ACTA UNIVERSITATIS WRATISLAVIENSIS
No 4006

Studia nad Autorytaryzmem i Totalitaryzmem 42, nr 2
Wrocław 2020

https://doi.org/10.19195/2300-7249.42.2.11

MARCIN ROJSZCZAK
ORCID: 0000-0003-2037-4301
Politechnika Warszawska
marcin.rojszczak@pw.edu.pl

# Nieograniczone programy inwigilacji elektronicznej a koncepcja państwa autorytarnego

**Abstrakt:** W trwającej od dwudziestu lat dyskusji na temat granic dopuszczalnej inwigilacji w państwach demokratycznych nadal nie wypracowano jednego, powszechnie akceptowalnego stanowiska. Problem ten zajmuje badaczy z różnych dziedzin nauki — zarówno prawa, jak i socjologów czy filozofów. W istocie bowiem pytanie o granice inwigilacji jest pytaniem o definicję państwa, jego ustroju i formy sprawowanej władzy. W ostatnich latach szczególnego znaczenia nabiera dyskusja dotycząca masowej inwigilacji elektronicznej, a więc formy nadzoru, w której gromadzone są hurtowe ilości danych w celu ich dalszej analizy. Masowa inwigilacja w ocenie Komisji Weneckiej musi budzić uzasadnione skojarzenia z formą rządów niedemokratycznych. Jednocześnie jednak zwolennicy stosowania tego środka wskazują na nieuchronność jego stosowania, uwzględniając nowe wyzwania związane z zapewnieniem bezpieczeństwa w cyfrowym świecie.

Celem artykułu jest podjęcie wskazanej tematyki z innej perspektywy badawczej — w szczególności próba odpowiedzi na pytanie, czy niezależnie od wdrożonych zabezpieczeń prawnych sama koncepcja stosowania masowych środków inwigilacji elektronicznej może zostać pogodzona ze sposobem funkcjonowania państwa demokratycznego. Przyczynkiem do tych rozważań jest obserwacja, że inwigilacja tego typu naturalnie może być zastosowana jako mechanizm kontroli społecznej, ograniczania wolności słowa czy wpływania na preferencje wyborcze, to jest do celów, które choć bliskie państwom autorytarnym, są obce demokracji.

**Słowa kluczowe:** inwigilacja elektroniczna, masowa inwigilacja, społeczeństwo nadzorowane, panoptyzm.

## BULK SURVEILLANCE PROGRAMS AND THE CONCEPT OF AUTHORITARIAN STATE

Abstract

The discussion on the limits of scope of permissible surveillance in democratic states, which has been ongoing for twenty years, has not yet developed a single, universally acceptable position.

This problem occupies researchers from various fields of science — both law and sociologists or philosophers. In fact, the question about the limits of surveillance is a question about the definition of the state, its system and form of exercised power. In recent years, the discussion on mass electronic surveillance, i.e. the form of supervision, in which the bulk of data is collected for further analysis, has become particularly important. In the opinion of the Venice Commission, mass surveillance must have reasonable associations with the undemocratic form of government. At the same time, however, supporters of this measure point to the inevitability of its use taking into account the new challenges associated with ensuring public security in the digital world.

The aim of the article is to take up the above subject from a different research perspective — in particular an attempt to answer the question whether, regardless of the legal safeguards implemented, the very concept of using mass electronic surveillance can be reconciled with the functioning of a democratic state. The reason for these considerations is the observation that this type of surveillance can naturally be used as a mechanism of social control, limiting freedom of speech or influencing electoral preferences — that is, for purposes that, although close to authoritarian states, are alien to democracy.

**Keywords:** electronic surveillance, mass surveillance, surveillance society, panopticism.

# Wprowadzenie

Są w filozofii prawa koncepcje o wymiarze ponadczasowym i uniwersalnym. Niektóre z nich, mimo upływu setek lat od momentu ich sformułowania, nie tylko nie tracą na aktualności, ale w nowoczesnym, zdigitalizowanym społeczeństwie zyskują nowy wymiar, pozwalający przedefiniować nasze postrzeganie fundamentalnych pojęć, takich jak wolność czy bezpieczeństwo. Bez wątpienia do koncepcji tego rodzaju można zaliczyć ideę panoptykonu. Jeremy Betham, przedstawiając w XVII swoją wizję więzienia doskonałego, starał się zaprezentować, w jaki sposób dzięki zastosowaniu nowatorskiego — jak na owe czasy — połączenia wiedzy z zakresu psychologii, socjologii oraz architektury można udoskonalić funkcjonowanie systemu penitencjarnego. Panoptykon miał być więzieniem na swój sposób doskonałym, w którym zamiast fizycznej obecności strażników rolę nadzorcy mogliby pełnić sami osadzeni. Strażnicy mieli pozostać niewidoczni, ale — dzięki odpowiedniej konstrukcji budynku — jednocześnie mieć stały wgląd w zachowanie każdego skazanego. A więc to nie fizyczna obecność strażników miała zmusić więźniów do podporządkowania się ustalonym zasadom zachowania, ale poczucie ciągłej i nieustającej kontroli, połączone z niemożliwością weryfikacji, czy kontrola ta faktycznie jest stosowana. Dlatego Michel Foucault widział w propozycji Benthama nie tyle propozycję więzienia doskonałego, ile bardziej ogólną koncepcję kontroli społecznej, w której kluczowym elementem jest wytworzenie przekonania o wszechwiedzy rządzących, pozwalającej na zauważenie wszelkich działań jednostki.

To główny efekt panoptykonu — wzbudzić w uwięzionym świadome i trwałe przeświadczenie o widzialności, które daje gwarancję automatycznego funkcjo-

nowania władzy. Spowodować, by nadzór był nieprzerwanie skuteczny, nawet jeśli będzie nieciągły w działaniu; by doskonałość władzy czyniła zbędnym jego stałe sprawowanie; by ten architektoniczny aparat stał się mechanizmem do tworzenia i podtrzymywania zależności od władzy niezależnie od tego, kto ją sprawuje; słowem, by więźniowie podlegali władzy, której sami są nosicielami[1].

Foucault dostrzega zatem, że nie trzeba pilnować osadzonych, którzy pilnują się sami. I to jest właśnie ostateczny cel panoptykonu — wytworzyć przekonanie, że jakakolwiek forma niesubordynacji zostanie zauważona i ukarana, a przez to przekonać nadzorowanych, że sami powinni się kontrolować.

Z perspektywy drugiej dekady XXI wieku idea panoptykonu zyskała nowy wymiar interpretacji, w którym nowoczesne formy przetwarzania danych oraz wszechobecna cyfryzacja życia powodują, że celem nadzoru nie są więźniowie, ale całe społeczeństwo, poddane nieustannej kontroli i monitorowaniu ze strony organów władzy publicznej. Skoro niewidoczny nadzór może zmienić zachowanie poszczególnych jednostek, to w jaki sposób może wpłynąć na model funkcjonowania społeczeństwa?

W nauce prawa od lat badane jest zjawisko tak zwanego efektu mrożącego. Fenomen ten polega na samoograniczaniu się jednostek w korzystaniu ze swoich praw w obawie przed negatywnymi konsekwencjami, jakie mogą je spotkać ze strony władzy publicznej. Efekt mrożący ma szczególne znaczenie w zakresie praw podstawowych, w tym ochrony prywatności czy prawa do informacji. Unikanie poszukiwania interesujących treści w obawie przed reakcją organów państwa prowadzi do ograniczenia wolności wypowiedzi, co z kolei narusza jeden z fundamentów ustrojowych państwa demokratycznego. Już w XIX wieku John Stuart Mill, rozważając rolę swobody wyrażania poglądów, konstatował, że „żadne społeczeństwo, w którym swobody te nie są, na ogół biorąc, szanowane, nie jest wolne, bez względu na formę jego rządu”[2].

Efekt mrożący jest jednym, ale nie jedynym skutkiem rozbudowanych działań inwigilacyjnych państw, którego negatywne konsekwencje materializują się w przestrzeni praw podstawowych. Jego praktyczny wymiar ocenił Jonathan Penney, który opierając się na danych dotyczących statystyk wyszukiwania informacji w angielskojęzycznej dystrybucji Wikipedii, wykazał, że liczba osób zapoznających się z treściami dotyczącymi prowadzonych programów inwigilacyjnych spadła, a nie, jak można by się było spodziewać, wzrosła po ujawnieniu skali tych programów przez Edwarda Snowdena w 2013 roku[3].

---

[1] M. Foucault, *Nadzorować i karać. Narodziny więzienia*, przeł. T. Komendant, Warszawa 1998, s. 196.

[2] J. Mill, *O wolności*, [w:] *idem*, *Utylitaryzm — O wolności*, przeł. A. Kurlandzka, Warszawa 2006, s. 106.

[3] J. Penney, *Chilling effects: Online surveillance and Wikipedia use*, „Berkeley Technology Law Journal” 31, 2016, s. 117–182.

W ostatnich latach problem masowej inwigilacji stał się przedmiotem szczególnego zainteresowania opinii publicznej. Bez wątpienia przyczyniły się do tego nie tylko powracające informacje o skali działań inwigilacyjnych prowadzonych przez poszczególne państwa, lecz także wzrost świadomości i oczekiwań społecznych w zakresie ochrony prywatności. Także przedstawiciele nauki coraz częściej rozważają konsekwencje masowej inwigilacji nie tylko przez pryzmat jej wpływu na prawa i swobody osobiste, ale również konsekwencji dla prawidłowego rozwoju nowoczesnego społeczeństwa, opartego na wiedzy i informacji.

Celem niniejszego artykułu nie jest jednak analiza legalności stosowania rozbudowanych programów inwigilacyjnych czy wykazanie *de facto* ich nieprzydatności do realizacji celów, którym mają służyć. Tego typu problemy badawcze znalazły już rozwinięcie we wcześniejszych publikacjach autora, zarówno w zakresie omówienia standardów orzeczniczych TSUE i ETPC[4], jak i analizy krajowych przepisów inwigilacyjnych[5], w tym wprowadzonych w Polsce[6]. W pewnym zakresie niniejszy tekst stanowi kontynuację artykułu *Cztery fałszywe hipotezy na temat ochrony prywatności i masowej inwigilacji*, opublikowanego w 2018 roku na łamach „Państwa i Prawa"[7]. O ile jednak przywołane opracowanie było kierowane głównie do prawników, o tyle niniejszy artykuł w zamierzeniu autora — z uwagi na bardziej humanistyczny i interdyscyplinarny charakter — powinien zainteresować szerszy krąg odbiorców, być może prowokując dyskusję na zaprezentowane tematy także badaczy innych dyscyplin naukowych.

Celem rozprawy jest próba poszukiwania odpowiedzi na bardziej ogólny problem: czy samo istnienie rozbudowanych programów inwigilacyjnych, niezależnie od zastosowanych ograniczeń prawnych, jest zagrożeniem prawidłowego funkcjonowania państwa demokratycznego?[8] Można sformułować tę myśl

[4] M. Rojszczak, *Prawne podstawy prowadzenia masowej inwigilacji obywateli opartej na hurtowym i nieukierunkowanym przechwytywaniu danych w UE z uwzględnieniem dorobku orzeczniczego TSUE i ETPC*, „Studia Prawa Publicznego" 2017, nr 2 (18).

[5] Por. omówienie modelu prawnego Stanów Zjednoczonych: M. Rojszczak, *Prywatność w epoce Wielkiego Brata: podstawy prowadzenia programów masowej inwigilacji w systemie prawnym Stanów Zjednoczonych*, „Ius Novum" 2019, nr 1; Wielkiej Brytanii: *idem*, *UK electronic surveillance programmes in the context of protection of EU citizens' rights after Brexit*, „Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego" 16, 2018; Szwecji: *idem*, *The ECtHR's judgment in case of centrum för Rättvisa v. Sweden as a leading case for the review of domestic regulations on signals surveillance*, „Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego" 17, 2019.

[6] M. Rojszczak, *Prywatność a bezpieczeństwo publiczne — podstawy prawne prowadzenia programów masowej inwigilacji obywateli*, [w:] *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019.

[7] M. Rojszczak, *Cztery fałszywe hipotezy na temat ochrony prywatności i masowej inwigilacji*, „Państwo i Prawo" 2018, nr 10, s. 32–49.

[8] Czytelnicy zainteresowani tematyką wpływu uprawnień inwigilacyjnych państwa na model sprawowanych rządów mogą sięgnąć po artykuły opublikowane w numerze tematycznym czasopi-

inaczej: czy inwigilacja prewencyjna jest zatrutym owocem, który nie tylko nie wzmacnia fundamentów państwa demokratycznego, lecz także skutkuje ich erozją i przez samo istnienie zwiększa ryzyko powstania quasi-demokracji, w której zaburzona zostaje równowaga między wolnościami jednostki a uprawnieniami państwa, a stale nadzorowane społeczeństwo ukształtowane zostaje zgodnie z wolą rządzących?

Analiza tak zakreślonej tezy badawczej wymaga jednak choćby skrótowego odniesienia do zagadnień fundamentalnych, dotyczących sposobu rozumienia i definiowania pojęć„inwigilacja" (sekcja 2) oraz „demokracja" (sekcja 3), a także granic dopuszczalnej ingerencji w prawa podstawowe (sekcja 4). Zarówno „inwigilacja", jak i „demokracja" to terminy bardzo pojemne, mające różne znaczenia w zależności od obszaru prowadzonych badań, ale również oczekiwań społecznych oraz przyjętej formy rządów. Dopiero ustalając zakres działań państwa, które można uznać za przejaw realizacji programów inwigilacyjnych, możliwe będzie przeprowadzenie analizy wykazującej ich szkodliwy wpływ na kształt państwa demokratycznego. Odrębnym problemem badawczym wymagającym rozważenia jest skala tego negatywnego wpływu, w szczególności próba oceny, kiedy stopień tego wypaczenia należy uznać za na tyle poważny, że skutkuje powstaniem ułomnych form ustroju państwa, takich jak chociażby tak zwana demokracja nieliberalna czy, w skrajnej formie, państwo autorytarne.

## 1. Definicja i granice inwigilacji elektronicznej

Inwigilacja jako środek niejawnej obserwacji od setek lat jest stosowana do monitorowania aktywności jednostek pozostających w zainteresowaniu organów państwa. Co do zasady można ją podzielić na jednostkową (indywidualną) oraz nieograniczoną (określaną także jako masowa, nieukierunkowana lub hurtowa)[9].

sma „Surveillance & Society" (15, 2017, nr 3), w całości poświęconym temu zagadnieniu (*Surveillance and the Global Turn to Authoritarianism*). Zeszyt dostępny online: https://cli.re/Aam8oR (dostęp: 10.04.2020).

[9] Chociaż przymiotniki „nieukierunkowana" oraz „hurtowa" są stosowane zamiennie przy określaniu cech masowej inwigilacji, w praktyce pojęcia te nie są tożsame. Inwigilacja nieukierunkowana polega na gromadzeniu danych bez stosowania wyróżników pozwalających na wskazanie konkretnych osób, poddanych jej wykorzystaniu. Może zatem obejmować na przykład gromadzenie informacji dotyczących określonych grup społecznych, osób pozostających w związku z konkretnymi grupami politycznymi, religijnymi czy kulturalnymi. Z kolei inwigilacja hurtowa dotyczy sposobu gromadzenia danych i polega na przechwytywaniu wszystkich informacji, jakie mogą być pozyskane w dany sposób (na przykład przez podsłuchiwanie środków komunikacji elektronicznej). Inwigilacja hurtowa zazwyczaj jest nieukierunkowana, z kolei nieukierunkowana zazwyczaj jest realizowana przez techniki hurtowego gromadzenia informacji, ale nie zawsze musi tak być. Przykładem jest niemiecki program inwigilacji strategicznej, w którym przechwytywano całą łączność międzynarodową pomiędzy abonentami zlokalizowanymi na obszarze Niemiec a wybranych państw trzecich, pozostających w zainteresowaniu krajowych służb specjalnych. Zob. także przyp. 33.

Pierwszy rodzaj jest związany z gromadzeniem informacji na temat konkretnych osób lub grup osób, często w związku z prowadzonymi postępowaniami karnymi. Z kolei drugi rodzaj inwigilacji jest immamentnie związany z dynamicznym rozwojem techniki i wprowadzeniem coraz doskonalszych form przetwarzania informacji. Inwigilacja nieograniczona polega na gromadzeniu olbrzymich zbiorów danych (często pochodzących z przechwytywania łączności elektronicznej) w celu ich dalszej analizy. Jest to zatem środek prewencyjny, forma kontroli, w której rejestruje się wszelkie możliwe informacje (zazwyczaj ograniczone wyłącznie możliwościami technicznymi), także (a nawet zazwyczaj) niezwiązane z żadnymi działaniami przestępczymi, które dzięki zaawansowanej analizie mają pomóc w identyfikacji nieznanych wcześniej działań wymierzonych w istotne interesy państwa, takich jak terroryzm, pranie brudnych pieniędzy czy szpiegostwo. O ile przydatność tej formy inwigilacji w zwalczaniu przestępczości jest zagadnieniem nadal kwestionowanym i różnie ocenianym w nauce[10], o tyle nie ma wątpliwości, że jest środkiem przydatnym do realizacji celów kontroli społecznej, takich jak na przykład kształtowanie preferencji wyborczych[11]. Dlatego też niektórzy badacze wprost wskazują, że inwigilacja prewencyjna jest nie tyle środkiem nadzoru, ile narzędziem wypływu[12]. Inwigilacja nieograniczona odwraca zatem paradygmat będący fundamentem prawa karnego, w którym środki opresyjne są odpowiedzią, reakcją organów ścigania na popełnione lub uprawdopodobnione przestępstwo[13]. W inwigilacji nieograniczonej nie ma przestępstwa, a zatem i przestępcy, za to wszyscy mogą być podejrzani i obserwowani.

O ile inwigilacja jednostkowa była prowadzona od wieków, a pojawienie się nowych możliwości gromadzenia danych co najwyżej udoskonaliło tę formę monitorowania aktywności konkretnych osób, o tyle pojawienie się i dynamiczny

[10] Por. M. Cayford, W. Pieters, *The effectiveness of surveillance technology: What intelligence officials are saying*, „The Information Society" 2018, nr 2, s. 88–103; J. Reidenberg, *The data surveillance state in Europe and the United States*, „Wake Forest Law Review" 49, 2014, s. 583–608; M.H. Maras, *How to catch a terrorist: Is mass surveillance the answer?*, „Journal of Applied Security Research" 2010, nr 1, s. 20–41.

[11] W tym zakresie należy pamiętać, że inwigilacja może wpływać wieloaspektowo na proces wyborczy — zarówno sama obecność nadzoru może kształtować zachowania wyborców, jak i dane pozyskane w ten sposób mogą posłużyć do profilowania i przygotowania celowanych kampanii politycznych. Inwigilacja, rozumiana jako gromadzenie danych pozwalających na wnioskowanie w zakresie preferencji wyborczych, jest pojęciem wykraczającym poza działania państwa i obejmuje także środki będące w dyspozycji na przykład koncernów technologicznych. Zob. Z. Tufekci, *Engineering the public: Big data, surveillance and computational politics*, „First Monday" 2014, nr 7 (19), https://cli.re/9295o3 (dostęp: 5.11.2019).

[12] Por. N. Richards, *The dangers of surveillance*, „Harvard Law Review" 126, 2013, s. 1955–1956.

[13] Zob. rezolucja Parlamentu Europejskiego z dnia 12 marca 2014 roku w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych (2013/2188(INI)).

rozwój inwigilacji nieograniczonej jest immamentnie związany z rozwojem techniki. Dlatego też inwigilację nieograniczoną utożsamia się wprost z inwigilacją elektroniczną. Należy jednak pamiętać, że ta forma nadzoru rozwija się znacznie dłużej niż okres ostatnich kilkudziesięciu lat, nie jest więc wyłącznie efektem pojawienia się globalnego rynku usług łączności elektronicznej. Historycznie pierwsze systemy tego typu powstawały w obszarze obronności i bezpieczeństwa narodowego już w połowie XX wieku[14]. Celem ich wdrażania było w większości gromadzenie informacji przydatnych w obszarze polityki zagranicznej i bezpieczeństwa międzynarodowego, dlatego inwigilację elektroniczną do dzisiaj często zalicza się do kategorii zastosowań tak zwanego wywiadu sygnałowego (SIGINT, *signals intelligence*).

Rozwój i postępująca cyfryzacja dotyczą w oczywisty sposób także administracji publicznej. W efekcie każdego roku wdrażanych jest wiele nowych usprawnień w zakresie wykonywania zadań publicznych, które są możliwe wyłącznie dzięki zastosowaniu nowych, zaawansowanych form przetwarzania danych, w tym wykorzystujących takie techniki jak analityka *big data* lub uczenie maszynowe. Coraz częściej możliwości tych systemów są na tyle duże, że formułowane jest pytanie o możliwość ich zastosowania do innych celów, w tym pozaprawnych, związanych z inwigilacją konkretnych osób lub całych grup społecznych. Nie budzi wątpliwości, że podsłuch łączności elektronicznej to środek inwigilacyjny. Ale czy rozbudowane systemy wdrażane w ramach projektów inteligentnych miast również mogą być klasyfikowane w ten sposób? Jakie warunki muszą być spełnione, aby można było uznać projekt instalacji rozbudowanego systemu monitoringu wizyjnego za mający potencjał inwigilacyjny? W ostatnich miesiącach, na tle walki z pandemią koronawirusa, opinia publiczna poinformowana została o nowych formach monitorowania stosowanych w Chinach, wykorzystujących systemy monitoringu wizyjnego do typowania osób, które mogą być nosicielami choroby zakaźnej[15]. Abstrahując od oceny przydatności tego środka do celów walki z pandemią, należy podkreślić, że przykład ten obrazuje, w jaki sposób organy państwa, wprowadzając mechanizmy nadzoru do przestrzeni publicznej, mogą zmienić ich cel i charakter, dostosowując sposób wykorzystania do aktualnych potrzeb.

Przedstawione rozważania prowadzą do ważnej obserwacji: oceniając działania państwa w zakresie nadzoru nad aktywnością jednostek, konieczne jest zwrócenie uwagi nie tylko na środki, które bezpośrednio służą inwigilacji, lecz także na takie, które służąc innym zastosowaniom, mają faktyczny potencjał inwigilacyjny. Myśl tę trafnie podsumował David Lyon, wskazując, że możliwości

[14] Jednym ze znanych przykładów jest system globalnego nasłuchu łączności, znany pod nazwą ECHELON. Więcej na temat programu zob. L. Sloan, *ECHELON and the legal restraints on signals intelligence: A need for reevaluation*, „Duke Law Journal" 50, 2001, s. 1467–1510.

[15] Zob. L. Kuo, *'The new normal': China's excessive coronavirus public monitoring could be here to stay*, „The Guardian" 9.03.2020, https://cli.re/zPDZzd (dostęp: 10.04.2020).

inwigilacyjne określonego systemu „mogą być produktem ubocznym, uzupełnieniem lub nawet niezamierzoną konsekwencją innych procesów i praktyk; czasami dopiero po wdrożeniu jakiegoś systemu, tworzonego w innym celu, ujawnia się jego potencjał inwigilacyjny”[16].

Jak zatem zdefiniować ów „potencjał inwigilacyjny”? Jakkolwiek postulat Lyona jest trafny, to jednocześnie jego bezkrytyczne przyjęcie może spowodować, że niemal każda nowa aktywność władz publicznych w obszarze nowoczesnych technologii może być interpretowana i rozpatrywana jako mająca możliwy wymiar inwigilacyjny. W tym zakresie pomocna może być definicja zaproponowana przez Neila M. Richardsa, który opierając się na wcześniejszych pracach Lyona, wskazał cztery charakterystyczne cechy środków inwigilacyjnych: 1. skoncentrowanie na pozyskiwaniu informacji na temat jednostek; 2. systematyczność — definiowana jako cykliczne, okresowe podejmowanie obserwacji; 3. rutynowy charakter, to znaczy taki, który jest częścią działań normalnie podejmowanych przez organy państwa; 4. posiadanie określonego celu, którym, jak podaje Richards, rzadko jest wprowadzenie lub utrwalenie niedemokratycznego modelu władzy[17]. W takim rozumieniu system, który pozwala na systematyczne i rutynowe gromadzenie rozbudowanych informacji na temat jednostek, ma potencjał inwigilacyjny, nawet jeżeli w momencie jego wdrożenia taki cel nie jest deklarowany[18].

Inwigilacja elektroniczna to oczywiście nie tylko domena państw. Duże koncerny technologiczne mają możliwości profilowania użytkowników daleko wykraczające poza środki będące w dyspozycji organów publicznych większości państw. Jednocześnie podział na środki inwigilacji publicznej oraz prywatnej jest pozorny — organy ścigania oraz służby specjalne mogą korzystać z baz danych gromadzonych przez koncerny technologiczne, korzystając w tym celu zarówno z uprawnień wynikających z procedury karnej (zazwyczaj związanej z inwigilacją indywidualną), jak i — co bardziej niepokojące — także w obszarze realizacji celów bezpieczeństwa narodowego[19].

---

[16] D. Lyon, *Surveillance, power, and everyday life*, [w:] *The Oxford Handbook of Information and Communication Technologies*, red. R. Mansell *et al*., Oxford 2009. Tłum. M.R.

[17] Zob. N.M. Richards, *op. cit*., s. 1937.

[18] Systemem inwigilacyjnym będzie zatem system monitorowania przestrzeni publicznej, jeżeli zakres gromadzonych przez niego danych pozwoli na identyfikację jednostek (na przykład będzie korzystał z algorytmów rozpoznawania twarzy lub korelacji z innymi źródłami danych, na przykład geolokalizacją urządzeń abonenckich). Nie będzie nim jednak system kamer miejskich, jeżeli rejestrowany obraz nie pozwala na łatwe (automatyczne) przeszukiwanie rejestrowanych obrazów według identyfikatorów osobowych.

[19] Zob. szerzej I. Rubinstein, G. Nojeim, R. Lee, *Systematic government access to personal data: A comparative analysis*, „International Data Privacy Law” 2014, nr 2, s. 96–119; I. Brown, *Government access to private-sector data in the United Kingdom*, „International Data Privacy Law” 2012, nr 4, s. 230–238.

Oceniając skutki inwigilacji, nie sposób pominąć ewentualnego znaczenia jej nasilenia na potencjalne skutki dla praw i wolności osobistych. Zwolennicy stosowania nowoczesnych środków analitycznych, często mających potencjał inwigilacyjny, wskazują, że państwo nie może być bezbronne w walce z takimi zjawiskami jak wyłudzenia skarbowe czy poważna przestępczość. Na tej podstawie formują wniosek, że środki nadzoru stosowane w zakresie retencji danych telekomunikacyjnych czy monitorowania operacji finansowych nie mogą być porównywane z mechanizmami totalnej inwigilacji stosowanymi w państwach niedemokratycznych[20]. Z perspektywy niniejszej pracy takie rozróżnienie jest jednak bezcelowe; istotne jest, czy organy państwa poprzestają na gromadzeniu danych koniecznych do wykonywania swoich zadań, czy decydują się na gromadzenie danych nadmiarowych. Każdy przypadek gromadzenia danych nadmiarowych (co jest normą w wypadku środków prewencyjnych) *per se* dowodzi naruszenia zasady konieczności. Gromadząc dane pozostające bez związku z celem przetwarzania, organy państwa przekraczają granicę między inwigilacją indywidualną a nieukierunkowaną.

Współczesne formy inwigilacji elektronicznej nie powinny być zatem interpretowane wyłącznie przez pryzmat konkretnego, wąskiego obszaru zastosowań (na przykład przechwytywanie łączności elektronicznej), jak również wiązane wyłącznie z działaniami podejmowanymi przez wyspecjalizowane służby specjalne. Aby jednak skonkretyzować przedstawione w niniejszej pracy rozważania, w dalszej części artykułu pod pojęciem nieukierunkowanej (masowej) inwigilacji elektronicznej rozumiane będą środki pozwalające na gromadzenie rozbudowanych (nadmiarowych) informacji na temat aktywności podejmowanych przez duże grupy społeczne (potencjalnie: całe społeczeństwo), przy czym bez znaczenia jest, czy dane te zostały bezpośrednio zgromadzone przez organy publiczne[21]. W ten sposób z zakresu dalszej analizy wyłączone zostają systemy,

[20] Wbrew pozorom podział ten w wielu przypadkach może być iluzoryczny i niezwiązany z faktycznymi możliwościami technicznymi organów poszczególnych państw. W literaturze, także naukowej, Chiny przywoływane są jako przykład państwa, w którym mechanizmy inwigilacji zostały rozbudowane ponad poziom dotychczas znany. W tym samym jednak czasie w jednym z funkcjonujących w Polsce systemów administracji publicznej, służących do automatycznego gromadzenia i przetwarzania informacji pochodzących z krajowego systemu finansowego (w tym informacji o przelewach bankowych, saldach kont itp.) w latach 2016–2018, zgromadzono ponad 6 mld informacji o przeprowadzonych operacjach finansowych — J. Sarnowski, P. Selera, *Reducing the VAT gap: Lessons from Poland*, Polish Economic Institute 2019, s. 31, https://cli.re/bxx1BA (dostęp: 10.04.2020). Jest to wielkość porównywalna do ludności świata, przy czym w Polsce mieszka niecałe 39 mln ludzi. W erze analityki *big data* i przetwarzania dużych zbiorów danych nawet system informatyczny gromadzący wąski zakres informacji może z powodzeniem zostać wykorzystany do szczegółowego profilowania osób objętych monitoringiem.

[21] Należy pamiętać, że dane mogą być gromadzone nie tylko bezpośrednio przez organy publiczne, lecz także na ich zlecenie lub — co ma szczególne znaczenie w sektorze łączności elektronicznej — mogą przez podmioty prywatne w ramach wykonania ciążącego na nich obowiązku prawnego. Z perspektywy niniejszego artykułu nie jest ważne, kto i w jaki sposób zgromadził dane,

które co prawda służą monitorowaniu aktywności podejmowanych przez jednostki, ale nie pozwalają na gromadzenie danych nadmiarowych, a ich charakter jest ściśle powiązany z prawnie uznanym celem, do którego zostały ustanowione.

## 2. Państwo demokratyczne a autorytarne

Nie istnieje jedna, powszechnie akceptowalna definicja państwa demokratycznego. Z pewnością może być trudno wypracować taką definicję w dzisiejszych czasach, uwzględniając mozaikę różnych form ustroju państwa funkcjonujących na świecie, w których podobne zasady i cele zostały wyważone w odmienny sposób. Bez problemu można jednak wskazać pewne kluczowe koncepcje i zasady, które znajdują się pod ochroną państwa demokratycznego, jak również odstępstwa od nich, mogące wskazywać, że praktykowany model rządów nie powinien być już uznawany za demokratyczny. Z uwagi na pojemność tej tematyki zostanie ona przedstawiona wyłącznie w zarysie potrzebnym do zachowania spójności rozważań przedstawionych w niniejszym tekście.

Sposobem odróżnienia demokracji od autokracji jest odniesienie się do kompetencji i uprawnień organów władzy publicznej. W państwach demokratycznych prawa mają jednostki, organy publiczne natomiast mają tylko takie uprawnienia, które są niezbędne do wykonywania zadań powierzonych im przez prawo (umowę społeczną). Zwierzchnia rola narodu oznacza także służebną rolę organów państwa, których nadrzędnym celem jest poszanowanie praw i wolności osobistych. Z kolei jeżeli rządzący nie uznają się za skrępowanych ograniczeniami prawnymi w realizacji swoich celów politycznych, sprawowana przez nich władza nie może zostać uznana za mającą mandat demokratyczny.

Współcześnie uznaje się, że sposobem zapewnienia trwałości demokracji i ochrony społeczeństwa przed rozszerzaniem się uprawnień państwa w sposób zwiększający ryzyko nadużycia władzy jest zorganizowanie modelu rządów z wykorzystaniem wielu zabezpieczeń prawnych (*checks and balances*), z których najważniejszymi są zasada rządów prawa oraz podział władzy. Oba zabezpieczenia mają także kluczowe znaczenie dla ograniczania uprawnień inwigilacyjnych państwa: poszanowanie reguły rządów prawa wymaga, aby wszelkie ograniczenia w przestrzeni praw podstawowych uwzględniały zasadę konieczności i proporcjonalności; z kolei trójpodział władzy wyklucza możliwość stosowania opresyjnych środków, takich jak inwigilacja elektroniczna, wyłącznie wolą egzekutywy.

Prawdą jest jednak, że — zwłaszcza współcześnie — coraz popularniejszy staje się pogląd, że demokracja ukształtowana z zachowaniem tego typu zabezpieczeń prawnych nie jest efektywna, jakoby ograniczając rządzących w realizacji

ale czy informacje te mogą być legalnie wykorzystane przez podmioty publiczne do realizacji ich własnych celów.

postulatów i programów, które głosili, zyskując mandat wyborczy. Zwolennicy takiej koncepcji wskazują, że zakres ograniczeń i zabezpieczeń prawnych nie może uniemożliwiać czy znacząco utrudniać skutecznego rządzenia, nierzadko wymagającego podejmowania głębokich strukturalnych reform. W takim ujęciu głównym zadaniem rządzących powinna być realizacja swoich deklaracji wyborczych, a mechanizmy kontroli państwa — ustanowione w celu równoważenia ryzyka nadużycia władzy (takie jak niezależne organy administracji czy sądy) — nie powinny utrudniać tego zadania. Argumentację tego typu przedstawiają między innymi zwolennicy tak zwanego modelu demokracji nieliberalnej, a więc formy ustroju przyznającej rządzącym znacznie większą swobodę nieskrępowanego działania przy jednoczesnym utrzymaniu demokratycznych zasad wyboru organów władzy publicznej[22]. W istocie jednak demokracja nieliberalna jest oksymoronem: demokracja, która nie jest liberalna — to jest taka, w której prawo nie jest narzędziem ochrony jednostki przed imperium władzy państwowej — nie jest demokracją. Jest upośledzoną, niepełną wersją rządów autorytarnych[23]. Nie wymaga szerszego wyjaśnienia, że mandat organów władzy pochodzący z wolnych wyborów nie przesądza o formie sprawowanych rządów. Podobnie sam fakt zgodności decyzji rządzących z wolą większości społeczeństwa nie dowodzi demokratycznego ustroju państwa. Historia ludzkości — także ta nieodległa i łącząca się z tragicznymi doświadczeniami związanymi z nazizmem — zawiera wiele przykładów, że demokracja nieliberalna jest niczym innym jak pełzającą formą dyktatury. Dlatego rację ma Tony Bunyan, podnosząc, że obserwowane obecnie przemiany mogą wskazywać na przejście do nowej ery, którą nazywa „demokratycznym autorytaryzmem"[24]. W ustroju tym definiowana na nowo zasada rządów prawa i erozja transparentności oraz rozliczalności organów władzy przed obywatelami ma prowadzić do podważenia koncepcji kontroli demokratycznej.

Skoro rządy demokratyczne charakteryzują się służebną rolą organów państwa, to w sposób oczywisty w modelu tym rządzący wyposażeni są tylko w takie uprawnienia i przywileje, które są im niezbędne, a nie przydatne, aby realizować swoje zadania. Przenosząc tę tezę na grunt problematyki rozbudowanych

[22] Fareed Zakaria jako jeden z pierwszych zdefiniował w ten sposób demokrację nieliberalną, porównując sposoby sprawowania rządów w wielu tak zwanych słabych demokracjach. W przypadku takich ustrojów demokracja miała być postrzegana jako system wyboru organów władzy w drodze demokratycznych wyborów. Natomiast w czasie pomiędzy wyborami rządzący mogli niemal dowolnie sprawować swój mandat, z pominięciem kontroli i podziału władz. Por. Ł. Kołtuniak, *Nieliberalna demokracja a państwo prawa. Przypadek Węgier Wiktora Orbana*, „Internetowy Przegląd Prawniczy TBSP UJ" 2017, nr 8 (38), s. 173–178.

[23] Podobnie wskazuje Andrzej Antoszewski, uznając, że „demokracją nieliberalną jest pewien stan przejściowy, nieuchronnie prowadzący albo do restauracji demokracji liberalnej, albo też do mniej lub bardziej zaawansowanego autorytaryzmu" — *idem*, *Demokracja nieliberalna jako projekt polityczny*, „Przegląd Europejski" 2018, nr 2, s. 26.

[24] T. Bunkyan, *Just over the horizon — the surveillance society and the state in the EU*, „Race and Class" 51, 2010, nr 3, s. 8–9.

programów inwigilacyjnych, oznacza to, że organy władzy publicznej gromadzące dane nadmiarowe, a więc takie, których nie można uznać za niezbędne do wykonywania zadań publicznych, nie służą społeczeństwu, ale realizują własne cele. Model państwa, w którym taka aberracja jest możliwa i akceptowalna, z pewnością nie może być uznany za w pełni demokratyczny.

Jednym z największych dorobków nauki prawa XX wieku jest zdefiniowanie i ugruntowanie ponadnarodowego systemu ochrony praw człowieka. Uznanie, że istnieje kanon praw podstawowych, niezbywalnych i przynależnych jednostce niezależnie od woli rządzących, był ważnym krokiem na drodze ku budowie nowoczesnego społeczeństwa. Poszanowanie godności człowieka jako źródła wszelkich praw i wolności jednostki powinno być stałym wyróżnikiem działalności państwa. W efekcie każde prawo, niezależnie jak potrzebne by nie było w ocenie rządzących czy oczekiwane i akceptowane przez część czy nawet większość społeczeństwa, nie zasługuje na uchwalenie, jeżeli nie szanuje tej godności. W dzisiejszych czasach — w dobie masowego profilowania setek milionów użytkowników Internetu — zbyt rzadko pamiętamy, że podstawą demokracji jest właśnie poszanowanie godności człowieka.

## 3. Granice dopuszczalnej inwigilacji w państwach demokratycznych

Prawo do prywatności nie jest prawem absolutnym, a zakres i sposób wprowadzanych ograniczeń zależy od przyjętego modelu prawnego. Także wyważenie prawnej ochrony prywatności oraz innych praw podstawowych, takich jak prawo do bezpieczeństwa, może być zapewniane w odmienny sposób przez poszczególnych prawodawców.

Pierwszym aktem prawnomiędzynarodowym, który wprowadzał prawnie wiążące zobowiązania w zakresie poszanowania prywatności była Europejska Konwencja Praw Człowieka (EKPC). Z uwagi na jej duże, ponadregionalne znaczenie w utrwalaniu zasad ochrony praw podstawowych, a przez to wzmacnianie rządów demokratycznych, a także bogate orzecznictwo Europejskiego Trybunału Praw Człowieka (ETPC) w zakresie interpretacji jej postanowień zasadne wydaje się przybliżenie kryteriów, jakie muszą zostać spełnione, aby działania inwigilacyjne państwa można uznać za mieszczące się w ramach tego, co jest dopuszczalne w państwie demokratycznym.

ETPC wielokrotnie zajmował się problematyką tajnych programów inwigilacyjnych. W jednym ze swoich pierwszych orzeczeń wydanych w tym zakresie Trybunał uznał, że każdy przypadek gromadzenia danych przez organy władzy publicznej prowadzi do ingerencji w prawo do prywatności[25]. W tym zakresie

[25] Wyrok ETPC z 16 lutego 2000 roku, *Amann v. Szwajcaria*, skarga nr 27798/95, ECHR 2000-II, pkt 70. Wyroki ETPC dostępne w bazie online: https://hudoc.echr.coe.int/.

nie ma znaczenia, czy zgromadzone dane były dalej przetwarzane (wykorzystane przez organy państwa) ani jaki był zamierzony cel takiego przetwarzania[26]. Jednak sam fakt stwierdzenia ingerencji nie przesądza o jej nielegalności. Dopuszczalna jest ingerencja wprowadzona przepisami rangi ustawowej oraz konieczna w demokratycznym państwie prawa. Trybunał w wielu orzeczeniach wyjaśnił, że pierwszy warunek należy utożsamiać nie tyle z wprowadzeniem ograniczenia w regulacjach ustawowych, ale ze spełnieniem szerszego kryterium, tak zwanej przewidywalności prawa. Oznacza to, że osoba, która może stać się podmiotem inwigilacji, musi mieć możliwość oceny, jakie jej aktywności mogą spotkać się z zastosowaniem środków nadzorczych ze strony państwa[27]. W tym zakresie Trybunał podkreślił znaczenie zasady rządów prawa jako fundamentu ograniczającego ryzyko nadużycia władzy poprzez ustanowienie odpowiednich zabezpieczeń proceduralnych stojących na przeszkodzie w stosowaniu środków inwigilacyjnych bez zewnętrznej, niezależnej kontroli.

W orzecznictwie ETPC można też odnaleźć szczegółowe wskazówki w zakresie interpretacji kryterium „konieczności w demokratycznym społeczeństwie". W tym zakresie Trybunał wprowadził odrębne pojęcie, jakim jest „ścisła konieczność" [28]. Spełnienie warunku ścisłej konieczności przy zarządzeniu środków inwigilacyjnych wymaga nie tylko, aby informacje, które mają być pozyskane, były niezbędne z uwagi na prowadzone postępowanie karne, lecz także aby celów dowodowych nie można było zrealizować w inny, mniej inwazyjny sposób. W swoim standardzie orzeczniczym Trybunał wskazał również zestaw szczegółowych zabezpieczeń prawnych, które powinny funkcjonować w prawie krajowym, aby stosowanie środków inwigilacyjnych nie prowadziło do naruszenia zasady proporcjonalności i konieczności, a w efekcie nie wykraczało poza to, co jest niezbędne w demokratycznym społeczeństwie. Zabezpieczenia te dotyczą między innymi funkcji niezależnego nadzoru nad stosowaniem inwigilacji, dostępności ścieżki sądowej dla osób poddanych takim środkom, ograniczenia możliwości zarządzenia inwigilacji do przypadków najpoważniejszych przestępstw czy ustalenia procedur postępowania ze zgromadzonymi informacjami, gdy nie są one już potrzebne lub okazały się nieprzydatne dowodowo[29].

Z perspektywy podejmowanej tematyki badawczej szczególnie interesujące są sprawy, w których Trybunał zajmował się przypadkami programów nieograniczonej inwigilacji. W tym zakresie przywołania wymagają trzy sprawy — dotyczące

[26] Wyrok ETPC z 25 marca 1998, *Kopp v. Szwajcaria*, skarga nr 13/1997/797/1000, ECHR 1998-II, pkt 53.

[27] Postanowienie ETPC z 26 czerwca 2006 roku, *Weber i Saravia v. Niemcy*, skarga nr 549 34/00, ECHR 2006-XI, pkt 92–94.

[28] Wyrok ETPC z 12 stycznia 2016 roku, *Szabó i Vissy v. Węgry*, skarga nr 37138/14, pkt 73.

[29] Standard ETPC został szerzej omówiony w M. Rojszczak, *Prawne podstawy prowadzenia masowej inwigilacji*…, s. 177–182.

badania niemieckich[30], szwedzkich[31] i brytyjskich[32] przepisów inwigilacyjnych. W każdej ze spraw dokonano szczegółowej analizy prawa krajowego wraz ze wskazaniem, w jaki sposób prawodawca wprowadził poszczególne zabezpieczenia prawne oraz czy praktyka ich stosowania potwierdza ich skuteczność. Wyrok dotyczący przepisów szwedzkich i brytyjskich został wydany niedawno, bo w 2018 roku, jednak na skutek zastosowanych środków odwoławczych obie sprawy zostały przekazane do rozpoznania przez Wielką Izbę. Szczególnie interesujący jest kazus przepisów szwedzkich, które były wielokrotnie modernizowane i dostosowywane do orzecznictwa ETPC i TSUE. W efekcie ETPC uznał zgodność przepisów szwedzkich z konwencją — jest to pierwszy tego typu wyrok wydany od ponad 10 lat, w którym Trybunał potwierdził możliwość stosowania przepisów krajowych ustanawiających reżim hurtowej inwigilacji elektronicznej[33].

Trybunał w swoich orzecznictwie wyważa cele stojące za potrzebą prowadzenia rozbudowanych programów inwigilacyjnych z potrzebą ochrony praw jednostki. W tym zakresie potwierdza, że ochrona bezpieczeństwa publicznego przed najpoważniejszymi przestępstwami, takimi jak na przykład międzynarodowy terroryzm, jest zadaniem wpisującym się w koncepcję państwa demokratycznego. Zauważa też, że z perspektywy realizacji tego zadania przydatne może być prowadzenie tajnych programów inwigilacji. Przydatność ta nie przesądza jednak o konieczności stosowania tego typu środków, zwłaszcza gdy inwigilacja ma mieć charakter prewencyjny i zamiast służyć gromadzeniu dowodów w konkretnych sprawach, ma pomagać w budowaniu represyjnego modelu społeczeństwa. Dlatego też w sprawie *Roman Zakharow v. Rosja* Trybunał podkreślił, że tajne programy inwigilacji, stanowione z myślą o ochronie ważnych interesów państwa, mają potencjał do jego osłabienia, a nawet zniszczenia zasad demokracji[34].

Prawdą jest, że dotychczasowe orzecznictwo ETPC nie przesądza o niezgodności stosowania nieograniczonej inwigilacji elektronicznej z postanowieniami konwencji. Jednocześnie zawiera wiele wskazówek, które mogą prowadzić do takiego wniosku[35]. Intersującym przykładem jest wyrok w sprawie *Centrum för Rättvisa v. Szwecja*, w którym Trybunał potwierdził prawidłowość modelu

[30] *Weber i Saravia v. Niemcy*, zob. przyp. 27.

[31] Wyrok ETPC z 19 czerwca 2018 roku, *Centrum för Rättvisa v. Szwecja*, skarga nr 35252/08..

[32] Wyrok ETPC z 13 września 2018 roku, *Big Brother Watch v. Wielka Brytania*, skargi nr 581 70/13, 62322/14 i 24960/15.

[33] Wcześniej taka decyzja została wydana w sprawie *Weber i Saravia v. Niemcy*, w której Trybunał wprowadził pojęcie tak zwanego monitoringu strategicznego — środka inwigilacyjnego łączącego cechy inwigilacji indywidualnej oraz nieukierunkowanej. Obecnie legalność także tej formy inwigilacji jest kwestionowana, zob. C. Schaller, *Strategic surveillance and extraterritorial basic rights protection: German intelligence law after Snowden*, „German Law Journal" 18, 2018, s. 941–980.

[34] Wyrok ETPC z 4 grudnia 2015 roku, *Roman Zakharov v. Rosja*, skarga nr 47143/06, pkt 232.

[35] Zob. np. wyrok ETPC z 18 maja 2010 roku, *Kennedy v. Wielka Brytania*, skarga nr 26839/05, pkt 160, w którym Trybunał wskazał na brak możliwości hurtowego gromadzenia da-

prawnego przyjętego w Szwecji w zakresie stosowania nieograniczonej inwigilacji. Sprawa ta była szeroko komentowana w mediach jako przykład dowodzący możliwości stosowania nieograniczonej inwigilacji w zgodzie z zasadami ochrony praw człowieka. Taki wniosek nie odzwierciedlałby jednak faktycznej treści wydanego orzeczenia. Dość powiedzieć, że zakres zabezpieczeń wprowadzonych w prawodawstwie szwedzkim powoduje, że mechanizmy inwigilacji przypominają bardziej inwigilację ukierunkowaną (jednostkową), nie zaś nieukierunkowaną. Wątpliwości związane z zakresem dopuszczalnej ingerencji w prawo do prywatności przez nowoczesne formy inwigilacji elektronicznej stały się przyczyną skierowania do Trybunału kolejnych skarg[36] — niewykluczone, że wyroki, które zapadną w efekcie ich rozpoznania, pozwolą na wyjaśnienie części niejasności formułowanych w tym zakresie.

Omawiając kwestię granic dopuszczalnej inwigilacji w państwach demokratycznych oraz jej wpływu na przestrzeń praw podstawowych, nie sposób pominąć odniesienia do orzecznictwa TSUE. Z uwagi na ograniczenie w stosowaniu prawa UE w obszarze bezpieczeństwa narodowego[37]zakres spraw rozstrzyganych przed Trybunałem Luksemburskim nie obejmuje wprost kwestii zgodności stosowania takich środków jak masowe przechwytywanie łączności z Kartą praw podstawowych[38]. TSUE wypracował natomiast własną linię orzeczniczą w zakresie zgodności z prawem UE tak zwanego ogólnego obowiązku retencji danych. W serii precedensowych rozstrzygnięć Trybunał uznał niezgodność z prawem UE zarówno tak zwanej dyrektywy retencyjnej[39], jak i krajowych przepisów nakładających obowiązek retencji danych na operatorów telekomunikacyjnych[40]. Argumentacja

---

nych jako jedną z przesłanek do uznania, że ówczesne brytyjskie przepisy inwigilacyjne nie naruszały postanowień konwencji.

[36] Obecnie na rozpoznanie czekają sprawy dotyczące oceny między innymi francuskich (na przykład skarga nr 49526/15) oraz austriackich (skarga nr 3599/10) przepisów inwigilacyjnych. Dodatkowo na rozstrzygnięcie czeka także skarga złożona przez organizacje pozarządowe (*Privacy International v. Wielka Brytania*, skarga nr 46259/16), w których ponownie kwestionowane są regulacje brytyjskie.

[37] Co do zasady z zakresu prawa UE wyłączona jest działalność państw w obszarze bezpieczeństwa narodowego (por. art. 4 ust. 2 TUE). Ponieważ termin „bezpieczeństwo narodowe" nie został zdefiniowany w traktatach oraz w orzecznictwie TSUE, zakres jego interpretacji od lat jest przedmiotem dyskusji. Należy jednak pamiętać, że zgodnie z ugruntowanym orzecznictwem Trybunału „chociaż to do państw członkowskich należy podjęcie środków zmierzających do zagwarantowania ich bezpieczeństwa zewnętrznego i wewnętrznego, nie wynika z tego, że takie środki nie są wcale objęte zastosowaniem prawa wspólnotowego" — wyrok TSUE z 15 grudnia 2009 roku, *Komisja v. Włochy*, C-387/05, EU:C:2009:781, pkt 45).

[38] Trybunał wypowiadał się pośrednio o zgodności z prawem UE środków zakładających nieograniczone przetwarzanie danych użytkowników. Por. np. wyrok TSUE z 6 października 2015 roku, *Schrems*, C-362/14, EU:C:2015:650.

[39] Wyrok TSUE z 8 kwietnia 2014 roku, *Data Rights Ireland*, C-293/12 i C-594/12, EU:C:2014:238.

[40] Wyrok TSUE z 21 grudnia 2016 roku, *Tele 2 Sverige*, C-203/15 i C-698/15, EU:C:2016:970.

przyjęta w kolejnych rozstrzygnięciach opierała się na na wskazaniu nieproporcjonalności oraz konieczności stosowania środka, jakim jest nieukierunkowane gromadzenie szerokiego zakresu metadanych dotyczących łączności elektronicznej, w odniesieniu do wszystkich abonentów oraz wykonywanych przez nich połączeń. Chociaż przepisy dopuszczające stosowanie retencji są nadal stosowane w wielu państwach członkowskich (w tym w Polsce)[41], a stanowisko Trybunału w tym zakresie może się zmienić w przyszłych orzeczeniach[42], dotychczasowe orzecznictwo wskazuje na niemożliwość pogodzenia z prawem UE stosowania przez organy władzy publicznej środków nadzoru bazujących na hurtowym i nieograniczonym rejestrowaniu danych elektronicznych.

## 4. Inwigilacja prewencyjna a erozja demokracji

Kwestia zgodności programów nieograniczonej inwigilacji ze standardami ochrony praw człowieka jest problemem istotnym i aktualnym. Współcześnie, dzięki postępowi techniki skutkującym większą dostępnością tego typu systemów, narzędzia służące nieograniczonej inwigilacji są przedmiotem obrotu tak jak inne zaawansowane systemy informatyczne[43]. W efekcie w dyskursie coraz

[41] Zob. A. Lach, *Obowiązek retencji danych telekomunikacyjnych i udostępniania tych danych organom ścigania*, „Monitor Prawniczy" 2017, nr 1, s. 612–616; P. Brzeziński, *Stanowisko wybranych sądów konstytucyjnych państw członkowskich UE/WE w sprawie zgodności regulacji implementujących dyrektywę 2006/24/WE z prawami podstawowymi*, „Ius Novum" 2017, nr 1, s. 76–83; *National Data Retention Laws since the CJEU's Tele-2/Watson Judgment*, „Privacy International" 2017, s. 12–13, http://cli.re/68zdoe (dostęp: 10.04.2020).

[42] Na szczególną uwagę zasługują sprawy dotyczące brytyjskich (C-623/17) i belgijskich (C-520/18) przepisów ustanawiających możliwość dostępu do danych gromadzonych w celach realizacji bezpieczeństwa narodowego. Są to zatem sprawy, w których Trybunał będzie musiał przeprowadzić interpretację wyłączenia przewidzianego w art. 4(2) TUE w kontekście swojej wcześniejszej linii orzeczniczej, dotyczącej niezgodności z prawem UE ogólnego obowiązku retencji danych. W obu sprawach w styczniu 2020 roku opinię wydał rzecznik generalny Sánchez-Bordon, który zarekomendował podtrzymanie dotychczasowego stanowiska Trybunału także w przypadku przepisów krajowych ustanowionych „nie tylko w nie tylko w celu prowadzenia dochodzenia, wykrywania i ścigania przestępstw poważnych lub o mniejszej wadze, lecz także w celu zapewnienia bezpieczeństwa narodowego, obrony terytorium, bezpieczeństwa publicznego, zapobiegania nieuprawnionemu korzystaniu z systemu łączności elektronicznej" — por. opinia w sprawie C-520/18, pkt 155.

[43] Zob. Ch. Fuchs, *Societal and ideological impacts of Deep Packet Inspection (DPI) internet surveillance*, „Information, Communication and Society" 16, 2013, nr 8, s. 1328–1359, DOI: 10.1080/1369118X.2013.770544. Skala zjawiska spowodowała, że w sprawie wypowiedział się także Specjalny Sprawozdawca ONZ ds. wolności wypowiedzi, który zaproponował wprowadzenie uregulowań ograniczających swobodny obrót tego typu technologiami, tak aby ograniczyć możliwość ich wykorzystania do celów walki politycznej. Zob. T. Miles, *U.N. surveillance expert urges global moratorium on sale of spyware*, „Reuters" 18.07.2019, https://cli.re/YMNNoN (dostęp: 5.11.2019).

rzadziej podejmuje się kwestię, czy inwigilacja tego typu w ogóle powinna być środkiem stosowanym w państwach demokratycznych, zamiast tego koncentrując się na wskazywaniu, jakie zabezpieczenia prawne powinny być wprowadzone, aby ograniczyć ryzyka z nią związane. Nie ma jednak żadnych przekonujących dowodów dotyczących konieczności stosowania nieograniczonej inwigilacji[44]. Istnieją natomiast przesłanki wskazujące, że społeczeństwo pozbawione tej formy nadzoru będzie rozwijało się lepiej i w pełniejszy sposób korzystało z dobrodziejstw ery informacji.

### a) Inwigilacja przyzwyczaja społeczeństwo do stosowania środków autorytarnych

Historycznie programy masowej inwigilacji były rozwijane jako kontynuacja działań wywiadu elektronicznego. W efekcie odpowiedzialność za ich prowadzenie przypisywano bądź agencjom wyspecjalizowanym w prowadzeniu działań z zakresu rozpoznania elektronicznego (na przykład w USA, Wielkiej Brytanii czy Szwecji), bądź służbom specjalnym odpowiadającym za obszar bezpieczeństwa wewnętrznego (na przykład we Francji czy Niemczech). W każdym wypadku środki te znajdowały się jednak poza strukturami organów ścigania, a nadzór nad ich stosowaniem nie był regulowany procedurą karną. Działalność agencji wywiadowczych cechuje niejawność podejmowanych działań, co wydaje się zrozumiałe, biorąc pod uwagę, że od wieków działalność wywiadowcza i kontrwywiadowcza jest istotnym elementem mającym wpływ na bezpieczeństwo państwa. Czym innym jest jednak podejmowanie działań wywiadowczych rozumianych w sposób tradycyjny, a więc ukierunkowanych na pozyskiwanie wiedzy i rozpoznawanie zagrożeń zewnętrznych lub o charakterze międzynarodowym, a czym innym gromadzenie danych o znaczeniu *stricte* wewnętrznym. W państwach demokratycznych służby wywiadowcze mają zazwyczaj ustawowy zakaz prowadzenia działalności na terenie własnego państwa[45] właśnie dlatego, aby ich szerokie uprawnienia oraz tajność związana z podejmowanymi działaniami nie zwiększały ryzyka nadużycia władzy. W innym bowiem wypadku zamiast stać na straży interesu państwa mogłyby się stać narzędziem realizacji celów pozaprawnych,

[44] W zakresie badań dotyczących skuteczności masowej inwigilacji w typowaniu osób podejrzanych o zaangażowanie w przypadki poważnej przestępczości zob. M. Rojszczak, *Cztery fałszywe hipotezy*…, s. 44–46.

[45] Przykładem takich regulacji są krajowe przepisy będące podstawą działania Agencji Wywiadu (AW) — zob. art. 6 ust. 3 ustawy o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu (tekst jedn. Dz.U. z 2018 r. poz. 2387): „Działalność AW na terytorium Rzeczypospolitej Polskiej może być prowadzona wyłącznie w związku z jej działalnością poza granicami państwa, a realizacja czynności operacyjno-rozpoznawczych […] jest dopuszczalna wyłącznie za pośrednictwem Szefa ABW".

na przykład związanych z walką z opozycją polityczną lub wolnością słowa[46]. Dlatego też wyposażanie agencji wywiadowczych — czy szerzej: służb specjalnych — w środki pozwalające na gromadzenie hurtowych ilości danych elektronicznych na temat własnego społeczeństwa tworzy przestrzeń do wprowadzenia modelu opresyjnego państwa, w którym działające niejawnie agencje rządowe będą dysponowały wiedzą o każdym i na każdy temat, pozostając jednocześnie poza realną kontrolą społeczną[47]. Scenariusz ten jest doskonale znany — jest bowiem powszechny w państwach niedemokratycznych. W ten sposób zarysowuje się ważny wniosek: pomimo różnych ocen przydatności masowej inwigilacji w państwach demokratycznych nie ma wątpliwości, że jest to środek wpisujący się w koncepcję i mechanizmy funkcjonowania państw niedemokratycznych. Od wieków istotnym elementem funkcjonowania państw niedemokratycznych był rozbudowany aparat bezpieczeństwa wewnętrznego. Jego celem było zapobieganie niepokojom społecznym, walka z opozycją, ograniczanie działalności dziennikarskiej czy innych form wolności słowa, a w ogólności dławienie wszelkich form niezależności zagrażającej rządzącym, a więc cały zestaw działań obcych państwom demokratycznym. Realizacja tych celów wymagała informacji, które wcześniej były uzyskiwane za pomocą rozbudowanych struktur agentury, a obecnie mogą być pozyskiwane w nieznanej dotychczas skali ze środków komunikacji

[46] Należy przypomnieć, że nawet w krótkiej — bo zaledwie trzydziestoletniej — historii rządów demokratycznych w Polsce w debacie publicznej kilkukrotnie formułowano zarzuty dotyczące zbyt ekstensywnych uprawnień inwigilacyjnych służb specjalnych, które miały być wykorzystywane do realizacji celów pozaprawnych. Przykładem jest tak zwana sprawa inwigilacji prawicy w latach dziewięćdziesiątych czy nagłośnione w 2015 roku podejrzenia o prowadzenie na szeroką skalę inwigilacji dziennikarzy. W obu sprawach w przestrzeni publicznej formułowano liczne oskarżenia, które nie zostały potwierdzone w toku prowadzonych postępowań karnych. Zob. *Inwigilacji dziennikarzy nie było*, „Polityka" 30.07.2019, https://cli.re/VVp5MR (dostęp: 5.11.2019).

[47] Przykładem mogą być tezy zawarte w wyrokach polskich sądów administracyjnych, w których podtrzymano decyzje o odmowie udzielenia informacji publicznej wydane przez szefów poszczególnych służb specjalnych. W uzasadnieniu odnaleźć można argumentację, że „z uwagi na wagę i specyfikę zadań ABW uznać należy, że niejawną nie jest tylko treść informacji zawartej w materiałach pozyskanych w wyniku czynności operacyjno-rozpoznawczych, czy też w ramach współpracy prowadzonej z partnerami zagranicznymi, ale także sposób jej pozyskiwania, a nawet samo potwierdzenie faktu jej posiadania, bowiem fakt ten pośrednio może wskazywać na jedyny możliwy sposób jej uzyskania, jakim jest prowadzenie czynności operacyjno-rozpoznawczych" — wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 27 maja 2016 roku, sygn. II SA/Wa 214/16. Co więcej, sądy uzasadniały również odmowę udzielenia informacji nie tylko obiektywnymi przesłankami, ale bliżej niesprecyzowanymi zagrożeniami zewnętrznymi: „Trzeba też zwrócić uwagę na to, że obecna sytuacja polityczna na świecie, wzrastające zagrożenie terroryzmem oraz walki zbrojne na Ukrainie, wymagają zachowania daleko idącej ostrożności w ujawnianiu informacji mających związek z działalnością służb specjalnych" — wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 11 grudnia 2015 roku, sygn. II SA/Wa 1330/15.

elektronicznej. Nie dziwi zatem, że systemy masowej inwigilacji znajdują zastosowanie w takich państwach jak Chiny[48] czy państwa arabskie[49].

Według ujawnionych informacji amerykańska Agencja Bezpieczeństwa Wewnętrznego (National Security Agency, NSA) od wielu lat ma pełny dostęp do wiadomości e-mail przesyłanych przez wszystkich użytkowników głównych dostawców usług pocztowych (w tym na przykład Google czy Yahoo)[50]. Z kolei Centrala Łączności Rządowej (Government Communications Headquarters, GCHQ), brytyjska agencja wywiadu elektronicznego, prowadziła program przechwytywania i analizowania zdjęć pochodzących z kamer internetowych zainstalowanych w prywatnych komputerach milionów użytkowników, z których istotna część zawierała treści intymne[51]. Natomiast polskie służby specjalne (ABW i CBA) mogą — z pominięciem kontroli sądowej — analizować szczegółowe informacje pochodzące z krajowego systemu finansowego, w tym na przykład pozwalające na ustalenie, z jakich świadczeń medycznych korzystamy czy jakie organizacje pozarządowe wspieramy finansowo. Czy czytanie prywatnych wiadomości e-mail milionów gospodyń domowych można uznać za środek konieczny do podniesienia poziomu bezpieczeństwa państwa? Czy gromadzenie nagich zdjęć przez służby specjalne to środek stosowany w państwach demokratycznych? Czy wreszcie wiedza na temat zakresu świadczeń medycznych, z których korzysta autor tego artykułu, może poprawić ochronę Polski przed zdarzeniami

[48] W Chinach środki inwigilacyjne znajdują szerokie spektrum zastosowań obcych państwom demokratycznym, jak ograniczanie wolności wypowiedzi, praktykowania religii czy praw mniejszości etnicznych. Zob. np. J. Leibold, *Surveillance in China's Xinjiang region: Ethnic sorting, coercion, and inducement*, „Journal of Contemporary China" 2019, DOI: 10.1080/10670564.2019.1621529. Należy jednak pamiętać, że Chiny to także eksporter technologii związanych z masową inwigilacją. W tym zakresie sprzedaż tego typu systemów może być postrzegana jako sposób rozprzestrzeniania stosowanego w Chinach opresyjnego modelu inwigilacji w skali globalnej, zob. P. Mozur, J. Kessel, M. Chan, *Made in China, exported to the world: The surveillance state*, „The New York Times" 24.04.2019, https://cli.re/M3DNek (dostęp: 5.11.2019).

[49] Zob. np. analizę przedstawioną przez J. Odell w artykule *Inside the dark web of the UAE's surveillance state*, „Middle East Eye" 1.03.2018, https://cli.re/92z4y4 (dostęp: 5.11.2019): „W 2016 r. przedstawiciele policji w Dubaju potwierdzili, że uprawnione organy monitorują użytkowników na 42 platformach społecznościowych; z kolei rzecznik Urzędu Regulacji Telekomunikacji ZEA wskazał, że wszystkie profile w mediach społecznościowych i strony internetowe są śledzone przez odpowiednie agencje. […] W rezultacie dziesiątki osób, które krytykowały rząd Zjednoczonych Emiratów Arabskich w mediach społecznościowych, zostały zatrzymane, zniknęły lub były torturowane".

[50] O przydatności tej formy pozyskiwania informacji może świadczyć to, że w trzydziestodniowym okresie, między grudniem 2012 a styczniem 2013 roku, w ramach tylko jednego programu wywiadowczego — MUSCULAR, prowadzonego wspólnie przez służby brytyjski i amerykańskie, przechwycono 181 mln rekordów danych. Opis programu MUSCULAR zob. B. Gellman, A. Soltani, *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, „The Washington Post" 30.10.2013, https://goo.gl/bYqr9f (dostęp: 5.11.2019).

[51] S. Ackerman, J. Ball, *Optic Nerve: Millions of Yahoo webcam images intercepted by GCHQ*, „The Guardian" 28.02.2014, http://cli.re/Lmrj8p (dostęp: 5.11.2019).

terrorystycznymi? Odpowiedzi na te pytania są oczywiste, a jednak często umykają w dyskursie związanym z potrzebą stosowania masowej inwigilacji w państwach demokratycznych. Strach przed terroryzmem oraz przekonanie, że tylko niejawnie działające służby, wyposażone w najbardziej zaawansowane systemy, są w stanie przeciwdziałać najpoważniejszej przestępczości, przeważa nad próbą bardziej wyważonej analizy.

Naturalnie można wprowadzić wiele zabezpieczeń prawnych, które ograniczą możliwość gromadzenia danych wrażliwych lub przetwarzania informacji na podstawie zgód blankietowych. Jest to jednak próba przekształcenia systemów inwigilacji nieukierunkowanej w systemy inwigilacji indywidualnej. To oczywiście jest możliwe (czego najlepszym przykładem jest sposób funkcjonowania szwedzkiej agencji wywiadu elektronicznego — FRA[52]), takie działanie jednak tylko z pozoru mityguje ryzyko nadużycia władzy. Systemy masowej inwigilacji nie zostały bowiem zaprojektowane, aby gromadzić dane na temat pojedynczych jednostek. Ich celem jest hurtowe przechwytywanie danych, a następnie poddawanie ich analizie w celu zidentyfikowania konkretnych wzorców. Zakres prowadzonej analizy może być oczywiście ograniczony prawnie, jednak przepisy te nie zmienią potencjału regulowanej technologii.

Już samo istnienie systemów pozwalających na hurtowe przechwytywanie łączności, nadzorowanych w dodatku przez służby specjalne, których działalność z definicji wiązana jest z gryfem tajności, może tworzyć w społeczeństwie przekonanie o wszechwiedzy organów państwa. W efekcie w społeczeństwie utrwalane jest przeświadczenie, że rządzący wiedzą wszystko o wszystkich, co z jednej strony może skutkować utratą zaufania do instytucji demokratycznych, a z drugiej — podejrzeniem, że wiedza ta może być wykorzystywana do celów kontroli społecznej.

## b) Inwigilacja a swoboda wyrażania poglądów i stabilność procesu wyborczego

Postrzeganie systemów masowej inwigilacji jako narzędzi służących hurtowemu gromadzeniu dużych ilości danych jest pewnym uproszczeniem. W rzeczywistości narzędzia tego typu składają się co najmniej z trzech komponentów, często będących oddzielnymi platformami informatycznymi: pierwszy odpowiada za gromadzenie danych, drugi — za ich agregację i automatyczną analizę, a trzeci — za udostępnianie raportów i danych źródłowych upoważnionym użytkownikom. Dopiero dane poddane analizie zyskują wartość, pozwalają bowiem wyciągać wnioski i podejmować decyzje. W rzeczywistości tylko niewielki procent pierwotnie zgromadzonych danych jest przydatny do celów dalszej analizy[53].

[52] Försvaretsradioanstalt; kompetencje i uprawnienia FRA zostały szerzej omówione w M. Rojszczak, *The ECtHR's judgment…*

[53] Przedstawiony sposób działania dotyczy nie tylko systemów stosowanych do przechwytywania łączności elektronicznej, lecz także systemów służących do analizy danych finansowych czy

Według dostępnych opracowań już na podstawie publicznie dostępnych informacji pozyskanych na temat danego użytkownika z jednego portalu społecznościowego (w tym jego aktywności, publikowanych treści, reakcji na treści publikowane przez innych) istnieje możliwość opracowania profilu pozwalającego na wnioskowanie na temat nieznanych wcześniej cech danej osoby, na przykład jej preferencji światopoglądowych[54]. Im więcej danych, tym profile mogą być bardziej dokładne. Firmy profesjonalnie zajmujące się budowaniem profili konsumenckich mają bazy dotyczące kilkuset milionów osób, przy średniej liczbie ponad tysiąca punktów danych na temat każdej z nich[55]. Siłą profilowania nie jest pozyskiwanie szczegółowych danych na temat jednostki, ale bardzo dużej liczby danych opisujących jej typowe, codzienne zachowanie i interakcje. Mając do dyspozycji miliony tego typu profili, można automatycznie szukać zależności i korelacji, identyfikując podobne wzorce zachowań. Co więcej, w analogiczny sposób można nie tylko identyfikować preferencje, lecz także na nie wpływać, na przykład kierując treści przygotowane z uwzględnieniem zapatrywań światopoglądowych konkretnej grupy osób.

Przedstawiony opis przedstawia sposób wykorzystania przetwarzania analityki dużych zbiorów danych (*big data*), który już dzisiaj jest możliwy. W ujawnionej w 2018 roku tak zwanej aferze Cambridge Analityca dane dotyczące około 50 mln użytkowników serwisu Facebook były profilowane w celu zwiększania skuteczności prowadzonej kampanii wyborczej[56]. Podobne techniki, polegające na profilowaniu użytkowników mediów społecznościowych połączonym z dotarciem do nich z przekazem mającym ukształtować ich preferencje wyborcze, były również stosowane w trakcie kampanii referendalnej dotyczącej wystąpienia Wielkiej Brytanii z UE. W tym drugim wypadku dodatkowego znaczenia nadaje fakt, że według oficjalnego raportu rządu brytyjskiego działania tego typu miały być prowadzone z inspiracji obcych państw, w szczególności Rosji[57]. Przykłady

innych, wyspecjalizowanych systemów analitycznych. W każdym przypadku dane są przetwarzane w znacznej części w sposób w pełni automatyczny, a wykorzystanie zaawansowanych algorytmów ma pomóc w identyfikacji zdarzeń, które powinny być poddane bardziej szczegółowej analizie przez operatorów.

[54] Zob. A. Ortigosa, R. Carro, J. Quiroga, *Predicting user personality by mining social interactions in Facebook*, „Journal of Computer and System Sciences" 2014, nr 1(80), s. 51–57. Przykłady celowanych kampanii politycznych w Polsce, wykorzystujących dane z portalu Facebook, przedstawiają P. Pawełczyk i J. Jakubowski w *Political marketing in the times of big data*, „Przegląd Politologiczny" 2017, nr 3, DOI: 10.14746/pp.2017.22.3.3.

[55] N. Singer, *You for sale*, „New York Times" 17.07.2012, https://goo.gl/reS5Q5 (dostęp: 5.11.2019).

[56] Omówienie sprawy, w tym zakres danych pozyskanych przez Cambridge Analytica i podmioty powiązane oraz zamierzony cel przetwarzania, przedstawiono w D. Carroll, *Cambridge Analytica is dead, long live our data*, „Boston Review" 24.05.2018, http://cli.re/g3mPAo (dostęp: 5.11.2019).

[57] Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': Interim report*, House of Commons 2018, s. 43–52, https://cli.re/JvqWBm (dostęp: 5.11.2019).

te obrazują, jak na podstawie publicznie dostępnych danych można realizować działania godzące w ustrojowe podstawy demokracji.

Jednym z podstawowych ograniczeń związanych z profilowaniem użytkowników na podstawie informacji pochodzących z portali społecznościowych jest niewystarczająca jakość danych. Dość powiedzieć, że znaczna część społeczeństwa nie ma konta w tego typu serwisach lub nie korzysta z nich aktywnie (na przykład nie wchodzi w interakcję z innymi użytkownikami). Ponadto użytkownicy z uwagi na reakcje otoczenia czy środowiska, w jakim funkcjonują, mogą nie prezentować niektórych przekonań czy poglądów. Te ograniczenia dotyczą jednak nie tyle samej analizy danych, ile źródła, które je gromadzi. W efekcie gdyby zamiast danych o niższej jakości, takich jak z portalu społecznościowego, algorytmy analityczne uzupełnić danymi pochodzącymi z przechwytywania łączności elektronicznej (na przykład wiadomości e-mail, chaty, dane z usług przechowywania w chmurze, takie jak Google Drive czy Microsoft OneDrive), ograniczenia te mogłyby zostać pokonane. Dostęp do takich danych mogą mieć organy władzy publicznej korzystające z systemów masowej inwigilacji. Co więcej, o ile w wypadku profilowania realizowanego przez podmioty komercyjne użytkownik — przynajmniej teoretycznie — ma wpływ na zakres gromadzonych o nim informacji (może chociażby zaprzestać korzystania z danej usługi), o tyle gdy naruszającym jest państwo, nie dość, że jednostka zazwyczaj nie dysponuje wiedzą o samym fakcie naruszenia[58], to jeszcze najczęściej nie istnieje łatwo dostępny i skuteczny środek pozwalający na ograniczenie zakresu gromadzonych danych. Trudno bowiem rozsądnie oczekiwać, aby osoby chcące chronić swoją prywatność zrezygnowały z wszystkich usług elektronicznych (w tym finansowych, takich jak usługi bankowe czy karty płatnicze), tym bardziej że takie działanie i tak nie byłoby skuteczne. Masowe gromadzenie i analizowanie danych jest bowiem równie skuteczne w profilowaniu osób na podstawie informacji, które na ich temat wymieniają inni. Jak wskazuje Jack Balkin, „uniemożliwienie prowadzenia obserwacji nie wystarcza już jako ochrona przed inwigilacją, ponieważ rząd nie musi obserwować jednostki, aby zdobyć wiedzę, którą może wykorzystać przeciwko niej”[59].

[58] Przykładem decyzji skutkującej naruszeniem prawa do prywatności milionów osób, a przy tym pozostającej niejawną jest postanowienie wydane przez amerykański Sąd ds. Inwigilacji Obcego Wywiadu (United States Foreign Intelligence Surveillance Court, FISC) z dnia 25 kwietnia 2013 roku, w którym nakazano podmiotom z grupy kapitałowej Verizon (jeden z głównych operatorów telekomunikacyjnych w Stanach Zjednoczonych) przekazywanie metadanych dotyczących połączeń krajowych i zagranicznych wykonywanych przez wszystkich użytkowników operatora. Ujawnienie treści postanowienia w sprawie Verizon było jednym z dowodów zwolenników ograniczenia uprawnień inwigilacyjnych na poparcie tezy o niewystarczających mechanizmach nadzoru ustanowionych w tym zakresie w USA. Treść postanowienia: https://cli.re/drp5Qq (dostęp: 5.11.2019).

[59] J. Balkin, *The constitution in the national surveillance state*, „Yale Law School Faculty Scholarship” 2008, z. 225, s. 13.

Podsłuchiwanie łączności elektronicznej tworzy zatem doskonałe narzędzie do kontroli społecznej, pozwalające nie tylko na dostarczanie rządzącym informacji na temat aktualnych nastrojów społecznych, lecz także na ich kształtowanie. Istnienie takiego środka prowadzi też do dalszych negatywnych zjawisk społecznych. Pierwszym jest zasygnalizowany już tak zwany efekt mrożący, będący w istocie praktyczną realizacją koncepcji panoptykonu w cyfrowym świecie. Jego skutkiem jest stosowanie przez użytkowników samoograniczenia w zakresie zapoznawania się z interesującymi ich treściami w przeświadczeniu, że wszelkie ich aktywności są monitorowane, a za próbę dotarcia do krytycznych dla rządzących informacji może spotkać ich kara. Prawo do informacji zawiera dwa komponenty: pierwszym jest swoboda w zapoznawaniu się z interesującymi nas treściami, drugim zaś wolność wypowiedzi, nierozerwalnie związana z wolnością myśli i przekonań. Nie dziwi zatem, że skoro inwigilacja powstrzymuje użytkowników od pozyskiwania interesujących ich informacji, to jest także barierą przed jej dalszym przekazywaniem, a więc ogranicza swobodę wyrażania poglądów i korzystania z wolności wypowiedzi. Anthony Mills na podstawie własnych badań opisał liczne przykłady negatywnego wpływu uprawnień inwigilacyjnych organów publicznych na pracę niezależnych dziennikarzy w kilkunastu państwach, w tym w Polsce[60]. Krytyka rządzących przez obywateli jest naturalnym i immamentnym elementem każdej demokracji. Wprowadzanie środków, które — nawet pośrednio — mogą tę krytykę zaburzać lub utrudniać, musi prowadzić do refleksji na temat motywów działania rządzących.

Inwigilacja elektroniczna nie musi ograniczać się wyłącznie do przechwytywania danych telekomunikacyjnych. Inną formą, znajdującą coraz szersze zastosowanie także w Polsce, jest nadzorowanie przestrzeni publicznej przez rozbudowane systemy monitoringu wizyjnego. W samej tylko Wielkiej Brytanii na monitoring wizyjny składa się około 4–6 mln kamer bezpieczeństwa, w Stanach Zjednoczonych takich urządzeń jest ponad 11 mln[61]. Z kolei Polska jest prekursorem we wdrażaniu systemów informatycznych pozwalających na masowe monitorowanie i przetwarzanie transakcji finansowych — w służącym takim celom systemie STIR przez dwa lata funkcjonowania zgromadzono dane na temat ponad 6 mld operacji finansowych dokonanych za pośrednictwem krajowego systemu bankowego[62]. Cyfryzacja powoduje zatem, że monitorowanie aktywności dużych grup osób (potencjalnie: całego społeczeństwa) może przebiegać wieloaspektowo,

[60] A. Mills, *Now you see me — now you don't: Journalists' experiences with surveillance*, „Journalism Practice" 13, 2019, nr 6, s. 690–707. Na marginesie tekstu Millsa warto zauważyć, że w swoich badaniach zaliczył Polskę — obok Węgier — do grupy państw o ograniczonej demokracji („demokracje nieliberalne"); pozostałe badane państwa członkowskie UE zostały zaliczone do demokracji liberalnych.

[61] M. Kohn, *Unblinking: Citizens and subjects in the age of video surveillance*, „Constellations" 17, 2010, nr 4, s. 574.

[62] J. Sarnowski, P. Selera, *op. cit.*

z wykorzystaniem różnych źródeł danych, co w rezultacie przekłada się na dalsze zwiększenie szczegółowości informacji uzyskiwanych z systemów inwigilacyjnych.

### c) Jednostka jako przedmiot, a nie podmiot regulacji

Istotnym elementem rozróżniającym współczesne formy inwigilacji elektronicznej od środków znanych wcześniej — także związanych z niejawną działalnością państwa, ale nieopartych na masowym przetwarzaniu danych, jest możliwość automatyzacji procesu podejmowania decyzji. Możliwość ta w istocie urealnia wizję państwa opresyjnego, w którym jednostka staje się przedmiotem wprowadzanych regulacji, a proces rządzenia może przebiegać z wykorzystaniem zdefiniowanych wcześniej reguł. Wyeliminowanie czynnika ludzkiego z procesu podejmowania decyzji bez wątpienia może przyspieszyć działanie administracji, wyeliminować proste błędy oraz zapewnić powtarzalność decyzji w przypadkach charakteryzujących się podobnym stanem faktycznym. Już dzisiaj automatyzacja procesów biznesowych jest wskazywana jako jeden z istotnych fundamentów nowej ewolucji przemysłowej, określanej terminem Przemysł 4.0. Coraz większa część operacji analitycznych oraz decyzyjnych w sektorze usług finansowych opiera się na systemach uczenia maszynowego. Także na polskim rynku oferowane są już nowoczesne produkty (*fintech*), w których profilowanie i korelowanie danych na temat danej osoby, pochodzących z różnych baz, wykorzystywane jest w celu zaproponowania oferty produktów finansowych dopasowanej do jej indywidualnych potrzeb[63].

Należy jednak odróżnić ryzyka związane z automatycznym podejmowaniem decyzji stosowanym w biznesie, które co do zasady opiera się (lub powinno się opierać) na danych o ustalonej jakości i przetwarzanych za zgodą (wiedzą) użytkownika, od ryzyk ujawniających się w wypadku podejmowania decyzji przez organ państwa, zwłaszcza wydawanych na podstawie niejawnych informacji pozyskiwanych w wyniku realizacji działań inwigilacyjnych. W 2018 roku opinia publiczna była zaniepokojona propozycją Departamentu Stanu Stanów Zjednoczonych wprowadzenia wymagania, aby wszystkie osoby ubiegające się o wydane amerykańskiej wizy musiały udostępnić urzędnikom do spraw imigracyjnych listę swoich profili w mediach społecznościowych, adresów e-mail oraz numerów telefonów, z których korzystali w ciągu pięciu lat od daty złożenia wniosku[64]. Pomimo krytyki wskazującej na negatywny wpływ nowych przepisów na wolność

[63] Szerzej na temat rynku *fintech*, możliwości związanych zastosowaniem analityki *big data* w sektorze usług finansowych oraz problemów z prawną regulacją nowych usług zob. W. Szpringer, *Nowe technologie a sektor finansowy* fintech *jako szansa i zagrożenie*, Warszawa 2017.

[64] B. O'Brien, *U.S. visa applicants to be asked for social media history: State Department*, „Reuters" 30.03.2018, https://cli.re/yZd5Ne (dostęp: 5.11.2019).

słowa propozycja Departamentu Stanu została wdrożona 1 czerwca 2019 roku[65]. Pozyskane w ten sposób informacje mogą służyć automatycznemu ustaleniu, czy w opinii służb ochrony państwa dana osoba jest zagrożeniem bezpieczeństwa państwa, a w związku z tym, czy należy jej odmówić wjazdu na teren USA. Realizacja przedstawionej propozycji może prowadzić do zredukowania roli urzędników imigracyjnych do operatorów algorytmu, którego konstrukcja i zasada działania będzie pozostawała niejawna, a przez to niepodatna na kontrolę czy faktyczną weryfikację działania. Także służby innych państw korzystają z wniosków płynących z analityki dużych zbiorów danych do wsparcia procesu podejmowania decyzji[66]. O przydatności tej formy inwigilacji najlepiej może świadczyć wypowiedź Michaela Haydena, byłego szefa CIA i NSA, który w 2014 roku, oceniając przydatność programów do hurtowego gromadzenia metadanych pochodzących z łączności elektronicznej, stwierdził: „zabijaliśmy ludzi na podstawie takich danych"[67].

Automatyczne podejmowanie decyzji przez organy publiczne wiąże się z dwoma najpoważniejszymi ryzykami: po pierwsze — nieprzejrzystością w zakresie algorytmów wnioskujących, po drugie — ograniczonymi możliwościami szukania ochrony prawnej przez jednostkę objętą skutkami wydanej decyzji. Kwestia transparentności podejmowanych decyzji jest naturalnym atrybutem działań administracji w każdym państwie demokratycznym. Możliwość przeanalizowania zasadności przyjętego wnioskowania przez organ administracji jest istotnym mechanizmem chroniącym przed arbitralnością, jednocześnie zwiększającym zaufanie do państwa i wiarygodność instytucji występujących w jego imieniu. W przypadku automatycznej decyzji jednostka dowiaduje się o jej wydaniu dopiero w momencie doświadczenia negatywnych skutków, co *de facto* oznacza, że nie ma możliwości wpłynięcia na jej zmianę w sposób zapobiegający materializacji tych skutków. Dlatego decyzje automatyczne stosowane w obszarze administracji publicznej mogą prowadzić do ograniczenia dostępnych opcji ochrony prawnej. Ryzyko to jest aktualne, w szczególności gdy decyzje tego typu bazują zarówno na niejawnych informacjach, jak i tajnych algorytmach wnioskujących. W takim wypadku to jednostka jest postawiona przed koniecznością dowodzenia, że nie stanowi zagrożenia, a więc w praktyce udowadniania swojej niewinności[68].

---

[65] S. Garcia, *U.S. requiring social media information from visa applicants*, „The New York Times" 2.06.2019, https://cli.re/mNAVzv (dostęp: 5.11.2019).

[66] Przykładem tego typu działań — niezwiązanym wprost z obszarem bezpieczeństwa narodowego — są systemy wdrażane w ramach tak zwanego uszczelniania systemu podatkowego, których głównym zadaniem jest typowanie transakcji podejrzanych. Dla przykładu zgodnie z polskimi przepisami regulującymi sposób funkcjonowania systemu STIR wyniki pochodzące z analiz prowadzonych przez ten system (tak zwane wskaźniki ryzyka) mogą być podstawą zablokowania środków podatnika na koncie bankowym na okres do 72 godzin (por. art. 119zv ustawy z 29 sierpnia 1997 roku — Ordynacja podatkowa, Dz.U. z 2019 r. poz. 900).

[67] J. Naughton, *Death by drone strike, dished out by algorithm*, „The Guardian" 21.02.2016, https://cli.re/X82KD4 (dostęp: 5.11.2019).

[68] Zob. J. Reidenberg, *op. cit.*, s. 605.

Skutkuje to naturalnym zachwianiem równowagi między uprawnieniami organów publicznych a prawami obywateli. Efektem jest erozja zaufania do instytucji państwa i — zauważalna także w dostępnych badaniach — utrata zaufania do możliwości skutecznego nadzoru nad stosowaniem środków inwigilacyjnych[69]. Wzajemne zaufanie jest jednym z fundamentów, bez którego formuła państwa demokratycznego nie może być w pełni zrealizowana. Dlatego, jak trafnie wskazuje Benjamin Goold, biorąc pod uwagę, że demokracja może funkcjonować tylko w atmosferze wzajemnego zaufania między rządem a rządzonymi, każdemu środkowi nadzoru, który grozi erozją lub zniszczeniem tego zaufania, należy się opierać, a przynajmniej dokładnie przeanalizować jego potencjalne koszty i korzyści[70].

Odpowiedzią na ryzyka związane z brakiem transparentności decyzji wydawanych na podstawie tajnych danych pochodzących z inwigilacji elektronicznej są liczne zabezpieczenia prawne, których wprowadzenie jest postulowane między innymi w orzecznictwie ETPC (por. wcześniejsze rozważania w tym zakresie). Zasadniczym problemem w przyjęciu założenia, że takie rozważanie może okazać się skuteczne, jest istniejąca — i nieusuwalna — asymetria w możliwościach i środkach jednostki umożliwiających kontrolowanie rządzących. Większość zabezpieczeń prawnych opiera się na powierzeniu ważnych funkcji nadzorczych czy kontrolnych innym instytucjom państwa (niezależnym organom, komisjom parlamentarnym, obudsmanom czy sądom). W każdym przypadku są to jednak *de facto* także organy państwa. Oznacza to, że bez zaufania do tych organów — wyrażającego przekonanie, że potrafią one przeciwstawić się niezgodnej z prawem działalności inwigilacyjnej — jednostka pozbawiona jest możliwości skutecznej ochrony przed ryzykiem nadużycia władzy. W 2014 roku ujawnione zostało — oznaczone jako ściśle tajne — postanowienie wydane przez amerykański sąd upoważniony do rozpatrywania wniosków dotyczących inwigilacji elektronicznej, zezwalające na przechwytywanie przez NSA całości metadanych związanych z łącznością elektroniczną przetwarzanych przez jednego z wiodących operatorów telekomunikacyjnych. Jedną niejawną decyzją sądu (niepodlegającą żadnej ścieżce zaskarżenia) prawo do prywatności kilkudziesięciu milionów osób zostało znacznie ograniczone. W tym zakresie nie jest już nawet istotne, że postanowienie

[69] Według badania przeprowadzonego przez Pew Research Center w 2014 roku, którego celem była ocena wpływu informacji na temat rozbudowanych programów inwigilacyjnych ujawnionych przez E. Snowdena na postrzeganie prywatności przez Amerykanów, 65% badanych wskazało, że w ramach prowadzonych działań antyterrorystycznych w niewystarczającym stopniu zdefiniowano granice „danych telefonicznych i internetowych, które rząd może gromadzić". Co istotne, pogląd ten przeważał we wszystkich grupach demograficznych. Por. M. Madden, L. Rainie, *Americans' attitudes about privacy, security and surveillance*, Pew Research Center 2015, s. 10–11, https://cli.re/BwYNjE (dostęp: 5.11.2019).

[70] B. Goold, *How much surveillance is too much? Some thoughts on surveillance, democracy, and the political value of privacy*, [w:] *Overvåkning i en rettsstat — Surveillance in a Constitutional Government*, red. D. Schartum, Bergen 2010, s. 46.

to nie zawierało żadnego uzasadnienia, dowodzącego konieczności wdrożenia tak ekstensywnego środka. O ile amerykański system prawny znacząco odbiega od europejskiego modelu ochrony prywatności, o tyle podobne nadużycia można także zidentyfikować w gronie państw członkowskich UE. Przykładem może być współpraca niektórych europejskich służb wywiadowczych z NSA, polegająca na umożliwieniu amerykańskiej agencji przechwytywania łączności własnych obywateli, aby potem dane te mogły zostać przekazane w ramach współpracy wywiadowczej do kraju pozyskania. W ten sposób omijane miały być ograniczenia związane z zakazem prowadzenia przez służby wywiadowcze działań operacyjnych na terenie własnego kraju, a także ograniczenia związane z sądową kontrolą stosowania środków inwigilacyjnych. O tego typu praktyki podejrzewane były między innymi służby niemieckie[71] oraz brytyjskie[72].

Efektem dostrzeżenia rosnącej roli masowego przetwarzania informacji na temat jednostek w funkcjonowaniu współczesnych demokracji oraz badań związanych ze skutkiem tego typu środków dla rozwoju relacji społecznych jest szeroko dyskutowana w ostatnich dziesięcioleciach koncepcja „nadzorowanego społeczeństwa" (ang. *surveillance society*)[73]. Termin ten jest stosowany do określenia modelu społeczeństwa, którego istotnym elementem są szeroko stosowane mechanizmy nadzoru, opierające się na gromadzeniu, rejestrowaniu, przechowywaniu i analizowaniu informacji na temat grup i jednostek. W koncepcji społeczeństwa nadzorowanego inwigilacja nie ma jedynie charakteru zewnętrznej obserwacji (na przykład związanej z działalnością organów państwa), ale jest obecna na różnych płaszczyznach życia społecznego i przenika codzienne funkcjonowanie jednostki. Społeczeństwo nadzorowane nie ucieka od kontroli, bo, po pierwsze, ucieczka ta jest niemożliwa, a po drugie, kontrola ta jest jednym ze sposobów regulowania relacji społecznych. Próba wiązania rozwoju społeczeństw nadzorowanych wyłącznie z działalnością inwigilacyjną państw byłaby jednak nadmiernym uproszczeniem. Przemiany te są bardziej efektem rosnącej roli informacji we współczesnej gospodarce, a w szczególności postępujących procesów globalizacji[74].

[71] K. Biermann, Y. Musharbash, *A dubious deal with the NSA*, „Zeit Online" 26.08.2015, https://cli.re/AaqwE8 (dostęp: 5.11.2019).

[72] Fakt zatajenia przez GCHQ korzystania z baz danych NSA, zawierających także informacje na temat obywateli brytyjskich, był jedną z przyczyn wydania przez IPT, organ sądowy zajmujący się nadzorem nad stosowaniem uprawnień śledczych, wyroku stwierdzającego naruszenie prawa przez GCHQ. Zob. O. Bowcott, *UK–US surveillance regime was unlawful 'for seven years'*, „The Guardian" 6.02.2015, https://cli.re/NMqqV7 (dostęp: 5.11.2019).

[73] Szerzej na temat koncepcji nadzorowanego społeczeństwa zob. D. Wood, *The 'surveillance society': Questions of history, place and culture*, „European Journal of Criminology" 6, 2009, nr 2, s. 179–194.

[74] T. Bunkyan, *op. cit.*, s. 1.

## d) Inwigilacja dąży do prewencyjnego modelu kary, ustalanej zanim popełnione zostanie przestępstwo

> Programy inwigilacyjne to kolejny krok w kierunku stworzenia w pełni prewencyjnego państwa, w którym zmianie ulegnie utrwalony w państwach demokratycznych paradygmat prawa karnego, zgodnie z którym jakakolwiek ingerencja w prawa podstawowe podejrzanych wymaga zatwierdzenia przez sędziego lub prokuratora na podstawie racjonalnego podejrzenia, natomiast promowane będzie połączenie egzekwowania prawa i działań wywiadowczych o zatartych i osłabionych zabezpieczeniach prawnych, często niezgodne z kontrolą i równowagą demokratyczną oraz prawami podstawowymi, szczególnie w kwestii domniemania niewinności[75].

Domniemanie niewinności oraz wina jako podstawa odpowiedzialności to podstawowe filary prawa karnego. Osoba, która nie popełniła czynu zabronionego, nie możne zostać skazana, przy czym karalność danego występku nie może być oceniana z perspektywy przepisów nieobowiązujących w czasie jego popełnienia (*nullum crimen sine lege*). Chociaż istnieje możliwość skazania sprawcy za usiłowanie popełnienia przestępstwa, to jednak także w tym wypadku usiłowanie to musi zostać wykazane — udowodnione, nie może być przedmiotem spekulacji czy domniemań.

W przypadku masowej inwigilacji zależność ta ulega odwróceniu: państwo gromadzi wszelkie informacje, aby wykazać winę, gdyby przestępstwo zostało popełnione. Zatem wszyscy są podejrzani, ale o nieznane jeszcze przestępstwo, które nie zostało popełnione. Zwolennicy stosowania rozbudowanych programów inwigilacyjnych wskazują, że takie działanie jest niezbędne, aby wyprzedzać aktywności ekstremistów, a w efekcie zapobiegać najpoważniejszym zdarzeniom, w tym o charakterze terrorystycznym. Chociaż możliwe jest dowodzenie niespójności wnioskowania stojącego za tą tezą, przyjmijmy na potrzeby dalszych rozważań jej prawdziwość. Aby zobrazować pełniej niebezpieczeństwo związane z takim rozumowaniem, przyjmijmy nawet, że gromadzenie informacji na temat całego społeczeństwa może być środkiem pozwalającym na wykrycie każdego, nawet najdrobniejszego przestępstwa, zanim zostanie popełnione. Doprowadzając ten przykład do skrajnej postaci, przyjmijmy, że środek ten będzie także bezbłędny, to jest nieobarczony jakimkolwiek ryzykiem nietrafnego wytypowania przyszłego przestępcy. A zatem na potrzeby przykładu: masowa inwigilacja jako środek pozwalający wykryć 100% przestępstw w sposób prewencyjny i bez ryzyka popełnienia błędu. Czy w takim — skrajnie doskonałym — przypadku społeczeństwo, w którym w wyniku stosowania rozbudowanych środków nadzoru każde przestępstwo zostanie wykryte, zanim zostanie popełnione, można uznać za wolne?

Truizmem jest wskazywanie, że działanie nawet pojedynczej osoby nie może być w pełni opisane i przewidziane z całkowitą pewnością za pomocą algorytmów analitycznych. Nawet duże badania populacyjne, opierające się na *big data*, nie-

[75] Rezolucja Parlamentu Europejskiego z 12 marca 2014 roku, zob. przyp. 13.

jednokrotnie doprowadzały do nieprawdziwych wyników[76]. Można wskazać także przypadki, gdy mające bardzo humanitarne założenia badania, w których bazowano na dużych zbiorach danych, prowadziły do tragicznych skutków[77]. Nie ma powodu do przyjęcia założenia, że organy władzy publicznej, prowadząc niejawne programy inwigilacyjne i przetwarzając uzyskane w ten sposób dane w tajny, nieprzejrzysty sposób, mogą uzyskać wyniki obarczone mniejszym marginesem błędu. Niezależnie zatem, jakie są intencje rządzących i mechanizmy ochrony przed arbitralnością podejmowanych decyzji, inwigilacja elektroniczna jest i pozostanie sposobem wspierającym, ale niezastępującym typowanie osób podejrzewanych o przygotowywanie lub popełnienie najpoważniejszych przestępstw. Dlatego też, jak zauważa Bart Jacobs, niemal we wszystkich przypadkach aktów terrorystycznych ich sprawcy byli wcześniej znani organom ścigania, często pozostawali nawet pod nadzorem środków inwigilacyjnych[78]. To z kolei prowadzi do wniosku, że inwigilacja powinna być stosowana w sposób zindywidualizowany, a nie nieograniczony. W innym bowiem wypadku jej stosowanie nie może być pogodzone z celami prowadzenia postępowania karnego (ustaleniem winy przy zachowaniu prawa do obrony i domniemania niewinności), co oznacza, że taki środek nie mógłby znaleźć zastosowania w ramach działania państwa demokratycznego.

Przedstawione rozważania prowadzą do następującej konstatacji: celem masowej inwigilacji jest gromadzenie nadmiarowych (zbędnych dowodowo w czasie pozyskiwania) informacji na temat znacznej części społeczeństwa. Do gromadzenia danych na temat podejrzanych aktywności konkretnych osób wystarczające jest korzystanie z mniej inwazyjnych, ukierunkowanych środków nadzoru. Dlatego jakiekolwiek mechanizmy inwigilacji prewencyjnej bazujące na hurtowym gromadzeniu danych nie mogą być uznane za niezbędne do walki z najpoważniejszą

[76] Przykładem może być serwis Google Flu, który został opracowany do przewidywania sezonowych epidemii grypy na podstawie analizy zapytań kierowanych przez użytkowników przeglądarki Google. Przez długi czas Google Flu wymieniane było jako przykład zastosowań *big data* w obszarze ochrony zdrowia. Projekt — z uwagi na duże rozbieżności prognoz względem sytuacji rzeczywistej — został zakończony w 2013 roku. Zob. D. Lazer *et al.*, *The parable of Google Flu: Traps in big data analysis*, „Science" 2014, nr 343, s. 1203.

[77] Przykładem mogą być wyniki uzyskane przez T. Emmens i A. Phippen, dotyczące powiązania samookaleczania ze skłonnościami samobójczymi. Celem badań była weryfikacja istnienia tej korelacji oraz wprowadzenie programu edukacyjnego realizowanego online i ukierunkowanego na zapobieganie samookaleczeniom wśród młodych osób. Wbrew intencjom naukowców w trakcie badania pojawiło się ryzyko, że badania w istocie przyczynią się do zwiększenia liczby samobójstw — jak się okazało, dla niektórych chorych samookaleczenie może być formą wyrażania emocji i pozwalać na odsunięcie decyzji o samobójstwie. Zob. T. Emmens, A. Phippen, *Evaluating online safety programs*, Harvard Berkman Center for Internet and Society 2010, s. 7–8, https://cli.re/P3A5Wb (dostęp: 5.11.2019).

[78] B. Jacobs, *Keeping our surveillance society non-totalitarian*, „Amsterdam Law Forum" 2009, nr 1 (4), s. 29–30.

przestępczością, a jednocześnie kreują znaczną przestrzeń do nadużyć i nieprawidłowości w zakresie prowadzenia postępowań karnych.

## e) Inwigilacja a agenda kolejnych rządów

Stan, w którym organy publiczne wiedzą więcej o obywatelach, niż potrzebują do wykonywana powierzonych im zadań, przy jednoczesnej nietransparentności podejmowanych działań, można nazwać asymetrią informacyjną. Aby odpowiednio ocenić wpływ takiej asymetrii na trwałość podstaw ustrojowych państwa, należy uwzględnić nie tylko cel jej utrzymywania przez aktualnie rządzących, ale również ryzyka związane z odmiennymi celami, które mogą być zdefiniowane przez kolejne rządy. Ten sam system inwigilacyjny, który dzisiaj służy typowaniu terrorystów, jutro może służyć typowaniu przeciwników politycznych. Co więcej, w języku populistów nierzadko obie grupy opisywane są w ten sam sposób[79].

Przykładem tego, że inwigilacja może stać się narzędziem przemiany ustroju państwa w kierunku modelu autorytarnego, jest Turcja. Jeszcze kilkanaście lat temu państwo to było prezentowane jako kraj o aspiracjach demokratycznych i prozachodnich. Jednak wraz ze wzmacnianiem się rządów Recepa Erdoğana oraz dominacji Partii Sprawiedliwości i Rozwoju (tur. Adalet ve Kalkınma Partisi, AKP) na lokalnej scenie politycznej ocena ta szybko zaczęła się dezaktualizować. Narzędziem zwalczania opozycji wewnętrznej stały się środki inwigilacyjne, stosowane bardzo szeroko i bez realnej kontroli ze strony sądów, na podstawie tak zwanych zgód blankietowych[80]. Znowelizowane w 2014 roku przepisy wprowadziły dalsze rozszerzenie możliwości cenzurowania treści online i monitorowania użytkowników Internetu. Zgodnie z wprowadzonym prawem internetowym (ustawa 5651) możliwe stało się cenzurowanie stron internetowych w ciągu kilku godzin bez nakazu sądowego. Z kolei zmienione prawo o państwowych służbach wywiadowczych (ustawa nr 6532) umożliwiło tureckiej Narodowej Agencji Wywiadowczej uzyskanie dostępu do wszelkich informacji przetwarzanych na temat osób fizycznych w sposób cyfrowy i tradycyjny, pochodzących z wszystkich instytucji publicznych i prywatnych, jak również do przechwytywania łączności

[79] Przyczyną jest potrzeba poszukiwania przez polityków populistycznych zewnętrznego wroga, przeciwko któremu można jednoczyć wyborców. Ciekawy pogląd na tym tle przedstawił Amichai Magen, zauważając podobieństwa pomiędzy populizmem a dżihadyzmem: „Jak na ironię tak dżihadyści, jak i populiści przejawiają wrogość do pluralizmu. Obie grupy postrzegają rzeczywistość jako konflikt »synów światła i synów ciemności«, w którym nie ma miejsca na poglądy alternatywne. […] W atmosferze strachu i nieufności »zagrożenie terrorystyczne« może służyć jako wymówka dla tłumienia sprzeciwu i zapewnienia jedności pomiędzy działaniami wywiadu, organów ścigania oraz sądów z celami rządzącej partii oraz jej silnego przywódcy" — *idem*, *Fighting terrorism: The democracy advantage*, „Journal of Democracy" 29, 2018, nr 1, s. 121–122.

[80] Zob. ustalenia zawarte w wyroku ETPC z 18 lipca 2017 roku, *Mustafa Sezgin Tanrıkulu v. Turcja*, skarga nr 27473/06, pkt 5 i 6.

elektronicznej bez jakiejkolwiek kontroli sądowej[81]. Przykład Turcji powinien być znaczący dla środowiska międzynarodowego jeszcze z jednego powodu. Jak zauważa Ozgun Topak, Turcja to przykład kraju, w którym państwo, doskonaląc swoje środki nadzorcze, przeszło od inwigilacji ukierunkowanej, wymierzonej w konkretne osoby oraz grupy społeczne, do inwigilacji nieukierunkowanej, mającej charakter masowy, pomocnej w walce z wszystkimi, którzy sprzeciwiają się rządom Erdoğana i AKP[82].

Problem erozji zabezpieczeń prawnych oraz dostosowania mechanizmów inwigilacyjnych do zmiennej optyki aktualnie rządzących to jednak także problem zauważalny w rozwiniętych demokracjach. Amerykańskie przepisy federalne, regulujące zasady stosowania nieograniczonej inwigilacji, były w ciągu ostatnich 15 lat kilkukrotnie nowelizowane. W zależności od aktualnej koniunktury politycznej ustawodawca w kolejnych nowelizacjach albo wzmacniał uprawnienia państwa oraz ograniczał mechanizmy nadzoru nad działalnością służb (na przykład Patriot Act 2001[83]), albo wprowadzał dodatkowe zabezpieczenia prawne i limitował możliwości inwigilacji obywateli (na przykład Freedom Act 2015[84]). Niezależnie od intencji prawodawcy istotne znaczenie dla zakresu uprawnień wykonywanych przez agencje rządu miała jednak wola aktualnie urzędującego prezydenta, wyrażana między innymi w formie tak zwanych rozporządzeń wykonawczych. I tak prezydent Donald Trump w jednym ze swoich pierwszych rozporządzeń polecił agencjom rządu federalnego zniesienie wszelkich praw, które mogłyby zostać przyznane obcokrajowcom w zakresie prawa do prywatności na mocy odpowiednich przepisów ustawy o ochronie prywatności[85]. Niezależnie od oceny faktycznego skutku prawnego rozporządzenia wydanego przez prezydenta bez wątpienia akt ten był wyraźną deklaracją polityczną, wspierającą przyjętą przez nową administrację strategię „America First".

Wydaje się, że zarówno decyzja Donalda Trumpa, a zwłaszcza łatwość, z jaką zerwał on z wcześniejszą polityką rządu federalnego, jak i praktyka rządów Recepa Erdoğana są oczywistymi przykładami możliwości uchylenia istniejących ograniczeń prawnych przy odpowiednio zdeterminowanej egzekutywie oraz skorodowanym systemie trójpodziału władzy. Z tej perspektywy akceptowanie stanu,

[81] O. Topak, *The making of a totalitarian surveillance machine: Surveillance in Turkey under AKP rule*, „Surveillance & Society" 15, 2017, nr 3–4, s. 539.

[82] *Ibidem*, s. 537.

[83] Ustawa federalna USA z 26 października 2001 roku (USA Patriot Act of 2001), sygn. 107-56, tekst ogłoszony: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf (dostęp: 5.11.2019).

[84] Ustawa federalna USA z 2 lipca 2015 roku (USA Freedom Act of 2015); sygn. 114-23, tekst ogłoszony: https://www.congress.gov/114/bills/hr2048/BILLS-114hr2048enr.pdf (dostęp: 5.11.2019).

[85] Problematyka szerzej omówiona w M. Rojszczak, *Skuteczność ochrony praw podmiotów danych wynikających z prawa UE w świetle umowy Tarcza Prywatności oraz prawodawstwa federalnego USA*, „Transformacje Prawa Prywatnego" 2018, nr 1, s. 129–130.

w którym instytucje państwowe zostaną wyposażone w narzędzia, za pomocą których możliwe jest naruszanie praw podstawowych na masową skalę, tworzy stałe i nieprzemijające ryzyko dla fundamentów systemu demokratycznego. Jak trafnie wskazała Katerina Hadjimatheou, jest nieuniknione, że władza opierająca się na inwigilacji zostanie w końcu nadużyta: „jeżeli chcemy zapobiec takiej możliwości, w pierwszej kolejności należy uniemożliwić korzystanie rządzącym z takich narzędzi”[86].

## Podsumowanie

Kwestia zgodności programów nieograniczonej inwigilacji ze standardami ochrony praw człowieka jest problemem istotnym i aktualnym. Współcześnie, dzięki postępowi techniki skutkującemu większą dostępnością tego typu systemów, narzędzia służące masowej inwigilacji są przedmiotem obrotu tak jak inne zaawansowane systemy informatyczne. Szacuje się, że wdrożenie środków pozwalających na hurtowe przechwytywanie łączności elektronicznej to dla średniej wielkości państwa koszt około 15 mln euro rocznie[87]. Jest to kwota marginalna, jeśli zestawi się ją z wielkością budżetów przeznaczanych na obronność. Zatem w dzisiejszym świecie dostęp do tego typu systemów nie jest limitowany ani barierą technologiczną (brakiem dostępu do odpowiedniej technologii), ani kosztami wdrożenia czy utrzymania. Można więc przyjąć, że potrzebna technologia jest w zasięgu możliwości każdego państwa, które chce masowo inwigilować swoich obywateli. Co więcej, koncerny funkcjonujące w państwach rozwiniętych nie wzbraniają się przed sprzedażą tej technologii państwom niedemokratycznym, w przypadku których jest oczywiste, że inwigilacja tego typu będzie kolejnym narzędziem opresji wewnętrznej[88].

Czy zatem wizja „nadzorowanego społeczeństwa” to także model przyszłych demokracji? Odpowiedź na pytanie, czy państwa demokratyczne potrzebują masowej inwigilacji, nie jest oczywista. Rozważając ten problem, warto jednak zauważyć, że wątpliwości tych nie ma w wypadku państw niedemokratycznych. Rozbudowane programy inwigilacji warunkują skuteczne zarządzanie państwem autorytarnym — potrzeba wiedzy o nastrojach i niepokojach społecznych charakteryzuje działanie organów władz publicznych, które swojego mandatu nie

[86] K. Hadjimatheou, *Ethics and surveillance in authoritarian and liberal states*, The Surveille Project 2013, s. 9, https://cli.re/qmKnDv (dostęp: 5.11.2019).

[87] J. Assange, *Cypherpunks: Freedom and the Future of the Internet*, New York-London 2012, s. 46–47.

[88] Zob. informacje na temat sprzedaży przez brytyjski koncern BAE Systems technologii masowej inwigilacji do Arabii Saudyjskiej, Zjednoczonych Emiratów Arabskich, Omanu, Kataru, Algierii i Maroka w R. Evans, *BAE ‘secretly sold mass surveillance technology to repressive regimes’*, „The Guardian” 15.06.2017, http://cli.re/LXdRn4 (dostęp: 5.11.2019).

zawdzięczają procesowi demokratycznemu. Już sam ten fakt powinien być wystarczającym powodem, aby tego typu środków nie wprowadzać w państwie demokratycznym. Veronika Nagy wskazuje z kolei, że „przemianę rządów demokratycznych we władzę autorytarną obrazuje asymetria w uprawnieniach inwigilacyjnych pomiędzy państwem a jego obywatelami”[89]. Bez wątpienia do zwiększenia tej asymetrii przyczynia się stosowanie narzędzi inwigilacji nieograniczonej.

Masowa inwigilacja przyczynia się także do erozji tak zwanego uzasadnionego oczekiwania prywatności. Termin ten, mający szczególne znaczenie w systemie prawnym Stanów Zjednoczonych, ale w ostatnich latach stosowany również w orzecznictwie ETPC[90], odnosi się do potrzeby ochrony jednostki przed nieuprawnioną ingerencją wszędzie tam, gdzie może ona, uwzględniając subiektywne i obiektywne przesłanki, oczekiwać, że jej prywatność będzie respektowana[91]. Powszechność oraz masowy charakter inwigilacji prowadzi do zmiany oczekiwań społecznych w zakresie granic dopuszczalnej ingerencji w prywatność ze strony organów władzy publicznej. Ponieważ coraz większy zakres ingerencji jest tolerowany, zmieniają się granice, w których jednostka może szukać ochrony, korzystając z testu uzasadnionego oczekiwania prywatności. To swoiste „przyzwyczajanie się” do życia w środowisku nadzorowanym powoduje, że brak przejrzystości i transparentności w prowadzonych działaniach inwigilacyjnych są traktowane — także przez sądy — jako naturalny element funkcjonowania organów państwa w warunkach państwa demokratycznego[92].

---

[89] V. Nagy, *How to silence the lambs? Constructing authoritarian governance in post-transitional Hungary*, „Surveillance & Society” 15, 2017, nr 3–4, s. 447–455.

[90] Należy jednak pamiętać, że w linii orzeczniczej ETPC test uzasadnionego oczekiwania prywatności ma znaczenie pomocnicze i nieprzesądzające o zasadności dochodzenia przez jednostkę ochrony prawnej. Zob. wyrok ETPC z 24 kwietnia 2018 roku, *Benedik v. Słowenia*, skarga nr 62357/14, pkt 101 i przywołane tam orzecznictwo.

[91] Omówienie testu uzasadnionego oczekiwania prywatności oraz powiązanej z nim doktryny strony trzeciej w przepisach federalnych USA z perspektywy problematyki stosowania środków inwigilacyjnych zob. E. Carolan, *Surveillance and the individual's expectation of privacy under the fourth amendment*, „Cambridge Law Journal” 71, 2012, nr 2, s. 250–254.

[92] Por. np. teza Naczelnego Sądu Administracyjnego zawarta w wyroku z 28 kwietnia 2016 roku (sygn. I OSK 2620/14), w którym sąd wskazał, że nieprzejrzystość co do zakresu technik wykorzystywanych przez ABW ma charakter prewencyjny: „Dla osób, które potencjalnie zainteresowane są działalnością przestępczą, w zakresie objętym działaniem organu, sama informacja o posiadanych przez organ możliwościach technicznych ma niebagatelne znaczenie. Osoby takie, mając wiedzę w tym zakresie, muszą się bowiem liczyć z ryzykiem tego, że organy ścigania skorzystają z posiadanych środków, a więc w efekcie mogą próbować zabezpieczyć się przed oddziaływaniem takich środków posiadanych przez organy państwa. To zaś w konsekwencji może utrudnić organowi wykonywanie jego ustawowych działań, a więc może narazić państwo polskie na uszczerbek. Reasumując, niewiedza po stronie osób łamiących prawo, co do informacji objętej niniejszym wnioskiem, ma charakter prewencyjny, utrudniający działania przestępcze”. Jest to zatem pogląd dokładnie przeciwstawny formułowanemu w orzecznictwie ETPC (por. wcześniejsze rozważania dotyczące „przewidywalności” prawa w zakresie ustanawiania środków inwigilacyjnych).

Współczesny model ochrony praw człowieka, przeważający w państwach demokratycznych, zbudowany został w odpowiedzi na tragiczne doświadczenia związane z rządami totalitarnymi, zwłaszcza z faszyzmem. Przepisy, których stosowanie nie może być pogodzone z poszanowaniem godności człowieka, nie zasługują na nazwanie ich prawem. I nie ma przy tym znaczenia, czy regulacje te konstytuują tak skrajne i haniebne naruszenia jak ustawy norymberskie, czy sankcjonują stosowanie nowoczesnych środków inwigilacji całego społeczeństwa. Obecnie dyskusja na temat zakresu stosowania środków nieukierunkowanej inwigilacji prowadzona jest w wielu państwach demokratycznych, w tym europejskich. W rozważaniach tych warto jednak uwzględnić jeszcze jeden głos, postulujący, że demokracja przetrwa także bez stosowania tego typu opresyjnych środków i że żadna korzyść, jaką można w wyniku ich stosowania uzyskać, nie wynagrodzi kosztów społecznych, które zapłacą przyszłe pokolenia.

## Bibliografia


Ackerman S., Ball J., *Optic Nerve: Millions of Yahoo webcam images intercepted by GCHQ*, „The Guardian" 28.02.2014, http://cli.re/Lmrj8p.

Antoszewski A., *Demokracja nieliberalna jako projekt polityczny*, „Przegląd Europejski" 2018, nr 2.

Assange J., *Cypherpunks: Freedom and the Future of the Internet*, New York-London 2012.

Balkin J., *The constitution in the national surveillance state*, „Yale Law School Faculty Scholarship" 2008, z. 225.

Biermann K., Musharbash Y., *A dubious deal with the NSA*, „Zeit Online" 26.08.2015, https://cli.re/AaqwE8.

Bowcott O., *UK–US surveillance regime was unlawful 'for seven years'*, „The Guardian" 6.02.2015, https://cli.re/NMqqV7.

Brown I., *Government access to private-sector data in the United Kingdom*, „International Data Privacy Law" 2012, nr 4.

Brzeziński P., *Stanowisko wybranych sądów konstytucyjnych państw członkowskich UE/WE w sprawie zgodności regulacji implementujących dyrektywę 2006/24/WE z prawami podstawowymi*, „Ius Novum" 2017, nr 1.

Bunkyan T., *Just over the horizon — the surveillance society and the state in the EU*, „Race and Class" 51, 2010, nr 3.

Carolan E., *Surveillance and the individual's expectation of privacy under the fourth amendment*, „Cambridge Law Journal" 71, 2012, nr 2.

Carroll D., *Cambridge Analytica is dead, long live our data*, „Boston Review" 24.05.2018, http://cli.re/g3mPAo.

Cayford M., Pieters W., *The effectiveness of surveillance technology: What intelligence officials are saying*, „The Information Society" 2018, nr 2.

Digital, Culture, Media and Sport Committee, *Disinformation and 'fake news': Interim Report*, House of Commons 2018, https://cli.re/JvqWBm.

Emmens T., Phippen A., *Evaluating online safety programs*, Harvard Berkman Center for Internet and Society 2010, https://cli.re/P3A5Wb.

Evans R., *BAE 'secretly sold mass surveillance technology to repressive regimes'*, „The Guardian" 15.06.2017, http://cli.re/LXdRn4.

Foucault M., *Nadzorować i karać. Narodziny więzienia*, przeł. T. Komendant, Warszawa 1998.

Fuchs Ch., *Societal and ideological impacts of Deep Packet Inspection (DPI) internet surveillance*, „Information, Communication and Society" 16, 2013, nr 8, DOI: 10.1080/1369118X.2013.770544.

Garcia S., *U.S. requiring social media information from Visa applicants*, „The New York Times" 2.06.2019, https://cli.re/mNAVzv.

Gellman B., Soltani A., *NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say*, „The Washington Post" 30.10.2013, https://goo.gl/bYqr9f.

Goold B., *How much surveillance is too much? Some thoughts on surveillance, democracy, and the political value of privacy*, [w:] *Overvåkning i en rettsstat — Surveillance in a Constitutional Government*, red. D. Schartum, Bergen 2010.

Hadjimatheou K., *Ethics and surveillance in authoritarian and liberal states*, The Surveille Project 2013, https://cli.re/qmKnDv.

*Inwigilacji dziennikarzy nie było*, „Polityka" 30.07.2019, https://cli.re/VVp5MR.

Jacobs B., *Keeping our surveillance society non-totalitarian*, „Amsterdam Law Forum" 2009, nr 1 (4).

Kohn M., *Unblinking: Citizens and subjects in the age of video surveillance*, „Constellations" 17, 2010, nr 4.

Kołtuniak Ł., *Nieliberalna demokracja a państwo prawa. Przypadek Węgier Wiktora Orbana*, „Internetowy Przegląd Prawniczy TBSP UJ" 2017, nr 8 (38).

Kuo L., *'The new normal': China's excessive coronavirus public monitoring could be here to stay*, „The Guardian" 9.03.2020, https://cli.re/zPDZzd.

Lach A., *Obowiązek retencji danych telekomunikacyjnych i udostępniania tych danych organom ścigania*, „Monitor Prawniczy" 2017, nr 1.

Lazer D., Kennedy R., King G., Vespignani A., *The parable of Google Flu: Traps in big data analysis*, „Science" 2014, nr 343.

Leibold J., *Surveillance in China's Xinjiang region: Ethnic sorting, coercion, and inducement*, „Journal of Contemporary China" 2019, DOI: 10.1080/10670564.2019.1621529.

Lyon D., *Surveillance, power, and everyday life*, [w:] *The Oxford Handbook of Information and Communication Technologies*, red. R. Mansell *et al*., Oxford 2009.

Madden M., Rainie L., *Americans' attitudes about privacy, security and surveillance*, Pew Research Center 2015, https://cli.re/BwYNjE.

Magen A., *Fighting terrorism: The democracy advantage*, „Journal of Democracy" 29, 2018, nr 1.

Maras M.H., *How to catch a terrorist: Is mass surveillance the answer?*, „Journal of Applied Security Research" 2010, nr 1.

Miles T., *U.N. surveillance expert urges global moratorium on sale of spyware*, „Reuters" 18.07.2019, https://cli.re/YMNNoN.

Mill J., *O wolności*, [w:] *idem*, *Utylitaryzm — O wolności*, przeł. A. Kurlandzka, Warszawa 2006.

Mills A., *Now you see me — now you don't: Journalists' experiences with surveillance*, „Journalism Practice" 13, 2019, nr 6.

Mozur P., Kessel J., Chan M., *Made in China, exported to the world: The surveillance state*, „The New York Times" 24.04.2019, https://cli.re/M3DNek.

Nagy V., *How to silence the lambs? Constructing authoritarian governance in post-transitional Hungary*, „Surveillance & Society" 15, 2017, nr 3–4.

*National Data Retention Laws since the CJEU's Tele-2/Watson Judgment*, „Privacy International" 2017, http://cli.re/68zdoe.

Naughton J., *Death by drone strike, dished out by algorithm*, „The Guardian" 21.02.2016, https://cli.re/X82KD4.

O'Brien B., *U.S. visa applicants to be asked for social media history: State Department*, „Reuters" 30.03.2018, https://cli.re/yZd5Ne.

Odell J., *Inside the dark web of the UAE's surveillance state*, „Middle East Eye" 1.03.2018, https://cli.re/92z4y4.
Ortigosa A., Carro R., Quiroga J., *Predicting user personality by mining social interactions in Facebook*, „Journal of Computer and System Sciences" 2014, nr 1 (80).
Pawełczyk P., Jakubowski J., *Political marketing in the times of big data*, „Przegląd Politologiczny" 2017, nr 3, DOI: 10.14746/pp.2017.22.3.3.
Penney J., *Chilling effects: Online surveillance and Wikipedia use*, „Berkeley Technology Law Journal" 31, 2016.
Podkowik J., *Privacy in the digital era — Polish electronic surveillance law declared partially unconstitutional: Judgment of the Constitutional Tribunal of Poland of 30 July 2014, K 23/11*, „European Constitutional Law Review" 11, 2015.
Postanowienie ETPC z 26 czerwca 2006 roku, *Weber and Saravia v. Niemcy*, skarga nr 54934/00, ECHR 2006-XI.
Reidenberg J., *The data surveillance state in Europe and the United States*, „Wake Forest Law Review" 49, 2014.
Rezolucja Parlamentu Europejskiego z dnia 12 marca 2014 roku w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych (2013/2188(INI)).
Richards N., *The dangers of surveillance*, „Harvard Law Review" 126, 2013.
Rojszczak M., *Cztery fałszywe hipotezy na temat ochrony prywatności i masowej inwigilacji*, „Państwo i Prawo" 2018, nr 10.
Rojszczak M., *The ECtHR's judgment in case of centrum för Rättvisa v. Sweden as a leading case for the review of domestic regulations on signals surveillance*, „Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego" 17, 2019.
Rojszczak M., *Prawne podstawy prowadzenia masowej inwigilacji obywateli opartej na hurtowym i nieukierunkowanym przechwytywaniu danych w UE z uwzględnieniem dorobku orzeczniczego TSUE i ETPC*, „Studia Prawa Publicznego" 2017, nr 2 (18).
Rojszczak M., *Prywatność a bezpieczeństwo publiczne — podstawy prawne prowadzenia programów masowej inwigilacji obywateli*, [w:] *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019.
Rojszczak M., *Prywatność w epoce Wielkiego Brata: podstawy prowadzenia programów masowej inwigilacji w systemie prawnym Stanów Zjednoczonych*, „Ius Novum" 2019, nr 1.
Rojszczak M., *Skuteczność ochrony praw podmiotów danych wynikających z prawa UE w świetle umowy Tarcza Prywatności oraz prawodawstwa federalnego USA*, „Transformacje Prawa Prywatnego" 2018, nr 1.
Rojszczak M., *UK electronic surveillance programmes in the context of protection of EU citizens' rights after Brexit*, „Problemy Współczesnego Prawa Międzynarodowego, Europejskiego i Porównawczego" 16, 2018.
Rubinstein I., Nojeim G., Lee R., *Systematic government access to personal data: A comparative analysis*, „International Data Privacy Law" 2014, nr 2.
Sarnowski J., Selera P., *Reducing the VAT gap: Lessons from Poland*, Polish Economic Institute 2019, https://cli.re/bxx1BA.
Schaller C., *Strategic surveillance and extraterritorial basic rights protection: German intelligence law after Snowden*, „German Law Journal" 18, 2018.
Singer N., *You for sale*, „The New York Times" 17.07.2012, https://goo.gl/reS5Q5.
Sloan L., *ECHELON and the legal restraints on signals intelligence: A need for reevaluation*, „Duke Law Journal" 50, 2001.
Szpringer W., *Nowe technologie a sektor finansowy* fintech *jako szansa i zagrożenie*, Warszawa 2017.

Topak O., *The making of a totalitarian surveillance machine: Surveillance in Turkey under AKP rule*, „Surveillance & Society" 15, 2017, nr 3–4.
Tufekci Z., *Engineering the public: Big data, surveillance and computational politics*, „First Monday" 2014, nr 7 (19), https://cli.re/9295o3.
Wood D., *The 'surveillance society': Questions of history, place and culture*, „European Journal of Criminology" 6, 2009, nr 2.
Wyrok ETPC z 25 marca 1998 roku, *Kopp v. Szwajcaria*, skarga nr 13/1997/797/1000, ECHR 1998-II.
Wyrok ETPC z 16 lutego 2000 roku, *Amann v. Szwajcaria*, skarga nr 27798/95, ECHR 2000-II.
Wyrok ETPC z 18 maja 2010 roku, *Kennedy v. Wielka Brytania*, skarga nr 26839/05.
Wyrok ETPC z 4 grudnia 2015 roku, *Roman Zakharov v. Rosja*, skarga nr 47143/06.
Wyrok ETPC z 12 stycznia 2016 roku, *Szabó i Vissy v. Węgry*, skarga nr 37138/14. Wyrok ETPC z 18 lipca 2017 roku, *Mustafa Sezgin Tanrıkulu v. Turcja*, skarga nr 27473/06.
Wyrok ETPC z 24 kwietnia 2018 roku, *Benedik v. Słowenia*, skarga nr 62357/14.
Wyrok ETPC z 19 czerwca 2018 roku, *Centrum för Rättvisa v. Szwecja*, skarga nr 35252/08.
Wyrok ETPC z 13 września 2018 roku, *Big Brother Watch v. Wielka Brytania*, skargi nr 58170/13, 62322/14 i 24960/15.
Wyrok Naczelnego Sądu Administracyjnego z 28 kwietnia 2016 roku, sygn. I OSK 2620/14.
Wyrok TSUE z 15 grudnia 2009 roku, *Komisja v. Włochy*, C-387/05, EU:C:2009:781.
Wyrok TSUE z 8 kwietnia 2014 roku, *Data Rights Ireland*, C-293/12 i C-594/12, EU:C:2014:238.
Wyrok TSUE z 6 października 2015 roku, *Schrems*, C-362/14, EU:C:2015:650.
Wyrok TSUE z 21 grudnia 2016 roku, *Tele 2 Sverige*, C-203/15 i C-698/15, EU:C:2016:970.
Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 11 grudnia 2015 roku, sygn. II SA/Wa 1330/15.
Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 27 maja 2016 roku, sygn. II SA/Wa 214/16.