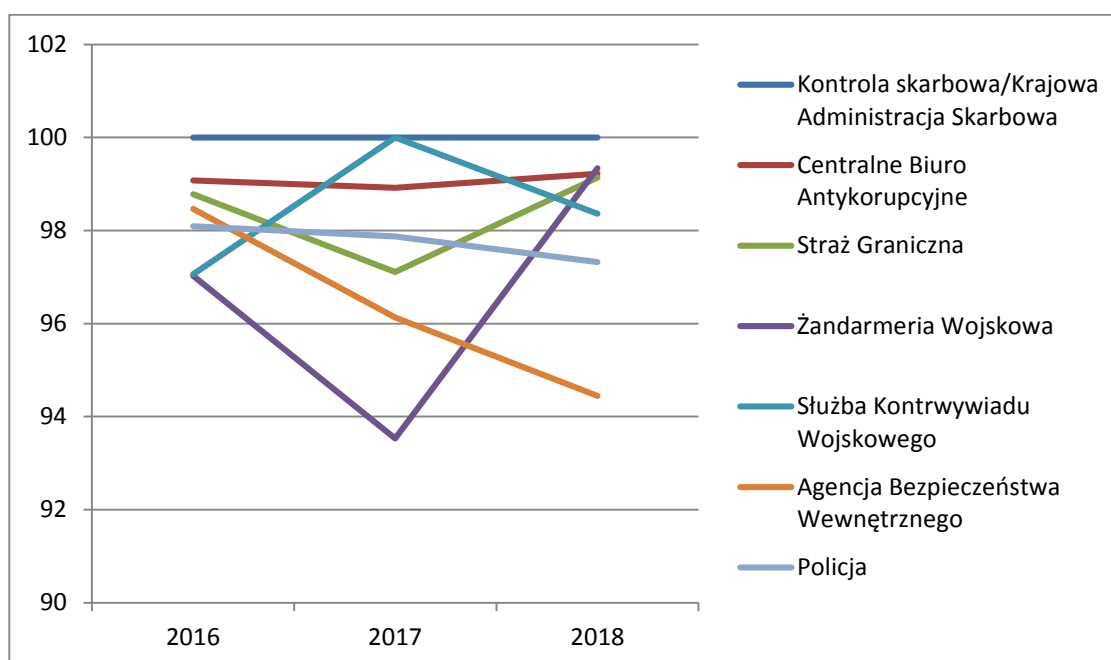
Widoczne jest zwiększające się zainteresowanie kontrolą operacyjną ze strony CBA. W 2016 r. instytucja ta wnioskowała o objęcie kontrolą 217 osób, w 2017 r. – 278, a w 2018 r. – 385. W roku ubiegłym uplasowała się na drugim miejscu, za Policją, wyprzedzając SG (wnioski dotyczące 348 osób).

Godnymi odnotowania instytucjami nieobecnymi na wykresie są: Służba Ochrony Państwa i Biuro Nadzoru Wewnętrzny, które powstały na początku 2018 r. W odróżnieniu od swojego poprzednika, Biura Ochrony Rządu, SOP jako instytucja ochrony najważniejszych osób i obiektów w państwie została wyposażona w uprawnienia do stosowania kontroli operacyjnej. W ubiegłym roku nie skorzystała z nich jednak ani razu, co jednak nie dziwi, jako że struktury operacyjne SOP są dopiero tworzone. Także BNW, instytucja zupełnie nowa w systemie bezpieczeństwa RP, nie skorzystała jeszcze z tego uprawnienia.

W „jawnej rocznej informacji” nie są wprost podane informacje dotyczące tego, jaki jest udział procentowy prokuratorów w OW, można jednak ustalić to sumując liczbę OW instytucji bezpieczeństwa i odejmując ją od liczby wszystkich OW. Na tej podstawie można łatwo stwierdzić, że w porównaniu do kontroli operacyjnej, kontrola procesowa jest zjawiskiem o marginalnej skali. W 2016 r. prokuratorzy wnioskowali o objęcie kontrolą 106 osób, w 2017 r. – 162, a w 2018 r. – 114. Analogiczny zabieg pozwala ustalić, jak często sądy wydają postanowienia odmowne dotyczące zarządzenia kontroli procesowej. W 2016 i 2017 r. wystąpiły po dwa takie przypadki, a w 2018 r. – trzy.

Dwa kolejne wykresy rozwijają dane z wykresów 2. i 3., wskazując na to, której instytucji najtrudniej było przeforsować swoje wnioski. W pierwszej kolejności przedstawiona zostanie kwestia zgody prokuratorów.

Wykres. 4. Kontrola operacyjna w latach 2016–2018 – odsetek OW, które uzyskały zgodę prokuratora w podziale na instytucje bezpieczeństwa.

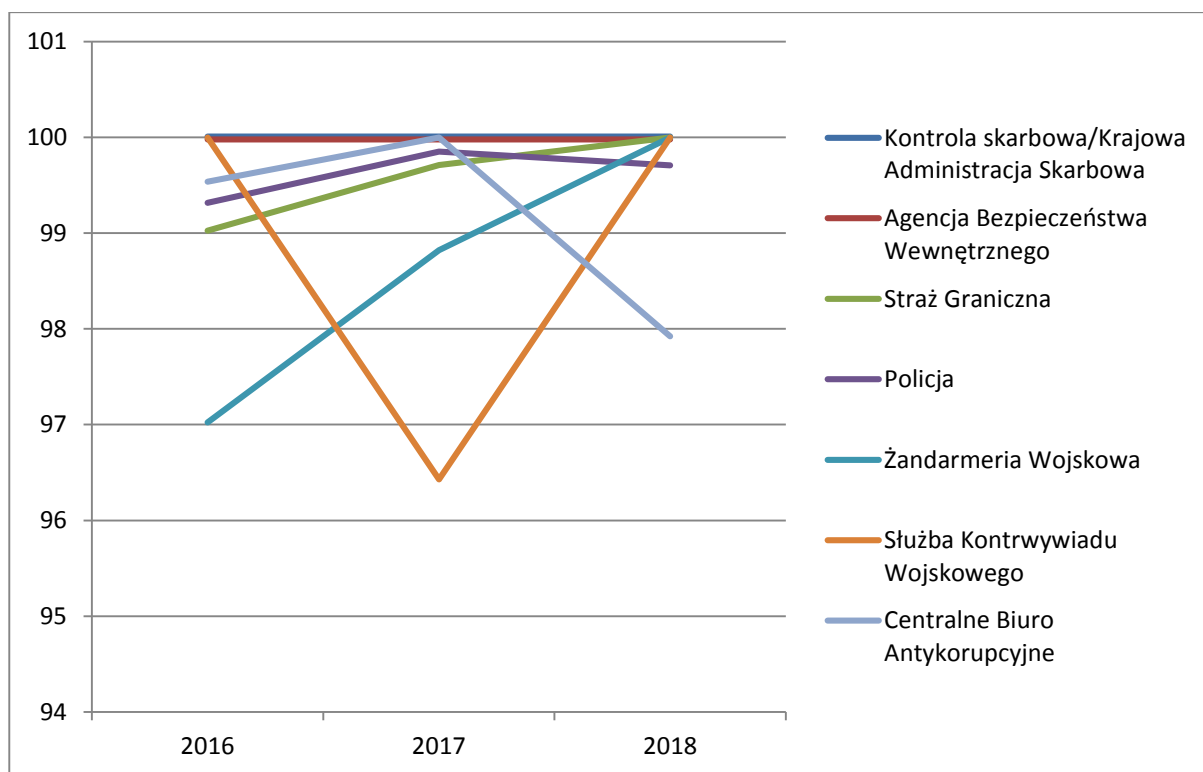


Tym, co rzuca się w oczy, jest bardzo wysoka skuteczność wniosków – prokuratorzy odrzucają zaledwie kilka procent z nich. Jediną instytucją, która może poszczycić się stuprocentową skutecznością, jest KAS. Instytucja ta została utworzona w 2017 r. w wyniku połączenia administracji podatkowej, Służby Celnej i kontroli skarbowej. Ta ostatnia mogła stosować kontrolę operacyjną i KAS, a konkretnie działająca w jej ramach Służba Celno-Scarbowa, przejęły tę kompetencję. W latach 2016–2018 instytucja wnioskowała o objęcie kontrolą operacyjną 36 osób i we wszystkich przypadkach prokurator wyraził na to zgodę. Najgorszy procentowo wynik przypadł w udziale ŻW. W 2017 r. wnioskowała o objęcie kontrolą 170 osób, prokurator nie wyraził zgody na wnioski dotyczące 11 z nich (6,5%).

Jeśli chodzi o ujęcie liczbowe, to niekwestionowanym liderem w zakresie niezyskanej zgody prokuratorskiej jest oczywiście Policja. W latach 2016–2018 prokuratorzy nie zgodzili się na objęcie kontrolą 335 osób, co stanowi liczbę pięciokrotnie wyższą niż suma przypadków dotyczących wszystkich pozostałych instytucji razem wziętych. Wynika to jednak z liczby policyjnych OW, która jest 4,5 razy większa niż liczba OW wszystkich pozostałych instytucji.

Zamieszczony poniżej wykres przedstawia analogiczne dane dotyczące postanowień sądów.

Wykres. 5. Kontrola operacyjna w latach 2016–2018 – odsetek OW, w przypadku których sądy wydały postanowienie o zarządzeniu kontroli operacyjnej, w podziale na instytucje bezpieczeństwa.



Statystyki wykazują, że uzyskanie pozytywnego postanowienia sądu jest właściwie formalnością, niezależnie od tego, która instytucja jest wnioskodawcą. Postanowienia odmowne mają charakter incydentalny, a Agencja Bezpieczeństwa Wewnętrznego i kontrola skarbowa/Krajowa Administracja Skarbowa w ogóle nie zetknęły się z nimi w latach 2016–2018.

W ujęciu liczbowym sądy odrzuciły oczywiście najwięcej OW Policji (55 w trzy lata), a w ujęciu procentowym – Służby Kontrwywiadu Wojskowego (3,6% w 2017 r.) i Żandarmerii Wojskowej (3% w 2016 r.).

2. Pozyskiwanie danych telekomunikacyjnych, pocztowych i internetowych

2.1. Najważniejsze pojęcia, podstawa prawna i procedura

Drugim typem inwigilacji jest przetwarzanie pochodzących z retencji danych telekomunikacyjnych, pocztowych i internetowych. Retencja danych polega na zatrzymywaniu przez operatorów-usługodawców informacji o aktywności usługobiorców. Firmy oferujące tego rodzaju usługi, czyli np. operatorzy telefonii komórkowej czy dostawcy internetu, są zobowiązane przez rok przechowywać informacje o działaniach swoich klientów, np. o wybieranych numerach i realizowanych połączeniach (billingi), logowaniu się urządzeń (geolokalizacja), adresie IP komputera czy odwiedzanych stronach internetowych. Jest to czynność rutynowa i dotyczy każdego użytkownika.

Pozyskiwanie również tych danych odbywa się w dwóch trybach: procesowym i pozaprocesowym, czyli w ramach czynności operacyjno-rozpoznawczych. O dostęp do nich mogą wnioskować te same instytucje, o których była mowa wcześniej – służby policyjne i specjalne oraz Biuro Nadzoru Wewnętrznego, a także – na podstawie Kodeksu postępowania karnego – prokuratorzy (na etapie postępowania przygotowawczego) i sędziowie (na etapie postępowania sądowego). Regulują to przepisy poszczególnych ustaw kompetencyjnych (np. art 20c ustawy o Policji) i [art. 218 kpk](#) poświęcony obowiązkowi wydania korespondencji, przesyłek i danych.

Przetwarzanie danych telekomunikacyjnych, internetowych i pocztowych w trybie pozaprocesowym różni się od kontroli operacyjnej kilkoma ważnymi aspektami, które sprawiają, że jest rozwiązaniem zdecydowanie powszechniejszym.

Po pierwsze, nie jest objęte klauzulą subsydiarności. Uprawnione instytucje mogą więc sięgać po dane nie tylko wtedy, gdy „inne środki okazały się bezskuteczne albo będą nieprzydatne”, ale za każdym razem, kiedy uznają to za stosowne. Chodzi nie tylko o zwalczanie przestępstw, ale także o działania prowadzone w celu „ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych”. Po drugie, pozyskiwanie danych może odbywać się bez udziału firmy oferującej daną usługę. Instytucje bezpieczeństwa nie muszą każdorazowo zwracać się z wnioskiem do dostawcy usług internetowych czy telekomunikacyjnych z wnioskiem o udostępnienie danych

dotyczących aktywności danego użytkownika, tylko mogą je pozyskać we własnym zakresie, przy pomocy stałego, bezpiecznego łącza. Warunkiem jest zawarcie porozumienia z daną firmą–operatorem. Po trzecie, przetwarzać można jedynie dane „niestanowiące treści”, a więc np. dotyczące długości rozmowy telefonicznej, ale nie jej przebiegu, czy o adresacie wysłanego maila, ale nie o jego zawartości. Po czwarte, w odróżnieniu od kontroli operacyjnej, pozyskiwanie tych danych w ramach czynności operacyjno-rozpoznawczych (pozaprocesowych) nie jest objęte uprzednią kontrolą sądową. Zamiast tego stosowana jest kontrola następcza (*ex post*), polegająca na prowadzonej w trybie półrocznym sprawozdawczości. Niepotrzebna jest więc zgoda prokuratora czy postanowienie sądu. Raz na sześć miesięcy uprawnione instytucje przekazują sądom okręgowym informacje o liczbie pozyskanych danych, sądy zaś przekazują je ministrowi sprawiedliwości. Ten z kolei, do 30 czerwca każdego roku, przekazuje parlamentowi „zagregowaną informację” dotyczącą minionych 12 miesięcy.

Obowiązek ten wprowadziła Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw, czyli tzw. ustawa inwigilacyjna (zob. [szerszej na jej temat](#)), która znowelizowała ustawy Prawo o ustroju sądów powszechnych z 2001 r. i Prawo o ustroju sądów wojskowych z 1997 r. Datowana na 4 czerwca 2019 r. „zagregowana informacja” obejmująca rok ubiegły została opublikowana 10 czerwca.

Jeśli zaś chodzi o pozyskiwanie danych na gruncie kodeksu postępowania karnego, czyli w trybie procesowym, to wspomniany art. 218 stanowi, że podmioty działające w obszarze pocztowym, telekomunikacyjnym czy transportowym wydają sądowi lub prokuratorowi korespondencję i przesyłki oraz dane objęte obowiązkiem zatrzymania i przechowywania, które „mają znaczenie dla toczącego się postępowania”. Udostępnienie danych jest obowiązkiem tych podmiotów, a wnioski sądów i prokuratur mają postać żądań zawartych w postanowieniach. Tego rodzaju pozyskiwanie danych jest zwolnione nawet z następczej formy kontroli. Nie jest też w tym zakresie prowadzona sprawozdawczość. To ważne, ponieważ kierowane do operatorów prokuratorskie postanowienia o wydanie danych są prozą dnia codziennego. Od spraw drobnych, takich jak oszustwa internetowe począwszy, na tych dotyczących najpoważniejszych przestępstw skończywszy, żądanie udostępnienia danych, takich jak dane osobowe użytkowników, wykaz połączeń czy miejsce logowania, jest standardową praktyką. Trzeba jednak zauważyć, że osoby, których dane pozyskano w tym trybie, są o tym informowane. Może to zostać odroczone na okres „niezbędny ze względu na dobro sprawy”, ale informacja musi trafić do nich do czasu zakończenia postępowania. Specyfika tej formy pozyskiwania danych jest na tyle odmienna od formy operacyjno-rozpoznawczej, że trudno w ogóle uznawać ją za inwigilację.

2.2. „Zagregowana informacja na temat przetwarzania danych telekomunikacyjnych, pocztowych i internetowych oraz wyników przeprowadzonych kontroli”

„Zagregowane informacje” to dwu- lub trzypięciostopniowe, lakoniczne dokumenty. Ustawa zobowiązuje ministra sprawiedliwości do informowania o liczbie przetwarzanych danych telekomunikacyjnych, pocztowych i internetowych, z podziałem na rodzaj danych, oraz

o wynikach przeprowadzonych kontroli. Dodatkowo, minister zamieszcza w „zagregowanej informacji” ogólny podział instytucjonalny.

Zdecydowana większość (97,5%) przetworzonych w latach 2016–2018 danych to dane telekomunikacyjne. Dane internetowe stanowią 1,8%, a pocztowe – 0,6%. Nie wiadomo, jaka część z nich to dane pobrane za pośrednictwem usługodawców, a jaką instytucje bezpieczeństwa przetworzyły przy użyciu stałych łącz.

Nie jest zresztą jasne, jak wiele porozumień z firmami–operatorami zawarły służby. W 2017 r. SG odpowiedziała pozytywnie na pytanie Fundacji Panoptykon [informując](#), że zawarła pięć porozumień ustanawiających stałe łącza. ŻW przekazała Fundacji informację o podpisaniu czterech porozumień, a Policja i CBA poinformowały, że nie skorzystały z tej możliwości. Aby dowiedzieć się, czy coś zmieniło się przez dwa i pół roku od [publikacji](#) tych danych, można złożyć wniosek o informację publiczną. Pod koniec czerwca 2019 r. Naczelny Sąd Administracyjny [oddalił](#) jednak skargę kasacyjną Fundacji Panoptykon dotyczącą odmowy udostępnienia informacji na temat liczby porozumień zawartych przez ABW. Oznacza to, że dostęp do tych informacji może być jeszcze trudniejszy.

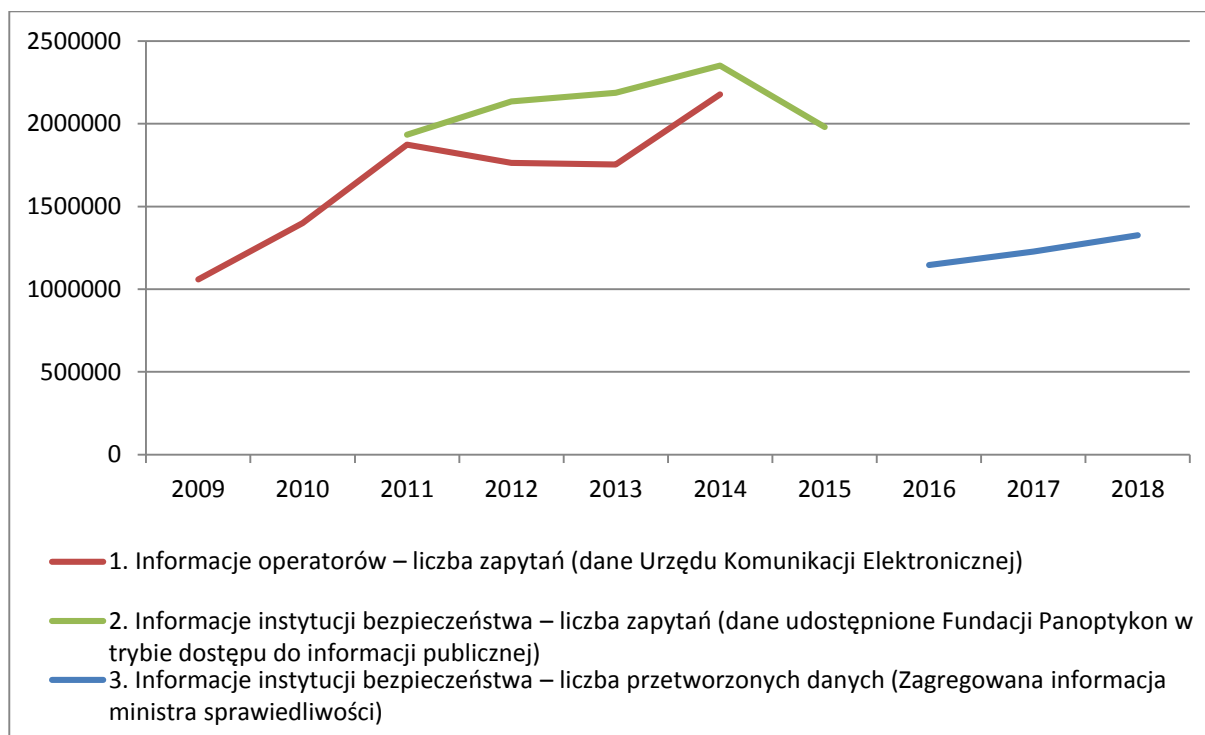
Zamieszczony poniżej wykres przedstawia pozyskane w latach 2016–2018 dane telekomunikacyjne. Umieszczono je na szerszym, choć nieco kłopotliwym tle porównawczym. Wymaga to kilku zdań wyjaśnienia.

Dane porównawcze są dostępne dzięki nieprzewodzonej już przez Urząd Komunikacji Elektronicznej (UKE) sprawozdawczości w tym zakresie i działaniom Fundacji Panoptykon.

Jeśli chodzi o UKE, to dostępne są dane z lat 2009–2014, obejmujące liczbę żądań udostępnienia danych telekomunikacyjnych, z którymi do operatorów zgłaszały się uprawnione instytucje. Dane dostępne dzięki Fundacji Panoptykon obejmują lata 2011–2015. Ich źródłem są same instytucje bezpieczeństwa, do których Fundacja co roku zwracała się z wnioskami o udostępnienie informacji publicznej w zakresie pozyskiwania danych pochodzących z retencji.

Wykres 6. przedstawia informacje dotyczące danych telekomunikacyjnych zebrane przez UKE i Fundację Panoptykon oraz przedstawione parlamentowi przez ministra sprawiedliwości w ramach „zagregowanej informacji” z lat 2016–2018.

Wykres 6. Dane telekomunikacyjne w latach 2009–2018 – liczba zapytań i przetworzonych danych.

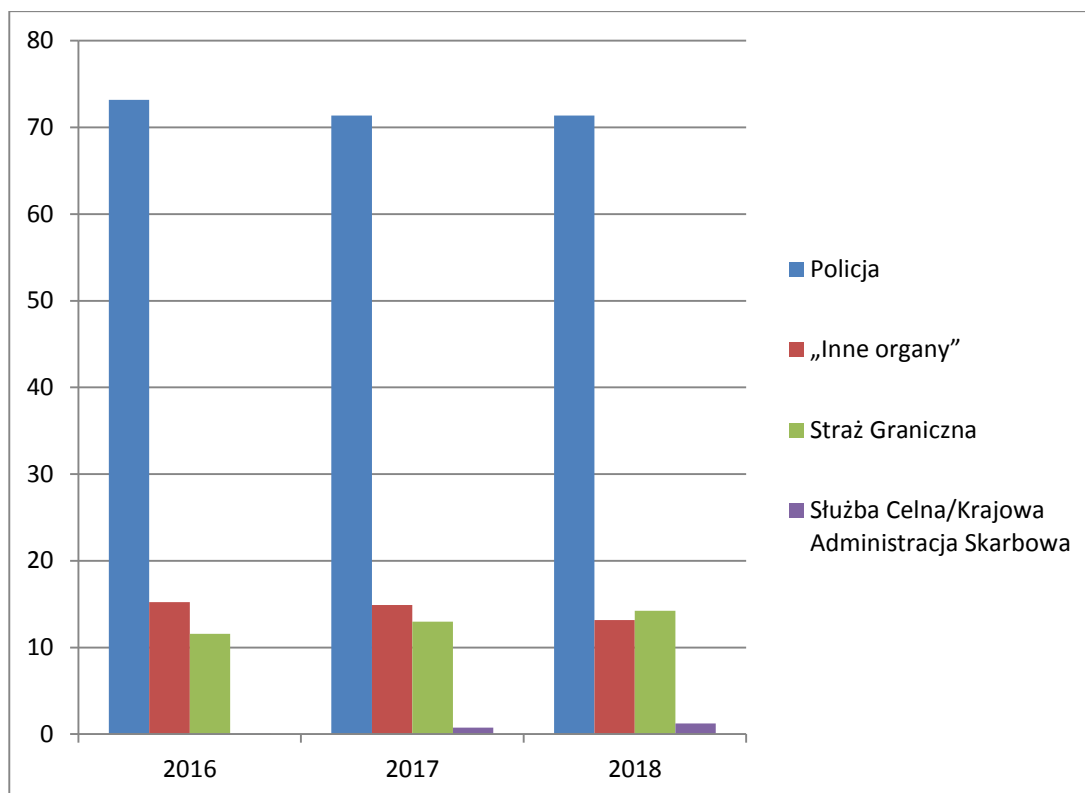


Trzeba zauważyć, że dane UKE (seria 1 na wykresie) uwzględniają zapytania wszystkich uprawnionych instytucji, w tym sądów i prokuratur (nieprzedstawionych w seriach 2 i 3) oraz instytucji bezpieczeństwa, które nie udzieliły odpowiedzi na pytania Fundacji Panoptykon (seria 2). Pomimo węższego grona podmiotów, liczba zapytań wykazywanych przez instytucje bezpieczeństwa (seria 2) była konsekwentnie wyższa niż liczba zapytań wykazywanych przez operatorów (seria 1). Przedstawione powyżej liczby należy traktować bardzo ostrożnie, mając na uwadze, że ich wartość porównawcza jest ograniczona. Sam UKE zwracał uwagę, że nieporównywalność publikowanych przezeń informacji z informacjami służb specjalnych czy Policji „wynika ze stosowania odmiennych kryteriów definiowania zapytań, czy też klasyfikowania przypadków udostępnienia danych retencyjnych”.

Porównując informacje przedstawione w seriach 2 i 3 można zauważyć, że w 2016 r. liczba przetworzonych danych telekomunikacyjnych spadła o 40% w porównaniu do roku poprzedniego. Wy tłumaczenie tego faktu jest proste – „zagregowana informacja” ministra sprawiedliwości nie uwzględnia danych abonenckich, czyli podstawowych informacji dotyczących np. imienia i nazwiska oraz adresu abonenta, do którego należy dany numer telefonu. Przetwarzanie tych danych zwolniono w 2016 r. z następczej kontroli sądowej. Oznacza to, że instytucje nie tylko nie potrzebują zgody prokuratora i postanowienia sądu, aby pozyskać takie informacje, ale też nie muszą prowadzić w tym zakresie jakiegokolwiek statystyki i polityki informacyjnej. Dzięki analizom Fundacji Panoptykon wiadomo, że dane abonenckie składały się na około 35–45% wszystkich zapytań służb, co tłumaczy dystans dzielący serie 1. i 2. oraz 3.

Kolejny wykres przedstawia przetwarzane w latach 2016–2018 dane telekomunikacyjne z podziałem na instytucje bezpieczeństwa. Kategoria „inne organy”, którą posługuje się minister sprawiedliwości, obejmuje ABW, SKW, CBA i ŻW. Obejmowała także wywiad skarbowy, który obecnie prowadzony jest w ramach KAS.

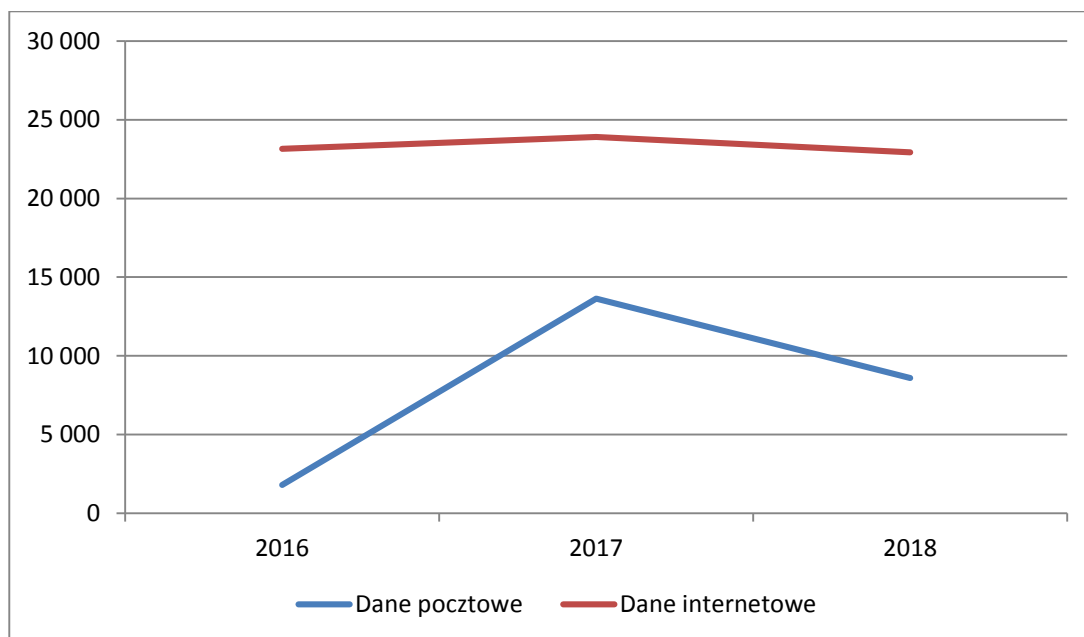
Wykres 7. Dane telekomunikacyjne w latach 2016–2018 – procent przetworzonych danych w podziale na instytucje bezpieczeństwa.



W 2018 r. Policja przetworzyła 945,9 tys. danych telekomunikacyjnych. Nie wiadomo, jakiego rodzaju były to dane – jaką ich część stanowiły billingi, a jaką dane geolokalizacyjne. Jest to zauważalny regres, jako że informacje te zamieszczono w pierwszej „zagregowanej informacji” opublikowanej w 2017 r. Dane telekomunikacyjne podzielono w niej na raporty połączeń (billingi), lokalizacje stacji abonenckich, dane użytkowników i inne dane. Ich udział procentowy w liczbie przetworzonych danych telekomunikacyjnych przedstawiał się następująco: 76,9%, 13,6%, 7% i 2,5%. Minister sprawiedliwości nie wyjaśnił, dlaczego w 2018 i 2019 r. zrezygnowano z publikowania tego podziału. Nie zmienia się to, że nie wiadomo, ilu osób dotyczyły przetworzone dane telekomunikacyjne, ani jaki był powód ich przetwarzania.

Kolejny wykres przedstawia dane internetowe i pocztowe. W tym przypadku przedstawienie szerszego tła porównawczego nie jest możliwe, ograniczyłem się więc do podania informacji dotyczących lat 2016–2018.

Wykres 8. Dane internetowe w latach 2016–2018 – liczba przetworzonych danych.



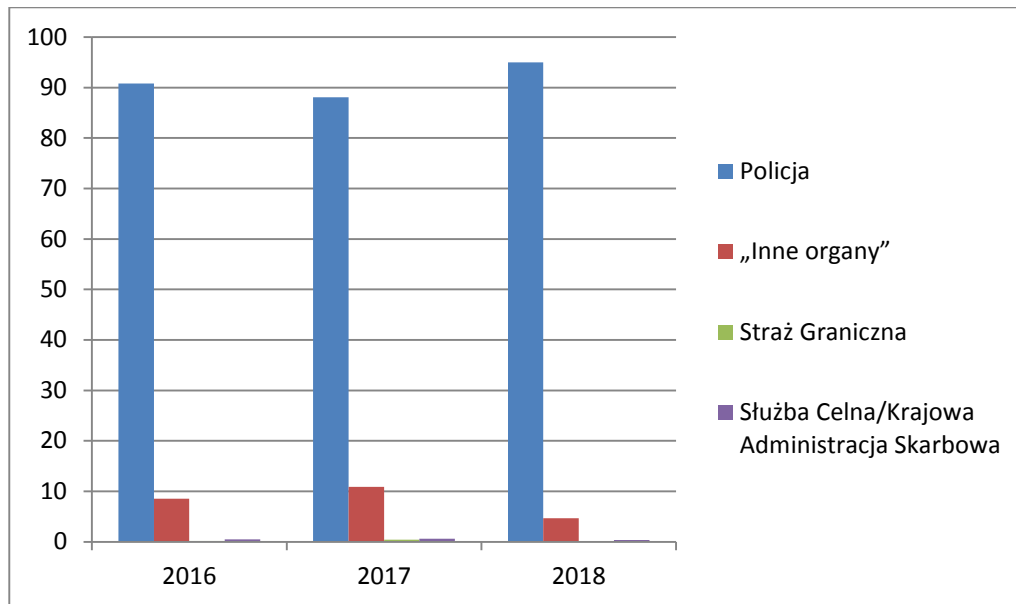
Tak jak w przypadku danych telekomunikacyjnych, dane uszczegóławiające typ pobranych danych nie są dostępne, choć w „zagregowanej informacji” obejmującej 2016 r. znalazł się podział danych internetowych na raporty połączeń (24,6%) i liczbę wystąpień o użytkowników (75,4%).

Liczby te budzą wiele wątpliwości, nie wiadomo np., dlaczego w 2017 r. liczba pozyskanych danych pocztowych wzrosła o 650% (z 1,8 tys. do 13,6 tys.), by w roku 2018 r. zmniejszyć się o jedną trzecią (8,6 tys.).

Dzięki [Fundacji Panoptykon](#) wiadomo, że w 2014 r. instytucje skierowały do firm oferujących usługi internetowe 52,2 tys. zapytań dotyczących danych użytkowników, a w 2015 r. – 217,7 tys. W styczniu 2016 r. Maciej Wąsik, sekretarza stanu w kancelarii Prezesa Rady Ministrów, zastępca koordynatora służb specjalnych, [poinformował posłów](#), że Policja „średniorocznie zadaje 60 tys. tego typu zapytań”. „Zagregowana informacja” z 2017 r. wskazuje, że w roku poprzednim przetworzono 23,1 tys. danych. Oznacza to dziesięciokrotny (jeśli za punkt odniesienia przyjmiemy dane Fundacji) lub trzykrotny (jeśli punktem odniesienia będą dane przekazane przez Wąsika) spadek, którego nie sposób wyjaśnić. Od trzech lat liczba przetworzonych danych internetowych utrzymuje się na podobnym poziomie.

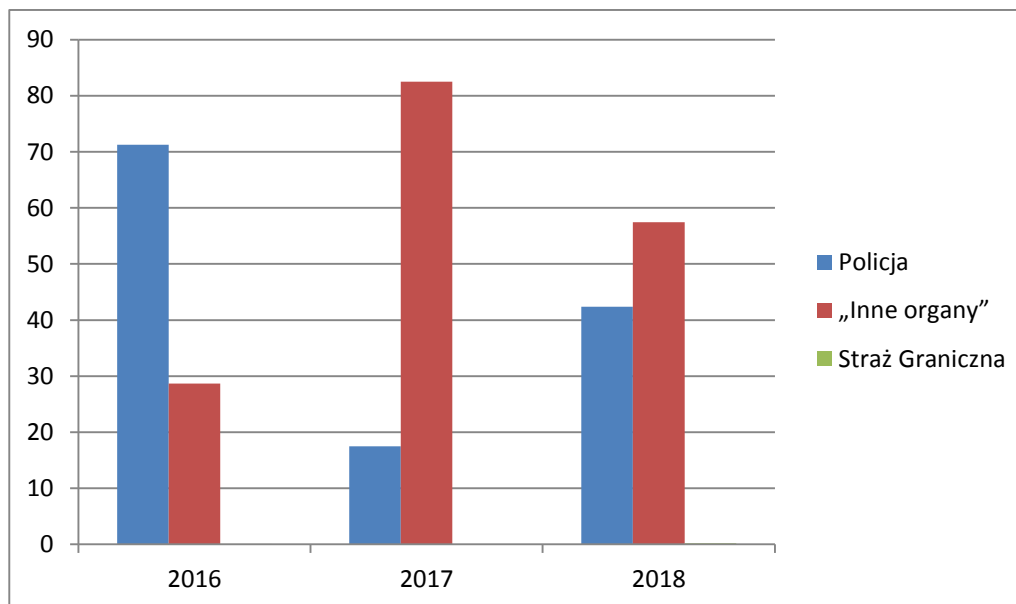
Kolejne dwa wykres przedstawiają dane internetowe i pocztowe w podziale na instytucje, analogicznie do wykresu 7.

Wykres 9. Dane internetowe w latach 2016–2018 – procent przetworzonych danych w podziale na instytucje bezpieczeństwa.



Niekwestionowanym liderem w zakresie przetwarzania danych internetowych pozostaje Policja. W 2018 r. przetworzyła 21,8 spośród 22,9 tys. danych. Niemal niewidoczne na wykresie KAS i SG przetworzyły – odpowiednio – 76 i 6 danych.

Wykres 10. Dane pocztowe w latach 2016–2018 – procent przetworzonych danych w podziale na instytucje bezpieczeństwa.

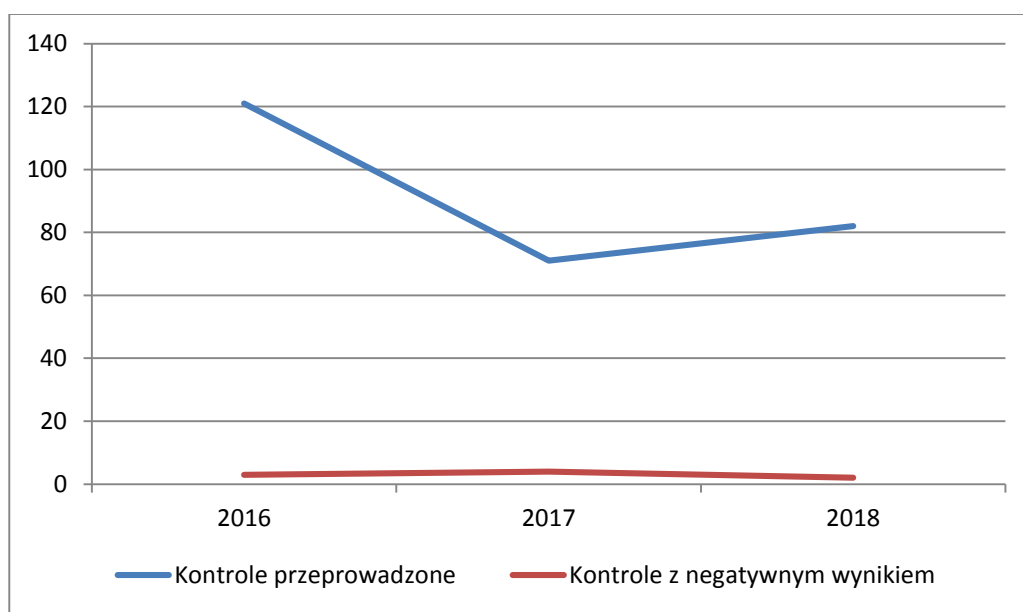


Inaczej wyglądają dane dotyczące danych pocztowych. Policja dominowała w tym zakresie tylko w 2016 r., a w 2017 r. wyprzedziły ją „inne organy”. W 2018 r. kolejność nie uległa zmianie, chociaż Policja przetworzyła 2,5 razy więcej danych internetowych niż w roku poprzednim.

Policja przetworzyła w 2018 r. 3,6 tys. danych pocztowych, „inne organy” – 4,9 tys., a niewidoczna na wykresie SG – 15. Jakiego rodzaju były to dane, które „inne organy” są tak bardzo zainteresowane przesyłkami pocztowymi Polaków i dlaczego – nie wiadomo.

Ostatni wykres dotyczący przetwarzania danych przedstawia liczbę i wyniki kontroli nad procesem.

Wykres 11. Kontrola przetwarzania danych telekomunikacyjnych, pocztowych i internetowych w latach 2016–2018.



Jak wspomniano, kontrolę nad przetwarzaniem danych sprawują sądy okręgowe: powszechne i wojskowe. Instytucje przetwarzające dane co pół roku przekazują sądom informacje dotyczące liczby przypadków pozyskania danych oraz kwalifikacji prawnej czynów, które były podstawą przetwarzania danych lub innych powodów (np. działań poszukiwawczych lub ratowniczych). Ustawy nie precyzują, jak powinna wyglądać tego rodzaju kontrola. W jej ramach sąd „może zapoznać się z materiałami uzasadniającymi” przetwarzanie danych, ale nie musi tego zrobić. Sąd informuje właściwą instytucję o wynikach kontroli, ale ustawy nie przewidują żadnych sankcji związanych ze stwierdzonymi nieprawidłowościami.

W praktyce wszystko zależy więc od sędziego, który może ograniczyć kontrolę do sprawdzenia przedłożonych przez instytucje danych tabelarycznych (przykładową tabelę można obejrzeć [tutaj](#)), albo przyjrzeć się bliżej wybranym sprawom. Z pewnością jednak nie wszystkim, z uwagi na ich liczbę. W 2017 r. [sąd okręgowy w Gdańsku](#) ocenił, że rozwiązania ustawowe nie stwarzają „możliwości zweryfikowania, czy sięgnięcie po informacje było niezbędne, celowe i należyte uzasadnione w kontekście subsydiarności działań operacyjnych, a więc nie daje podstawy do przeprowadzenia realnej – spełniającej standardy ochrony praw człowieka – kontroli uzyskiwania przez Policję danych telekomunikacyjnych, pocztowych lub internetowych”.

Wiadomo, że nadużycia się zdarzają – Policja sięgała np. po dane w kontekście wykroczeń, na co nie pozwala polskie prawo. Opinia publiczna nie dysponuje też żadnymi instrumentami, które umożliwiłyby interpretację informacji dotyczących przeprowadzonych kontroli. Jest jednak jasne, że fakt, iż minister sprawiedliwości wykazał zaledwie dwie zakończone negatywnym wynikiem kontrole dotyczące 2018 r., nie należy interpretować jako informacji, że w sposób nieuprawniony przetworzono dwie sztuki danych. Chodzi raczej o to, że w minionym roku uchybienia wykazały dwa sądy okręgowe. Nie wiadomo, ile danych pozyskano bezpodstawnie i jakiej liczby osób one dotyczyły.

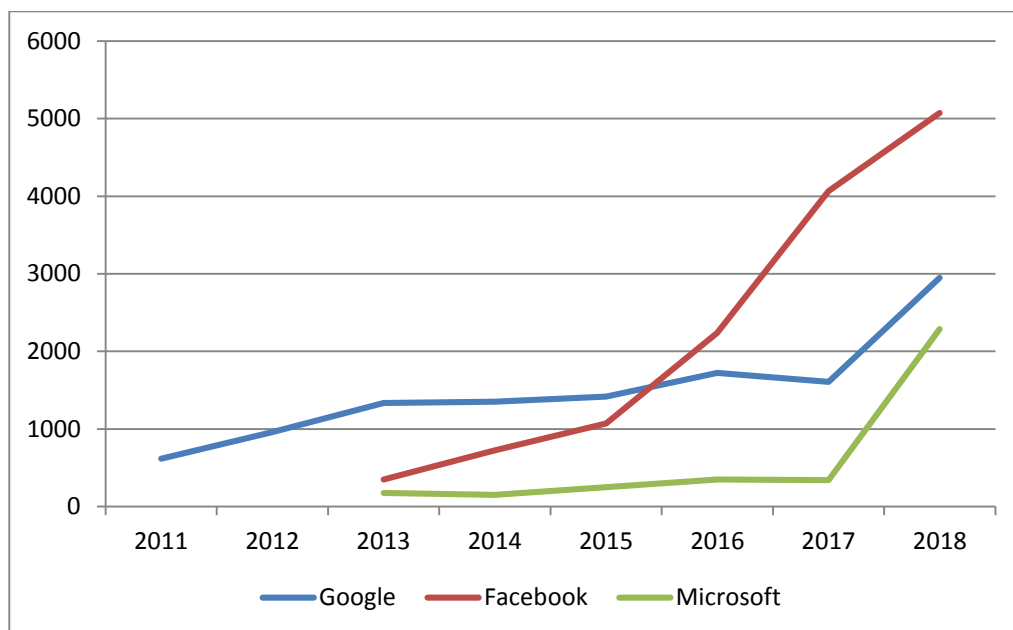
3. Informacje podmiotów komercyjnych

Trzecie źródło informacji ma charakter pozapaństwowy. W ramach korporacyjnych polityk transparentności swoje informacje udostępniają firmy sektora szeroko rozumianych usług informatycznych, w tym największe amerykańskie korporacje. Zliczają one liczbę zapytań, które kierują do nich uprawnione instytucje, uwzględniając liczbę wyrażonych zgód, liczbę kont/użytkowników, których dotyczyły zapytania, oraz procent wniosków odrzuconych. Szczególnie istotne są dane podmiotów największych, czyli Facebooka, Amazona, Google'a, Microsoftu i Apple'a, nazywanych zbiorczo FAGMA. W kontekście polskim Amazon i Apple nie odgrywają jednak istotnej roli, podobnie jak coraz popularniejszy Twitter. Wielką trójkę, będącą obiektem szczególnego zainteresowania za strony polskich instytucji, tworzą Facebook, Google i Microsoft.

Zamieszczony poniżej wykres przedstawia informacje dotyczące liczby użytkowników/kont wskazanych we wnioskach polskich instytucji w latach 2013–2018. W przypadku firmy Google dostępne są jeszcze dane za lata 2009–2010, są one jednak niepełne, w związku z czym nie znalazły się na wykresie. Nie ma na nim również danych Amazona – lakoniczny raport korporacji rozróżnia jedynie dwie kategorie państw: Stany Zjednoczone i wszystkie pozostałe. Skala zapytań wśród tych drugich jest zresztą minimalna. Apple i Twitter dzielą wprawdzie przypadki na państwa i dane dotyczące Polski są dostępne, gdyby jednak umieścić je na wykresie, byłyby niemal niezauważalne. Przykładowo, w pierwszej połowie 2018 r. (dane za drugą połowę są ciągle niedostępne) polskie instytucje skierowały do firmy z Cupertino wnioski w sprawie udostępnienia danych dotyczących 32 urzędów i ośmiu kont użytkowników. Równie niewielka jest skala zainteresowania Twitterem – wnioski dotyczyły zaledwie 37 kont użytkowników.

Zupełnie inaczej wyglądają dane wspomnianej wielkiej trójki. W ich przypadku liczby użytkowników/kont wskazanych we wnioskach idą w tysiące.

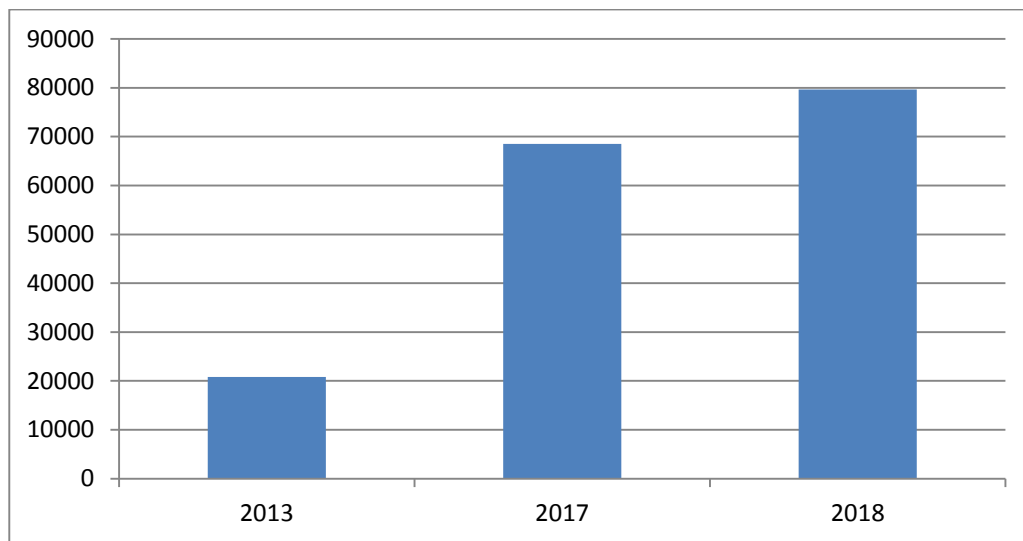
Wykres 12. Liczba użytkowników/kont wskazanych we wnioskach o udostępnienie danych, złożonych przez polskie instytucje w latach 2011–2018.



W przypadku wszystkich trzech korporacji zauważalny jest stały wzrost zainteresowania danymi użytkowników. W 2018 r. polskie instytucje wnioskowały o udostępnienie informacji dotyczących 5 tys. kont/użytkowników Facebooka, 2,9 tys. Google'a i 2,2 tys. Microsoftu. W porównaniu do poprzedniego roku oznacza to wzrost o – odpowiednio – 20%, 54% i 85%.

Widocznego w ostatnich latach zdecydowanego wzrostu (zwłaszcza w zakresie Facebooka) zainteresowania tymi danymi nie należy łączyć ze zmianą władzy w Polsce. To raczej znak czasów – zainteresowanie danymi w dyspozycji wielkiej trójki rośnie powszechnie. Zamieszczony poniżej wykres przedstawia sumę liczby użytkowników/kont Facebooka wskazanych we wnioskach o udostępnienie danych, złożonych przez instytucje państw członkowskich Unii Europejskiej w latach 2017–2018. Dla porównania dodano również dane dotyczące roku 2013 r. Trzeba zaznaczyć, że Facebook jest tutaj rozumiany jako firma, a nie jako usługa i dane obejmują nie tylko serwis społecznościowy o tej nazwie, ale także usługi Instagram, Messenger, Oculus i Whatsapp.

Wykres 13. Liczba użytkowników/kont Facebooka wskazanych we wnioskach o udostępnienie danych, złożonych przez instytucje państw członkowskich Unii Europejskiej w 2013, 2017 i 2018 r.

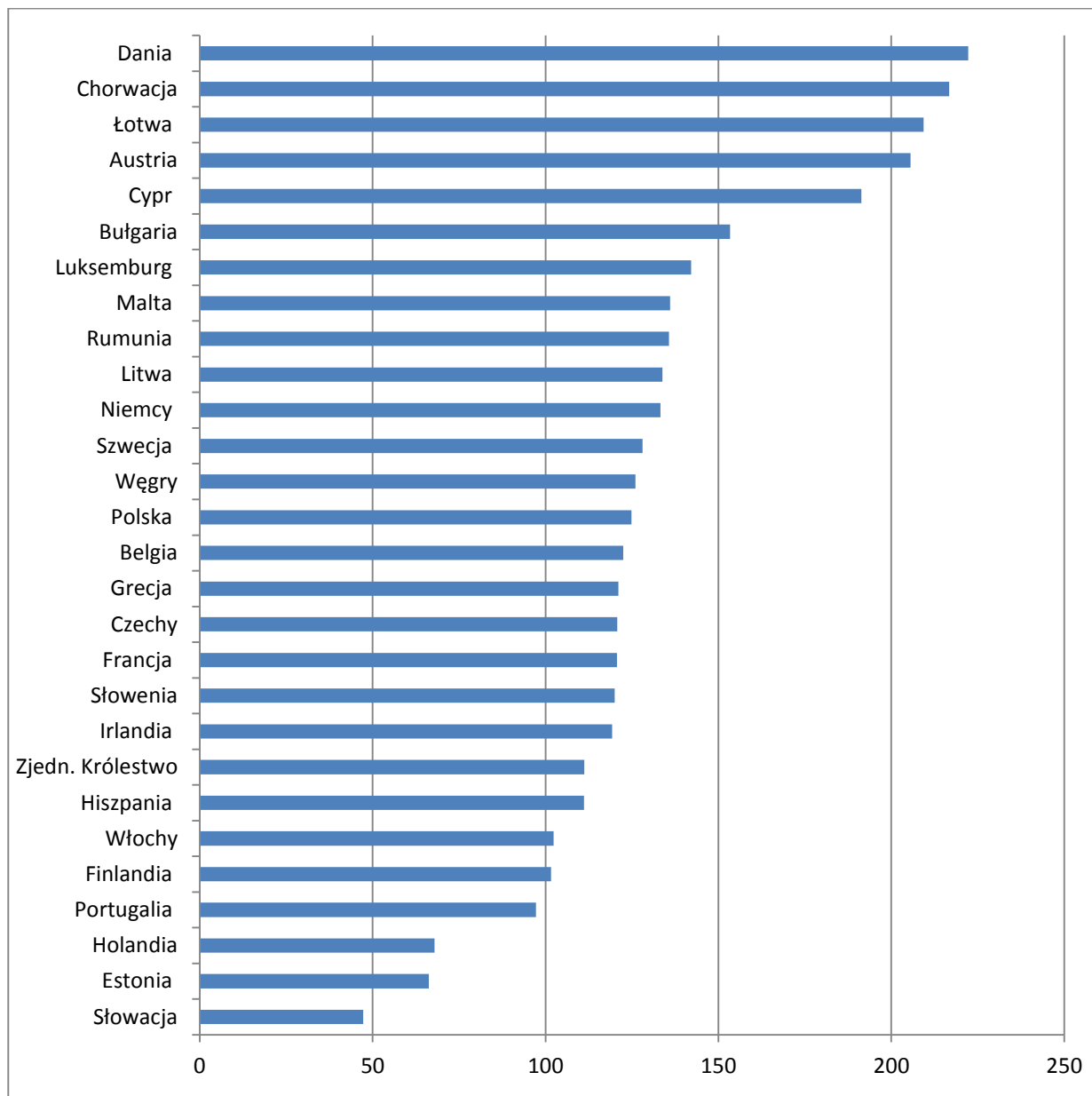


We wszystkich wnioskach złożonych do Facebooka w 2013 r. przez instytucje państw członkowskich UE domagały się one udostępnienia danych dotyczących 20,8 tys. kont/użytkowników, w 2017 r. – 68,5 tys., a w 2018 r. – 79,6 tys. Dla porównania, analogiczne dane dotyczące USA wynoszą odpowiednio 38,7 tys., 105,9 tys. i 134,1 tys.

Spośród państw członkowskich UE w 2018 r. o udostępnienie danych dotyczących największej liczby użytkowników/kont Facebooka wnioskowały Zjednoczone Królestwo (wnioski dotyczące 19,9 tys. użytkowników/kont), Niemcy (17 tys.), Francja (12,5 tys.), Włochy (8,3 tys.), Polska (5 tys.) i Hiszpania (4,5 tys.), wyraźnie wyprzedzając resztę stawki. W decydującej mierze wynika to z pewnością z wielkością ich populacji – wymieniona szóstka to państwa zdecydowanie najludniejsze w Unii Europejskiej.

Dynamika wzrostu zainteresowania danymi nie jest jednolita, co obrazuje zamieszczony poniżej wykres. Przedstawia on odpowiedź na pytanie, jaki procent liczby użytkowników/kont Facebooka wskazanych we wnioskach o udostępnienie danych w 2018 r. stanowiły analogiczne liczby z 2017 r. Wartość 100% oznacza, że instytucje danego państwa wskazały we wnioskach z 2018 r. taką samą liczbę kont/użytkowników, jak w 2017 r., 200% oznacza dwukrotny wzrost liczby kont/użytkowników, a 50% – ich dwukrotny spadek.

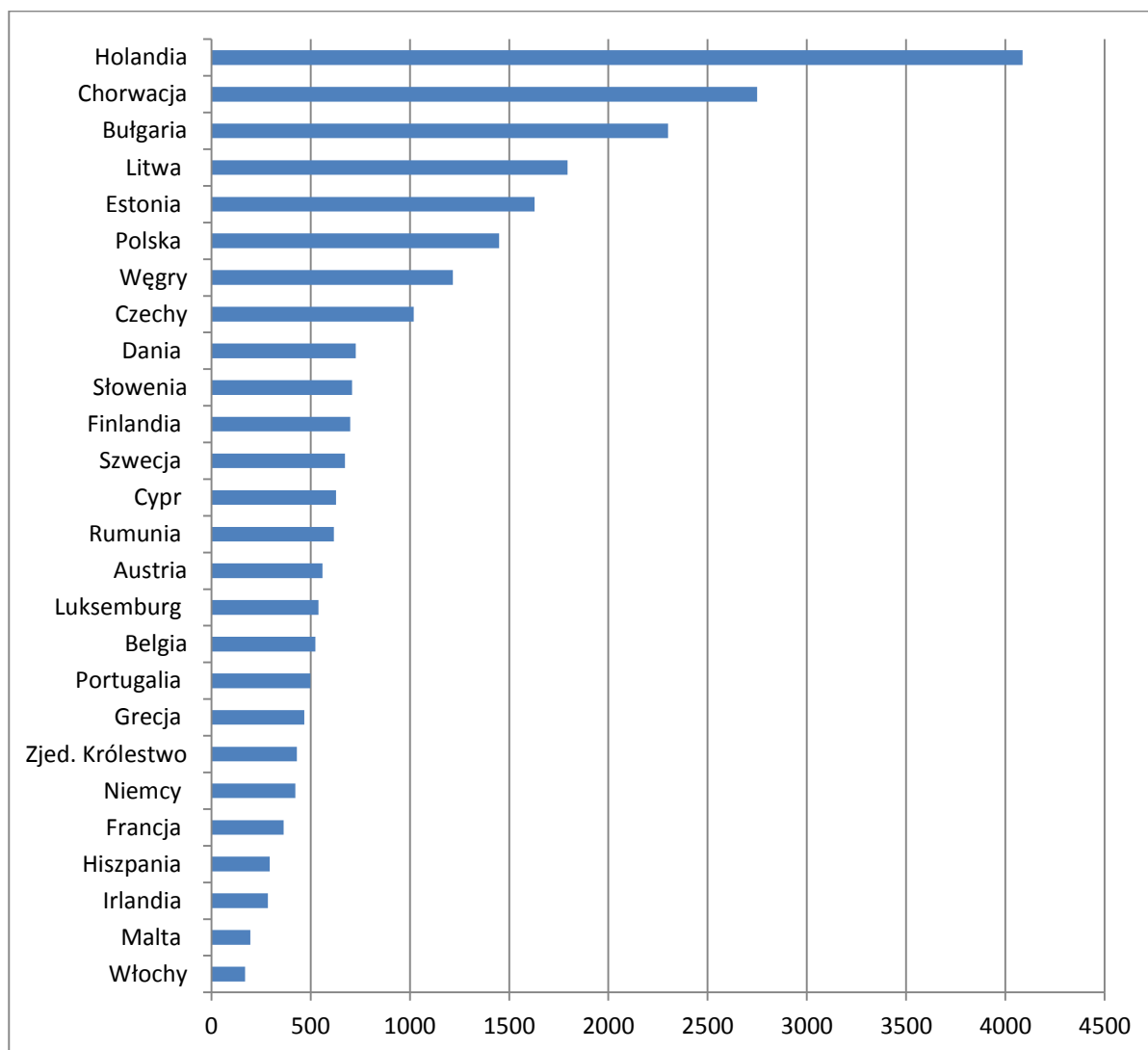
Wykres 14. Stosunek procentowy liczby użytkowników/kont Facebooka wskazanych we wnioskach o udostępnienie danych, złożonych przez instytucje państw członkowskich Unii Europejskiej w 2018 r., w relacji do 2017 r.



Największy procentowy wzrost dotyczy instytucji duńskich, które w 2018 r. były zainteresowane ponad dwukrotnie większą liczbą kont/użytkowników Facebooka niż w roku poprzednim. Tylko w przypadku czterech państw zanotowano spadek. Polska uplasowała się w środku stawki. W 2017 r. nadwiślańskie instytucje chciały pozyskać dane dotyczące 4 tys. kont/użytkowników Facebooka, a w 2018 r. – 5 tys., co oznacza wzrost o jedną czwartą w przeciągu roku.

Kolejny wykres przedstawia analogiczne dane, 2018 r. zestawiono w nim jednak z 2013 r. Analogicznie, 100% oznacza utrzymanie *status quo*.

Wykres 15. Stosunek procentowy liczby użytkowników/kont Facebooka wskazanych we wnioskach o udostępnienie danych, złożonych przez instytucje państw członkowskich Unii Europejskiej w 2018 r., w relacji do 2013 r.

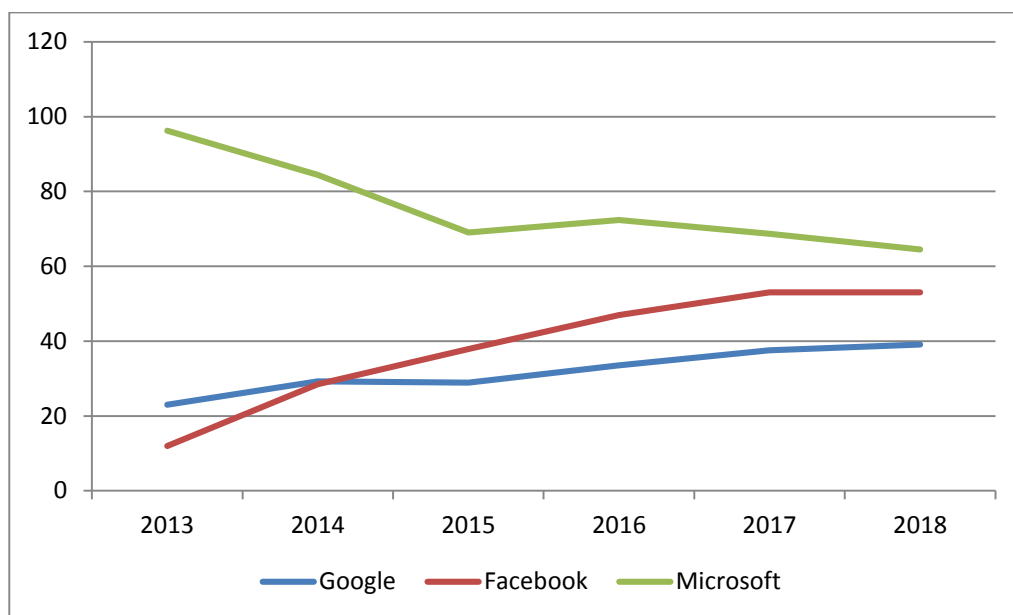


Na wykresie nie znalazły się Łotwa i Słowacja, które w 2013 r. nie złożyły żadnych wniosków. Zestawienie otwiera Holandia, której instytucje w 2018 r. złożyły wnioski dotyczące ponad czterdziestokrotnie większej liczby użytkowników/kont Facebooka niż w 2013 r. Wzrost zanotowano we wszystkich państwach UE, a Polska znalazła się w czołówce stawki. W 2013 r. polskie instytucje wnioskowały o dane dotyczące 350 kont/użytkowników Facebooka, a w 2018 r., jak już wspomniano, o dane 5 tys., co oznacza ponad czternastokrotny wzrost.

Zmienia się też podejście korporacji do udostępniania danych. Obrazuje to zamieszczony poniżej wykres 16. Trzeba jeszcze raz podkreślić, że wykresy 12.–15. przedstawiają liczbę użytkowników/kont, których dotyczyły wnioski, a nie liczbę wniosków. Przykładowo w okresie styczeń–czerwiec 2013 r. polskie instytucje skierowały do Facebooka 233 wnioski, które dotyczyły 158 kont użytkowników. W tym samym okresie do Microsoftu wpłynęło 55 polskich wniosków, które dotyczyły 76 kont/użytkowników. Przedstawiony na wykresie

16. procentowy wskaźnik zgód odnosi się natomiast do liczby wniosków, a nie liczby kont/użytkowników.

Wykres 16. Odsetek wyrażonych zgód na złożone przez polskie instytucje w latach 2013–2018 wnioski.



Dane dotyczące Google’a i Facebooka wskazują, że instytucje te coraz częściej pozytywnie rozpatrują wnioski polskich instytucji. Inaczej wygląda to w przypadku Microsoftu. Przed laty gigant z Redmond rozpatrywał pozytywnie niemal wszystkie wnioski, a obecnie – „zaledwie” dwie trzecie. Trzeba jednak wziąć pod uwagę, że w stosunku do 2013 r. liczba skierowanych do niego przez polskie instytucje wniosków wzrosła dwukrotnie, a liczba danych użytkowników/kont, których te wnioski dotyczyły – trzynastokrotnie. Spadku wskaźnika wyrażonych zgód nie należy więc zapewne interpretować jako konsekwencji bardziej restrykcyjnej polityki Microsoftu.

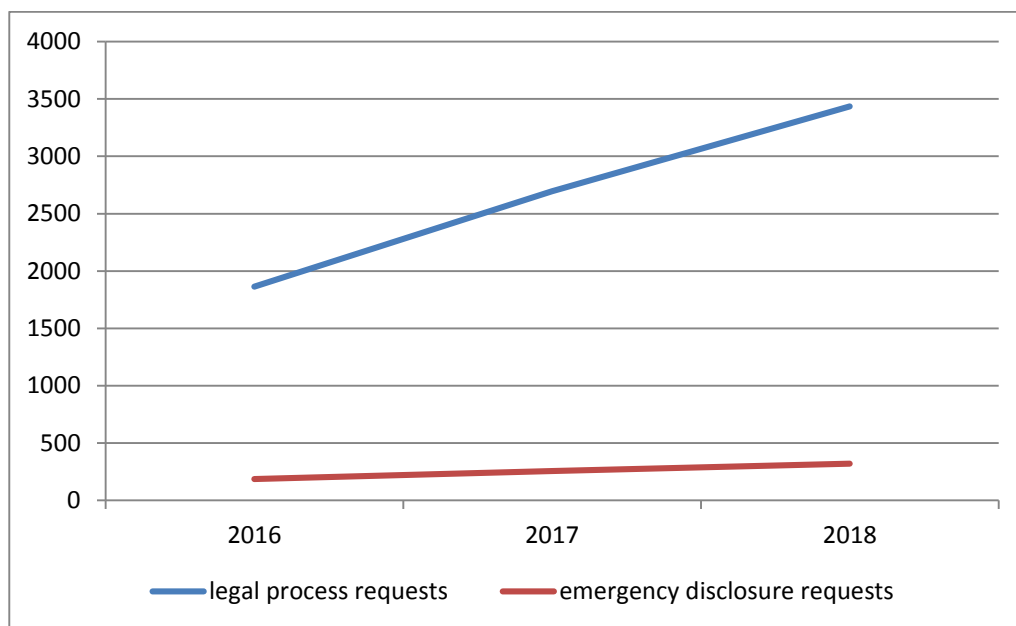
Rozważając statystyki dotyczące odrzuconych wniosków, trzeba też pamiętać, że chociaż w związku z decyzją odmowną nie przekazano wnioskodawcy informacji o użytkowniku, nie oznacza to, że nie przekazano ich w ogóle. Możliwym jest, że instytucja złożyła dotyczący tej samej osoby wniosek ponownie i tym razem został on zaakceptowany. Sama akceptacja wniosku nie musi mieć zresztą charakteru całkowitego – firmy wykazują bowiem wnioski rozpatrzone pozytywnie w części lub całości.

Nie wiadomo oczywiście, czego dokładnie dotyczyły składane wnioski. Microsoft oferuje jedynie ogólną informację, jaka część wniosków dotyczyła treści, a jaka danych jej niestanowiących. Przykładów wniosków dotyczących pierwszego typu danych jest tak mało, że są zupełnie niewidoczne w statystyce. Google dzieli wnioski na „żądania ujawnienia w sytuacjach nadzwyczajnych”, „prośby o zachowanie danych” i „inne wnioski prawne”, a Facebook na „*emergency disclosure requests*” i „*legal process requests*”. Nie tłumaczy tego wprawdzie dokładnie, ale przez te pierwsze należy zapewne rozumieć

przetwarzanie danych internetowych w ramach czynności operacyjno-rozpoznawczych, a przez te drugie – przetwarzanie danych internetowych na gruncie Kodeksu postępowania karnego, jak również kontrolę operacyjną i procesową (dostęp do danych będących treścią).

Zamieszczony poniżej wykres przedstawia dane Facebooka w podziale na te dwa typy wniosków. Dostępne są jednak wyłącznie informacje obejmujące lat 2016–2018.

Wykres 17. Liczba wniosków składanych przez polskie instytucje do Facebooka w latach 2016–2017 z podziałem na typy.



Zdecydowanie dominują więc wnioski wykraczające poza ratowanie życia lub zdrowia ludzkiego bądź wsparcie działań poszukiwawczych lub ratowniczych.

4. Podsumowanie, czyli po co nam statystyki inwigilacyjne?

Chociaż dostępne dane dotyczące skali inwigilacji są dość skąpe, można przetwarzać je na wiele sposobów, poszukując ogólnych prawidłowości, trendów i cykli koniunkturalnych. Wszystkie te dociekania są jednak mocno ograniczone przez niejawnosć kluczowych informacji. Jest ona nie tylko czymś naturalnym, ale także pożądanym. Nie ulega wątpliwości, że wiele informacji dotyczących kontroli operacyjnej i procesowej oraz przetwarzania danych musi pozostać poza domeną publiczną. Wątpliwości dotyczą jednak nie ogólnej zasady, tylko zakresu tego, co opinia publiczna wiedzieć powinna.

Statystyki oferują ograniczony wgląd w inwigilacyjne tendencje, jednocześnie generując szereg pytań. Przykładowo, wiadomym jest, że polscy prokuratorzy i sędziowie niemal zawsze akceptują wnioski instytucji bezpieczeństwa dotyczące kontroli operacyjnej, ale nie jest jasne dlaczego tak się dzieje. Można zastanawiać się, czy wynika to z przekonujących uzasadnień organów wnioskujących, czy też biurokratycznego automatyzmu, z którego

wyłączane są jedynie rażące przypadki. Można też pytać, co jest przyczyną niewyrażenia zgody czy wydania postanowienia odmownego. Ostatnia z kwestii jest tym istotniejsza, że część (nie wiadomo jak duża) wniosków o zarządzenie kontroli operacyjnej trafia do prokuratora generalnego, który jest organem zależnym od bieżącego układu politycznego.

Trudno znaleźć racjonalne argumenty przemawiające za tak lakoniczną sprawozdawczością. Mało przekonującym wydaje się pogląd, że poznanie przez opinię publiczną statystyki dotyczącej powodów niezarządzenia kontroli operacyjnej mogłoby narazić na szwank prowadzenie czynności operacyjno-rozpoznawczych przez polskie służby policyjne czy specjalne. Nie jest dziwnym, że politykom i instytucjom bezpieczeństwa nie zależy na tym, aby informować opinię publiczną, jak często składane są wnioski o założenie podsłuchu nieposiadające odpowiedniej podstawy prawnej. W interesie społecznym jest jednak wyrażanie przekonania, że tego rodzaju informacje powinny być dostępne.

Tego rodzaju głosy są często traktowane w przestrzeni publicznej jako alarmistyczne, czemu towarzyszą dwa koronne argumenty. Po pierwsze, „uczciwi ludzie nie mają się czego obawiać”, a po drugie – nie należy utożsamiać niejawności z patogennością. Czynności inwigilacyjne są wprawdzie realizowane przy ograniczonym nadzorze i kontroli ze strony opinii publicznej, ale nie oznacza to, że są tego nadzoru czy kontroli w ogóle pozbawione. Nadużycia, jeśli już w ogóle się zdarzają, niekoniecznie mają powszechny charakter.

Oba te argumenty bazują na nieuprawnionym założeniu, że postulaty transparentności wynikają ze strachu przed państwem, albo z niechęci do niego. Można interpretować je dokładnie odwrotnie, jako wyrazy troski o państwo i jego instytucje. *Feedback* ze strony społeczeństwa jest w takich sytuacjach niezbędny, to on w dużej mierze wytwarza presję na reformy, generuje postulaty uszczelnienia procedur, egzekwuje adekwatność środków i ich możliwą nieinwazyjność.

Pomiędzy prowadzeniem nieodzownych dla każdego państwa czynności inwigilacyjnych a wolnościami obywatelskimi musi znajdować się korzystna dla obu stron, państwa i społeczeństwa, równowaga. Chodzi więc nie o rewolucję, tylko o doskonalenie instytucji. Temu właśnie służą działania Rzecznika Praw Obywatelskich czy organizacji pozarządowych, które procesami sądowymi i składanymi wnioskami o dostęp do informacji publicznej równoważą naturalną hermetyczność służb policyjnych i specjalnych.

Jeszcze innym argumentem jest wyrażane czasem przekonanie, że skala problemu jest wyolbrzymiona, jako że inwigilacja dotyczy tylko niewielkiej części społeczeństwa. To oczywiście kwestia czysto subiektywna, ale szersza perspektywa może skłaniać do odmiennej refleksji. W latach 2010–2018 sama tylko Policja wnioskuje o objęcie kontrolą operacyjną 41,4 tys. ludzi, czyli mniej więcej tylu, ilu mieszka w Świnoujściu. W sumie w tych

latach zarządzono kontrolę operacyjną lub procesową wobec 50,4 tys. osób. Skala przetwarzania danych pochodzących z retencji jest nieporównywalnie większa. W samym tylko 2018 r. przetworzono ponad 1,3 mln danych telekomunikacyjnych. Nawet przyjmując, że na jednego inwigilowanego posiadacza telefonu przypadało 20 przetworzonych danych, zjawisko dotyczyło 66 tys. ludzi. Należy zakładać, że jego skala będzie rosła z każdym kolejnym rokiem.

Można oczywiście przyjąć, że statystyki zakłamują rzeczywistość i stwarzają jedynie złudzenie społecznego nadzoru i kontroli. Ich brak byłby jednak dla opinii publicznej jeszcze dotkliwszy, zgodnie z zasadą *anceps remedium melius quam nullum*. Dzięki statystykom można przynajmniej stwierdzić z niejaką pewnością: wiem, że nie wiem.

Statystyk inwigilacyjnych nie należy więc traktować jako gotowych odpowiedzi, a raczej jako empiryczne podstawy do zadawania konkretnych pytań.

Wszystkie obliczenia, dane procentowe, wykresy i tabele pochodzą od autora.