



Analiza

KBN

Nr 11 (126) / 2023

28 sierpnia 2023 r.



Niniejsza publikacja ukazuje się na warunkach międzynarodowej licencji publicznej Creative Commons 4.0 – uznanie autorstwa – na tych samych warunkach – użycie niekomercyjne.

This work is licensed under a Creative Commons Attribution – NonCommercial – ShareAlike 4.0 International License

Raport inwigilacyjny (edycja 2022)

[Arkadiusz Nyzio](#)

W drugiej połowie każdego roku publikowane są cztery rodzaje informacji obrazujących skalę inwigilacji w Polsce w roku poprzednim. Warto przyrzeć się statystykom dotyczącym bilingów, podsłuchów, kontroli korespondencji i danych użytkowników, którymi w 2022 r. interesowały się polskie instytucje bezpieczeństwa. Jak zawsze w przypadku prowadzonych przez nie niejawnych działań, informacje są skąpe, a w ślad za każdą niepełną odpowiedzią podąża szereg pytań i wątpliwości.

Najważniejsze wnioski:

1. W 2022 r. zarządzono kontrolę operacyjną lub procesową wobec 6,2 tys. osób, co jest piątym najwyższym wynikiem odkąd prowadzona jest sprawozdawczość w tym zakresie (czyli od trzynastu lat). To spadek o 10% w stosunku do roku poprzedniego.
2. W latach 2010–2022 zarządzono kontrolę wobec prawie 74 tys. osób, wnioski dotyczyły zaś ponad 76 tys. Oznacza to sumaryczną skuteczność wynoszącą prawie 97%.
3. Podmiotem, który wnioskował o objęcie kontrolą operacyjną największej liczby osób, była w 2022 r. Policja (87%). Na drugim miejscu uplasowała się Straż Graniczna (3,3%), a na trzecim – ABW (3%).

4. Praktycznie wszystkie wnioski o zarządzenie kontroli zostają przyjęte. W 2022 r. prokuratorzy odrzucili 2% wniosków, a sądy – 0,6%. Od 2016 r. wskaźnik skuteczności wniosków przekracza 97% i nie inaczej było w ubiegłym roku.
5. Policja prowadziła kontrolę operacyjną przede wszystkim w związku przestępstwami przeciwko porządkowi publicznemu (przestępczość zorganizowana), przeciwko mieniu (rozboje, oszustwa) i narkotykowymi.
6. W latach 2016–2021 każdy rok przynosił rekordową liczbę przetworzonych danych telekomunikacyjnych, pocztowych i internetowych. W 2022 r. odnotowano jednak nieznaczny spadek (o 1,5%). Wynika on z mniejszej liczby przetworzonych danych telekomunikacyjnych – wskaźniki dotyczące danych internetowych i pocztowych wzrosły. 74,5% wszystkich danych przetworzyła Policja.
7. Przetworzono rekordową liczbę danych pocztowych (ponad 22 tys.), co oznacza wzrost o jedną czwartą w stosunku do 2021 r. Blisko połowę z nich przetworzyła Policja.
8. Liczba przetworzonych danych internetowych niemal nie uległa zmianie w stosunku do 2021 r. (ponad 20 tys.). 82% z nich przetworzyła Policja.
9. Rośnie liczba użytkowników/kont w usługach korporacji Meta (Facebook, Instagram, Messenger, Whatsapp), o które pytają polskie instytucje. W 2022 r. wystosowały wnioski o udostępnienie danych ponad 15 tys. kont/użytkowników – 40 razy więcej niż w 2013 r. i o 17% więcej niż w 2021 r. W Unii Europejskiej przodują Niemcy (51,8 tys.) i Francja (30,1 tys.), Polska zajmuje trzecie miejsce.
10. Powstała już dziesiąta instytucja mogąca prowadzić w Polsce kontrolę operacyjną i dwunasta, która może operacyjnie przetwarzać dane telekomunikacyjne, pocztowe i internetowe – Inspektorat Wewnętrzny Służby Więziennej.
11. Wciąż rośnie liczba tzw. przestępstw katalogowych, w związku z którymi instytucje mogą wnioskować o zarządzenie kontroli operacyjnej.
12. Procedura kontroli uprzedniej i następczej nad czynnościami operacyjno-rozpoznawczymi pozostaje głęboko wadliwa.

Informacje wprowadzające

Po pierwsze, uprawnione instytucje **przetwarzają** w Polsce dane związane z komunikacją międzyludzką i aktywnością teleinformatyczną (np. korespondencją mailową lub rozmową telefoniczną) w dwóch **trybach**:

- Procesowym – czyli w związku z toczącym się postępowaniem przygotowawczym, będącym pierwszym stadium (etapem) postępowania karnego. Postanowienie o wszczęciu jednej z form postępowania przygotowawczego, czyli śledztwa lub dochodzenia, jest wydawane jeśli zachodzi uzasadnione podejrzenie popełnienia przestępstwa, z urzędu lub na skutek zawiadomienia o przestępstwie. W postanowieniu określa się czyn będący przedmiotem postępowania i jego kwalifikację prawną.

Przepisy dotyczące postępowania przygotowawczego zawiera Kodeks postępowania karnego (kpk). W związku z tym ten tryb nazywa się „kodeksowym”.

- Pozaprosesowym – czyli na tzw. przedpolu postępowania karnego. W tym przypadku nie toczy się postępowanie przygotowawcze, niekoniecznie doszło w ogóle do popełnienia przestępstwa. W tym przypadku mówimy o czynnościach operacyjno-rozpoznawczych prowadzonych poza przepisami kpk, na podstawie ustaw kompetencyjnych właściwych służb (np. Policji lub służb specjalnych). W związku z tym ten tryb nazywa się „pozakodeksowym”. Zebrane w toku prowadzenia czynności operacyjno-rozpoznawczych informacje mogą (ale nie muszą) stać się podstawą do wszczęcia postępowania.

Po drugie, uprawnione instytucje przetwarzają w Polsce dane dwojakiego **rodzaju**:

- Dane stanowiące treść – czyli obejmujące informacje na temat „zawartości” komunikacji (np. treść wysłanego maila). Poświęcona jest im [część 1. raportu](#).
- Dane niestanowiące treści (tzw. metadane) – czyli obejmujące informacje na temat samego faktu wystąpienia komunikacji/aktywności (np. godzina wysłania maila i jego adresat). Poświęcona jest im [część 2. raportu](#).

Procedura przetwarzania danych zależy od **trybu** i ich **rodzaju**. Niniejszy raport poświęcony jest trybowi pozaprosesowemu i obu typom danych. Tryb procesowy został w nim częściowo uwzględniony jedynie w celu porządkującym i uzupełniającym problematykę. Trzeba wyraźnie podkreślić, że tytułowe potoczne sformułowanie „inwigilacja” odnosi się do czynności operacyjno-rozpoznawczych, a nie do danych przetwarzanych na gruncie kpk. Omawiany tu obszar czynności operacyjno-rozpoznawczych (COR lub praca operacyjna) zalicza się do **techniki operacyjnej**.

Sama czynność „przetwarzania”, zgodnie z [rozporządzeniem RODO](#), oznacza „operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie”.

Trzeba podkreślić, że polskie instytucje nie mają prawa do przełamania teleinformatycznych zabezpieczeń – włamywania się do smartfonów czy kont użytkowników internetowych usług.

Uzupełnieniem raportu są informacje o liczbie zapytań dotyczących kont i użytkowników, które polskie instytucje kierują do największych korporacji informatycznych ([część 3.](#)).

1. Kontrola operacyjna i procesowa

1.1. Najważniejsze pojęcia, podstawa prawna i procedura

Niejawne przetwarzanie danych stanowiących treść komunikacji pomiędzy ludźmi odbywa się drogą **kontroli operacyjnej** (w ramach czynności operacyjno-rozpoznawczych) lub **kontroli procesowej** (na gruncie kpk, w związku z toczącym się postępowaniem). Najczęściej łączy się je z podsłuchami, obejmują jednak także np. kontrolę zawartości przesyłek pocztowych, maili, SMS-ów i MMS-ów, zapisu rozmowy poprzez komunikatory internetowe oraz uzyskiwanie i utrwalanie obrazu lub dźwięku z pomieszczeń, środków transportu lub miejsc „innych niż miejsca publiczne”. Sam podsłuch nie musi mieć związku z telekomunikacją (podsłuch telefoniczny – PT; podsłuch telefonii komórkowej – PTK), ale może polegać na stosowaniu urządzeń rejestrujących różnego rodzaju sygnały, np. ukrytych kamer lub pluskiew podsłuchowych (tzw. podsłuch pokojowy, PP). Kontrola polegająca na przetwarzaniu treści komunikacji w sieci nazywana jest kontrolą korespondencji internetowej (KKI).

Przetwarzanie danych stanowiących treść odbywa się więc zarówno na gruncie kpk, czyli po wszczęciu postępowania („kontrola i utrwalanie rozmów”, najczęściej nazywane po prostu kontrolą procesową), jak i pozaprocesowo, w ramach czynności operacyjno-rozpoznawczych (kontrola operacyjna). Obie te formy nazywane są popularnie „podsłuchem procesowym” i „pozaprocesowym”.

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 bezpieczeństwa muszą składać do sądów okręgowych uzasadnione wnioski o jej zarządzenie.

Wydając postanowienie o zarządzeniu kontroli operacyjnej, sąd uruchamia prawny „zegar”. Od tego momentu właściwa instytucja dysponuje określonym w postanowieniu czasem prowadzenia kontroli operacyjnej. Analogicznie jest z czytaniem korespondencji czy podsłuchem w pomieszczeniach. Kontrola operacyjna odnosi się więc do przyszłości, a nie do przeszłości – wydane przez sąd postanowienie nie oznacza, że można przetwarzać np. treści maili czy smsów sprzed okresu jej zarządzenia. Trzeba też zaznaczyć, że treść rozmów telefonicznych nie podlega obowiązkowi retencji (zob. [2.1.](#)). Innymi słowy, rozmowy telefoniczne nie są rutynowo utrwalane i przechowywane przez operatorów na potrzeby instytucji państwa.

W Polsce o zarządzenie kontroli operacyjnej wnioskować mogą cztery służby policyjne; Policja, Straż Graniczna (SG), Żandarmeria Wojskowa (ŻW) i Służba Celno-Skarbowa (SCS) działająca w ramach Krajowej Administracji Skarbowej (KAS); oraz trzy służby specjalne:

Centralne Biuro Antykorupcyjne (CBA), Agencja Bezpieczeństwa Wewnętrznego (ABW) i Służba Kontrwywiadu Wojskowego (SKW). Ponadto kompetencję tę posiadają Biuro Nadzoru Wewnętrznego (BNW), jednostka organizacyjna Ministerstwa Spraw Wewnętrznych i Administracji oraz trudna do sklasyfikowania Służba Ochrony Państwa (SOP).

Nowością jest przyznanie tego uprawnienia kolejnej, już dziesiątej instytucji. Mowa o Inspektoracie Wewnętrznym Służby Więziennej (IWSW), który wprowadziła do polskiego porządku normatywnego [ustawa z 22 lipca 2022 r.](#) To kolejny – obok BNW – osobliwy twór w polskim systemie bezpieczeństwa. IWSW jest jednostką organizacyjną Służby Więziennej, ale nie podlega jej dyrektorowi generalnemu, tylko jest nadzorowana przez ministra sprawiedliwości. 5 października 2022 r. powołano pełnomocnika [do spraw jej utworzenia](#). 21 grudnia 2022 r. minister sprawiedliwości nadał IWSW [regulamin organizacyjny](#), a 9 grudnia 2022 r. określił procedurę [kontroli operacyjnej](#) prowadzonej przez instytucję.

Każda z instytucji prowadzi kontrolę operacyjną w granicach swoich właściwości przedmiotowych (czyli w zakresie tego, czym się zajmuje) i podmiotowych (czyli w zakresie tego, kim się zajmuje). Najszerszy katalog przedmiotowy i podmiotowy posiada oczywiście Policja.

Przed złożeniem wniosku do sądu zainteresowane zarządzeniem kontroli operacyjnej instytucje muszą jeszcze uzyskać zgodę właściwego prokuratora – okręgowego lub generalnego. Tabela 1. przedstawia organy decyzyjne w zakresie kontroli operacyjnej.

Tabela 1. Właściwe organy w zakresie 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, Biura Spraw Wewnętrznych i Centralnego Biura Zwalczania Cyberprzestępczości, 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 zastępca)	generalny	okręgowy w Warszawie
Krajowa Administracja Skarbowa	szeft (po upoważnieniu – także jego zastępca)	generalny	okręgowy w Warszawie
Centralne Biuro Antykorupcyjne	szeft (po upoważnieniu – także jego zastępca)	generalny	okręgowy w Warszawie

Agencja Bezpieczeństwa Wewnętrznego	szeft (po upoważnieniu – także jego zastępcą)	generalny	okręgowy w Warszawie
Biuro Nadzoru Wewnętrznego	inspektor nadzoru wewnętrznego (po upoważnieniu – także jego zastępcą)	generalny	okręgowy w Warszawie
Żandarmeria Wojskowa	komendant główny, komendant oddziału – za zgodą komendanta głównego (po upoważnieniu – także ich zastępcy)	generalny lub zastępcą prokuratora okręgowego do spraw wojskowych – w przypadku wniosków komendantów oddziałów lub ich zastępców	wojskowy okręgowy
Służba Kontrwywiadu Wojskowego	szeft (po upoważnieniu – także jego zastępcą)	generalny	wojskowy okręgowy w Warszawie
Inspektorat Wewnętrzny Służby Więziennej (nie rozpoczął jeszcze działać)	szeft (po upoważnieniu – także jego zastępcą)	generalny	okręgowy w Warszawie

Od przedstawionej powyżej reguły istnieją dwa wyjątki, jest też jedno specyficzne rozwiązanie.

Po pierwsze, chodzi o tryb specjalny dotyczący przypadków „niecierpiących zwłoki”, czyli takich, w których występuje ryzyko utraty informacji oraz zatarcia lub zniszczenie dowodów. W takich sytuacjach kontrola operacyjna może być zarządzona po uzyskaniu zgody właściwego prokuratora, ale bez postanowienia sądu. Organ uprawniony do prowadzenia kontroli jest wówczas 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. Po kontrolę operacyjną w trybie specjalnym może sięgać każda spośród wymienionych instytucji.

Po drugie, szef ABW może zarządzić podsłuchiwanie „osoby niebędącej obywatelem” RP w celu „rozpoznawania, zapobiegania lub zwalczania przestępstw o charakterze terrorystycznym”. Zarządzenie (wraz z uzasadnieniem) szef ABW musi „niezwłocznie” przekazać prokuratorowi generalnemu i ministrowi koordynatorowi służb specjalnych (jeżeli został powołany). Prokurator generalny może nakazać zaprzestanie czynności. Udział sądu w tej procedurze nie jest przewidziany. Nie dysponujemy też jakimikolwiek informacjami dotyczącymi tego, jak często ABW sięga po to uprawnienie. Należy dodać, że jest to rozwiązanie w sposób jaskrawy niezgodne z polską konstytucją. Minęło już siedem lat jego obowiązywania.

Po trzecie, ustawą z 22 listopada 2013 r. [o postępowaniu wobec osób z zaburzeniami psychicznymi](#) stwarzających zagrożenie życia, zdrowia lub wolności seksualnej ustanowiono instytucje osoby „stwarzającej zagrożenie” i „nadzoru prewencyjnego”. O uznaniu osoby za stwarzającą zagrożenie i o zastosowaniu wobec niej nadzoru prewencyjnego decyduje

sąd wydając stosowne postanowienie. Za prowadzenie „nadzoru prewencyjnego” osoby „stwarzającej zagrożenie” odpowiada powiatowa (miejska, rejonowa) Policja. W tym celu może ona prowadzić czynności operacyjno-rozpoznawcze oraz „weryfikować gromadzić i przetwarzać informacje udzielane przez tę osobę oraz uzyskane w wyniku czynności operacyjno-rozpoznawczych”. Jeśli weryfikowanie tych informacji „napotyka trudności” **lub** jeśli „zachodzi uzasadniona obawa, że osoba, wobec której zastosowano nadzór prewencyjny, czyni przygotowania do popełnienia” określonych przestępstw¹, może zostać zarządzona kontrola operacyjna. Odbывается to w trybie analogicznym do opisanego powyżej (wniosek Policji na szczeblu województwa, zgoda prokuratora okręgowego, postanowienie sądu okręgowego).

Tajnością o szczególnej skali objęte są czynności operacyjno-rozpoznawcze prowadzone przez wywiady – Agencję Wywiadu (AW) i Służbę Wywiadu Wojskowego (SWW). O autoryzacji ich „inwigilacyjnych” działań zewnętrznych oficjalnie nie wiadomo dosłownie nic. Natomiast realizacja przez nie kontroli operacyjnej na terenie Polski jest dopuszczalna wyłącznie w związku z ich „działalnością poza granicami państwa” i jedynie za pośrednictwem instytucji kontrwywiadowczych, czyli ABW (w przypadku AW) oraz SKW lub ABW (w przypadku SWW).

Wniosek o zarządzanie kontroli operacyjnej właściwa instytucja bezpieczeństwa przedstawia wraz z „materiałami uzasadniającymi potrzebę zastosowania kontroli operacyjnej”. Ustawodawca nie stworzył zamkniętego katalogu informacji, które muszą znaleźć się we wniosku, wskazał jednak – analogicznie we wszystkich ustawach kompetencyjnych – że muszą być to „w szczególności”:

1. „Numer sprawy i jej kryptonim, jeżeli został jej nadany”;
2. „Opis przestępstwa z podaniem, w miarę możliwości, jego kwalifikacji prawnej”;
3. „Okoliczności uzasadniające potrzebę zastosowania kontroli operacyjnej, w tym stwierdzonej bezskuteczności lub nieprzydatności innych środków”;
4. „Dane osoby lub inne dane pozwalające na jednoznaczne określenie podmiotu lub przedmiotu, wobec którego stosowana będzie kontrola operacyjna, ze wskazaniem miejsca lub sposobu jej stosowania”;
5. „Cel, czas i rodzaj prowadzonej kontroli operacyjnej”.

We wniosku o zarządzanie kontroli właściwa instytucja bezpieczeństwa powinna zatem umieścić informację o rozwiązaniu technicznym, przy pomocy którego będzie ona prowadzona.

¹ Chodzi o przestępstwa przeciwko wolności seksualnej i obyczajności (np. zgwałcenie i wymuszenie czynności seksualnej czy seksualne wykorzystanie małoletniego) oraz przestępstwa przeciwko życiu i zdrowiu zagrożone karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat (np. zabójstwo).

W odniesieniu do punktu 4. wprowadzającego **obowiązek indywidualizacji** trzeba podkreślić, że możliwe są tzw. wnioski na N.N., czyli dotyczące osoby, której tożsamości nie ustalono. Składając wniosek, właściwa instytucja może nie dysponować jeszcze danymi osobowymi figuranta. Zostaną one ustalone już w toku kontroli operacyjnej.

[Od 2016 r.](#), dzięki orzeczeniu Trybunału Konstytucyjnego, rodzaje kontroli operacyjnej zostały określone jednobrzmiąco we wszystkich ustawach kompetencyjnych właściwych instytucji. Ustawodawca wskazał, że kontrola operacyjna polega na:

1. „Uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych”;
2. „Uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne”;
3. „Uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej”;
4. „Uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych”;
5. „Uzyskiwaniu dostępu i kontroli zawartości przesyłek”.

Podmiot świadczący usługi, z którymi wiąże się realizacja kontroli operacyjnej (firma telekomunikacyjna, operator pocztowy, dostawca usług internetowych), jest zobowiązany do zapewnienia (na własny koszt) warunków technicznych i organizacyjnych umożliwiających jej prowadzenie.

Kontrola operacyjna w Polsce może być stosowana po spełnieniu dwóch kryteriów prawnych: proporcjonalności i subsydiarności.

Proporcjonalność oznacza, że kontrolę operacyjną można stosować tylko w odniesieniu do ściśle określonych czynów zabronionych – wymienionych enumeratywnie w ustawach kompetencyjnych poszczególnych służb przestępstw umyślnych ściganych z oskarżenia publicznego (**tzw. przestępstwa katalogowe**). Przedsięwzięte środki prawne powinny być adekwatne do charakteru czynu zabronionego. Policja nie może więc podsłuchiwać nikogo w związku z kradzieżą, ale w związku z rozbojem – już tak. Samo sformułowanie „przestępstwa katalogowe” jasno wskazuje, że wykluczone jest stosowanie kontroli operacyjnej (podobnie jak procesowej) w związku z wykroczeniami, np. zakłóceniem spokoju lub porządku publicznego.

Należy dodać, że katalog przestępstw jest ciągle rozszerzany, czemu nie towarzyszy zainteresowanie opinii publicznej. Przykładowo, od 30 listopada 2020 r. policjanci mogą stosować kontrolę operacyjną w związku z wytwarzaniem, posiadaniem lub obrotem nowymi

substancjami psychoaktywnymi (NSP), czyli tzw. dopalaczami. Wprowadzająca to rozwiązanie [ustawa z 30 kwietnia 2020 r.](#) została poparta przez niemal cały Sejm. O wiele szersza zmiana miała miejsce pod koniec 2021 r., a przyniosła ją ustawa [powołująca policyjne Centralne Biuro Zwalczania Cyberprzestępczości](#). Z dniem 12 stycznia 2022 r. policyjny katalog przestępstw powiększono aż o dziewięć pozycji².

Także w 2023 r. nastąpiły w tym zakresie zmiany. Przykładowo, w policyjnym katalogu znalazły się kolejne trzy artykuły kk. Po pierwsze, 13 stycznia 2023 r. przyjęto ustawę nowelizującą Kodeks postępowania cywilnego i inne ustawy. Dodała ona do kodeksu karnego art. 156a penalizującą nakłanianie innej osoby „do spowodowania u niej ciężkiego uszczerbku na zdrowiu”. Od razu ten artykuł dodano do policyjnego katalogu. Po drugie, ta sama ustawa wprowadziła do kk art. 191b penalizujący doprowadzenie innej osoby „do zawarcia małżeństwa lub związku, który odpowiada małżeństwu w kręgu wyznaniowym lub kulturowym sprawcy” przy użyciu przemocy, groźby bezprawnej lub przez „nadużycie stosunku zależności lub wykorzystanie krytycznego położenia”. Wspomniana nowelizacja weszła w życie 15 sierpnia. Po trzecie, do tej pory w policyjnym katalogu znajdował się art. 228 § 1 i 3–5 kk (sprzedajność pełniącego funkcję publiczną). Od 1 października będzie to art. 228 § 1 i 3–6. Dodany do katalogu Policji art. 228 § 6 kk brzmi: „Karom (...) podlega odpowiednio także ten, kto, w związku z pełnieniem funkcji publicznej w państwie obcym lub w organizacji międzynarodowej, przyjmuje korzyść majątkową lub osobistą albo jej obietnicę lub takiej korzyści żąda, albo uzależnia wykonanie czynności służbowej od jej otrzymania”.

Również katalog SG uległ zmianie. Po pierwsze, 15 sierpnia przybył wspomniany art. 191b. Po drugie, zmiana, która wejdzie w życie 1 października, dotyczy art. 264 kk (nielegalne przekroczenie granicy). Dotychczas w katalogu SG był art. 264 § 2 i 3 kk. Zostanie on jednak rozbudowany o nowy art. 264 § 4 kk, który brzmi: „Karze (...) podlega ten, kto organizuje innym osobom przekraczanie wbrew przepisom granicy innego państwa, jeżeli obowiązek ścigania takiego czynu wynika z ratyfikowanej przez Rzeczpospolitą Polską umowy międzynarodowej”.

Trzeba też podkreślić, że wyłomem w kryterium proporcjonalności są opisane powyżej rozwiązania zawarte w ustawie z 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi. Chodzi m.in. o sytuację, w której Policja wnioskuje o kontrolę operacyjną w związku z „napotkanymi trudnościami” w weryfikowaniu informacji o osobie „stwarzającej zagrożenie”. Oczywiście dostrzegł to RPO, [wnosząc](#) w maju 2014 r. do Trybunału Konstytucyjnego o stwierdzenie niezgodności właściwego artykułu (art. 23 ust. 2) z ustawą zasadniczą.

² Chodzi o przestępstwa: elektronicznej korupcji seksualnej małoletniego (art. 200a), propagowania pedofilii (art. 200b), wprowadzenia w błąd instytucji użyteczności publicznej co do zagrożenia, czyli fałszywego alarmu (art. 224a), bezprawnego uzyskania informacji, czyli hackingu komputerowego (art. 267), niszczenia danych informatycznych (art. 268a), zakłócania systemu komputerowego (art. 269a), wytwarzania programów komputerowych służących do zakłócania systemu komputerowego (art. 269b), kradzieży z włamaniem (art. 279) i oszustwa komputerowego (art. 287).

Zwracał też uwagę na niepokrywanie się katalogu przestępstw ujętego w tej ustawie o postępowaniu wobec osób z zaburzeniami psychicznymi z katalogiem zawartym w ustawie o Policji (ten pierwszy jest szerszy). W listopadzie 2016 r. TK [umorzył](#) jednak postępowanie w tym zakresie, stwierdzając, że argumentacja RPO dotyczyła nie tyle zgodności przepisu ustawy z konstytucją, co była „*de facto* żądaniem przeprowadzenia kontroli horyzontalnej dwóch przepisów ustawowych”.

Kryterium **subsydiarności** (pomocniczości) zawiera się w formule: „gdy inne środki okazały się bezskuteczne albo będą nieprzydatne”. Tym samym kontrola operacyjna nie może być rozwiązaniem, po które sięga się „z automatu”, domyślnie, ale dopiero po rozważeniu i wyczerpaniu innych możliwości. Ma to zabezpieczać jednostkę przed niepotrzebnym „pójściem na skróty” przez służby.

Jest też kryterium będące syntezą proporcjonalności i subsydiarności – można nazwać je „selektywnością”.

Kontrola operacyjna powinna być możliwie jak najmniej inwazyjna – zwłaszcza w odniesieniu do osób trzecich. Podśłuchiwanie osoby X nierozzerwalnie wiąże się z inwigilowaniem jej otoczenia. Kontrola operacyjna powinna być więc zorganizowana w taki sposób, aby do niejawnego przetworzenia danych stanowiących treść doszło w jak najmniej dotkliwy dla niezwiązanych ze sprawą sposób.

Zagadnienia te rozważają sędziowie w ramach kontroli uprzedniej sprawowanej nad kontrolą operacyjną. Najpierw rozstrzygają, czy wnioskowana kontrola operacyjna posiada odpowiednią podstawę prawną. Przykładowo, jeśli Policja wnioskowałaby o zarządzenie kontroli operacyjnej w związku z kradzieżą, sąd miałby obowiązek wydać postanowienie odmowne, wskazując w uzasadnieniu, że art. 278 kk nie jest wymieniony w ustawie o Policji jako przesłanka prowadzenia kontroli operacyjnej. Inaczej byłoby w związku z rozbojem, gdyż art. 280 kk znajduje się w policyjnym katalogu.

Następnie sąd rozważa, czy spełniono przesłankę subsydiarności. W swoim wniosku właściwa instytucja bezpieczeństwa musi uzasadnić, że „inne środki okazały się bezskuteczne” lub wyjaśnić, dlaczego są „nieprzydatne”.

W trzeciej kolejności sędzia upewnia się, czy i w jakim zakresie (technicznym, czasowym) proponowane przez wnioskodawców rozwiązania narażają na szwank prywatność osób z otoczenia figuranta (i jego samego).

Sąd nie rozstrzyga zatem jedynie o tym, czy kontrola operacyjna może mieć miejsce, ale rozważa całość zagadnienia: jej cel, czas i rodzaj czynności. Każdorazowo dokonuje ważne-

nia treści wniosku z przepisami konstytucji: prawem do ochrony prywatności (art. 47), tajemnicą komunikowania się (art. 49) i prawem do autonomii informacyjnej (art. 51). W art. 51 ust. 2 ustrojodawca określił, że władze publiczne „nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym”. Punktem odniesienia jest art. 31 ust. 3 konstytucji, który określa dopuszczalne ograniczenia w korzystaniu z konstytucyjnych wolności i praw³. Ważnym punktem odniesienia jest też *Konwencja o ochronie praw człowieka i podstawowych wolności*, którą Polska ratyfikowała trzydzieści lat temu.

W sensie formalnym kontrola operacyjna poprzedzona jest więc rozbudowaną procedurą wstępną. W praktyce sądowa kontrola uprzednia ma jednak w dużej mierze wadliwy lub wręcz fasadowy charakter. Sędzia otrzymuje od właściwej instytucji krótki formularz zawierający podstawowe informacje (zob. [policyjny wzór wniosku i wzór postanowienia sądu](#)). Postanowienia nie wydaje skład orzekający – z powodu konieczności ochrony informacji niejawnych sędziowie nie mają możliwości konsultowania sprawy między sobą. Nie mogą korzystać z rady funkcjonariuszy czy posiłkować się wsparciem merytorycznym zewnętrznych ekspertów. Każde tego rodzaju działanie wiązałoby się z odpowiedzialnością karną i dyscyplinarną. Decyzja jest podejmowana jednoosobowo. Jedynym instrumentem, jakim dysponuje mający wątpliwości sędzia, jest zarządzenie posiedzenia z udziałem przedstawiciela instytucji-wnioskodawcy i właściwego prokuratora.

Aby odrzucić wniosek o kontrolę operacyjną, sędzia musi dysponować jakimś argumentem. Musi też swoją decyzję uzasadnić. Jeżeli we wniosku podana jest poprawna podstawa prawna i jeżeli znajdzie się w nim przekonujące uzasadnienie wraz z formułą o spełnieniu warunku subsydiarności, to wniosek nie może, tylko musi zostać zaakceptowany. Jeśli sędzia wykryje wadę prawną (np. wnioskodawca zamierza stosować podsłuch w związku z przestępstwem spoza „swojego” katalogu lub przy użyciu nieadekwatnego lub niepotrzebnie inwazyjnego rozwiązania technicznego), ma obowiązek zwrócić na to uwagę i wydać postanowienie odmowne. Przysługuje na nie oczywiście zażalenie, zgodnie z procedurami kpk. Służba może też poprawić wniosek i złożyć go ponownie.

Nie ma w Polsce sędziów „etatowo” zajmujących się kontrolą operacyjną. Prowadzenie kontroli uprzedniej nad kontrolą operacyjną jest po prostu jednym z obowiązków sądów. Sama tylko Policja w 2022 r. złożyła blisko 10 tys. wniosków (czyli składała średnio jeden co 53 minuty) dotyczących ponad 5,5 tys. osób. Tymczasem w 2020 roku wakaty w sądownictwie wynosiły około [10%](#). Zarzucone ogromem wniosków sądy, zwłaszcza warszawski, mogą więc wprawdzie zażądać od wnioskodawców dodatkowych materiałów i wyjaśnień,

³ Art. 31 ust. 1 ustawy zasadniczej stanowi: „Ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób. Ograniczenia te nie mogą naruszać istoty wolności i praw”.

ale nie tylko nie mają czasu, aby uczynić z tego regularną praktykę, ale przede wszystkim nie mają ku temu podstaw, jako że od strony formalnej zazwyczaj wszystko się zgadza. Nie istnieją również systemowe rozwiązania dotyczące szkoleń dla sędziów w tym zakresie. Ani studia prawnicze, ani aplikacja sędziowska nie oferują merytorycznego przygotowania dotyczącego czynności operacyjno-rozpoznawczych.

Jeśli zaś chodzi o kontrolę procesową, to zarządza ją sąd na wniosek prokuratora (wyjąwszy „wypadki niecierpiące zwłoki”). Także i ta forma kontroli dotyczy zamkniętego katalogu najpoważniejszych przestępstw, który jest ujęty w [art. 237](#) Kodeksu postępowania karnego. Instytucja kontroli i utrwalania rozmów (kontrola procesowa, podsłuch procesowy) uregulowana jest na tyle odmiennie od kontroli operacyjnej, że nie sposób uznawać ją za instytucję kontrowersyjną. Jej stosowanie jest dopuszczalne wyłącznie w stosunku do osoby podejrzanej lub oskarżonego, a także w stosunku do pokrzywdzonego lub innej osoby, z którą może się kontaktować oskarżony lub która może mieć związek ze sprawcą lub z grożącym przestępstwem. Okres prowadzenia kontroli procesowej jest ściśle ograniczony (zob. dalej), a osoba, która jest jej przedmiotem, zostaje o tym poinformowana najpóźniej z końcem postępowania. Na postanowienie dotyczące kontroli i utrwalania rozmów telefonicznych przysługuje też zażalenie. Zainteresowana osoba może domagać się w nim zbadania zasadności oraz legalności prowadzonych wobec niej czynności. Tego rodzaju gwarancje są nieobecne w odniesieniu do kontroli operacyjnej.

Zwraca uwagę chociażby brak w polskim prawie instytucji obowiązku informowania osoby o zakończeniu prowadzenia wobec niej kontroli operacyjnej (obowiązek notyfikacji), której wprowadzenia domagał się Trybunał Konstytucyjny. W styczniu 2022 r. posłowie opozycji złożyli w Sejmie [projekt ustawy](#) (EW-020-768/22) zmierzający do wprowadzenia obowiązku notyfikacji. Do momentu zamknięcia niniejszego tekstu nie nadano mu nawet numeru druku. Z pewnością nie zostanie on rozpatrzony w IX kadencji Sejmu.

1.2. „Jawna roczna informacja”

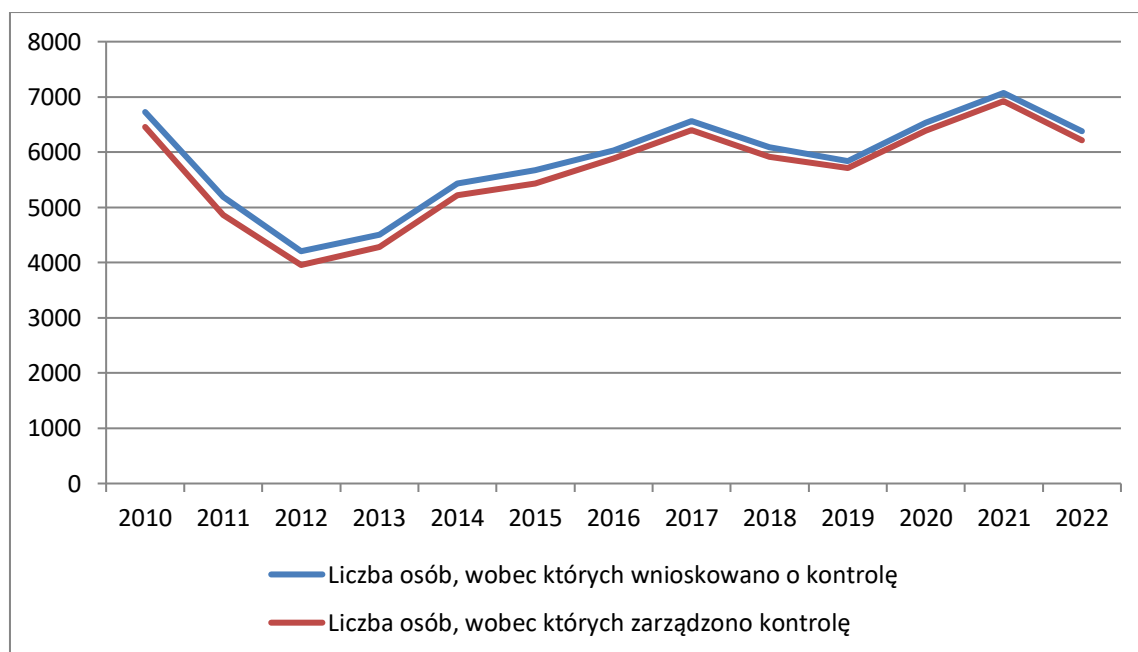
Pod koniec 2009 r., na fali kontrowersji związanych z inwigilowaniem dziennikarzy, ówczesny premier Donald Tusk stwierdził, że podsłuchy zakłada się w Polsce „zbyt łatwo”. Kilka miesięcy później do Sejmu trafił rządowy projekt nowelizacji kpk i niektórych innych ustaw ([druk z 31 marca 2010 r.](#)). Drogą tej ustawy, [przyjętej zgodnie](#) przez wszystkie siły parlamentarne, 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 obowiązującej wówczas 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 2 czerwca 2023 r. „jawna roczna informacja” obejmująca 2022 r. została opublikowana 6 czerwca. Poniższy wykres 1. przedstawia najważniejsze ujęte w niej dane, czyli liczbę osób, których dotyczyły złożone wnioski i osób objętych kontrolą, osadzone na szerszym tle historycznym.

Trzeba zaznaczyć, że w „jawnym rocznym informacjach” jest mowa o liczbie osób wskazanych we wnioskach, a nie o liczbie wniosków. Dla uproszczenia wyводу będę zatem posługiwał się akronimem OW, oznaczającym liczbę osób, których dotyczyły wnioski („osobownioski”).

Wykres. 1. Kontrola operacyjna i procesowa w latach 2010–2022 – liczba OW i osób, wobec których zarządzono kontrolę



W ostatnich kilku latach widoczny był trend wzrostowy, a w 2021 r. odnotowano rekordowy wynik w całym okresie objętym sprawozdawczością. W ubiegłym roku liczba wniosków była jednak niższa. W 2022 r. zarządzono kontrolę operacyjną lub procesową wobec 6,2 tys. osób, przy 6,9 tys. osobach w 2021 r. i 6,4 tys. w 2020 r.

Mogłoby się wydawać, że, przedstawiając sprawę obrazowo, w każdej polskiej gminie w 2022 r. znajdowały się 2,5 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 2022 r. mogły jeszcze trwać kontrole zarządzane w 2021 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 zarządzania 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 kpk 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](#).

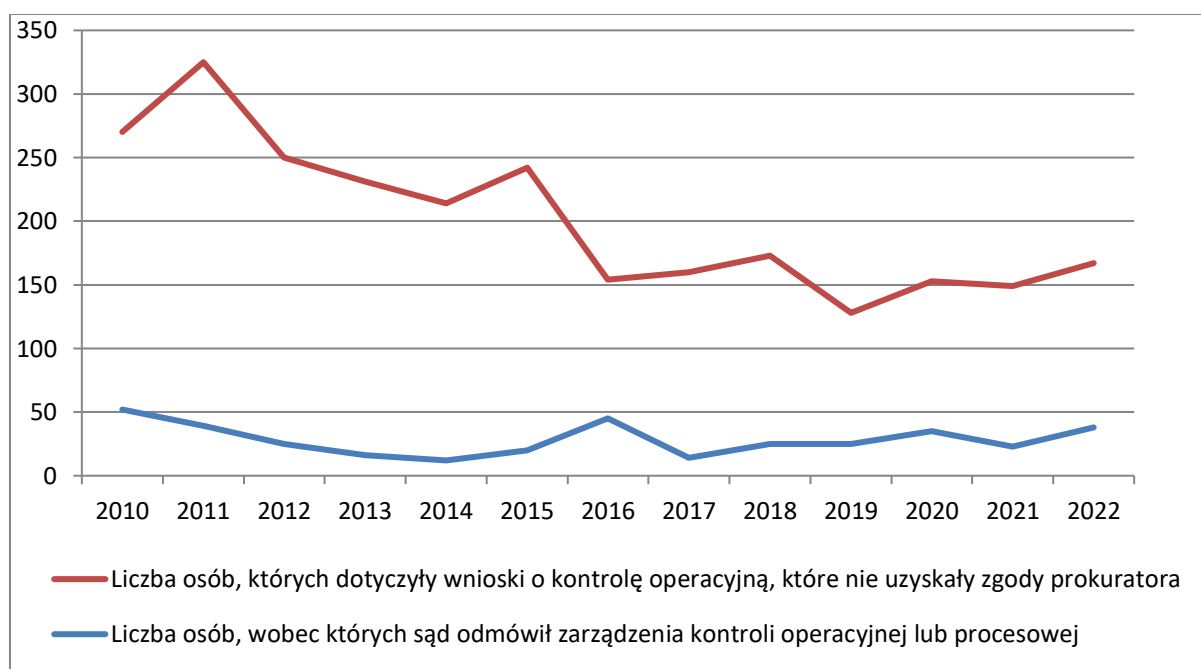
Tak więc, przykładowo, od wiosny 2021 r. mógł być prowadzony podsłuch operacyjny, zarządzony na wniosek Policji, w związku z chęcią uzyskania i utrwalenia dowodów w zakresie przestępstwa płatnej protekcji. Jeśli przyczyny zarządzania kontroli nie ustawały, a w jej trakcie pojawiły się nowe okoliczności, podsłuch mógł być stosowany na początku 2022 r., przy czym ostatnią fazę przedłużenia zarządzano jeszcze w 2021 r.

Nie wiadomo więc, jaka jest całościowa liczba 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 (poza kontrolą prowadzoną przez Policję).

Utrzymuje się również trend polegający na tym, że niemal wszystkie osoby, których dotyczy wnioski, stają się przedmiotem kontroli. Od 2016 r. wskaźnik ten przekracza 97%. Jeśli instytucje wnoszą 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 2010–2022 – liczba OW, które nie uzyskały zgody prokuratora i wobec których sędziowie wydali postanowienia odmowne.



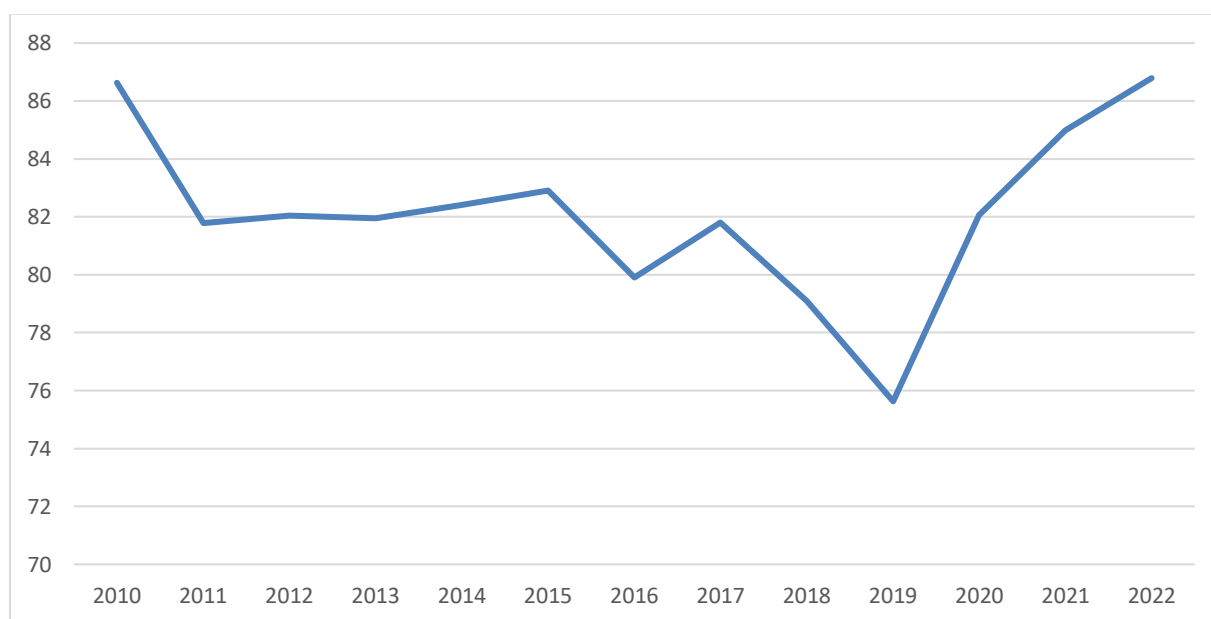
O tym, że kontrola nie zostaje zarządzona, częściej decydują prokuratorzy niż sędziowie. Nie należy jednak wyciągać z tego wniosku, że postawa sądów jest bardziej „liberalna”. Przyczyna tej dysproporcji tkwi w procedurze. Jak wspomniano, tryb ustanawiania kontroli operacyjnej jest, w odróżnieniu od kontroli procesowej, trzystopniowy – 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 niepokojącym sygnałem, świadczącym o tym, że niezawisli sędziowie muszą korygować zbyt pobłażliwe podejście prokuratury. Od 2010 r. ani razu nie zdarzyło się, aby liczba osób, w przypadku których sąd odmówił zarządzenia kontroli, przekroczyła 0,8% wszystkich OW. W 2022 r. wyniosła 0,6% (w 2021 r. – 0,3%).

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

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 4., który uszczegóławia dane dotyczące liczby osób objętych kontrolą. Poprzedza go wykres 3. obrazujący rosnący w ostatnich latach udział Policji we wszystkich OW.

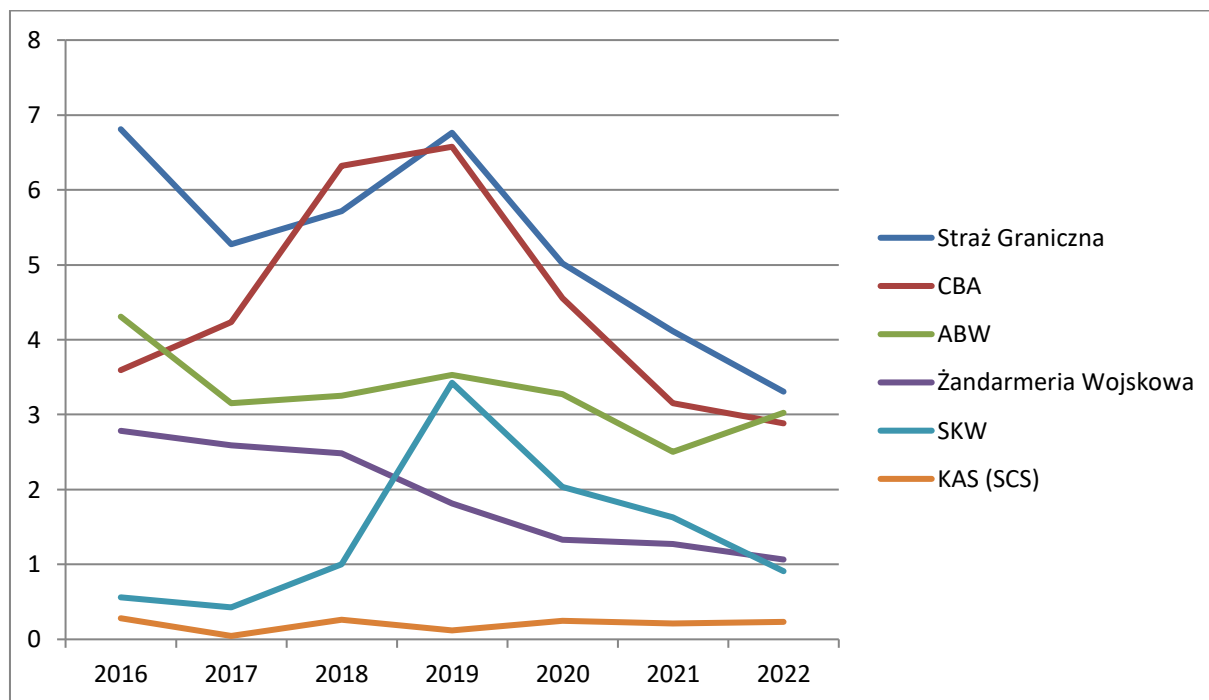
Wykres 3. Kontrola operacyjna w latach 2010–2022 – procentowy udział Policji w ogólnej liczbie OW.



W 2022 r. odnotowano rekordowy udział Policji we wszystkich OW. Pozostałe podmioty odpowiadały za zaledwie 13% (w 2021 r. – 15%). Ich procentowy udział ilustruje wykres 4.

Przepaść oddzielająca Policję, która w 2022 r. wygenerowała wnioski o kontrolę operacyjną dotyczące ponad 5,5 tys. osób, od pozostałych instytucji (w sumie 729) jest ogromna i taka z pewnością pozostanie. Decyduje o tym szeroki zakres zadań tej instytucji.

Wykres 4. Kontrola operacyjna w latach 2016–2022 – procentowy udział poszczególnych instytucji bezpieczeństwa (poza Policją) w ogólnej liczbie OW.



Przez kilka lat widoczne było zwiększające się zainteresowanie kontrolą operacyjną ze strony CBA. W 2016 r. instytucja ta wnioskowała o objęcie kontrolą 217 osób, w 2017 r. – 278, w 2018 r. – 385, a w 2019 r. – 384. W 2020 r. trend wzrostowy został zatrzymany, jako że CBA wnioskowało o kontrolę operacyjną wobec 298 osób. Kolejny spadek miał miejsce w 2021 r. (223). W 2022 r. jej wnioski dotyczyły tylko 184 osób. Tym samym CBA uplasowało się na czwartym miejscu, za Policją (wnioski dotyczące 5538 osób), SG (211) i ABW (193). Pierwsza trójka z lat 2019–2021 (Policja, SG, CBA) została tym samym zmieniona, a ABW powróciło na podium po raz pierwszy od 2016 r.

Godnymi odnotowania nieobecny na wykresie 4. są SOP i BNW, które powstały na początku 2018 r. W odróżnieniu od swojego poprzednika, Biura Ochrony Rządu, 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 (podobnie jak w latach 2018–2021). Także BNW nie skorzystało dotąd z tego uprawnienia, podobnie jak powstały niedawno IWSW.

Z niejasnych przyczyn 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. Analogiczny zabieg pozwala ustalić, jak często sądy wydają postanowienia odmowne dotyczące zarządzenia kontroli procesowej. Efekt tych obliczeń ilustruje zamieszczona poniżej tabela 2.

Tabela 2. Kontrola procesowa – liczba OW prokuratorów i ich skuteczność.

Rok	Liczba osób, o objęcie których kontrolą procesową wnioskowali prokuratorzy	Liczba osób, w przypadku których sądy wydały postanowienia odmowne	Skuteczność prokuratorских wniosków (w %)
2016	106	2	98,1
2017	162	2	98,8
2018	114	3	97,4
2019	125	3	97,6
2020	97	6	93,8
2021	151	12	92
2022	114	23	80
suma	869	51	bd.
średnio	124	7	94

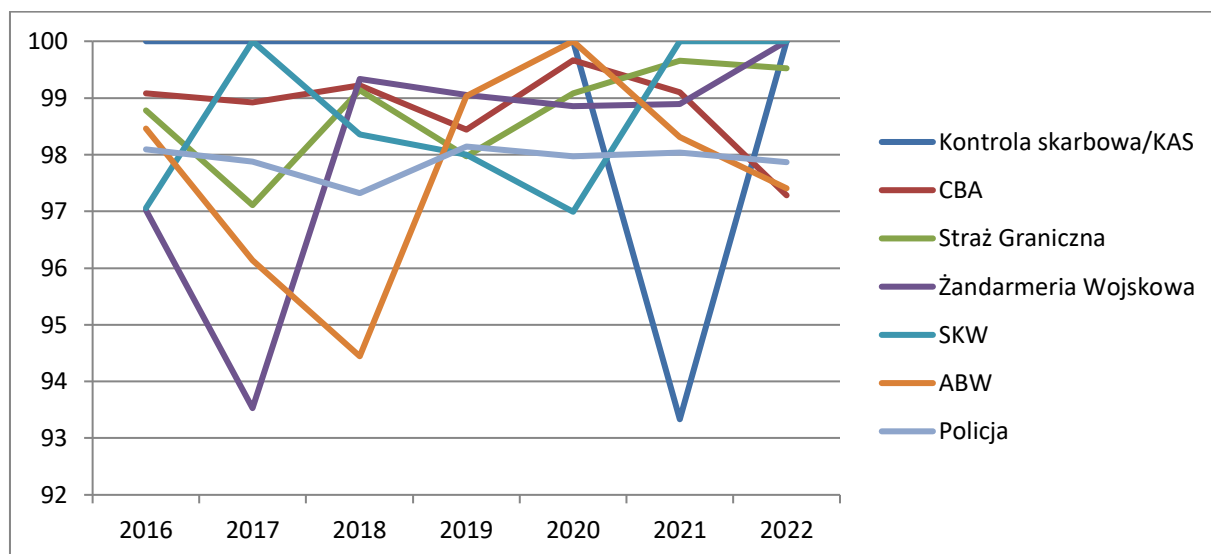
W latach 2016–2022 kontrolę procesową zarządzono wobec 869 osób. Oznacza to, że w porównaniu do kontroli operacyjnej jest zjawiskiem o marginalnej skali (pięćdziesiąt razy mniejszym). Zwraca uwagę fakt, że skuteczność prokuratorских wniosków jest coraz mniejsza, a 2022 r. był pod tym względem rekordowy.

Dwa kolejne wykresy (5. i 6.) rozwijają dane z wykresów 2.–4., wskazując, której instytucji najtrudniej było przeforsować swoje wnioski. W pierwszej kolejności przedstawiona zostanie kwestia zgody prokuratorów.

Tym, co rzuca się w oczy, jest bardzo wysoka skuteczność wniosków – prokuratorzy odrzucają zaledwie kilka procent z nich. Najgorszy wskaźnik procentowy skuteczności wniosków w 2022 r. przypadł w udziale CBA (97,3%). Na drugim miejscu uplasowała się ABW (prokuratorzy odrzucili wnioski dotyczące 2,6% osób), a na trzecim – Policja (2,1%).

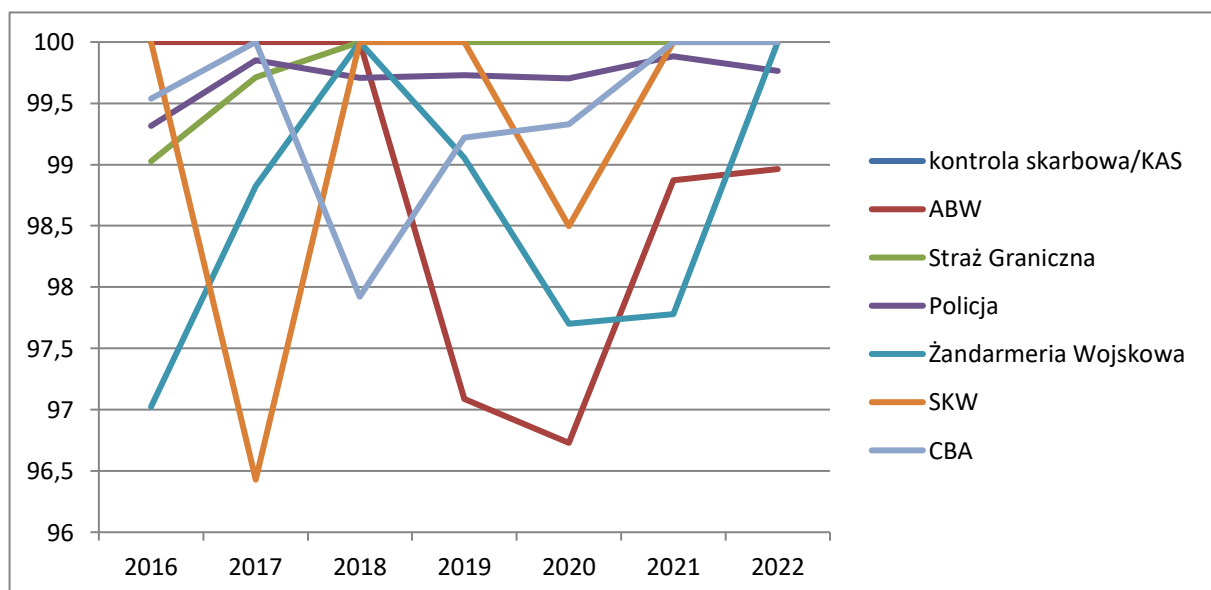
Jedyną instytucją, która może poszczycić się blisko stuprocentową skutecznością w latach 2016–2022, jest „skarbowka”. Krajowa Administracja Skarbowa została utworzona w 2017 r. w wyniku połączenia administracji podatkowej, Służby Celnej i kontroli skarbowej. Ta ostatnia mogła stosować kontrolę operacyjną i KAS, a konkretnie działająca w jej ramach SCS, przejęła tę kompetencję. W latach 2016–2022 tzw. skarbowka i KAS wnioskowały o objęcie kontrolą operacyjną 89 osób. Tylko w przypadku jednej osoby prokurator generalny zakwestionował jej wniosek (w 2021 r.).

Wykres 5. Kontrola operacyjna w latach 2016–2022 – odsetek OW, które uzyskały zgodę prokuratora w podziale na instytucje bezpieczeństwa.



Jeśli chodzi o ujęcie liczbowe, to niekwestionowanym liderem w zakresie nieuzyskanej zgody prokuratorskiej jest oczywiście Policja. W latach 2016–2022 prokuratorzy nie zgodzili się na objęcie kontrolą 762 osób wymienionych w jej wnioskach, co stanowi więcej niż sześciokrotność sumy przypadków dotyczących wszystkich pozostałych instytucji razem wziętych. Wynika to jednak z liczby policyjnych OW, która w tych latach była blisko pięć razy wyższa niż liczba OW wszystkich pozostałych instytucji. Zamieszczony poniżej wykres 6. przedstawia analogiczne dane dotyczące postanowień sądów.

Wykres 6. Kontrola operacyjna w latach 2016–2022 – odsetek OW, w przypadku których sądy wydały postanowienie o zarządzeniu kontroli operacyjnej, w podziale na instytucje bezpieczeństwa.



Statystyki wskazują, że uzyskanie pozytywnego postanowienia sądu jest właściwie formalnością, niezależnie od tego, która instytucja jest wnioskodawcą. Postanowienia odmowne

mają charakter incydentalny, a kontrola skarbową i KAS w ogóle nie zetknęły się z nimi w latach 2016–2022 (dlatego też są niewidoczne na wykresie).

W ujęciu liczbowym sądy odrzuciły oczywiście najwięcej OW Policji (103 przez ostatnie siedem lat), a w ujęciu procentowym – SKW (3,6% w 2017 r.) i ABW (3,3% w 2020 r.). W 2022 r. aż pięć z siedmiu instytucji-wnioskodawców nie spotkało się z odmową sądu: SKW, CBA, KAS, SG i ŻW. Zakwestionowano tylko wnioski Policji i ABW.

Zamieszczona poniżej tabela 3. przedstawia łączną liczbę OW w podziale na poszczególne instytucje i ich łączną skuteczność (czyli uwzględniając zarówno prokuratorów, jak i sądy).

Tabela 3. Osobownioski w latach 2016–2022 w podziale na instytucje bezpieczeństwa i ich sumaryczna skuteczność.

Instytucja	Liczba osób, których dotyczyły wnioski (% wszystkich OW)	Liczba osób, wobec których zarządzono kontrolę	Łączna skuteczność wniosków (%)
Policja	36 332 (83,2)	35 467	97,6
Straż Graniczna	2330 (5,3)	2295	98,5
CBA	1969 (4,5)	1938	98,4
ABW	1455 (3,3)	1405	96,5
Żandarmeria Wojskowa	840 (1,9)	808	96,2
SKW	629 (1,4)	616	97,9
kontrola skarbową/ KAS	89 (0,2)	88	98,9
suma	43 644	42 617	b.d.

Całościowa skuteczność wniosków w latach 2016–2022 wynosi 97,6%.

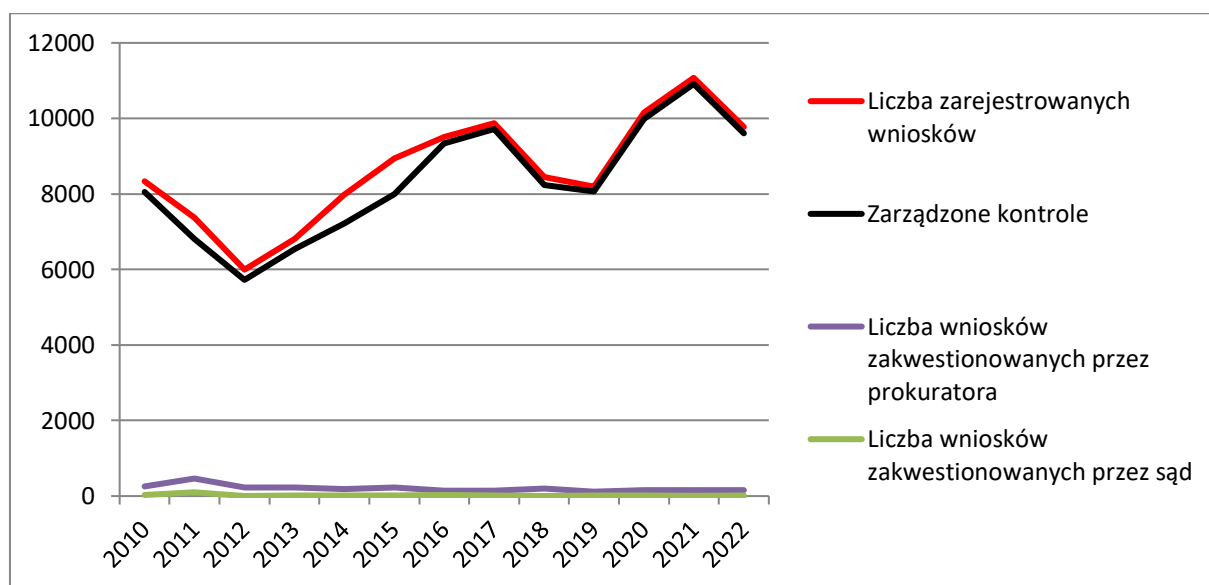
Trzeba zauważyć, że udział służb specjalnych w kontroli operacyjnej jest niewielki. Przez ostatnich siedem lat wnioskowały o objęcie kontrolą operacyjną 4053 osób (9,3%), zaś za pozostałe przypadki odpowiadają służby policyjne.

1.3. Informacja ministra spraw wewnętrznych i administracji

Dysponujemy też drugim typem materiałów źródłowych dotyczących kontroli operacyjnej. On również został wprowadzony w 2011 r. – drogą nowelizacji ustawy o Policji. Minister właściwy do spraw wewnętrznych został zobowiązany przedstawiać corocznie (do 30 czerwca) parlamentowi informację o kontroli operacyjnej prowadzonej przez Policję. W 2018 r. obowiązek ten rozbudowano o dwie nowe instytucje podległe ministrowi: SOP

i BNW, przy czym – jak wspomniano – obie instytucje nie skorzystały dotąd z tych uprawnień. Warto dodać, że podobna sprawozdawczość nie była i nie jest prowadzona w odniesieniu do innej instytucji podległej MSWiA – SG. Z datowanym na 30 czerwca 2023 r. dokumentem opinia publiczna mogła się zapoznać 5 lipca.

Wykres 7. Wnioski Policji o zastosowanie kontroli operacyjnej (zarejestrowane, zarządzane i zakwestionowane) w latach 2010–2022.



Dane te nie pokrywają się z wykresem 1. z oczywistego powodu – obejmuje on liczbę osób, których dotyczyły wnioski (OW), tutaj jest zaś mowa o liczbie wniosków. Katedra Bezpieczeństwa Narodowego UJ wielokrotnie zwracała uwagę, że ta różnica w raportowaniu jest nonsensowna – wprowadza niepotrzebne zamieszanie i wzbudza obawy opinii publicznej. Głos w tej sprawie zabierali też parlamentarzyści. Wreszcie dostrzegł to prawodawca, wprowadzając 8 lipca 2022 r. [nowy sposób](#) raportowania kontroli operacyjnej. Sekretarz stanu w MSWiA Maciej Wąsik [wyjaśniał](#) we wrześniu 2022 r. na posiedzeniu Komisji Administracji i Spraw Wewnętrznych: „Wprowadzono narzędzie umożliwiające Policji przedstawianie z ogólnej liczby zarejestrowanych wniosków i zarządzeń o zastosowaniu kontroli operacyjnej liczby wniosków i zarządzeń dotyczących osób, co umożliwi w praktyce porównanie przedstawionych przez Policję danych z danymi prokuratury”. Rozporządzenie weszło w życie latem 2022 r., dlatego sprawozdawczość za 2021 r. została przedstawiona jeszcze w starym trybie. Nowe ujęcie zaprezentowano w dokumencie z 2023 r. obejmującym 2022 r.

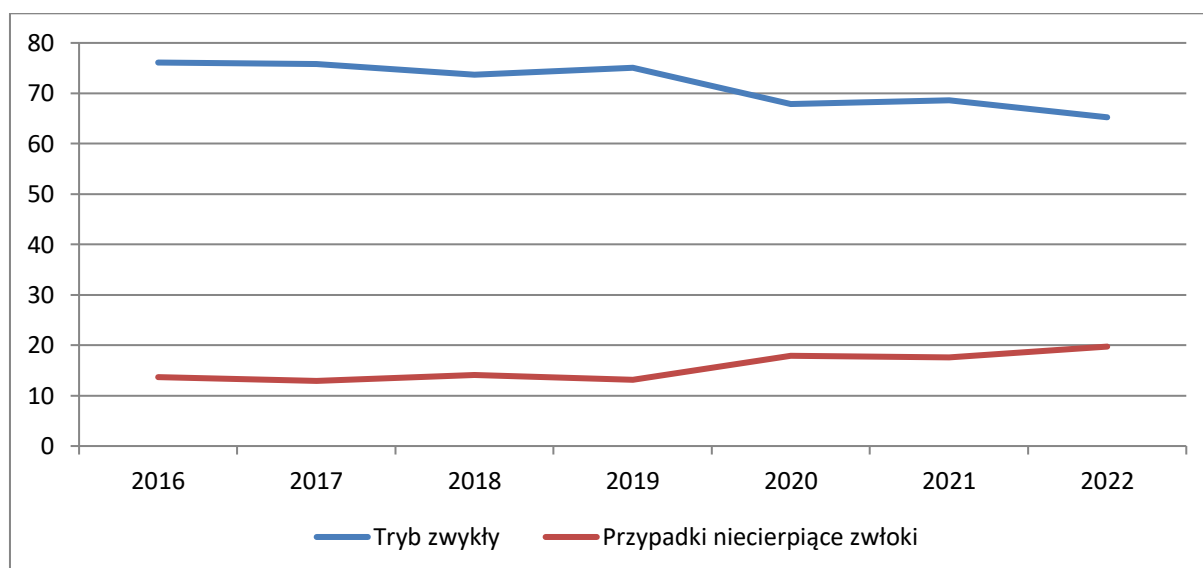
W 2022 r. Policja wnioskowała o objęcie kontrolą 5538 osób, złożyła zaś 9781 wniosków. Liczba wniosków obejmuje wnioski o przedłużenia (choć nie zawsze – zob. dalej). Poza tym przyczyną tej dysproporcji jest typ i przedmiot kontroli (np. odrębne wnioski dotyczące różnych numerów telefonów tej samej osoby).

Kolejny wykres dotyczy wspomnianego wcześniej trybu specjalnego zarządzania kontroli, dotyczącego przypadków „niecierpiących zwłoki”. Najczytelniej byłoby przedstawić go w ujęciu procentowym, ale jest to utrudnione z uwagi na różnice w raportowaniu. Można domyślać się, że w latach 2010–2011 i 2014–2015 nie zaliczono przedłużeń do ogólnej sumy zarządzeń. Przykładowo, w 2010 r. zarządzono 8053 kontrole, w tym 6312 w trybie zwykłym i 1741 w trybie specjalnym ($6312 + 1741 = 8053$). Tymczasem informacja ministra wspomina jeszcze o 565 przedłużeniach. Należy więc sądzić, że właściwszą liczbą przedstawiającą kontrole zarządzane w 2010 r. jest 8618, ponieważ każde przedłużenie kontroli jest zarządzeniem kontroli.

Natomiast w 2021 r. odnotowano 9612 zarządzeń, w tym 6271 w trybie zwykłym i 1897 w trybie specjalnym. Po odjęciu ich sumy od ogólnej liczby zarządzeń otrzymujemy 1444, czyli wskazaną w informacji liczbę przedłużeń.

Wydaje się być to czytelne, nie chciałem jednak opierać się na przypuszczeniu, stąd kolejny wykres obejmuje jedynie lata 2016–2022, w których raportowano przedłużenia w ten sam sposób.

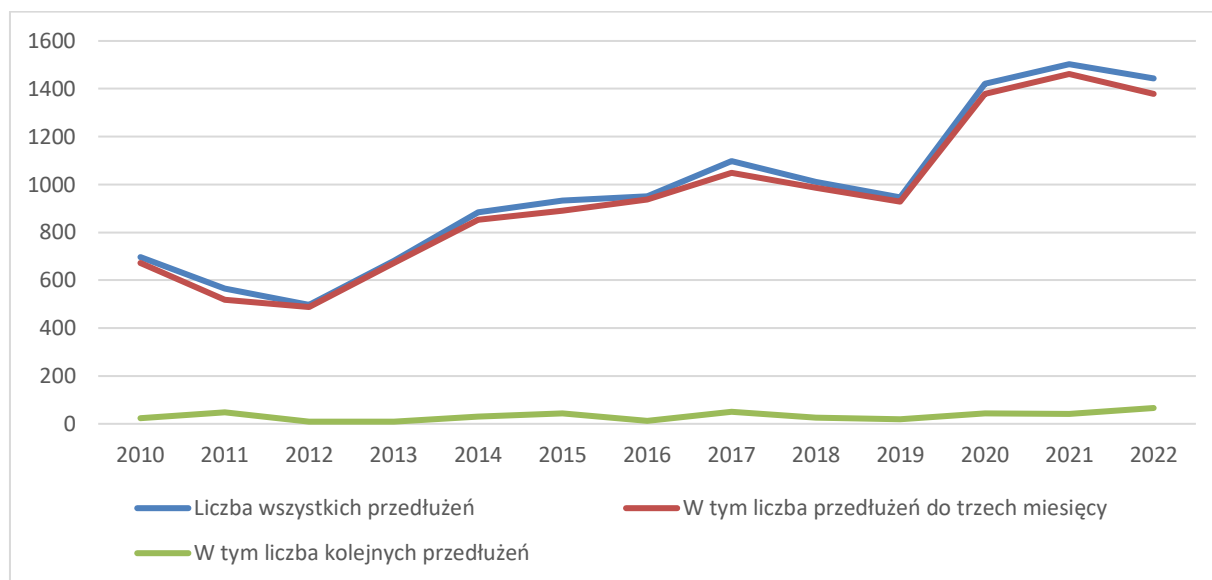
Wykres 8. Zarządzona kontrola operacyjna, o którą w latach 2016–2022 wnioskowała Policja, w podziale na tryb (w %).



W przypadku Policji zdecydowanie dominuje tryb zwykły. Tryb specjalny obejmuje średnio 15% wszystkich przypadków, przy czym w ostatnich dwóch latach był rekordowo wysoki (18–19%).

Jak wspomniano, minister przedstawia także informacje dotyczące liczby przedłużeń kontroli operacyjnej, o które wnioskowała Policja.

**Wykres 9. Zarządzone przedłużenia kontroli operacyjnej, o które w latach 2010–2022 wniosko-
wała Policja (suma i okresy przedłużeń).**



Trend wzrostowy jeśli chodzi o liczbę krótkich, „domyślnych” przedłużeń został więc zatrzymany, odnotowano natomiast rekordowy poziom „kolejnych przedłużeń”. W ogromnej większości przypadków Policja ogranicza się do kontroli trwającej do pół roku (czyli maksymalnie trzy miesiące kontroli plus przedłużenie trwające maksymalnie trzy miesiące). W 2022 r. doszło do 66 wykraczających poza tę granicę przedłużeń będących konsekwencją wniosków Policji.

Dysponujemy również danymi dotyczącymi typów przestępstw, w związku z którymi zarejestrowano policyjne wnioski. Obejmują one jedynie lata 2016–2022. Z uwagi na szeroką rozpiętość danych ich przedstawienie w formie wykresu nie jest możliwe. Trzeba jednak zaznaczyć, że dominują przestępstwa przeciwko porządkowi publicznemu⁴ (2016 – 1018, 2017 – 6915, 2018 – 5473, 2019 – 5704, 2020 – 7179, 2021 – 7 676, 2022 – 6 340), dystansując przestępstwa przeciwko mieniu⁵ (2016 – 1684, 2017 – 1746, 2018 – 1283, 2019 – 980, 2020 – 481, 2021 – 1322, 2022 – 1 698). Pozostałe typy obejmują średnio kilkaset (np. przestępczość gospodarcza, przestępstwa przeciwko życiu i zdrowiu, przestępstwa przeciwko działalności instytucji państwowych oraz samorządu terytorialnego), kilkadziesiąt (przestępstwa przeciwko obrotowi pieniędzmi i papierami wartościowymi) lub kilka przypadków (przestępstwa przeciwko wymiarowi sprawiedliwości, przeciwko Rzeczypospolitej Polskiej, przeciwko wolności seksualnej) w skali roku.

⁴ Spośród nich (art. 252–264a kk) do tzw. przestępstw katalogowych Policji należą: branie zakładnika (art. 252 kk) oraz branie udziału w zorganizowanej grupie i związku przestępczym (art. 258 kk).

⁵ Spośród nich (278–295 kk) do tzw. przestępstw katalogowych Policji należą: kradzież z włamaniem (art. 279 kk), rozbój (art. 280 kk,) kradzież rozbójnicza (art. 281 kk), wymuszenie rozbójnicze (art. 282 kk), podłączenie się do cudzego aparatu telefonicznego (art. 285 kk), oszustwo (art. 286 kk) i oszustwo komputerowe (art. 287 kk).

Oddzielnie należy odnotować ogromny wzrost zarejestrowanych wniosków związanych z przestępczością narkotykową⁶. Po raz pierwszy wyodrębniono ją w informacji za 2016 r. (4549 przypadków, pierwsze miejsce). W dokumentach za lata 2017–2018 była nieobecna, w informacji za 2019 r. powróciła (228 przypadków, szóste miejsce), w 2020 r. pobito w tym względzie rekord (6022 przypadki, drugie miejsce), w 2021 r. odnotowano 1269 takich przypadków (trzecie miejsce), a w 2022 r. – 998 (również trzecie).

2. Przetwarzanie danych telekomunikacyjnych, pocztowych i internetowych

2.1. Najważniejsze pojęcia, podstawa prawna i procedura

Drugim rodzajem danych przetwarzanych przez polskie instytucje bezpieczeństwa są dane niestanowiące treści: telekomunikacyjne, pocztowe i internetowe. Pozyskiwane są przede wszystkim następujące rodzaje danych:

a) w kategorii danych telekomunikacyjnych:

- raporty połączeń, czyli tzw. dane billingowe – dla numeru telefonu, dla numeru IMEI (unikalny numer każdego urządzenia) i dla stacji bazowej (BTS),
- lokalizacje stacji abonenckich – określenie bieżącego położenia telefonu (geolokalizacja),
- dane użytkowników – ustalenie danych osoby w oparciu o numer telefonu lub ustalenie numeru telefonu danej osoby,

b) w kategorii danych internetowych:

- raporty połączeń – np. odwiedzane strony internetowe,
- dane użytkowników – ustalanie danych osobowo-adresowych dla danego numeru IP lub adresu mailowego czy ustalenie usługi internetowej w oparciu o adres czy numery PESEL, NIP i REGON,

c) kategorii danych pocztowych:

- dane o użytkownikach i usługach – np. dane osobowo-adresowe odbiorców i nadawców.

Zgodnie z ustawą Prawo telekomunikacyjne z 2004 r., operatorzy publicznych sieci telekomunikacyjnych i dostawcy publicznie dostępnych usług telekomunikacyjnych mają obowiązek prowadzić retencję danych. Nazywamy w ten sposób zatrzymywanie przez operatorów-usługodawców informacji o aktywności usługobiorców. Firmy oferujące tego rodzaju

⁶ W art. 19 ust. 1 pkt 5 ustawy o Policji prawodawca dodał do tzw. przestępstw katalogowych Policji przestępstwa: „nielegalnego wytwarzania, posiadania lub obrotu bronią, amunicją, materiałami wybuchowymi, środkami odurzającymi, substancjami psychotropowymi, ich prekursorami lub nowymi substancjami psychoaktywnymi oraz materiałami jądrowymi i promieniotwórczymi”. Przestępczością narkotykową określają przepisy karne zawarte w Ustawie o przeciwdziałaniu narkomanii z 29 lipca 2005 r.

usługi, np. operatorzy telefonii komórkowej, są zobowiązane przez rok⁷ przechowywać informacje o aktywności swoich klientów, np. o wybieranych numerach. Jest to czynność rutynowa i dotyczy aktywności każdego użytkownika. Dostawcy usług internetowych i pocztowych przechowują tego rodzaju dane przez okres, który jest im potrzebny do świadczenia usługi.

W związku z przyjęciem w 2018 r. dyrektywy UE ustanawiającej Europejski Kodeks Łączności Elektronicznej (2018/1972) pojawiła się konieczność transponowania jej przepisów do prawa krajowego państw członkowskich. Deadline ustalono na koniec grudnia 2020 r. Polska do dzisiaj nie wywiązała się z tego obowiązku, dopiero w grudniu 2022 r. przedkładał stosowny [projekt ustawy](#). Prawo telekomunikacyjne miało zostać zastąpione przez Prawo komunikacji elektronicznej. W kwietniu 2023 r. projekt został wycofany, co oznacza, że transpozycja nastąpi najwcześniej zimą 2023/2024. W świetle wycofanego projektu obowiązek retencji miał zostać znacząco poszerzony. W projekcie postępowano się określeniem „przedsiębiorca komunikacji elektronicznej”, które obejmowało nie tylko przedsiębiorstwa telekomunikacyjne, ale także podmioty świadczące „publicznie dostępną usługę komunikacji interpersonalnej niewykorzystującą numerów”, a zatem dostawców usług poczty elektronicznej, komunikatorów internetowych czy czatów. Pojawia się więc pytanie, w jaki sposób Polska miałaby egzekwować wywiązywanie się z tego obowiązku przez podmioty zagraniczne, np. amerykańskie *technology companies*. Prędzej czy później sprawa implementacji dyrektywy 2018/1972 wróci pod obrady Sejmu, a wraz z nią powrócą kontrowersje dotyczące skali i okresu retencji danych internetowych.

Przetwarzanie danych niestanowiących treści także odbywa się w dwóch trybach: procesowym i pozaprocesowym, czyli w ramach czynności operacyjno-rozpoznawczych.

W uprawnienie wyposażono te same instytucje, o których była mowa wcześniej – służby policyjne i specjalne oraz SOP, BNW i IWSW. Różnica polega na tym, że, w odróżnieniu od kontroli operacyjnej, AW i SWW nie muszą w tym zakresie sięgać po pośrednictwo ABW lub SKW. Tym samym aż 12 podmiotów wyposażono w Polsce w prawo do operacyjnego przetwarzania danych niestanowiących treści. Regulują to przepisy ustaw kompetencyjnych, a uszczegóławiają przepisy wewnętrzne (np. [zarządzenie](#) komendanta głównego Policji z marca 2022 r.).

⁷ Tak zwana dyrektywa retencyjna UE z 2006 r. (2006/24/WE) zobowiązała państwa członkowskie do wprowadzenia w obszarze telekomunikacyjnym retencji danych w okresie od 6 do 24 miesięcy. W 2009 r. Polska, jako jedno z nielicznych państw członkowskich, zdecydowała się na wprowadzenie maksymalnego okresu dwóch lat. Już w 2012 r. skrócono go do 12 miesięcy, argumentując, że „największe znaczenie i wartość mają dane pochodzące z ostatniego roku” i wskazując, że dwuletni okres retencji wiąże się z ogromnymi kosztami dla operatorów. Warto zaznaczyć, że w 2014 r. Trybunał Sprawiedliwości UE stwierdził nieważność tzw. dyrektywy retencyjnej, uznając ją za rozwiązanie zbyt inwazyjne.

Operacyjne przetwarzanie danych telekomunikacyjnych, internetowych i pocztowych różni się od kontroli operacyjnej w kilku ważnych aspektach, które sprawiają, że jest rozwiązaniem zdecydowanie powszechniejszym. Po pierwsze, nie jest ono objęte klauzulą subsydiarności. Uprawnione instytucje mogą więc sięgać po dane tego rodzaju nie tylko wtedy, gdy „inne środki okazały się bezskuteczne albo będą nieprzydatne”, ale zawsze wtedy, kiedy uznają to za stosowne – w granicach swoich właściwości. Obejmują one działanie w celu:

- „zapobiegania lub wykrywania przestępstw, przestępstw skarbowych albo w celu ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych” (Policja),
- „zapobiegania lub wykrywania przestępstw oraz przestępstw skarbowych” (SG),
- „realizacji zadań” (ABW, SKW, CBA),
- „zapobiegania lub wykrywania przestępstw, w tym przestępstw skarbowych”, albo w celu „ratowania życia lub zdrowia ludzkiego bądź wsparcia działań poszukiwawczych lub ratowniczych” (ŻW),
- „zapobiegania przestępstwom skarbowym” i przestępstwom lub wykrywania tych przestępstw oraz wykonania zadań związanych z „ujawnianiem i odzyskiwaniem mienia zagrożonego przypadkiem” (SCS),
- „rozpoznania, zapobiegania i wykrywania przestępstw” (SOP),
- „zapobiegania lub wykrywania przestępstw” (BNW),
- „rozpoznawania i wykrywania przestępstw oraz zapobiegania im” (IWSW).

O celu przetwarzania danych niestanowiących treści przez AW i SWW ustawodawca nie wspomina.

Sformułowania te są bardzo ogólne, a brak klauzuli subsydiarności jest krytykowany jako pole do potencjalnych nadużyć. Przykładowo, Rzecznik Praw Obywatelskich [wskazywał w 2021 r.](#), że użyte przez ustawodawcę sformułowania nie spełniają wymogu jasności przepisów. Oględnie ujęty cel przetwarzania danych może oznaczać „brak selektywności już na etapie rozpoczęcia pozyskiwania (...), czyli możliwości uzyskiwania przez służby danych w postępowaniach w sprawie bliżej nieokreślonych czynów zabronionych, bez względu na ich szkodliwość społeczną”. Z kolei brak subsydiarności otwiera możliwość wykorzystywania danych „nie tylko wówczas, gdy jest to rzeczywiście konieczne do wykrywania lub zapobiegania przestępstwom, ale także wtedy, gdy jest to po prostu najprostsze i najwygodniejsze”.

Po drugie, tak jak w przypadku kontroli operacyjnej, przedsiębiorca telekomunikacyjny, operator pocztowy i usługodawca świadczący usługi drogą elektroniczną muszą nieodpłatnie udostępnić dane niestanowiące treści właściwej instytucji bezpieczeństwa. Przetwarzanie danych niestanowiących treści może jednak odbywać się bez udziału firmy oferującej daną usługę. Instytucje bezpieczeństwa nie muszą każdorazowo zwracać się z wnioskami

do dostawców usług internetowych, przedsiębiorców telekomunikacyjnych i operatorów pocztowych z wnioskami o udostępnienie danych dotyczących aktywności danego użytkownika. Mogą przetwarzać je we własnym zakresie, przy pomocy stałego, bezpiecznego połączenia. Warunkiem jest zawarcie porozumienia z daną firmą-operatorzem.

Po trzecie, w odróżnieniu od kontroli operacyjnej, operacyjne przetwarzanie danych nie-
stanowiących treści 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 przetworzonych 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 14 lipca 2023 r. „zagregowana informacja” obejmująca rok ubiegły została opublikowana 21 lipca.

Trzeba zaznaczyć, że powyższy punkt nie odnosi się do danych abonenckich, czyli podstawowych informacji dotyczących np. imienia i nazwiska oraz adresu abonenta, do którego należy numer telefonu. Przetwarzanie tego rodzaju 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.

W trybie procesowym uprawnienie przetwarzania danych telekomunikacyjnych, internetowych i pocztowych przysługuje prokuratorom (na etapie postępowania przygotowawczego) i sądom (na etapie postępowania sądowego). Umocowano je w [art. 218 kpk](#), poświęconym obowiązkowi wydania korespondencji, przesyłek i danych. Artykuł ten stanowi, że właściwe podmioty 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.

Przetwarzanie danych w trybie procesowym jest zwolnione z następczej formy kontroli. Nie jest też w tym zakresie prowadzona sprawozdawczość. Kierowane do operatorów prokuratorskie postanowienia o wydanie danych są prozą dnia codziennego. Od spraw drobnych, takich jak oszustwa internetowe, do tych dotyczących najpoważniejszych prze-

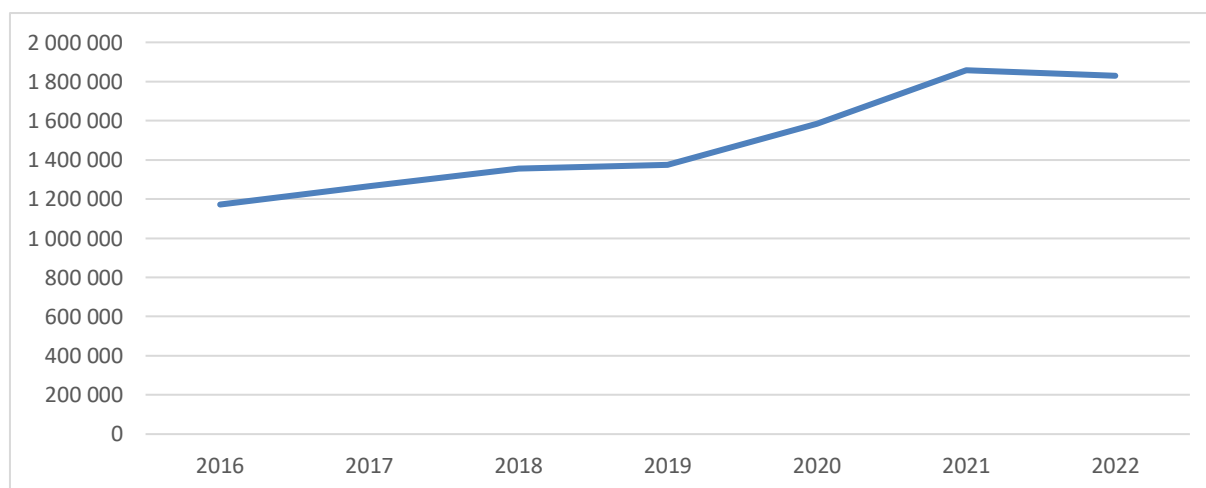
stępstw skończywszy, żądanie udostępnienia danych, takich jak dane osobowe użytkowników, wykaz połączeń czy miejsca logowania, jest standardową praktyką. Osoby, których dane przetworzono w tym trybie, są o tym informowane. Może to zostać odroczone na okres „niezbędny ze względu na dobro sprawy”, ale informacja musi trafić do nich do czasu zakończenia postępowania. Specyfika tej formy przetwarzania danych jest na tyle odmienna od trybu operacyjno-rozpoznawczego, że – tak jak kontrola procesowa – nie powinna być traktowana jako inwigilacja.

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

„Zagregowane informacje” to dwu- lub trzystronicowe, 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.

Z roku na rok rośnie liczba danych niestanowiących treści przetworzonych w trybie czynności operacyjno-rozpoznawczych. Ilustruje to wykres 10.

Wykres 10. Liczba danych niestanowiących treści przetworzonych w trybie czynności operacyjno-rozpoznawczych w latach 2016–2022.



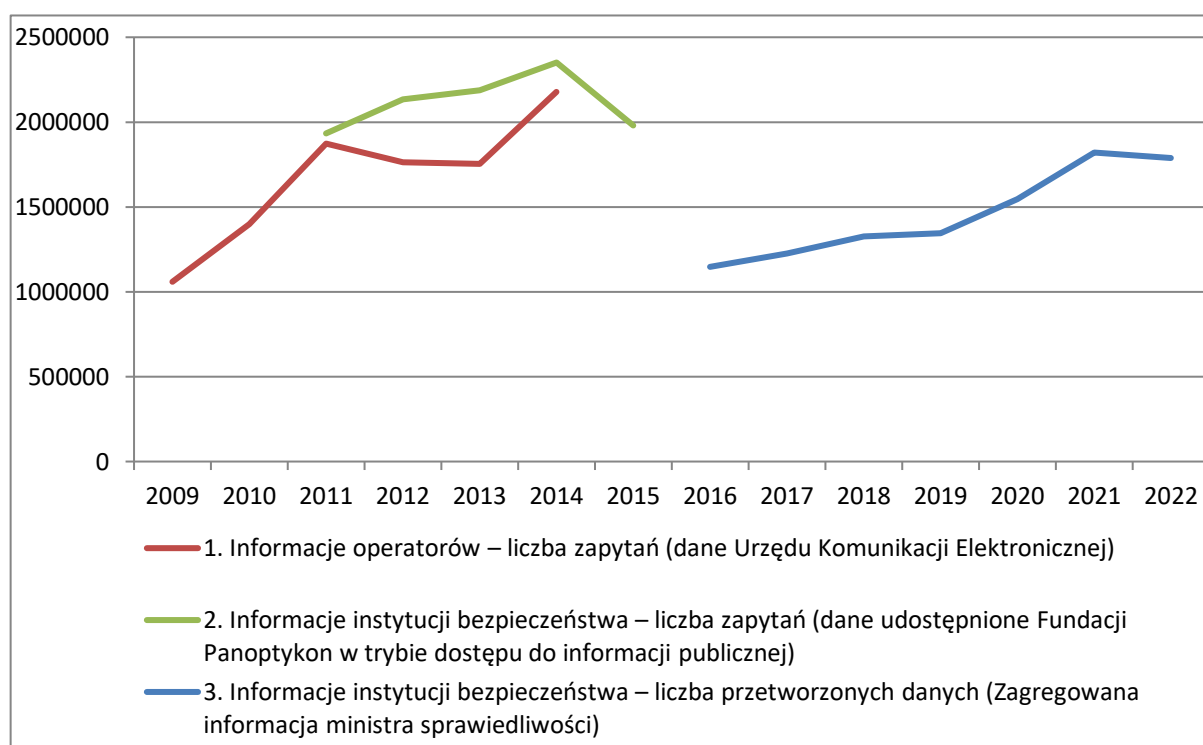
Zdecydowana większość (97,7%) danych przetworzonych w latach 2016–2022 to dane telekomunikacyjne. Dane internetowe stanowią 1,5%, a pocztowe – 0,8%. Nie wiadomo, jaka część z nich to dane przetworzone za pośrednictwem usługodawców, a jaką instytucje bezpieczeństwa przetworzyły przy użyciu stałych łącz.

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 wnioski 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 11. przedstawia przetworzone w latach 2016–2022 dane telekomunikacyjne. Umieszczono je na szerszym, choć nieco kłopotliwym tle porównawczym. Wymaga to kilku zdań wyjaśnienia.

Wykres 11. Dane telekomunikacyjne w latach 2009–2022 – liczba zapytań i przetworzonych danych.



Historyczne dane porównawcze są dostępne dzięki nieprowadzonej 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 przetwarzania danych pochodzących z retencji.

Wykres 11. przedstawia informacje dotyczące danych telekomunikacyjnych zebrane przez UKE i Fundację Panoptykon oraz przedstawione parlamentowi przez ministra sprawiedliwości w ramach „zagregowanej informacji” z lat 2016–2022.

Trzeba zauważyć, że dane UKE (seria 1 na wykresie) uwzględniają zapytania wszystkich uprawnionych instytucji, w tym sądów i prokuratorów (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”.

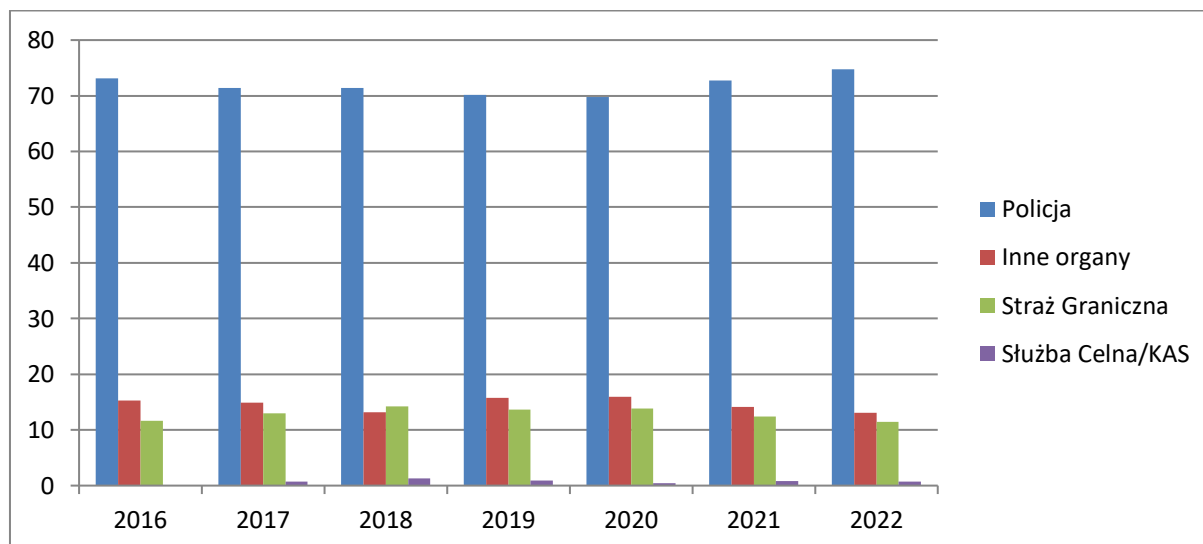
Porównując informacje przedstawione w seriach 2 i 3 można zauważyć, że w 2016 r. liczba przetworzonych danych telekomunikacyjnych spadła o 40% w porównaniu do roku poprzedniego. Wytłumaczenie tego faktu jest proste – „zagregowana informacja” ministra sprawiedliwości nie uwzględnia danych abonenckich. Dzięki analizom Fundacji Panoptykon wiadomo, że składały się one na około 35–45% wszystkich zapytań służb, co tłumaczy dystans dzielący serie 2. i 3.

W latach 2016–2021 r. każdy kolejny rok przynosił rekordową liczbę przetworzonych danych telekomunikacyjnych. Trend ten został zatrzymany w 2022 r. W 2020 r. przetworzono ponad 1,5 mln danych telekomunikacyjnych, w 2021 r. – ponad 1,8 mln, a w 2022 r. – niecałe 1,8 mln.

Kolejny wykres przedstawia przetwarzane w latach 2016–2022 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.

W 2022 r. Policja przetworzyła ponad 1,3 mln danych telekomunikacyjnych (75%, rekordowy wynik). Nie wiadomo, jakiego rodzaju były to dane – jaką ich część stanowiły billingi, a jaką dane geolokalizacyjne. Jest to regres – 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%. Nie wiadomo, dlaczego w latach 2018–2022 zrezygnowano z publikowania tego podziału.

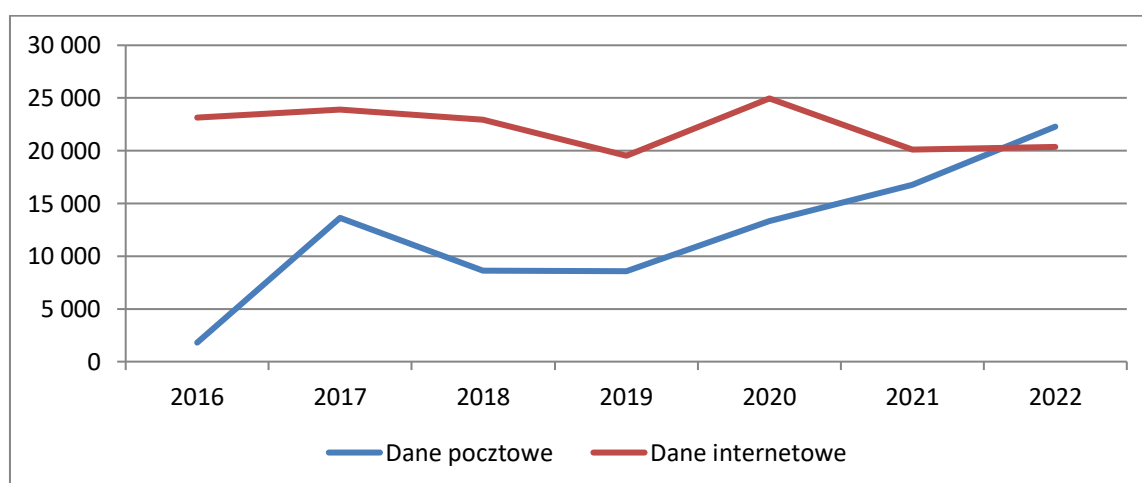
Wykres 12. Dane telekomunikacyjne w latach 2016–2022 – procent przetworzonych danych w podziale na instytucje bezpieczeństwa.



Nie zmienia się to, że nie wiadomo, ilu osób dotyczyły przetworzone dane telekomunikacyjne, ani jaki był powód ich przetwarzania.

Kolejny wykres (13.) przedstawia dane internetowe i pocztowe. W tym przypadku przedstawienie szerszego tła porównawczego nie jest możliwe, ograniczyłem się więc do podania informacji dotyczących lat 2016–2022.

Wykres 13. Dane internetowe i pocztowe w latach 2016–2022 – liczba przetworzonych danych.



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

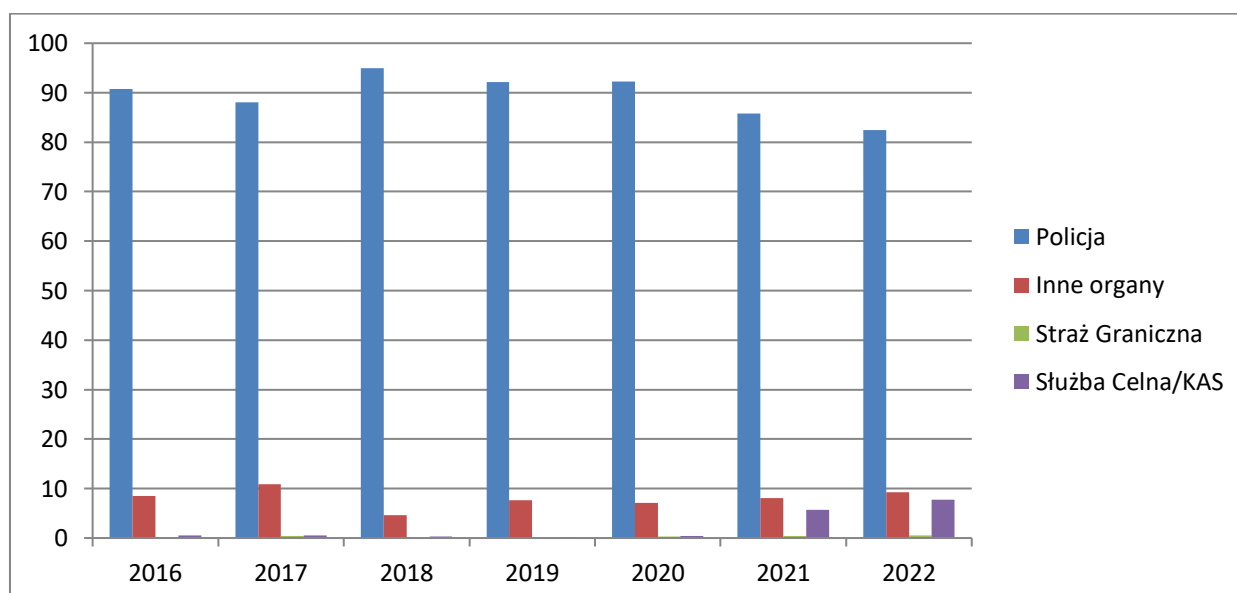
Liczby te budzą wiele wątpliwości, nie wiadomo np., dlaczego w 2017 r. liczba przetworzonych danych pocztowych wzrosła o 650% (z 1,8 tys. do 13,6 tys.), by w roku 2018 r. zmniejszyć się o jedną trzecią (8,6 tys.). W 2020 r. liczba przetworzonych danych pocztowych i internetowych wyraźnie wzrosła, odpowiednio o 54 i 28%. Natomiast w 2022 r. odnotowano dalszy wzrost przetwarzanych danych pocztowych (o około jedną trzecią) i status quo w odniesieniu do danych internetowych.

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, sekretarz 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 przyjmujemy dane Fundacji) lub trzykrotny (jeśli punktem odniesienia będą dane przekazane przez Wąsika) spadek, który trudno wyjaśnić.

Tak niewielka skala przetwarzania danych internetowych może budzić zdziwienie, zwłaszcza wobec faktu, że liczba użytkowników internetu w Polsce wciąż rośnie: w 2010 r. po raz pierwszy przekroczyła 60%, w 2017 r. wykroczyła poza barierę 70%, a w 2021 r. wynosiła ponad 85%. Wynika to ze wspomnianego braku prawnego obowiązku retencji w zakresie komunikacji internetowej. Należy zakładać, że jego wprowadzenie przyniosłoby raptowny zwiększenie liczby przetwarzanych danych internetowych.

Kolejne dwa wykresy (14. i 15.) przedstawiają dane internetowe i pocztowe w podziale na instytucje, analogicznie do wykresu 12.

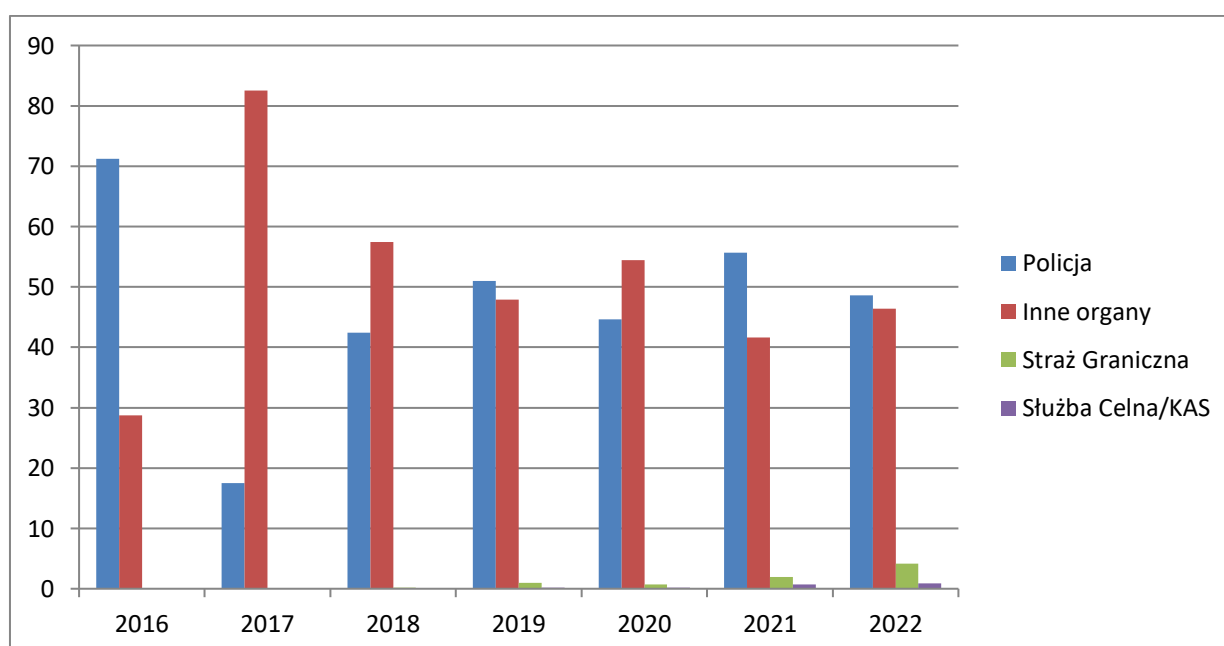
Wykres 14. Dane internetowe w latach 2016–2022 – procent przetworzonych danych w podziale na instytucje bezpieczeństwa.



Niekwestionowanym liderem w zakresie przetwarzania danych internetowych pozostaje Policja. W 2022 r. przetworzyła blisko 17 tys. spośród ponad 20 tys. danych (82%). Drugie i trzecie miejsce zajmowały i nadal zajmują – odpowiednio – „inne organy” i Służba Celna/KAS. Ta ostatnia była w poprzednich latach niemal niewidoczna na wykresie, przetwarzając średnio około 90 danych rocznie. W 2022 r. przetworzyła natomiast 1586 danych, czyli niemal tyle, ile w sześciu poprzednich latach łącznie.

Inaczej wyglądają dane dotyczące danych pocztowych. W latach 2017–2018 i w 2020 r. przewagę miały „inne organy”. Policja dominowała natomiast w 2016, 2019, 2021 i 2022 r.

Wykres 15. Dane pocztowe w latach 2016–2022 – odsetek przetworzonych danych w podziale na instytucje bezpieczeństwa.

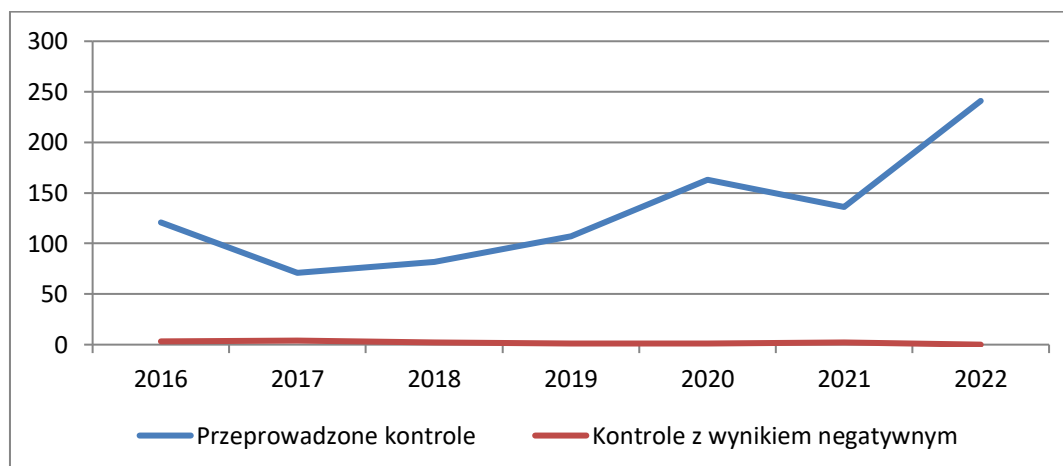


Policja przetworzyła w 2022 r. 10,8 tys. danych pocztowych (49%), „inne organy” – 10,3 tys. (46%), a niemal niewidoczna na wykresie SG – 936 (4%). Czwarty raz z rzędu dane pocztowe przetworzył aparat celno-skarbowy (nie robił tego w latach 2016–2018) i ponownie była to liczba rekordowa (192, czyli 0,9% wszystkich).

Jakiego rodzaju były to dane, który (lub które) spośród „innych organów” są szczególnie zainteresowane przesyłkami pocztowymi i dlaczego – nie wiadomo.

Ostatni wykres dotyczący przetwarzania danych (16.) przedstawia liczbę i wyniki następczej kontroli nad procesem.

Wykres 16. Kontrola przetwarzania danych telekomunikacyjnych, pocztowych i internetowych w latach 2016–2022.



Rekordowa liczba kontroli w 2022 r. zbiegła się z pierwszym w historii sprawozdawczości wynikiem, w którym nie stwierdzono ani jednego uchybienia.

Jak wspomniano, kontrolę nad przetwarzaniem danych sprawują sądy okręgowe: powszechne i wojskowe. Instytucje przetwarzające dane co pół roku przekazują sądom informacje dotyczące liczby przypadków przetworzonych 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 przyrzeć 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 należyście 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”.

Na początku 2020 r. Piotr Gąciarek, sędzia Sądu Okręgowego w Warszawie, [przekonywał](#), że przepisy wymagają nowelizacji. Tak relacjonował swoje doświadczenia z opisywaną kontrolą ex post: „Prezes Sądu Okręgowego w Warszawie wyznaczał mnie do tego zadania już trzy razy. I za każdym razem miałem wrażenie, że to kontrola mocno iluzoryczna. Dlaczego?”

Taką kontrolę sędzia przeprowadza niezależnie od innych powierzonych mu zadań. Tak uznał ustawodawca, nie typując do tego zadania osobnego organu. Obok spraw karnych, jakie prowadzę, kartkowałem więc dziesiątki stron. Gdybym miał dokładnie przejrzeć wszystkie materiały dostarczone przez służby, inne działania musiałbym odłożyć na bok”.

Przyznał, że brakowało mu „czasu i narzędzi”, aby przeprowadzić należyłą kontrolę. Tłumaczył: „Kontrolowałem w miarę możliwości. W praktyce wygląda to tak, że dostaję wykaz kilkuset spraw, jakimi w ostatnim półroczu zajmowała się policja czy służby specjalne. Chodziło o zebrane dane telefoniczne, czyli bilingi, lokalizacje do stacji bazowej, z którą łączy się aparat. A także pocztowe – adresy, miejsca nadania przesyłek, ich odbioru, oraz internetowe – raporty o połączeniach z siecią, numery IP, dane osobowe, adresy e-mail. Takich spraw bywało czasem ok. 500. Pod lupę wybierałem losowo 25, czasem 30. I zamykałem się w ciasnym pomieszczeniu kancelarii tajnej, gdzie spędzałem godziny na przeglądaniu dokumentów”. Zapytany o kryterium wyboru, odparł: „Trochę na chybił trafił, a trochę, gdy kwalifikacja sprawy była mniej typowa. Czyli gdy nie chodziło o grupę przestępczą, zabójstwo, zagrożenie bezpieczeństwa państwa. Krótko mówiąc: odrzucałem klasyczny kryminał. Sygnatura, data pobrania oraz kwalifikacja prawna. Na tej podstawie prosiłem o bardziej szczegółowe akta”.

Sędzia Gąciarek stwierdził, że nie natrafił na dane świadczące i nadużyciach, zarazem zaznaczył: „problem polega na tym, że szukałem po omacku. Nie wiedziałem, kogo dotyczą sprawy, które typuję do analizy. Czy chodzi o biznesmenów, polityków, dziennikarzy, prawników, lekarzy, pracowników korporacji czy nauczycieli. I co miałyby się dalej wydarzyć, gdybym znalazł coś budzącego wątpliwość, wymagającego dodatkowej wiedzy. Zgodnie z ustawą sąd zawiadamia o wynikach kontroli służbę, ale co zrobi ona z informacją o stwierdzonych uchybieniach? Tego nie wiemy”. Zdaniem Gąciarka problemem jest fakt, że „w obecnym stanie prawnym sędzia nie ma pewności, czy dostał do zbadania wszystkie materiały. Analizuje to, co otrzymał, wierząc, że to komplet danych. Jest więc to kwestia zaufania”.

Wśród postulowanych przez niego zmian znalazły się utworzenie nowego organu nadzorującego instytucje uprawnione do prowadzenia czynności operacyjno-rozpoznawczych. „I gdyby np. sędzia stracił owo zaufanie do służb, mógłby się do takiej instytucji poskarżyć i zainicjować kontrolę konkretnego postępowania. Byłby to realny bat na służby, bez względu na polityczną opcję, która akurat jest u władzy”. Kwestia ta była wielokrotnie przedmiotem refleksji na łamach komentarzy Katedry Bezpieczeństwa Narodowego, m.in. [przy okazji](#) omawiania powstałego pod auspicjami Rzecznika Praw Obywatelskich dokumentu pt. „Osiodłać Pegaza” i [w świetle pomysłów](#) dotyczących zespolenia polskich służb specjalnych.

Innym pomysłem Gąciarka jest wprowadzenie możliwości „kontroli z urzędu z inicjatywy RPO lub na wniosek obywatela na podstawie decyzji sądu”. Istotną kwestią jest również to, aby „konkretna osoba mogła dostać informację, czy podjęte wobec niej działania były zasadne”, a także wprowadzenie decentralizacji sądowej (adresatem wniosków służb specjalnych i Centralnego Biura Śledczego Policji jest wyłącznie Sąd Okręgowy w Warszawie, co tworzy „wąskie gardło”).

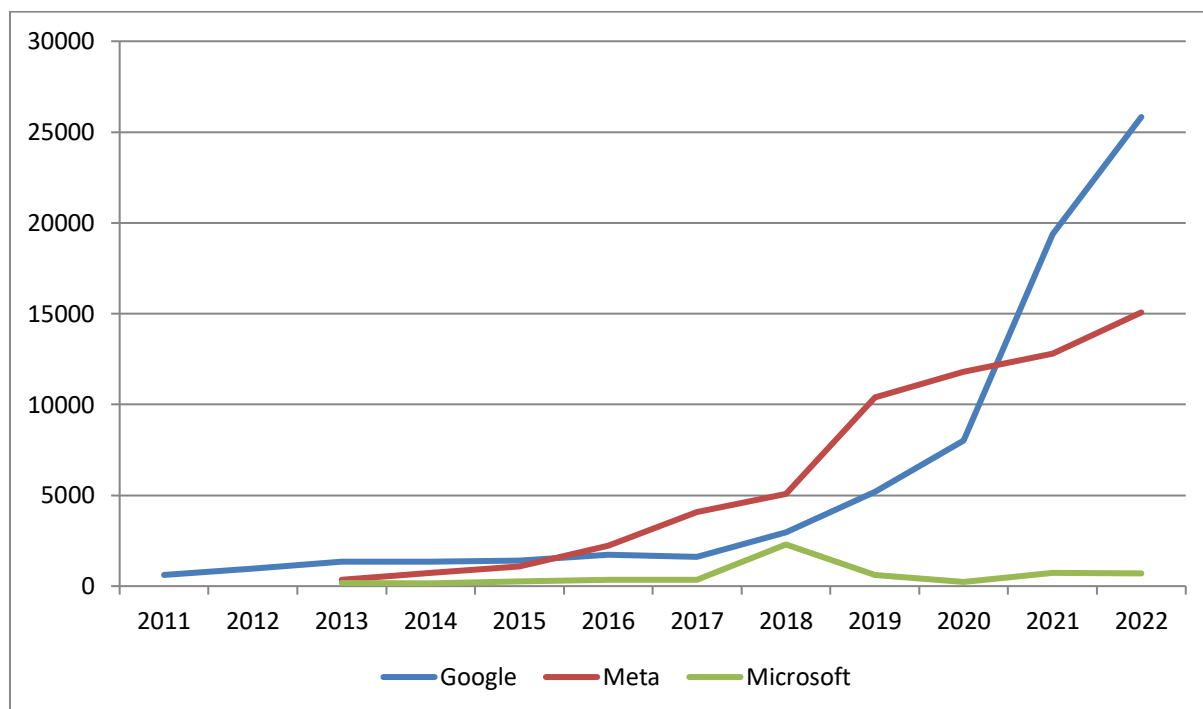
[Wiadomo](#), że nadużycia dotyczące przetwarzania danych się zdarzają – Policja sięgała np. po nie w kontekście wykroczeń, na co nie pozwala polskie prawo. Opinia publiczna nie dysponuje też żadnymi instrumentami, które umożliwiłyby interpretację informacji dotyczących przeprowadzonych kontroli. Jest jednak jasne, że fakt, iż minister sprawiedliwości wykazał zaledwie dwie zakończone negatywnym wynikiem kontrole dotyczące 2021 r., nie należy interpretować jako informacji, że w sposób nieuprawniony przetworzono jedną sztukę danych. Nie wiadomo, ile danych przetworzono bezpodstawnie i jakiej liczby osób one dotyczyły. Fakt, że ani jedna kontrola dotycząca 2022 r. nie zakończyła się wynikiem negatywnym, nie przesądza, że – przy tak wielkiej skali zjawiska – rzeczywiście nie doszło do jakichkolwiek uchybień.

3. Informacje podmiotów komercyjnych

W ramach polityk transparentności korporacje informatyczne w trybie półrocznym publikują liczbę zapytań, które kierują do nich uprawnione instytucje państwowe, uwzględniając liczbę wyrażonych zgód, liczbę kont/użytkowników, których dotyczyły zapytania, oraz procent wniosków odrzuconych. Szczególnie istotne są dane podmiotów największych, do których zaliczają się Meta, Amazon, Google, Microsoft i Apple (MAGMA). W kontekście polskim Amazon i Apple nie odgrywają jednak istotnej roli, podobnie jak X (były Twitter). Wielką trójkę, będącą obiektem szczególnego zainteresowania ze strony polskich instytucji, tworzą Meta, Google i Microsoft.

Zamieszczony poniżej wykres 17. przedstawia informacje dotyczące liczby użytkowników/kont wskazanych we wnioskach polskich instytucji przez ostatnich dwanaście lat. 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 – w lakonicznych raportach korporacji zaczęto niedawno publikować trochę więcej szczegółów, ale podział na kraje obejmuje jedynie największe państwa i kategorię „inne”.

Wykres 17. Meta, Google i Microsoft: liczba użytkowników/kont wskazanych we wnioskach o udostępnienie danych, złożonych przez polskie instytucje w latach 2011–2022.



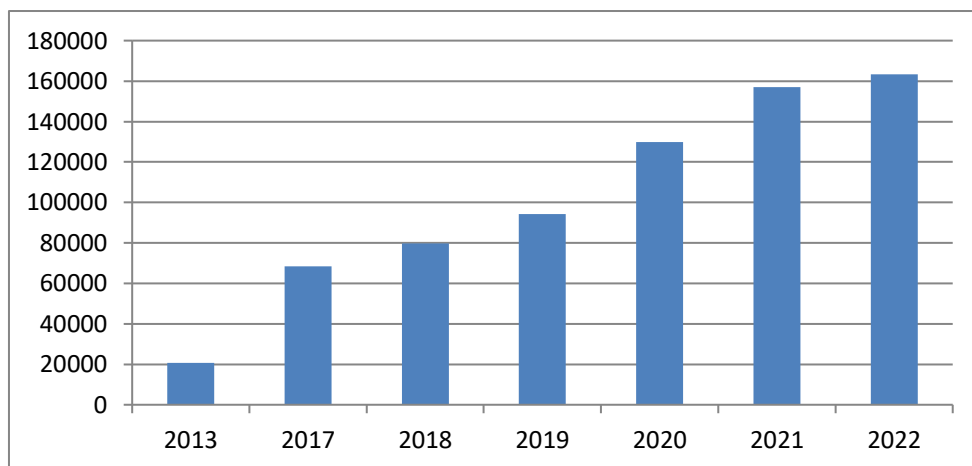
Apple i X prowadzą wprawdzie podział na państwa i dane dotyczące Polski są dostępne, gdyby jednak umieścić je na wykresie, byłyby niemal niezauważalne. Przykładowo, w 2021 r. (na razie tylko takie dane są dostępne) polskie instytucje skierowały do firmy z Cupertino wnioski w sprawie udostępnienia danych dotyczących 74 urzędzeń (w 2013 było to 15 urzędzeń, w 2014 – 58, w 2015 – 75, w 2016 – 37, w 2017 – 59, w 2018 – 62, w 2019 – 70, a w 2020 – 89). Równie niewielka i nieulegająca większym zmianom jest skala zainteresowania usługą X. W 2021 r. (aktualniejsze dane wciąż nie są dostępne) wnioski dotyczyły zaledwie 144 kont użytkowników (w 2016 – 18, w 2017 – 11, w 2018 – 58, 2019 – 186, 2020 – 140).

Inaczej wyglądają dane wspomnianej „wielkiej trójki”. W ich przypadku liczby użytkowników/kont wskazanych we wnioskach idą w tysiące.

W przypadku dwóch z trzech korporacji widoczny jest stały wzrost zainteresowania danymi użytkowników. W 2022 r. polskie instytucje wnioskowały o udostępnienie informacji dotyczących 15 tys. kont/użytkowników firmy Meta (m.in. usługi: Facebook, Instagram, Messenger i Whatsapp), co oznacza wzrost o 15%. Dane Google’a wskazują natomiast na kolejny skokowy wzrost (prawie 26 tys. wobec ponad 19 tys. w 2021 r. i ponad 8 tys. w 2020 r.). To drugi z kolei rok, w którym dane Google’a cieszyły się większym zainteresowaniem polskich instytucji niż dane Mety. W kontekście usług Microsoftu dynamika zmieniała się na przestrzeni lat. W 2022 r. nie miała miejsca widoczna zmiana w odniesieniu do poprzedniego roku.

Wzrost zainteresowania użytkownikami usług cyfrowych, zwłaszcza pochodzącymi z mediów społecznościowych, to znak czasów. Zamieszczony poniżej wykres 18. przedstawia sumę liczby użytkowników/kont korporacji Meta wskazanych we wnioskach o udostępnienie danych, złożonych przez instytucje państw członkowskich Unii Europejskiej w latach 2017–2022. Dla porównania dodano również dane dotyczące roku 2013 r.

Wykres 18. Liczba użytkowników/kont korporacji Meta wskazanych we wnioskach o udostępnienie danych, złożonych przez instytucje państw członkowskich Unii Europejskiej (i Zjednoczone Królestwo) w 2013 r. oraz w latach 2017–2022.



Wykres ten, podobnie jak wszystkie inne wykresy w raporcie, obejmuje również Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej, które wystąpiło z Unii Europejskiej 31 stycznia 2020 r. Zdecydowano się na to rozwiązanie, aby zachować ciągłość porównania danych.

Zamieszczona poniżej tabela przedstawia dynamikę zmian w tym zakresie.

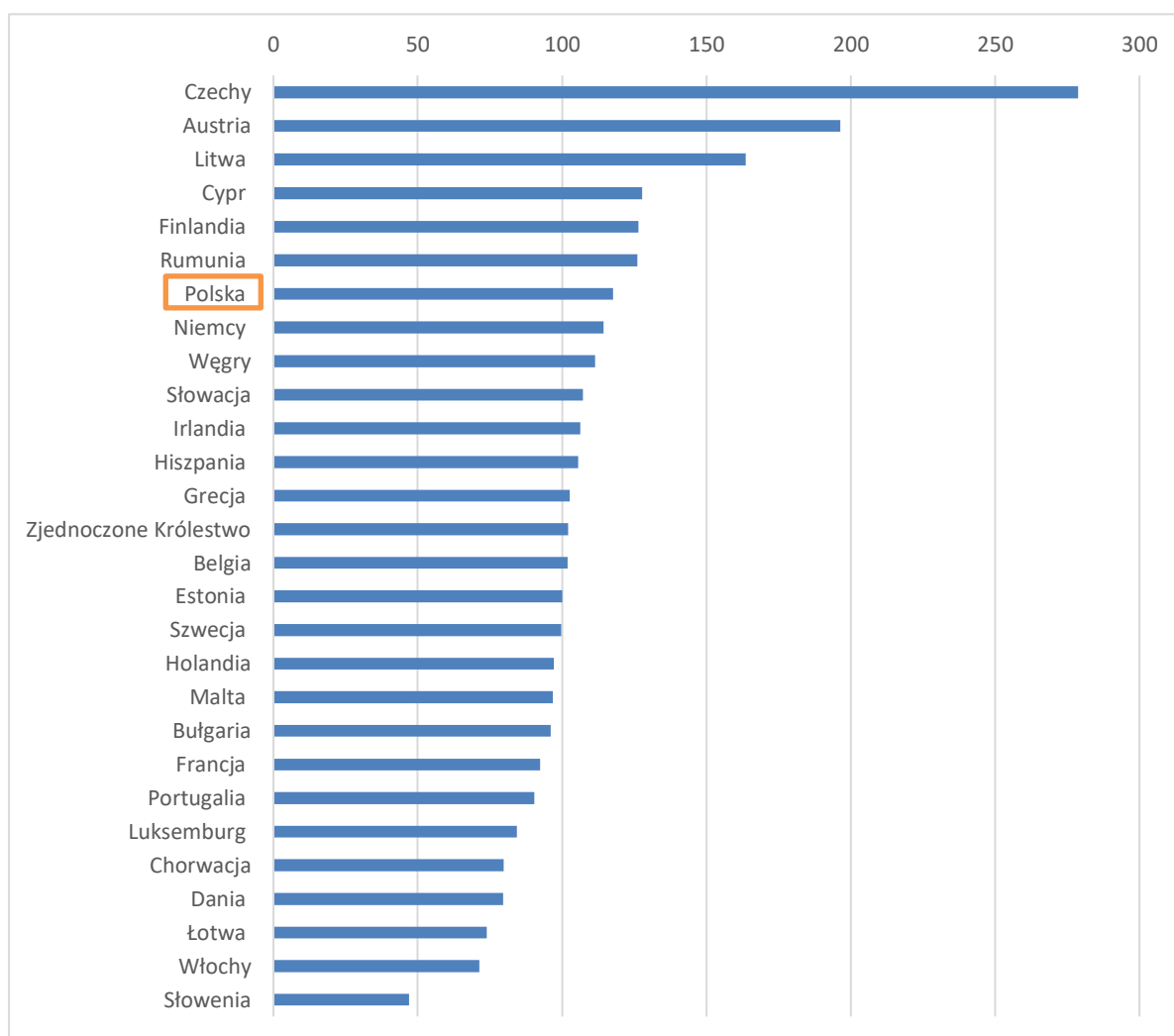
Tabela 4. Liczba użytkowników/kont korporacji Meta wskazanych we wnioskach o udostępnienie danych, złożonych przez instytucje państw członkowskich Unii Europejskiej (i Zjednoczone Królestwo) w 2013 r. i w latach 2017–2022 na tle Stanów Zjednoczonych (w tys.).

Rok	Unia Europejska i Zjednoczone Królestwo (dynamika w %)	Stany Zjednoczone (dynamika w %)
2013	20,8	38,7
2017	68,5	105,9
2018	79,6 (+ 16)	134,1 (+ 27)
2019	94,1 (+ 18)	164,8 (+ 23)
2020	129,7 (+ 38)	208,4 (+ 26)
2021	156,9 (+ 21)	214,8 (+ 3)
2022	163,2 (+ 4%)	236,9 (+ 10)

Spośród państw członkowskich UE i Zjednoczonego Królestwa w 2022 r. o udostępnienie danych dotyczących największej liczby użytkowników/kont usług korporacji Meta wniosko- wały Niemcy (wnioski dotyczące blisko 51,8 tys.), Francja (ponad 30,1 tys.), Zjednoczone Królestwo (ponad 25,2 tys.), Polska (ponad 15 tys.), Hiszpania (ponad 8,8 tys.) i Włochy (ponad 8,3 tys.), wyraźnie wyprzedzając resztę stawki. W decydującej mierze wynika to z pewnością z wielkość ich populacji – wymieniona szóstka to państwa zdecydowanie lud- niejsze od pozostałych. Państwa te zajęły niemal taką samą kolejność, co w 2021 r. (Hiszpa- nia i Włochy zamieniły się miejscami).

Dynamika wzrostu zainteresowania danymi nie jest jednolita, co obrazuje zamieszczony poniżej wykres 19.

Wykres 19. Stosunek procentowy liczby użytkowników/kont usług korporacji Meta wskazanych we wnioskach o udostępnienie danych, złożonych przez instytucje państw członkowskich Unii Eu- ropejskiej (i Zjednoczone Królestwo) w 2022 r., w relacji do 2021 r.

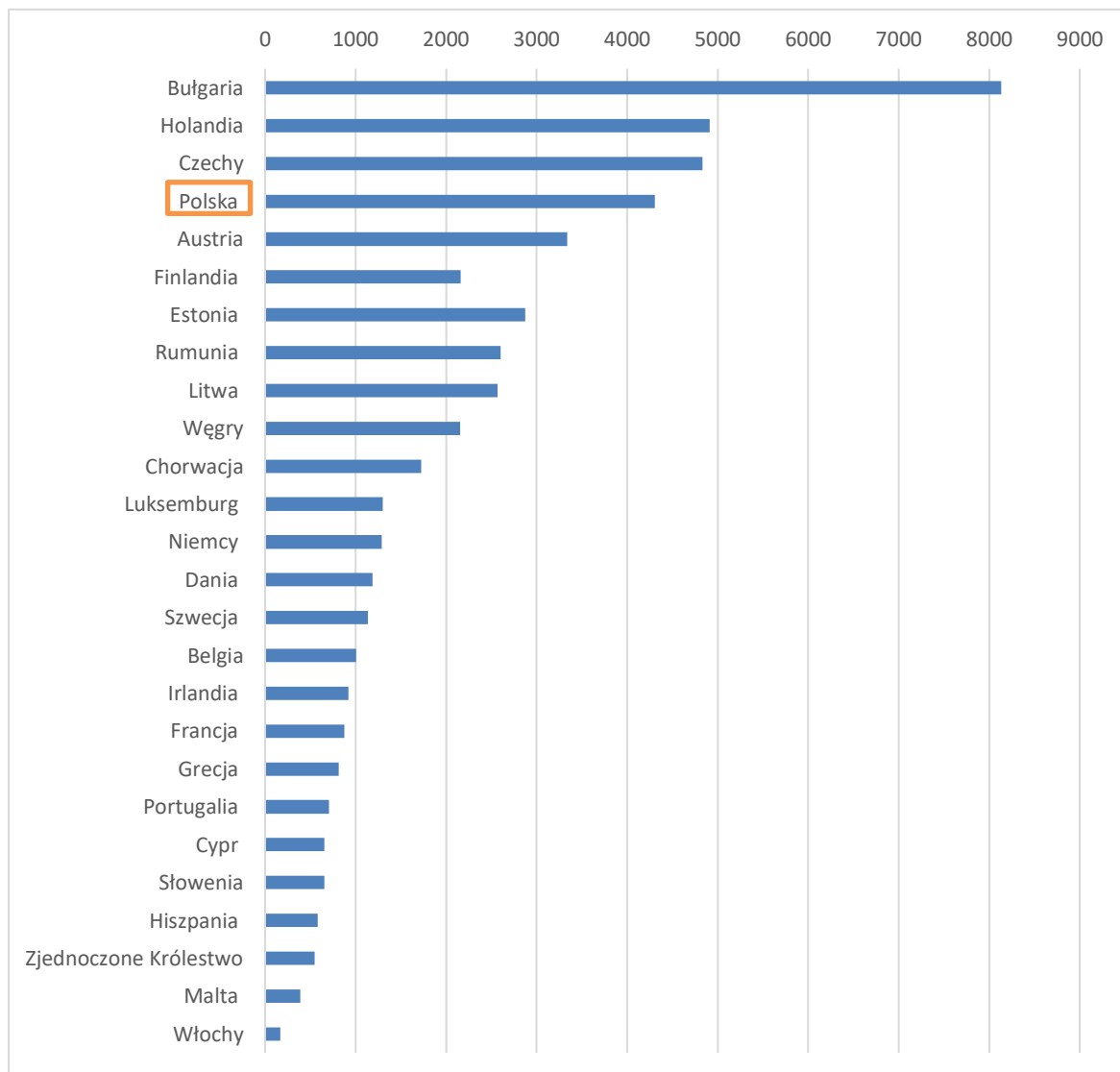


Przedstawia on odpowiedź na pytanie, jaki procent liczby użytkowników/kont korporacji Meta wskazanych we wnioskach o udostępnienie danych w 2022 r. stanowiły analogiczne

liczby z 2021 r. Wartość 100% oznacza, że instytucje danego państwa wskazały we wnioskach z 2021 r. taką samą liczbę kont/użytkowników, jak w 2020 r., 200% oznacza dwukrotny wzrost liczby kont/użytkowników, a 50% – ich dwukrotny spadek. W 15 spośród 28 państw doszło do wzrostu liczby kont/użytkowników, spadek był udziałem 12 z nich, a w Estonii odnotowano *status quo*. Tym razem największy procentowy wzrost dotyczy czeskich instytucji, które w 2022 r. były zainteresowane niemal trzykrotnie większą liczbą kont/użytkowników usług korporacji Meta niż w roku poprzednim. Jeśli chodzi o Polskę, to wzrost był znaczący. W 2021 r. nadwiślańskie instytucje chciały przetworzyć dane dotyczące 12,8 tys. kont/użytkowników korporacji Meta, a w 2022 r., jak już wspomiano – ponad 15 tys. (o ponad 17% więcej).

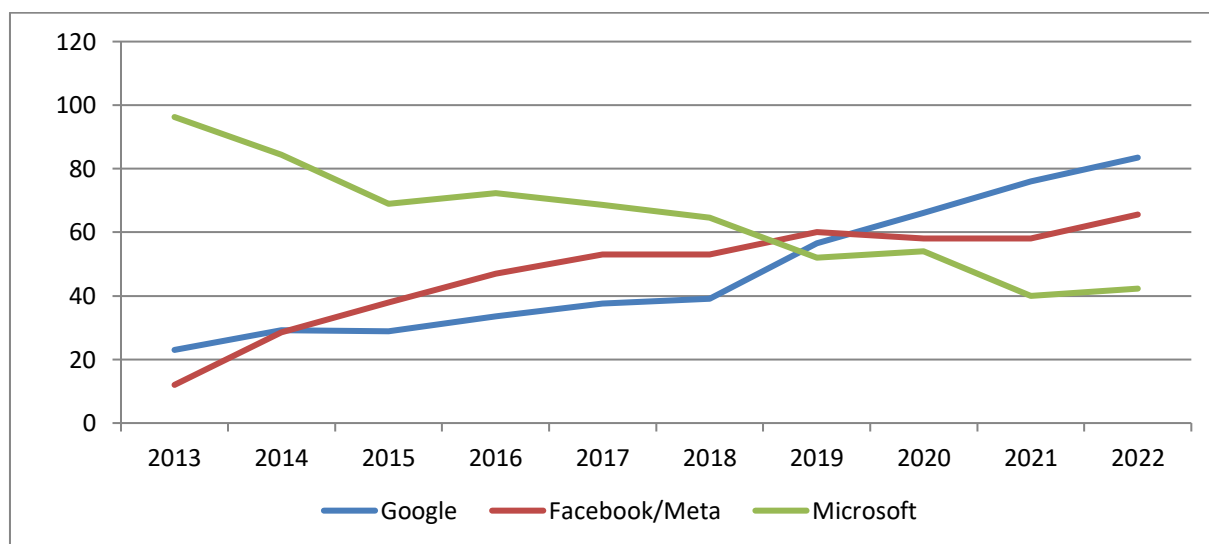
Kolejny wykres (20.) pełni tę samą funkcję, 2022 r. zestawiono w nim jednak z 2013 r. Analogicznie, 100% oznacza utrzymanie *status quo*.

Wykres 20. Stosunek procentowy liczby użytkowników/kont usług korporacji Meta wskazanych we wnioskach o udostępnienie danych, złożonych przez instytucje państw członkowskich Unii Europejskiej (i Zjednoczone Królestwo) w 2022 r., w relacji do 2013 r.



Zmienia się też podejście korporacji do udostępniania danych. Obrazuje to zamieszczony poniżej wykres 21. Trzeba jeszcze raz podkreślić, że wykresy 17.–20. przedstawiają liczbę użytkowników/kont, których dotyczyły wnioski, a nie liczbę wniosków. Przykładowo w pierwszym półroczu 2013 r. polskie instytucje skierowały do korporacji Facebook (obecna Meta) 233 wnioski, które dotyczyły 158 kont/użytkowników. W 2022 r. ponad 11,8 tys. wniosków dotyczyło ponad 15 tys. kont/użytkowników. Przedstawiony na wykresie 21. procentowy wskaźnik zgód zrealizowanych wniosków odnosi się natomiast do liczby wniosków, a nie liczby kont/użytkowników.

Wykres 21. Odsetek zrealizowanych wniosków złożonych przez polskie instytucje w latach 2013–2022.



* Dane Microsoftu za 2022 r. obejmują tylko pierwsze półrocze.

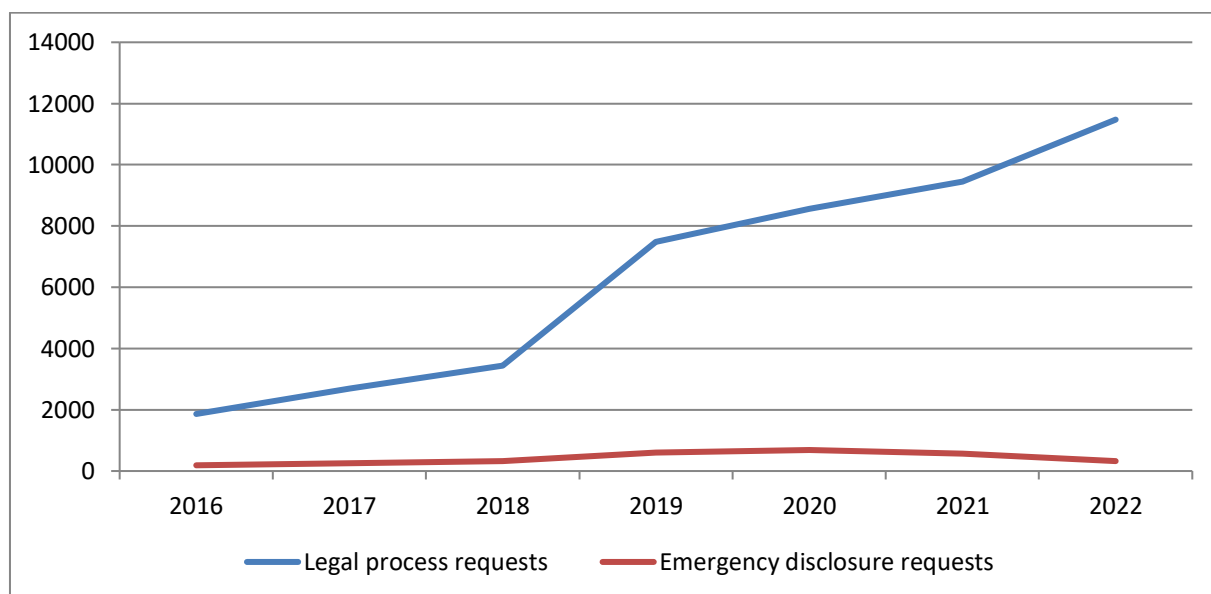
Google coraz częściej dostarcza dane w odpowiedzi na wnioski polskich instytucji. Podobnie jest z firmą Meta, choć w latach 2020–2021 odnotowano nieznaczny spadek. Odwrotnie wygląda to w przypadku Microsoftu. Przed dekadą gigant z Redmond realizował niemal wszystkie wnioski, ale szybko zaczął się wyraźny spadek. Nie wiadomo, czy wynika on z bardziej restrykcyjnej polityki Microsoftu, czy też ze wzrostu liczby wniosków (i związanej z tym proporcjonalnie większej liczby wniosków wadliwych prawnie lub niemożliwych do zrealizowania).

Rozważając statystyki dotyczące niezrealizowanych wniosków, trzeba pamiętać, że niekoniecznie oznaczają one, że wnioski zostały odrzucone (*rejected*). Także sama decyzja odmowna nie oznacza zresztą, że w ogóle nie przekazano wnioskodawcy informacji o użytkowniku/koncie. Możliwym jest, że instytucja złożyła dotyczący tego samego konta lub osoby wniosek ponownie i tym razem został on zrealizowany. Sama akceptacja wniosku nie musi mieć też charakteru całkowitego – wnioski mogą być zrealizowane w części lub całości. Jest też możliwa sytuacja, w której wniosku nie odrzucono, ale pożądaných danych nie udało się uzyskać. Microsoft nazywa tę sytuację *no data found*.

Nie wiadomo, czego dokładnie dotyczyły składane wnioski. Microsoft oferuje informację z podziałem na typ danych i tryb, czyli o tym, jaka część wniosków dotyczyła treści (*content*), a jaka danych jej niestanowiących (*non-content data*), a także czy wniosek był związany z naruszeniem prawa (*criminal*) czy wynikał z *emergencies*. Podział na tryb jest obecnie przedstawiany jedynie w kontekście tego, ile wniosków zostało zrealizowanych. Google dzieli wnioski na żądania ujawnienia w sytuacjach nadzwyczajnych, prośby o zachowanie danych i inne wnioski prawne, a Meta na *emergency requests* i *legal process*.

Zamieszczony poniżej wykres 22. przedstawia dane firmy Meta w podziale na te dwa typy wniosków. Dostępne są wyłącznie informacje obejmujące lata 2016–2022.

Wykres 22. Liczba wniosków składanych przez polskie instytucje do korporacji Facebook/Meta w latach 2016–2022 w podziale na typy.



Żadna z firm nie tłumaczy tego dokładnie, co kryje się pod daną kategorią – zwłaszcza w kontekście odmiennych rozwiązań prawnych poszczególnych państw.

W ostatnich latach Microsoft zmienił sposób raportowania tych informacji. Dzięki temu możliwe było przygotowanie poniższej tabeli.

Tabela 5. Wnioski składane przez polskie instytucje do Microsoftu w latach 2017–2022

Rok	Liczba wniosków (liczba kont/użytkowników)		Liczba zrealizowanych wniosków – treść (%)		Liczba zrealizowanych wniosków – <i>non-content data</i> (%)		Liczba wniosków niezrealizowanych z uwagi na brak danych – <i>no data found</i> (%)		Liczba wniosków odrzuconych z uwagi na wady formalne – <i>request rejected for not meeting legal requirements</i> (%)	
	<i>Criminal</i>	<i>Emergencies</i>	<i>Criminal</i>	<i>Emergencies</i>	<i>Criminal</i>	<i>Emergencies</i>	<i>Criminal</i>	<i>Emergencies</i>	<i>Criminal</i>	<i>Emergencies</i>
2017	179 (342)	3 (3)	0 (0)	0 (0)	82 (45,8)	1 (33,3)	41 (22,9)	1 (33,3)	56 (31,3)	1 (33,3)
2018	203 (2287)	6 (6)	0 (0)	0 (0)	73 (36)	4 (66,7)	58 (28,6)	1 (33,3)	72 (35,5)	1 (33,3)
2019	225 (618)	3 (3)	0 (0)	0 (0)	92 (40,9)	1 (33,3)	25 (11,1)	2 (66,7)	108 (48)	0 (0)
2020	195 (225)	8 (7)	0 (0)	0 (0)	80 (41)	5 (62,5)	26 (13,3)	1 (12,5)	89 (45,6)	2 (25)
2021	303 (709)	14 (14)	0 (0)	0 (0)	122 (40,3)	5 (35,7)	44 (14,5)	4 (28,6)	137 (45,2)	5 (35,7)
2022 (I półro- cze)	146 (157)	10 (9)	0 (0)	0 (0)	60 (41,1)	6 (60)	27 (18,49)	0 (0)	59 (40,41)	4 (40)

Zwraca uwagę fakt, że duża część wniosków nie jest realizowana z uwagi na uchybienia formalne i to, że w latach 2017–2022 nie zrealizowano ani jednego wniosku dotyczącego dostępu do danych stanowiących treść. Nie wiadomo jednak, czy takie wnioski zostały w ogóle złożone – takich informacji Microsoft nie podaje.

Podsumowanie, czyli po co nam statystyki?

Informacje dotyczące skali inwigilacji można zestawiać na wiele sposobów, poszukując ogólnych prawidłowości, trendów i cykli koniunkturalnych. Wszystkie te dociekania są jednak ograniczone przez niejawność kluczowych informacji. W wymiarze ogólnym jest ona nie tylko czymś naturalnym, ale także pożądanym. Nie ulega wątpliwości, że wiele informacji dotyczących kontroli operacyjnej oraz operacyjnego przetwarzania danych niestanowiących treści 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 trajektorie, 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 raczej 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 (oczywiście nie wiadomo jak duża) wniosków o zarządzenie kontroli operacyjnej trafia do prokuratora generalnego, który jest elementem 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.

Takie stanowisko bywa uznawane w przestrzeni publicznej za 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 ograniczonych 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. Jest dokładnie odwrotnie – są one wyrazem troski o państwo i jego instytucje. Reakcja ze strony społeczeństwa jest w takich sytuacjach niezbędna, to ona w dużej mierze wytwarza presję na reformy, generuje postulaty uszczelnienia procedur, egzekwuje adekwatność środków i ich możliwą nieinwazyjność.

Między skutecznością działania aparatu a transparentnością nie ma sprzeczności. Przeciwnie, transparentność generuje społeczne zaufanie, które z kolei przekłada się na łatwiejszy dostęp służb do informacji. Szczelnie zamknięte w swoim świecie instytucje bezpieczeństwa, nad którymi

efektywnej kontroli i nadzoru nie sprawują ani niezależne organy, ani opinia publiczna, to instytucje generujące nieufność i teorie spiskowe. Z kolei ich separacja od społeczeństwa przekłada się na tym większą skłonność do sięgania po środki techniki operacyjnej.

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

Jeszcze innym argumentem jest wyrażane czasem przekonanie, że skala problemu jest wyolbrzymiona, jako że inwigilacja dotyczy tylko niewielkiej części społeczeństwa. Szersza perspektywa może skłaniać do odmiennej refleksji. W latach 2010–2022 sama tylko Policja wniosowała o objęcie kontrolą operacyjną blisko 63 tys. ludzi. W sumie w tych latach zarządzono kontrolę operacyjną lub procesową wobec ponad 73,6 tys. osób. Skala przetwarzania danych niestanowiących treści jest nieporównywalnie większa. W samym tylko 2022 r. przetworzono blisko 1,8 mln danych telekomunikacyjnych. Nawet przyjmując, że na jednego „inwigilowanego” posiadacza telefonu przypadało 20 przetworzonych danych, zjawisko dotyczyło 90 tys. ludzi. Należy zakładać, że skala zjawiska będzie rosła.

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: wiem, czego nie wiem.

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

Rekomendacje

Kwestie ustawowego zabezpieczenia praw jednostki oraz uregulowania procedur kontroli i nadzoru nad prowadzeniem czynności operacyjno-rozpoznawczych przez polskie instytucje bezpieczeństwa często bywają przedmiotem namysłu w doktrynie. Skandal związany ze sprawą oprogramowania Pegasus, opisany przeze mnie w [odrębnym opracowaniu](#), potwierdza zasadność zgłaszanych w literaturze zastrzeżeń dotyczących jakości procedur dotyczących przetwarzania danych. Wdrożenie pożądanых zmian o charakterze ustrojowym wydaje się bardzo mało prawdopodobne w najbliższym czasie. W tej sytuacji zasadnym jest formułowanie postulatów minimalnych, niewymagających zmian ustawowych, sprowadzających się do czytelniejszej komunikacji organów bezpieczeństwa.

Nie w każdym wymiarze tajność jest siłą służb – zwłaszcza w dobie wojny w Ukrainie. Istotną wartością, mającą bezpośrednie przełożenie na skuteczność pracy operacyjnej, analitycznej i śledczej,

są społeczne zaufanie, wiarygodność i prestiż, o które bardzo trudno w sytuacji ograniczonej relacji ze społeczeństwem. Ich deficyt sprzyja spekulacjom, wpływając negatywnie na postrzeganie wszystkich służb.

Dlatego, w ramach swego planu minimum, postuluję:

1. Jeszcze dalej posunięte ujednoczenie raportowania ze strony Ministerstwa Spraw Wewnętrznych i Administracji, Ministerstwa Sprawiedliwości oraz prokuratora generalnego. Nie ma żadnego powodu, aby pozostawiać przekazywane dane domysłom.
2. Rozbudowę przekazywanych informacji. Przepisy ustawowe opisują jedynie warunki brzegowe i to od uprawnionych podmiotów zależy, ile informacji zostanie udostępnionych. Wszystkie uprawnione podmioty powinny przedstawiać społeczeństwu zarówno dokładną liczbę wniosków i zapytań, jak również liczbę osób, których te wnioski dotyczyły. Bezzasadne jest umieszczanie instytucji w szerszych kategoriach („inne organy”). Ponadto, przeprowadzone czynności powinny być przedstawiane w podziale na powód (kwalifikacja kodeksowa), tryb i – przynajmniej w przypadku kontroli operacyjnej – okres ich stosowania.
3. Szersze informowanie społeczeństwa o realizacji czynności operacyjno-rozpoznawczych. Corocznym sprawozdaniom powinny towarzyszyć konferencje prasowe poszczególnych instytucji i debata parlamentarna.
4. Przywrócenie stanowiska rzecznika prasowego ABW i powrót do publikowania corocznych „Raportów z działalności” tej instytucji.
5. Wprowadzenie elementarnej sprawozdawczości w zakresie wojskowych służb specjalnych i Żandarmerii Wojskowej.

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