

Kształtowanie społecznego odbioru inwigilacji – propozycje rozwiązań¹

Shaping public perception of surveillance – proposed solutions

Bartosz Bochyński

Autor niezależny

 <https://orcid.org/0009-0002-4180-2395>

Abstrakt

Artykuł przedstawia propozycje działań mających na celu kształtowanie pożądanego odbioru inwigilacji przez polskich obywateli. Autor poruszył w nim kwestie: terminologii dotyczącej kontroli operacyjnej i społecznego odbioru konkretnych pojęć obejmujących zagadnienia inwigilacji, wpływu zaufania do służb specjalnych i instytucji je nadzorujących na podejście społeczne do zagadnienia inwigilacji oraz poziomu świadomości społeczeństwa na temat bezpieczeństwa. W artykule zostały przytoczone wyniki badania ankietowego przeprowadzonego przez autora w 2023 r. i analiza materiałów na temat inwigilacji i jej społecznego odbioru. Na ich podstawie zaproponowano rozwiązania

¹ Artykuł powstał na podstawie pracy licencjackiej pt. *Kształtowanie społecznego odbioru inwigilacji w ramach zwiększania skuteczności działań antyterrorystycznych*, obronionej na Wydziale Bezpieczeństwa Narodowego Akademii Sztuki Wojennej w Warszawie. Autor wykorzystał fragmenty rozdziałów 2. i 4. oraz załącznik nr 1. Praca została nagrodzona w XIII edycji konkursu Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką dotyczącą bezpieczeństwa państwa w kontekście zagrożeń wywiadowczych, terrorystycznych, ekonomicznych.

mające na celu podnoszenie świadomości społeczeństwa dotyczące konieczności prowadzenia konkretnych czynności na rzecz bezpieczeństwa.

Słowa kluczowe

inwigilacja, bezpieczeństwo, antyterroryzm, służby specjalne

Abstract

The article presents proposals for actions aimed at shaping the desired perception of surveillance by Polish citizens. It addresses the following issues: the terminology of operational control and the public perception of specific concepts covering surveillance issues, the impact of trust in the special services and the institutions supervising them on the public's approach to the issue of surveillance, and the level of the public awareness of security. The article cites the results of a survey conducted by the author in 2023 and an analysis of material on surveillance and its public perception. Based on these, solutions are proposed to raise public awareness of the need for specific security activities.

Keywords

surveillance, security, antiterrorism, secret services

Wprowadzenie

Pojawienie się informacji o kolejnych uprawnieniach lub narzędziach służących inwigilacji stosowanych przez instytucje państwowe intensyfikuje debatę publiczną na temat tego zagadnienia. Ukazuje się wówczas wiele artykułów, programów i wypowiedzi przedstawiających mankamenty oraz nieprawidłowości dotyczące tego rodzaju działań². Prowadzi to do niezrozumienia, a czasem nawet konfliktu między społeczeństwem a służbami odpowiedzialnymi za bezpieczeństwo państwa.

² Zob. *Polska: Zmiany w ustawie o policji rażąco naruszają prawa człowieka*, Amnesty International, 29 I 2016 r., <https://www.amnesty.org.pl/polska-zmiany-w-ustawie-o-policji-ra%C5%BC%C4%85co-naruszaj%C4%85-prawa-cz%C5%82owieka/> [dostęp: 21 VII 2024]; *Ustawa antyterrorystyczna to „waterboarding” dla wolności słowa w sieci*, Fundacja Panoptykon, 10 V 2016 r., <https://panoptykon.org/wiadomosc/ustawa-antyterrorystyczna-waterboarding-dla-wolnosc-slowa-w-sieci> [dostęp: 21 VII 2024].

Przejawem tego konfliktu jest przeciwstawianie się społeczeństwa regulacjom uprawniającym służby do stosowania metod inwigilacyjnych. Analizując dostępne materiały w językach polskim i angielskim, można dostrzec, że dominują artykuły opisujące negatywne strony i skutki inwigilacji, brakuje natomiast tych, które uwzględniają jej pozytywne aspekty. To sprawia, że uzyskanie rzetelnych, neutralnych informacji jest utrudnione. Wypowiedzi specjalistów starających się przedstawić korzyści wynikające z działań inwigilacyjnych spotykają się z krytyką, w tym z posądzeniami o brak realizmu, niedostrzeganie negatywów czy długofalowych skutków. Brakuje także publikacji poświęconych zagadnieniom związanym z kształtowaniem odbioru tego rodzaju działań przez społeczeństwo.

W artykule wykorzystano badanie ankietowe skierowane do obywateli Polski powyżej 18. roku życia, ze zróżnicowanym poziomem wykształcenia i reprezentujących różne środowiska, w tym m.in. akademickie i związane z infrastrukturą krytyczną państwa. Ankieta została przygotowana z wykorzystaniem aplikacji Formularze Google i przeprowadzona w 2023 r. przez internet. W badaniu wzięło udział 60 osób.

Celem artykułu jest przedstawienie problemów związanych z negatywnym odbiorem społecznym inwigilacji oraz zaprezentowanie rozwiązań, które umożliwiłyby zmianę tego odbioru i zwiększenie w ten sposób skuteczności działań antyterrorystycznych prowadzonych z wykorzystaniem metod inwigilacyjnych.

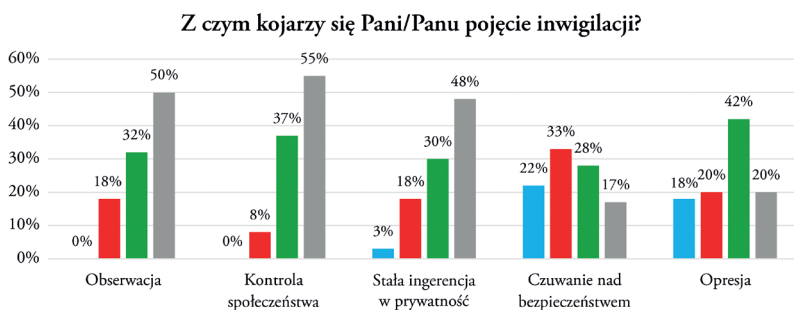
Konotacje związane z pojęciem inwigilacji

Jednym z problemów związanych z kontrolą operacyjną jest to, że wprowadzaniu nowych przepisów poszerzających uprawnienia służb w tym zakresie towarzyszy, jak już wspomniano, nieprzychylny przekaz medialny. Natłok negatywnych informacji, bez przeciwwagi w postaci pozytywów, wywołuje w społeczeństwie niechęć do tych rozwiązań. Prezentowanie niekorzystnych aspektów kontroli operacyjnej wiąże się niejednokrotnie z posługiwaniem się pojęciem inwigilacji. Aleksandra Kustra stwierdziła słusznie, że słowo inwigilacja jest silnie nacechowane pejoratywnie, gdyż kojarzy się najczęściej z opresją, działaniami państw autorytarnych i totalitarnych, w których uzyskiwane informacje służą do kontroli politycznej i manipulacji społeczeństwem³.

³ A. Kustra, *Inwigilacja – podstawowe znaczenia*, w: *Spółeczeństwo inwigilowane w państwie prawa*, P. Chrzczonowicz, V. Kwiatkowska-Darul, K. Skowroński (red.), Toruń 2003, s. 9–11.

W Polsce za sceptyczny stosunek do działań inwigilacyjnych w pewnym stopniu odpowiada doświadczenie kilkudziesięciu lat ustroju komunistycznego, w którym aparat państwowy i stosowane przez niego metody kojarzyły się z uciskiem. W okresie Polskiej Rzeczypospolitej Ludowej informacje zdobyte za pomocą środków pracy operacyjnej, w tym kontroli korespondencji czy podsłuchów⁴, były wykorzystywane w celach politycznych. W związku z tym w Polsce inwigilację łączy się w potocznym rozumieniu z działalnością wymierzoną przede wszystkim w społeczeństwo i zagrażającą wolności jednostki.

W badaniu ankietowym przeprowadzonym przez autora 90% respondentów odpowiedziało (z czego 55% zdecydowanie negatywnie, a 35% raczej negatywnie), że pojęcie inwigilacji ma dla nich wydźwięk negatywny. W odpowiedzi na pytanie zamknięte wielokrotnego wyboru o to, z czym kojarzy im się pojęcie inwigilacji, ankietowani znacznie częściej wskazywali, że z kontrolą społeczeństwa (55% w bardzo dużym stopniu, a 37% w dużym stopniu) i opresją (20% w bardzo dużym stopniu, a 42% w dużym stopniu) niż z czuwaniem nad bezpieczeństwem (17% w bardzo dużym stopniu, a 28% w dużym stopniu) – (wykres 1). Pierwotnie słowo inwigilacja (łac. *invigilare*) oznaczało śledzenie, obserwację czy nadzór, a także czuwanie nad kimś lub nad czymś i troskę o kogoś⁵. Wyniki pokazują, że pojęcie inwigilacji częściej kojarzy się negatywnie.



Wykres 1. Skojarzenia związane z pojęciem inwigilacji.

Źródło: opracowanie własne.

⁴ T. Ruzikowski, *Instrukcje pracy operacyjnej aparatu bezpieczeństwa (1945–1989)*, Warszawa 2004, s. 93.

⁵ P. Tomczyk, D. Mider, J. Grzegorzcyk, *Inwigilacja elektroniczna jako metoda pozyskiwania informacji – ewaluacja i prognozy*, „Studia Politologiczne” 2019, t. 54, D. Mider (red.), s. 260. <https://doi.org/10.33896/SPolit.2019.54.10>.

Jak zauważa Krzysztof Chmielarz, negatywna konotacja tego pojęcia to zjawisko obecne w debacie publicznej i w świadomości społeczeństwa. W terminologii prawniczej ma ono neutralne znaczenie ze względu na specyfikę języka prawniczego⁶. Można przypuszczać, że zastąpienie tego słowa innym, niemającym nacechowania pejoratywnego, pozwoliłoby na przeprowadzenie bardziej merytorycznego dialogu na temat tego typu czynności operacyjnych. Wskazane przez ankietowanych skojarzenia związane ze słowem inwigilacja potwierdzają jednak, że zmiana postrzegania tego zagadnienia jest trudnym zadaniem.

Kontrola operacyjna to pojęcie specjalistyczne, rzadziej używane w dyskursie publicznym niż inwigilacja. Aby znaleźć neutralny (nienacechowany) i częściej używany w języku potocznym zamiennik opisujący ten zbiór czynności, należałoby poszukiwać słów często stosowanych oraz odnoszących się do podobnego zakresu pojęciowego. Dobrym przykładem może być angielskie słowo *surveillance* (pol. nadzór), które oprócz kontroli operacyjnej w rozumieniu inwigilacji jest równocześnie powszechnie używane do określenia zjawiska obserwacji i systemów monitoringu wizyjnego lub cyfrowego. Może to prowadzić do wniosku, że skuteczne wypromowanie słowa monitoring jako potocznego określenia niejawnych czynności operacyjnych, w tym kontroli operacyjnej, pozwoliłoby na złagodzenie ich negatywnego odbioru społecznego.

Z odpowiedzi ankietowanych na pytanie zamknięte wynika, że w zdecydowanej większości (85%) uważają oni monitoring cyfrowy w miejscach publicznych za narzędzie poprawy bezpieczeństwa, a nie ograniczenia wolności (15%). Jednocześnie 31% respondentów zdecydowanie uważa, a 26% raczej uważa, że monitoring w miejscach publicznych nie godzi w ich prawo do prywatności. To wskazuje, że posługiwanie się słowem monitoring w kontekście kontroli operacyjnej mogłoby zwrócić uwagę społeczeństwa na pozytywny aspekt tych czynności i zaakcentować ich wpływ na bezpieczeństwo – tak, jak jest to w przypadku systemów monitoringu wizyjnego. Aby to osiągnąć, należałoby wdrożyć projekty społeczne z elementami promowania czynności kontroli operacyjnej pod nazwą monitoringu, które mogłyby pomóc w stworzeniu przeciwwagi dla negatywnie odbieranego przez opinię publiczną słowa inwigilacja.

⁶ K. Chmielarz, *Prawo do prywatności a bezpieczeństwo wewnętrzne państwa. Kontrola operacyjna i dane telekomunikacyjne w kontekście inwigilacji społeczeństwa*, Warszawa 2020, s. 78.

Zmiana społecznego postrzegania inwigilacji i służb specjalnych jest trudna, zwłaszcza w przypadku osób, które doświadczyły represji i nadużyć organów bezpieczeństwa PRL. Po upadku komunizmu zabrakło działań naprawiających wizerunek służb, dlatego tym bardziej istotne jest prowadzenie kampanii informacyjnych na ten temat. Powinny one być skierowane przede wszystkim do młodych ludzi, którzy nie tylko stanowią przyszłe kadry polskich służb specjalnych, lecz także będą kształtować środowisko, w którym te służby będą działać.

Zaufanie do służb specjalnych oraz nadzór nad ich działalnością

Pożądanym stanem byłoby pełne zaufanie społeczeństwa do służb specjalnych własnego państwa. Jest to jednak trudne do osiągnięcia nawet w bardzo świadomych społeczeństwach, takich jak np. izraelskie⁷. Rządy demokratyczne stworzyły więc mechanizmy nadzorujące działanie służb specjalnych, by chronić społeczeństwo przed nadużyciami. Społeczeństwo musi wiedzieć, że taka kontrola istnieje i jest skuteczna, aby móc budować w nim wysoki poziom zaufania do tych służb. Niezależny nadzór, m.in. w kwestii kontroli operacyjnej, nie musi jednak uniemożliwiać skutecznej pracy funkcjonariuszy. Potwierdza to również przykład Izraela.

Podjmując próbę analizy problemu, można zauważyć, że to nie same czynności będące elementem działań operacyjno-rozpoznawczych stanowią problem, lecz właśnie brak skutecznej kontroli nad nimi. W sposób merytoryczny zazwyczaj wypowiadają się osoby, które zdają sobie sprawę z wagi bezpieczeństwa i roli służb specjalnych w jego zapewnianiu i są dalekie od odbierania służbom uprawnień do kontroli operacyjnej. Wojciech Klicki z Fundacji Panoptykon stwierdził, że: (...) *kiedy mówimy o kontroli nad służbami, to nie mówimy o tym, żeby im zabrać jakieś uprawnienia, (...) żeby nie były skuteczne. Mówimy o tym, aby działania, które prowadzą, były monitorowane, nadzorowane przez kogoś z zewnątrz*⁸.

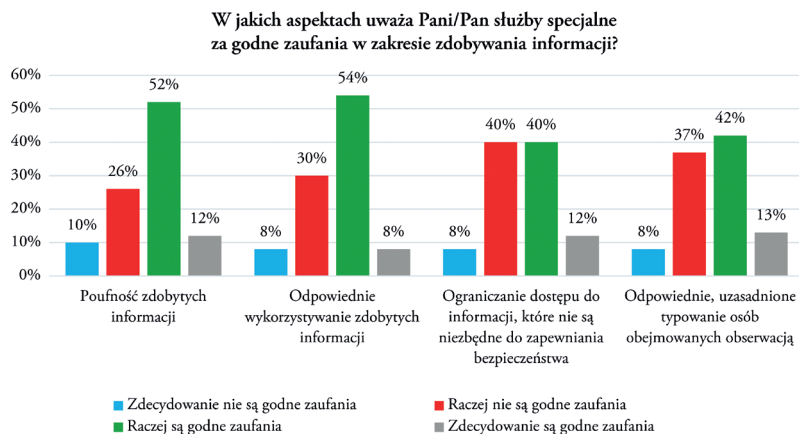
Ankietowani w zdecydowanej większości stwierdzili, że służby specjalne są skuteczne w zakresie zdobywania informacji istotnych dla

⁷ Fragment pracy licencjackiej, na podstawie której powstał ten artykuł, był poświęcony przedstawieniu przykładów społecznego podejścia do zagadnienia inwigilacji w państwach w różnych regionach świata, w tym społeczeństwa Izraela.

⁸ *Podsumowanie roku: czy 2022 r. był dobry dla wolności i prywatności?*, YouTube, 12 I 2023 r., <https://www.youtube.com/watch?v=TE-9QrbdDwA> [dostęp: 4 V 2023].

bezpieczeństwa państwa, z czego 20% uznało te działania za bardzo skuteczne, a 60% za raczej skuteczne.

Na pytanie zamknięte wielokrotnego wyboru o to, w których wskazanych aspektach związanych ze zdobywaniem informacji uważają oni służby specjalne za godne zaufania, ponad połowa respondentów uznała, że we wszystkich (wykres 2).



Wykres 2. Zaufanie do służb specjalnych w zakresie zdobywania informacji.

Źródło: opracowanie własne.

Poszerzanie uprawnień inwigilacyjnych, w szczególności dotyczących działań na masową skalę, wymaga jednak zdecydowanie większego zaufania ze strony społeczeństwa i przekonania, że uprawnienia te będą wykorzystywane jedynie w celu zapewniania bezpieczeństwa. Społeczeństwo musi mieć świadomość, że to nie ono jest celem prowadzonych działań, lecz są nim osoby, które stanowią poważne zagrożenie bezpieczeństwa państwa. Koncepcja *nontargets*⁹ (pol. osoby niebędące celem) jest jednym z kluczowych czynników sprawiających, że społeczeństwo nie sprzeciwia się szerokim uprawnieniom służb specjalnych swojego państwa. Wśród

⁹ Zob. S.A. Duke, *Nontargets: Understanding the Apathy Towards the Israeli Security Agency's COVID-19 Surveillance*, *Surveillance & Society*, 5 III 2021 r., <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/14271> [dostęp: 20 VI 2024]. <https://doi.org/10.24908/ss.v19i1.14271>. W artykule zaprezentowano sformułowanie odnoszące się do specyficznej postawy izraelskiego społeczeństwa, wynikającej ze świadomości, że to nie ono jest celem działania państwowych służb specjalnych.

osób, które wzięły udział w badaniu, 23% zdecydowanie, a 48% raczej się obawia, że informacje zebrane na ich temat w trakcie działań inwigilacyjnych mogłyby zostać wykorzystane przeciw nim nawet w sytuacji, gdy nie stanowiłoby zagrożenia bezpieczeństwa publicznego. Takie podejście utrudnia wprowadzenie tej koncepcji w Polsce.

Warunki do rozwijania świadomości *nontargets* może stworzyć odpowiednia kontrola zapobiegająca kierowaniu działań operacyjnych przeciwko niewłaściwym osobom. Nadzór zewnętrzny nad służbami, szczególnie w zakresie kontroli operacyjnej, to środek umożliwiający zmniejszenie obaw społeczeństwa w stosunku do tego rodzaju czynności operacyjno-rozpoznawczych i skuteczniejsze zapobieganie nadużyciom. Kontrolę powinny sprawować organy lub instytucje, które cieszą się zaufaniem społecznym. Najprostszym i najbardziej oczywistym rozwiązaniem jest kontrolowanie służb specjalnych przez ich własne, wewnętrzne jednostki. Wymaga to jednak bardzo wysokiego poziomu zaufania społecznego do danej służby jako całości instytucji, a jak wcześniej wskazano, niestety zarówno w Polsce, jak i w większości państw nie jest on wystarczająco wysoki, by można było polegać jedynie na ich samokontroli.

Specyfika działalności służb specjalnych sprawia, że praca operacyjna jest niejawną i wymaga zachowania tajemnicy informacji. Niezależny nadzór może być jednak realizowany w sposób zapewniający zarówno ochronę prywatności, jak i poufność działań. Istotne jest, by tę kontrolę sprawowały odpowiednie instytucje państwowe, takie jak organy parlamentarne i sądowe, które miałyby dostęp do informacji niejawnych o określonej klauzuli i byłyby w stanie zapewnić właściwy poziom kontroli przy zachowaniu tajemnicy. W przypadku Polski są to m.in. Rada Ministrów oraz Sejmowa Komisja do Spraw Służb Specjalnych. Badania przeprowadzone przez Centrum Badania Opinii Społecznej (CBOS) pokazują jednak, że zaufanie do rządu ma jedynie 32% badanych Polaków, a do parlamentu – 23%¹⁰.

Kontrola operacyjna powinna być odpowiednio uzasadniona oraz prowadzona zgodnie z określonymi procedurami i standardami. W Polsce zgodę na jej wprowadzenie wydają sądy. Według badań CBOS ponad połowa Polaków nie ufa jednak sądom¹¹. Taki brak zaufania nie jest sytuacją

¹⁰ *Zaufanie społeczne*, „Komunikat z badań CBOS” 2022, nr 37, https://www.cbos.pl/SPISKOM.POL/2022/K_037_22.PDF, s. 9 [dostęp: 20 VI 2024].

¹¹ Tamże.

charakterystyczną jedynie dla naszego kraju, jest zauważalny w różnym stopniu w wielu miejscach na świecie¹².

Społeczeństwo niemające zaufania do organów prowadzących nadzór nad służbami specjalnymi nie wierzy w rzetelność tego nadzoru, a samo nie ma możliwości kontrolowania. Ponadto gdy świadomość zagrożeń związanych z bezpieczeństwem państwa w społeczeństwie nie jest wystarczająco wysoka, by mogło ono właściwie ocenić konieczność zastosowania przez służby określonych środków, jest wysoce prawdopodobne, że będzie ono dążyło do ograniczania możliwości ingerencji przez te służby w prywatność i inne wolności.

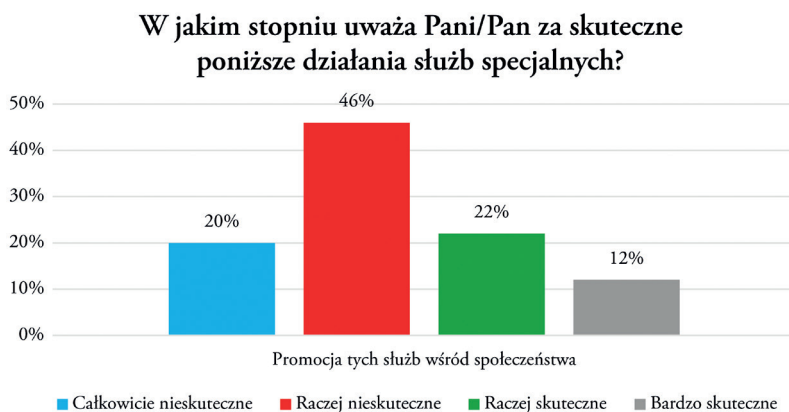
Warto zadać pytanie, czy istnieje szansa na pogodzenie skutecznego nadzoru nad służbami w zakresie kontroli operacyjnej z ich skutecznym działaniem. Wymaga to zachowania równowagi między faktycznymi potrzebami bezpieczeństwa a prawami i wolnościami obywatelskimi. Ważnym czynnikiem to umożliwiającym jest też stworzenie właściwych przepisów i procedur oraz przejrzystych ram działania. Można wskazać przykłady systemów bezpieczeństwa na świecie (np. Dania¹³), w których mechanizmy nadzoru, takie jak niezależne organy kontrolne, komisje parlamentarne, sądy czy prokuratury, których zadaniem jest monitorowanie działania służb specjalnych, cieszą się zaufaniem zarówno społeczeństwa, jak i samych służb.

Równocześnie z przywracaniem zaufania społecznego do instytucji nadzorujących służby specjalne powinno się podejmować działania mające na celu kształtowanie społecznego odbioru tych służb. Z przeprowadzonych badań ankietowych wynika, że 20% respondentów ocenia promowanie się służb specjalnych wśród społeczeństwa jako całkowicie nieskuteczne, a 46% jako raczej nieskuteczne (wykres 3). Należy zatem podjąć działania mające na celu zmianę podejścia do kwestii współpracy ze społeczeństwem, którego akceptacja i wsparcie są potrzebne tym instytucjom do osiągnięcia większej skuteczności.

¹² *OECD Survey on Drivers of Trust in Public Institutions – 2024 Results. Building Trust in a Complex Policy Environment*, OECD, 2024, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/07/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results_eeb36452/9a20554b-en.pdf [dostęp: 25 VII 2024].

¹³ *OECD Survey on Drivers of Trust in Public Institutions 2024 Results – Country Notes: Denmark*, OECD, 10 VII 2024 r., https://www.oecd.org/en/publications/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results-country-notes_a8004759-en/denmark_ac5b6973-en.html [dostęp: 23 VII 2024].

Potwierdzają to słowa płk. Grzegorza Małeckiego, byłego Szefa Agencji Wywiadu: (...) *zachodnie elity polityczno-rządowe oraz służby wywiadowcze mają pełną świadomość, że zaufanie do struktur bezpieczeństwa i wywiadu jest w warunkach współczesnych społeczeństw demokratycznych fundamentem ich działalności, bez którego tracą rację bytu i zdolność wykonywania zadań*¹⁴.



Wykres 3. Skuteczność promowania się służb specjalnych wśród społeczeństwa.

Źródło: opracowanie własne.

Zmieniające się środowisko działania służb specjalnych powoduje, że informowanie o działalności tych służb i ich promowanie powinny stanowić bardzo istotny element wizerunkowy. Jak stwierdziła mjr Anna Grabowska-Siwiec, ekspertka ds. bezpieczeństwa wewnętrznego i analizy danych: (...) *czas ciszy wokół służb już się skończył. (...) Żeby stworzyć wokół służb pozytywną atmosferę, trzeba (...) mówić o tym, co robią (...)*¹⁵. Istotne jest, by tam, gdzie to możliwe, działania były transparentne, a społeczeństwo było o nich informowane oraz by służby wyjaśniały, jakie procedury są stosowane w celu ochrony prywatności obywateli.

¹⁴ G. Małecki, *Służby wywiadowcze między zaufaniem a kontrolą*, InfoSecurity24, 19 XII 2017 r., <https://infosecurity24.pl/sluzby-specjalne/sluzby-wywiadowcze-miedzy-zaufaniem-a-kontrola-analiza> [dostęp: 2 V 2023].

¹⁵ *Kontrwywiad jest obszarem nieznanym i niezrozumiałym*, rozmowa J. Rauby z A. Grabowską-Siwiec, S. Kuligowską, YouTube, 16 I 2023 r., <https://www.youtube.com/watch?v=CMBE6e3qyHo> [dostęp: 2 V 2023].

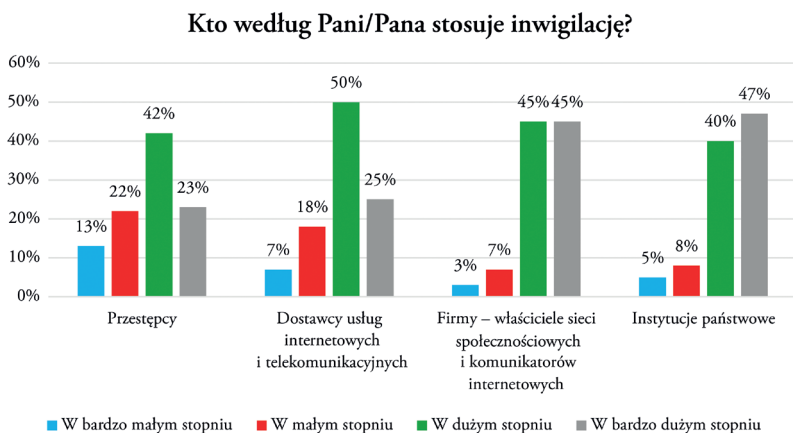
W Izraelu w 2018 r. Nadav Argaman, dyrektor Shabaku, czyli Izraelskiej Agencji Bezpieczeństwa (Israeli Security Agency), poinformował o skutecznym udaremnieniu 250 poważnych ataków terrorystycznych w zaledwie pół roku, co w znacznym stopniu umożliwiło kierowanej przez niego agencji wdrożenie zaawansowanych rozwiązań technologicznych, w tym inwigilacyjnych¹⁶. Takie działania pozwalają kształtować bardziej pozytywny odbiór inwigilacji wśród społeczeństwa, które ma możliwość dostrzec jej realny, pozytywny wpływ na bezpieczeństwo.

Sposób postrzegania inwigilacji przez społeczeństwo

Z ankiety wynika, że niewiele ponad połowa badanych (55%) byłaby w stanie poświęcić swoje prawo do prywatności na rzecz zwiększenia bezpieczeństwa przez uzyskanie przez polskie służby specjalne uprawnień do prowadzenia masowego monitoringu cyberprzestrzeni. Ankietowani mieli dokonać wyboru przy założeniu, że nie będzie dochodziło do nadużyć i niewłaściwego wykorzystania uzyskanych w ten sposób danych. Obecnie w przekazie medialnym w Polsce dominują negatywne opinie na temat zmian związanych z nowymi uprawnieniami inwigilacyjnymi tych służb. Taki wynik badań ankietowych może być związany z tym, że świadomość *nontargets* nie może wykształcić się w społeczeństwie, do którego dociera przekaz o niewłaściwym wykorzystywaniu uprawnień przez służby specjalne i które nie ma możliwości odniesienia go do informacji o korzyściach wynikających z takich rozwiązań.

Badani zapytani o to, w jakim stopniu wskazane podmioty stosują inwigilację (pytanie zamknięte wielokrotnego wyboru, wykres 4), stwierdzili, że w największym posługują się nią firmy odpowiadające za sieci społecznościowe i komunikatory internetowe (45% uważa, że stosują one inwigilację w bardzo dużym stopniu, a 45% w dużym stopniu) oraz instytucje państwowe (47% w bardzo dużym stopniu, a 40% w dużym stopniu).

¹⁶ J.A. Gross, *Shin Bet says 250 'significant terror attacks' thwarted since January*, The Times of Israel, 13 VI 2018 r., <https://www.timesofisrael.com/shin-bet-says-thwarted-250-significant-terror-attacks-since-january/> [dostęp: 2 V 2023].



Wykres 4. Skala inwigilacji stosowanej przez różne podmioty.

Źródło: opracowanie własne.

Wyniki wskazują, że badani podobnie ocenili stopień inwigilacji stosowanej przez big techy i instytucje państwowe. Inaczej jednak jest oceniane przez badanych zbieranie i wykorzystywanie informacji o użytkownikach przez wielkie firmy technologiczne o ugruntowanej pozycji¹⁷, a inaczej ich zbieranie przez służby. Firmy takie jak Apple, Android, Google czy Meta Platforms (właściciel m.in. serwisów: Facebook, Instagram i WhatsApp) stale informują o korzyściach wynikających z gromadzenia danych w ich aplikacjach. Na przykład Apple w 2022 r. udostępniło raport informujący o wpływie swojej aplikacji na poprawę stanu zdrowia, samopoczucia czy bezpieczeństwa użytkowników¹⁸. W przypadku Mety w zasadach użytkowania aplikacji są zawarte informacje o sposobie wykorzystywania danych m.in. w celu „personalizowania korzystania (...) z usług”¹⁹, świadczenia usług pomiarowych i analitycznych oraz w celu ochrony bezpieczeństwa użytkowników²⁰. Google natomiast zwraca uwagę, w jaki sposób dane nawigacyjne pomagają

¹⁷ P. Armstrong, S. Balitzky, A. Harris, *BigTech – implications for the financial sector*, ESMA Report on Trends, Risks and Vulnerabilities, nr 1, 2020, https://www.esma.europa.eu/sites/default/files/trv_2020_1-bigtech_implications_for_the_financial_sector.pdf [dostęp: 3 V 2023].

¹⁸ *Empowering people to live a healthier day. Innovation using Apple technology to support personal health, research, and care*, Apple, 20 VII 2022 r., <https://www.apple.com/newsroom/pdfs/Health-Report-July-2022.pdf> [dostęp: 3 V 2023].

¹⁹ *Zasady ochrony prywatności*, Meta, <https://pl-pl.facebook.com/privacy/policy/> [dostęp: 3 V 2023].

²⁰ Tamże.

ulepszać mapy i usługi lokalizacyjne oferowane przez firmę²¹, z których w grudniu 2021 r. korzystało ponad 21 mln polskich użytkowników²².

Przykładem wskazującym na brak kontroli przez te firmy nad gromadzonymi danymi może być informacja Google dotycząca oprogramowania Android dla urządzeń mobilnych. Nawet jeśli użytkownik dezaktywuje w ustawieniach urządzenia możliwość wykorzystywania lokalizacji przez aplikację, to nadal będzie ona rejestrować przybliżone położenie, wykorzystując adres IP urządzenia²³.

Wiele osób wyraża zgodę na działania inwigilacyjne prywatnych firm, często nie mając świadomości, na co właściwie przyzwala. Na pytanie o czytanie regulaminów wymagających zaakceptowania podczas rejestrowania lub logowania na stronach internetowych 22% ankietowanych odpowiedziało, że nigdy się z nimi nie zapoznaje, a 58%, że raczej tego nie robi. Ponadto połowa badanych stwierdziła, że przy powiadomieniu o gromadzeniu danych (np. plików cookies) podczas przeglądania stron internetowych zazwyczaj wybiera opcję „zaakceptuj wszystko”.

W Polsce dużą popularnością cieszą się zakupy przez internet²⁴. Podczas ich dokonywania kupujący często musi podać dane takie, jak: imię, nazwisko, numer telefonu, adres mailowy, adres zamieszkania. Spośród ankietowanych zapytanych o zaufanie do sprzedawcy w kwestii zabezpieczenia ich danych przed wyciekiem lub kradzieżą 17% wskazało, że zdecydowanie nie ma zaufania do sprzedającego, a 33%, że raczej nie ma. Ponadto 47% ankietowanych nie ufa (z czego 15% zdecydowanie, a 32% raczej nie ufa), że sprzedawca wykorzysta dane jedynie do realizacji zamówienia. Mimo to opór przed podawaniem takich danych jest mniejszy niż w przypadku informacji gromadzonych przez instytucje państwowe.

Może to wynikać m.in. ze wspomnianej wcześniej różnicy w odbiorze skutków wykorzystywania obu typów inwigilacji. W przypadku prywatnych firm skutki te są bowiem zauważalne i wymierne, a użytkownicy

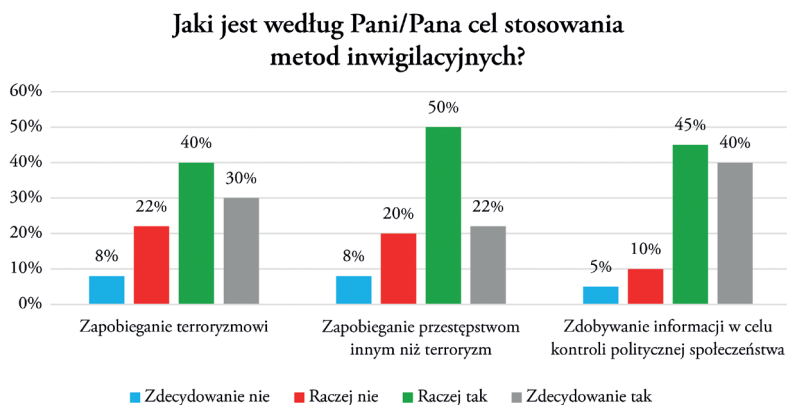
²¹ *Jak dane nawigacyjne pomagają ulepszać Mapy Google*, Google, https://support.google.com/maps/answer/10565726?hl=PL&ref_topic=6384263 [dostęp: 3 V 2023].

²² *Czołowe platformy z kategorii Mapy i lokalizatory w grudniu 2021 r.*, WirtualneMedia.pl, 7 II 2022 r., <https://static.wirtualnemediamedia.pl/media/images/2013/imagesnew/mapy-grudzien2021.jpg> [dostęp: 3 V 2023].

²³ *Zarządzanie ustawieniami lokalizacji na urządzeniu z Androidem*, Google, <https://support.google.com/accounts/answer/3467281?hl=pl> [dostęp: 3 V 2023].

²⁴ *E-commerce w Polsce 2022*, Gemius Polska, 29 IX 2022 r., <https://www.gemius.pl/wszystkie-artykuly-aktualnosci/raport-e-commerce-2022-juz-dostepny.html> [dostęp: 21 VII 2024].

traktują je jako korzyści ułatwiające codzienne funkcjonowanie. W przypadku służb specjalnych natomiast, mimo że 70% respondentów uważa, że celem stosowania metod inwigilacyjnych jest zapobieganie terroryzmowi (z czego 30% zdecydowanie tak, a 40% raczej tak), a 72%, że przestępstwom innym niż terroryzm (z czego 22% zdecydowanie tak, a 50% raczej tak), to aż 85% (z czego 40% zdecydowanie tak, a 45% raczej tak) za taki cel uważa również kontrolę polityczną społeczeństwa (pytanie zamknięte wielokrotnego wyboru, wykres 5).



Wykres 5. Cele działań inwigilacyjnych.

Źródło: opracowanie własne.

W kwestii potencjalnego wykorzystania inwigilacji w sposób masowy 84% badanych uważa, że wpływałaby ona odczuwalnie na ich życie codzienne (z czego 40% twierdzi, że zdecydowanie by wpływała, a 44% raczej by wpływała).

Polskie społeczeństwo nie jest odpowiednio często informowane, jak duża część działań wymaga użycia technicznych środków inwigilacji, jak to się dzieje np. w Izraelu. Jeżeli inwigilację przedstawi się jako istotny element zapewniania bezpieczeństwa, np. przez pokazanie w kampaniach społecznych sukcesów służb osiągniętych dzięki narzędziom kontroli operacyjnej, może to zmniejszyć opór społeczeństwa wobec niej.

Poziom świadomości społeczeństwa

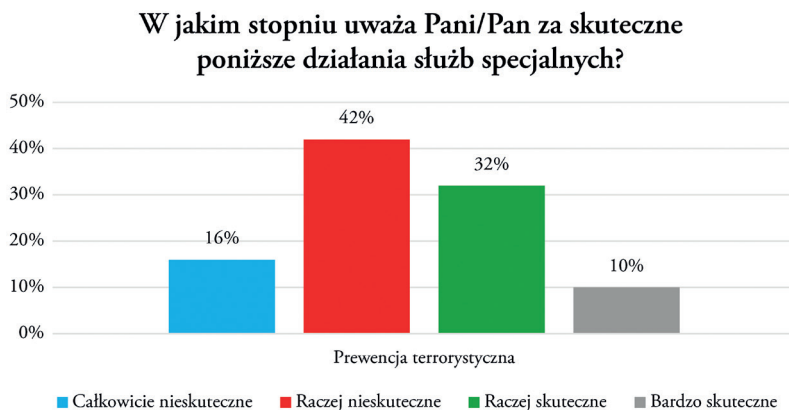
Czynnikiem, na który należy zwrócić uwagę w kontekście próby ukształtowania pozytywnego odbioru inwigilacji, jest poziom świadomości społeczeństwa. Po przeanalizowaniu zagadnienia świadomości antyterrorystycznej w izraelskim społeczeństwie, można zauważyć, że jednym z kluczowych aspektów determinujących podejście do izraelskich służb i wykorzystywanych przez nie metod jest wysoki poziom świadomości dotyczącej rzeczywistości, w jakiej to społeczeństwo funkcjonuje. Prewencja terrorystyczna stosowana przez izraelskie władze ma na celu doprowadzenie do stanu, w którym jak najwięcej obywateli będzie świadomych zagrożeń oraz będzie wiedzieć, jak postępować w przypadku ich wystąpienia.

Odpowiedni poziom świadomości zagrożeń wśród polskiego społeczeństwa jest więc niezbędny, aby możliwe było skuteczne promowanie metod zapobiegawczych i ochronnych. W badaniu ankietowym jedno z pytań dotyczyło wiedzy na temat stopnia alarmowego o zagrożeniu terrorystycznym aktualnie obowiązującego na terenie Rzeczypospolitej Polskiej. Jedynie 40% badanych prawidłowo wskazało jeden z dwóch stopni alarmowych (badanie zostało przeprowadzone w dniach 12–30 kwietnia 2023 r., gdy na całym terytorium RP obowiązywał drugi stopień alarmowy BRAVO oraz CHARLIE-CRP)²⁵. Prawie połowa respondentów (47%) nie wiedziała, jaki stopień alarmowy obowiązuje, a 13% stwierdziło, że nie wprowadzono żadnego stopnia alarmowego.

Z odpowiedzi ankietowanych wynika, że w Polsce prewencja terrorystyczna, rozumiana w tym przypadku jako organizowanie kampanii społecznych i szkoleń dla cywili, mimo starań i zaangażowania Centrum Prewencji Terrorystycznej Agencji Bezpieczeństwa Wewnętrznego (CPT ABW), nie była skuteczna. Jako całkowicie nieskuteczne takie działania służb oceniło 16% respondentów, a jako raczej nieskuteczne – 42% (wykres 6). Kampania społeczna *4U! – Uważaj! Uciekaj! Ukryj się! Udaremnij atak!* prowadzona przez CPT, zrealizowana na wysokim poziomie merytorycznym, wydaje się nieobecna w przestrzeni i debacie publicznej. Jedynie 8% badanych widziało spot wspomnianej kampanii. Jest to zdecydowanie

²⁵ Stopnie alarmowe CRP informują o możliwości wystąpienia zagrożeń terrorystycznych o określonej skali dotyczących systemów teleinformatycznych infrastruktury krytycznej lub administracji publicznej. Zob. *Rodzaje stopni alarmowych*, Serwis Rzeczypospolitej Polskiej, <https://www.gov.pl/web/mswia/rodzaje-stopni-alarmowych> [dostęp: 4 V 2023].

zbyt mało, aby skutecznie przekazywać informacje i wzorce zachowań kluczowe dla bezpieczeństwa antyterrorystycznego.



Wykres 6. Skuteczność prewencji terrorystycznej rozumianej jako organizowanie kampanii społecznych i szkoleń dla cywili.

Źródło: opracowanie własne.

Szkolenia antyterrorystyczne powinny być dostępne dla szerokiego grona obywateli i obowiązkowe dla pracowników instytucji publicznych oraz infrastruktury krytycznej państwa. Spośród badanych jedynie 30% wzięło kiedykolwiek udział w takim szkoleniu. Ponad połowa stwierdziła, że nie wie (15% zupełnie, a 37% raczej nie wie), jak zachować się w sytuacji zamachu terrorystycznego. Zapytani o to, co zrobiliby w przypadku zaobserwowania zdarzeń o potencjalnym charakterze terrorystycznym, w większości wskazali jednak prawidłowe zachowania. Pytania dotyczyły dwóch sytuacji. W przypadku strzelaniny w budynku publicznym 70% badanych w pierwszej kolejności podjęłoby decyzję o oddaleniu się z miejsca zdarzenia, co jest zgodne ze wzorcem zachowania *Run, Hide, Fight* (pol. Uciekaj, ukryj się, walcz) stosowanym w sytuacji zagrożenia ze strony aktywnego strzelca²⁶. W przypadku pakunku pozostawionego w autobusie 88% respondentów w pierwszej kolejności powiadomiłoby kierowcę, co jest prawidłowym zachowaniem wskazywanym m.in. przez CPT²⁷. W tym przypadku

²⁶ *FBI Active Shooter Safety Resources*, FBI, <https://www.fbi.gov/how-we-can-help-you/safety-resources/active-shooter-safety-resources> [dostęp: 1 V 2023].

²⁷ *Poradnik prewencji terrorystycznej*, ABW, Warszawa 2021, s. 47.

takie reakcje oznaczają jednak działania odruchowe lub oparte na logicznym myśleniu. Aby w sytuacji zagrożenia działać w świadomy, wyuczony sposób, właściwe zachowania muszą być dobrze przyswojone.

Podsumowanie

W przestrzeni publicznej rzadko są podejmowane działania mające na celu kształtowanie pozytywnego odbioru kontroli operacyjnej, dominują natomiast jednoznacznie krytyczne przekazy. Rozwiązaniem problemu negatywnego postrzegania tego rodzaju czynności operacyjnych może być więc prowadzenie szerokich kampanii społecznych ukazujących płynące z niej korzyści, np. życie w bezpiecznym kraju.

Budowanie zaufania społecznego jest procesem czasochłonnym, wymagającym dużego wysiłku. Może to być szczególnie trudne w odniesieniu do akceptacji i zrozumienia działań inwigilacyjnych. Jednak odpowiednia edukacja społeczeństwa oraz kampanie informacyjne na temat celów i procedur związanych z kontrolą operacyjną mogą przyczynić się do zwiększenia poziomu zaufania społecznego do działań służb specjalnych.

Istotne są zatem podnoszenie świadomości społeczeństwa na temat roli służb specjalnych w zapewnianiu bezpieczeństwa, konieczności prowadzenia konkretnych działań oraz rozwój edukacji antyterrorystycznej w Polsce. Przywoływany przykład Izraela dowodzi, że są to działania nie tylko pozwalające obywatelom samodzielnie dbać o własne bezpieczeństwo, lecz także ułatwiające pracę instytucjom państwowym. Świadomemu społeczeństwu, rozumiejącemu zagrożenie, przed którym ma być chronione, łatwiej jest wytłumaczyć potrzebę wprowadzenia określonych uprawnień.

Ostatnim wnioskiem z przeprowadzonych badań jest to, że Polacy na ogół nie są przeciwni zastosowaniu zdecydowanych środków zapobiegawczych, takich jak nieukierunkowane metody inwigilacyjne. Ponad połowa badanych (55%) wskazuje, że byłaby w stanie poświęcić swoje prawo do prywatności na rzecz zwiększenia bezpieczeństwa przez wyrażenie zgody na uzyskanie przez polskie służby specjalne uprawnień do prowadzenia masowego monitoringu cyberprzestrzeni. Oznacza to, że społeczeństwo traktuje bezpieczeństwo jako wartość wyższą, a jego zwiększanie może odbywać się kosztem prywatności.

Przedstawione propozycje działań pozwolą na zmniejszenie podejrzliwości obywateli i lęku przed działaniami służb oraz zwiększenie akceptacji

dla kontroli operacyjnej. Współpraca ze społeczeństwem stanowi bowiem we współczesnym świecie fundament skutecznej działalności instytucji państwowych, szczególnie w tak newralgicznym obszarze jak bezpieczeństwo.

Bibliografia

Chmielarz K., *Prawo do prywatności a bezpieczeństwo wewnętrzne państwa. Kontrola operacyjna i dane telekomunikacyjne w kontekście inwigilacji społeczeństwa*, Warszawa 2020.

Kustra A., *Inwigilacja – podstawowe znaczenia*, w: *Spółczesność inwigilowana w państwie prawa*, P. Chrzczonowicz, V. Kwiatkowska-Darul, K. Skowroński (red.), Toruń 2003.

Poradnik prewencji terrorystycznej, ABW, Warszawa 2021.

Ruzikowski T., *Instrukcje pracy operacyjnej aparatu bezpieczeństwa (1945–1989)*, Warszawa 2004.

Tomczyk P., Mider D., Grzegorzczak J., *Inwigilacja elektroniczna jako metoda pozyskiwania informacji – ewaluacja i prognozy*, „*Studia Politologiczne*” 2019, t. 54, D. Mider (red.), s. 258–294. <https://doi.org/10.33896/SPolit.2019.54.10>.

Wójtowicz T., *Jak pokonać ISIS? Metody walki z Państwem Islamskim*, „*Rocznik Bezpieczeństwa Międzynarodowego*” 2016, t. 10, nr 2, s. 87–109. <https://doi.org/10.34862/rbm.2016.2.11>.

Źródła internetowe

Armstrong P., Balitzky S., Harris A., *BigTech – implications for the financial sector*, ESMA Report on Trends, Risks and Vulnerabilities, nr 1, 2020, https://www.esma.europa.eu/sites/default/files/trv_2020_1-bigtech_implications_for_the_financial_sector.pdf [dostęp: 3 V 2023].

Czołowe platformy z kategorii Mapy i lokalizatory w grudniu 2021 r., WirtualneMedia.pl, 7 II 2022 r., <https://static.wirtualnemedi.pl/media/images/2013/imagesnew/mapy-grudzien2021.jpg> [dostęp: 3 V 2023].

Duke S.A., *Nontargets: Understanding the Apathy Towards the Israeli Security Agency's COVID-19 Surveillance*, *Surveillance & Society*, 5 III 2021 r., <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/14271> [dostęp: 20 VI 2024]. <https://doi.org/10.24908/ss.v19i1.14271>.

E-commerce w Polsce 2022, Gemius Polska, 29 IX 2022 r., <https://www.gemius.pl/wszystkie-artykuly-aktualnosci/raport-e-commerce-2022-juz-dostepny.html> [dostęp: 21 VII 2024].

Empowering people to live a healthier day. Innovation using Apple technology to support personal health, research, and care, Apple, 20 VII 2022 r., <https://www.apple.com/newsroom/pdfs/Health-Report-July-2022.pdf> [dostęp: 3 V 2023].

FBI Active Shooter Safety Resources, FBI, <https://www.fbi.gov/how-we-can-help-you/safety-resources/active-shooter-safety-resources> [dostęp: 1 V 2023].

Gross J.A., *Shin Bet says 250 'significant terror attacks' thwarted since January*, The Times of Israel, 13 VI 2018 r., <https://www.timesofisrael.com/shin-bet-says-thwarted-250-significant-terror-attacks-since-january/> [dostęp: 2 V 2023].

Jak dane nawigacyjne pomagają ulepszać Mapy Google, Google, https://support.google.com/maps/answer/10565726?hl=PL&ref_topic=6384263 [dostęp: 3 V 2023].

Kontrwywiad jest obszarem nieznanym i niezrozumiałym, rozmowa J. Rauby z A. Grabowską-Siwięc, S. Kuligowską, YouTube, 16 I 2023 r., <https://www.youtube.com/watch?v=CMbE6e3qyHo> [dostęp: 2 V 2023].

Małecki G., *Śłużby wywiadowcze między zaufaniem a kontrolą*, InfoSecurity24, 19 XII 2017 r., <https://infosecurity24.pl/sluzby-specjalne/sluzby-wywiadowcze-miedzy-zaufaniem-a-kontrola-analiza> [dostęp: 2 V 2023].

OECD Survey on Drivers of Trust in Public Institutions – 2024 Results. Building Trust in a Complex Policy Environment, OECD, 2024, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/07/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results_eeb36452/9a20554b-en.pdf [dostęp: 25 VII 2024].

OECD Survey on Drivers of Trust in Public Institutions 2024 Results – Country Notes: Denmark, OECD, 10 VII 2024 r., https://www.oecd.org/en/publications/oecd-survey-on-drivers-of-trust-in-public-institutions-2024-results-country-notes_a8004759-en/denmark_ac5b6973-en.html [dostęp: 23 VII 2024].

Podsumowanie roku: czy 2022 r. był dobry dla wolności i prywatności?, YouTube, 12 I 2023 r., <https://www.youtube.com/watch?v=TE-9QrbdDwA> [dostęp: 4 V 2023].

Polska: Zmiany w ustawie o policji rażąco naruszają prawa człowieka, Amnesty International, 29 I 2016 r., <https://www.amnesty.org.pl/polska-zmiany-w-ustawie-o-policji-ra%C5%BC%C4%85co-naruszaj%C4%85-prawa-cz%C5%82owieka/> [dostęp: 21 VII 2024].

Rodzaje stopni alarmowych, Serwis Rzeczypospolitej Polskiej, <https://www.gov.pl/web/mswia/rodzaje-stopni-alarmowych> [dostęp: 4 V 2023].

Ustawa antyterrorystyczna to „waterboarding” dla wolności słowa w sieci, Fundacja Panoptykon, 10 V 2016 r., <https://panoptykon.org/wiadomosc/ustawa-antyterrorystyczna-waterboarding-dla-wolnosci-slowa-w-sieci> [dostęp: 21 VII 2024].

Zarządzanie ustawieniami lokalizacji na urządzeniu z Androidem, Google, <https://support.google.com/accounts/answer/3467281?hl=pl> [dostęp: 3 V 2023].

Zasady ochrony prywatności, Meta, <https://pl-pl.facebook.com/privacy/policy/> [dostęp: 3 V 2023].

Zaufanie społeczne, „Komunikat z badań CBOS” 2022, nr 37, https://www.cbos.pl/SPISKOM.POL/2022/K_037_22.PDF [dostęp: 20 VI 2024].

Bartosz Bochyński

Absolwent studiów licencjackich na Akademii Sztuki Wojennej w Warszawie na kierunku bezpieczeństwo międzynarodowe i dyplomacja.

Kontakt: bbf16@interia.pl