INFOTEZY 2026 nr 1(20)
ISSN 2720-006X
e-ISSN 2083-3652

Karolina Czarnecka
Uniwersytet Jana Kochanowskiego w Kielcach
ORCID 0009-0002-8784-6000

Edward Snowden jako bohater debaty publicznej o nadzorze państwowym i ochronie prywatności w erze Internetu

Wprowadzenie

W XXI wieku w Stanach Zjednoczonych coraz wyraźniej widoczne są antagonizmy występujące między swobodą wypowiedzi, a próbami kontroli nad obiegiem informacji. Chociaż amerykańska kultura medialna od lat opiera się na różnorodności poglądów i autonomii dziennikarskiej, nowe zagrożenia i realia technologiczne znacząco wpłynęły na sposób, w jaki informacje są tworzone, przetwarzane i rozpowszechniane. Do największych wyzwań należą kwestie związane z bezpieczeństwem narodowym, cyberatakami oraz wyciekiem poufnych danych. Równocześnie zyskują na znaczeniu media społecznościowe i duże platformy internetowe, które coraz częściej decydują o tym, jakie treści zostają dopuszczone do obiegu, a które są usuwane lub ograniczane. Mimo konstytucyjnie zagwarantowanej wolności słowa, cenzura w Stanach Zjednoczonych istniała od zawsze, przyjmując różne formy. W pewnych sytuacjach uzasadniano ją względami bezpieczeństwa narodowego. Widoczne było to w czasie konfliktów zbrojnych czy napięć międzynarodowych, kiedy ograniczenia w dostępie do informacji miały chronić państwo przed zagrożeniami zewnętrznymi. Znacznie częściej jednak cenzura była narzędziem walki ideologicznej oraz politycznej i służyła do kształtowania opinii społecznej zgodnie z interesami władzy. Właśnie ten drugi rodzaj cenzury stanowi istotne tło dla sprawy Edwarda Snowdena, której konsekwencje wykraczają daleko poza problem bezpieczeństwa, ujawniając mechanizmy selektywnego dostępu do informacji oraz napięć między wolnością jednostki a interesem państwa.

Edward Snowden należy do grona kluczowych postaci współczesnej debaty publicznej o nadzorze państwowym i ochronie prywatności. Ujawnione przez niego w 2013 roku tajne dokumenty amerykańskich służb wywiadowczych doprowadziły do jednego z najpoważniejszych przecieków informacji w historii Stanów Zjednoczonych i odsłoniły rozległy system masowej inwigilacji prowadzonej przez National Security Agency (pol. Agencja Bezpieczeństwa Narodowego) [dalej: NSA] i jej zagranicznych partnerów. Wydarzenia te stały się impulsem do globalnej dyskusji.

Tematem niniejszego artykułu jest ukazanie prób cenzury mediów w XXI wieku na przykładzie sprawy Edwarda Snowdena. Zagadnienie to jest niezwykle istotne we współczesnym świecie, w którym informacja stała się jednym z kluczowych zasobów, a swobodny dostęp do niej stanowi fundament demokracji i społeczeństwa obywatelskiego. W dobie dynamicznego rozwoju technologii cyfrowych i globalnej wymiany danych, pytania o granice wolności słowa, rolę państwa w regulowaniu przekazu medialnego oraz prawa do informacji nabierają wyjątkowego znaczenia.

W artykule postarano się udzielić odpowiedzi na następujące pytania badawcze: 1. Kim jest Edward Snowden i jakie były motywy jego działalności?; 2. Jaki był zakres ujawnionych przez Edwarda Snowdena materiałów i jakie znaczenie miały one dla opinii publicznej?; 3. Jakie były reakcje społeczne, medialne i rządowe na informacje ujawnione przez Snowdena? Przygotowując artykuł zastosowano metodę analizy dokumentów, która umożliwiła zebranie i uporządkowanie dostępnych faktów i regulacji prawnych, a także ukazanie ich w szerszym kontekście społeczno-politycznym. Opracowując zagadnienie posiłkowano się, obok materiałów pochodzących z sieci, literaturą poświęconą osobie Edwarda Snowdena, w tym opublikowanymi przez niego wspomnieniami[1] oraz relacjami dziennikarzy, takich jak Glenn Greenwald[2] i Luke Harding[3].

Sprawa Edwarda Snowdena

Edward Joseph Snowden urodził się 21 czerwca 1983 roku w Elizabeth City w stanie Karolina Północna. Jego ojciec, Lonnie, pełnił służbę w amerykańskiej straży przybrzeżnej, natomiast matka, Elizabeth, pracowała jako urzędniczka w sądownictwie federalnym. Edward Snowden wychował się wraz ze starszą siostrą Jessicą w konserwatywnym środowisku rodzinnym. W dzieciństwie przeprowadził się z rodziną do stanu Maryland, w pobliże Waszyngtonu, co miało istotne znaczenie, ponieważ w bezpośrednim sąsiedztwie znajdowała się siedziba NSA[4]. Już w wieku kilkunastu lat Edward Snowden ujawniał wyraźne zainteresowania informatyką oraz szeroko rozumianą cyberkulturą. Pod pseudonimem „TheTrueHOOHA" stał się aktywnym użytkownikiem portalu „Ars Technica",

[1] E. Snowden, *Pamięć nieulotna*, Kraków 2019.

[2] G. Greenwald, *Snowden. Nigdzie się nie ukryjesz*, Warszawa 2014.

[3] L. Harding, *Polowanie na Snowdena*, Warszawa cop. 2014.

[4] Tamże, s. 23.

gdzie publikując niemal 800 wpisów, regularnie angażował się w dyskusje o charakterze technicznym. W swoich wypowiedziach przedstawiał zarówno sytuację zawodową, jak i życie prywatne, deklarując między innymi posiadanie certyfikatu bezpieczeństwa, wydanego przez Departament Stanu USA. Analiza tych wpisów ujawnia nie tylko wysokie kompetencje techniczne Snowdena, lecz także wyraziste, nierzadko kontrowersyjne poglądy polityczne i światopoglądowe. Konsekwentnie sprzeciwiał się nadmiernej ingerencji państwa w życie obywateli. Jego aktywność w sieci „urywa się" nagle w maju 2012 roku, ponieważ w tym czasie, zgodnie z ustaleniami dziennikarzy, rozpoczął przygotowania do ujawnienia dokumentów dotyczących masowej inwigilacji[5].

Wspomnienia Snowdena z okresu nauki w liceum mają charakter wyrywkowy i nie tworzą spójnej narracji. W tamtym czasie zmagał się z poważnymi problemami ze snem, nie był w stanie prawidłowo funkcjonować w ciągu dnia, a czas przeznaczony na odpoczynek, spędzał głównie przy komputerze, co dodatkowo umacniało jego związek z technologią. W Arundel High School nauczyciele tolerowali na ogół jego nawyk zasypiania na lekcjach, o ile nie zakłócał on przebiegu zajęć[6].

W wieku 16 lat Edward Snowden rozpoczął naukę w lokalnym college'u Anne Arundel Community College, gdzie uczęszczał na zajęcia z informatyki. Kształcenie w tym kierunku stanowiło naturalne rozwinięcie jego wcześniejszych zainteresowań nowoczesnymi technologiami, jednak ze względów zdrowotnych nigdy nie ukończył uczelni. Po rozwodzie rodziców jego sytuacja życiowa uległa dalszym zmianom. Początkowo mieszkał ze współlokatorem, a następnie przeprowadził się do matki, osiedlając się w Ellicott City – miejscowości położonej w bezpośrednim sąsiedztwie NSA, określanej potocznie mianem „Puzzle Palace". Codzienność Snowdena toczyła się zatem w cieniu jednej z kluczowych instytucji amerykańskiego aparatu bezpieczeństwa, co miało wpływ na jego późniejszy wybór ścieżki zawodowej. Momentem przełomowym w jego biografii okazał się okres po 2003 roku, kiedy inwazja Stanów Zjednoczonych na Irak skłoniła go do wstąpienia do armii. Snowden deklarował wówczas, że pragnie nieść pomoc osobom zniewolonym w odzyskaniu wolności[7]. W 2004 roku rozpoczął szkolenie w ośrodku Fort Benning. Szkolenie to miało przygotowywać rekrutów do służby w jednostkach specjalnych, a zatem zakładało wysoki poziom sprawności fizycznej i psychicznej. Ze względu na drobną posturę przy jednocześnie niskiej wadze, szybko zwrócił uwagę instruktorów, którzy nadali mu pseudonim „Śnieżynka". Pomimo dobrej kondycji fizycznej, Snowden wielokrotnie odnosił urazy w trakcie szkolenia, które ostatecznie uniemożliwiły mu kontynuowanie służby wojskowej[8].

[5] Tamże, s. 19-22.

[6] E. Snowden, *Pamięć*..., s. 83.

[7] L. Harding, *How Edward Snowden went from loyal NSA contractor to whistleblower*, https://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract, [dostęp: 22 listopada 2025].

[8] E. Snowden, *Pamięć*..., s. 115-117.

Po powrocie do domu Edward Snowden podjął pracę w Centrum Zaawansowanych Studiów Językowych na Uniwersytecie Maryland, które współpracowało z NSA. Początkowo zatrudniony był na stanowisku ochroniarza, w krótkim czasie powrócił do zadań związanych z technologiami informatycznymi. W 2006 roku znalazł zatrudnienie w dziale informatycznym Central Intelligence Agency (pol. Centralna Agencja Wywiadowcza) [dalej: CIA], gdzie kompetencje techniczne umożliwiły mu awans, mimo braku ukończonych studiów wyższych. W 2007 roku został oddelegowany do Genewy jako specjalista do spraw bezpieczeństwa teleinformatycznego przy ambasadzie Stanów Zjednoczonych, gdzie odpowiadał między innymi za zabezpieczenia sieciowe oraz wsparcie techniczne. W tym okresie coraz wyraźniej ujawniały się jego libertariańskie poglądy polityczne[9]. Snowden deklarował poparcie dla kandydata na prezydenta Rona Paula, jednocześnie krytycznie oceniając Baracka Obamę, a także działania administracji prezydenta w obszarze polityki zbrojeniowej oraz jawności informacji[10].

W Szwajcarii działalność CIA koncentrowała się na gromadzeniu informacji dotyczących sektora bankowego. Snowden był wówczas zatrudniony w amerykańskiej misji przy ONZ i posiadał paszport dyplomatyczny. Właśnie w tym okresie po raz pierwszy dostrzegł, na co gotowi byli agenci CIA. System awansów uzależniony był w znacznym stopniu od liczby zwerbowanych informatorów, co prowadziło do silnej rywalizacji między funkcjonariuszami i sprzyjało praktyce rekrutowania niemal każdego, kto mógł zostać wykorzystany, niezależnie od jego realnej wartości wywiadowczej. W ramach tych działań zdarzało się, że potencjalnych współpracowników celowo upijano do nieprzytomności, doprowadzając do ich zatrzymania przez policję, a następnie wyciągano ich za kaucją, budując w ten sposób relację opartą na długu wdzięczności. W Genewie Snowden spotkał również wielu przedstawicieli środowisk wywiadowczych, krytycznie nastawionych do wojny w Iraku i ogólnej polityki Stanów Zjednoczonych. Z uwagi na charakter pracy przy systemach komputerowych, Snowden dysponował szerokim, a w praktyce niemal nieograniczonym, dostępem do informacji dotyczących przebiegu tego konfliktu zbrojnego[11].

W 2009 roku zrezygnował z pracy w CIA i rozpoczął współpracę z NSA jako kontraktor firmy „Dell", początkowo w Japonii, a następnie na Hawajach. Zainteresowanie Japonią i jej kulturą, obecne u niego od czasów młodości, częściowo wyjaśniało jego pozytywne nastawienie do nowej funkcji i miejsca oddelegowania. W tym czasie coraz wyraźniej ujawniła się jego krytyczna ocena rosnącej skali nadzoru, prowadzonego przez amerykańskie służby. Doświadczenia z pracy w terenie doprowadziły go do przekonania, że działania wywiadu częściej generują szkody, niż przynoszą realne korzyści[12].

[9] Szerzej zob. K. Jasiński, *Główne idee libertarianzimu*, „Studia Warmińskie" 2022, vol. 59, s. 7-24.

[10] L. Harding, *Polowanie*…, s. 29-30.

[11] J. Bamford, *The most Wanted Man in the World*, https://interactive.wired.com/www-wired-com__2014__08__edward-snowden/index.html#ch-5, [dostęp: 23 listopada 2025].

[12] E. Snowden, *Pamięć*..., s. 218-219.

Podczas pracy Snowdena w NSA jednym z kluczowych wyzwań związanych z tworzeniem globalnego systemu odzyskiwania danych, była konieczność obsługi duplikatów informacji, wynikającej z masowego przesyłania identycznych plików pomiędzy komputerami. Prowadziło to do nadmiernego obciążenia nośników pamięci oraz kanałów transmisyjnych, co w praktyce utrudniło efektywne przekazywanie danych, m.in. do ośrodków, takich jak Fort Meade. Problem ten powierzono Snowdenowi, który miał go rozwiązać za pomocą deduplikacji, rozumianej jako proces identyfikacji unikalnych danych. Opracowany przez niego system analizował zawartość bloków danych w celu określenia ich niepowtarzalności, co umożliwiło przesyłanie wyłącznie tych plików, których kopii nie przechowano jeszcze w centralnej bazie. Zastosowanie deduplikacji, w połączeniu z rozwojem technologii magazynowania informacji, pozwoliło NSA na znaczne wydłużenie okresu przechowywania danych wywiadowczych. Postępująca miniaturyzacja i rosnące możliwości techniczne sprawiły, że nośniki o wcześniej nieosiągalnej pojemności stawały się dostępne w relatywnie krótkim czasie. W rezultacie NSA stopniowo zrezygnowała z praktyki usuwania danych, gromadząc je na wypadek ich potencjalnej przyszłej użyteczności. Celem tego podejścia było stworzenie nieulotnego systemu pamięci, opartego na maksymalnie szerokim gromadzeniu wszelkich możliwych informacji, niezależnie od ich bieżącej przydatności[13].

W ramach procedur obowiązujących w NSA stosowano protokoły służące klasyfikacji nazw kodowych oprogramowania. System nazewnictwa miał pozornie losowy charakter. Jednakże, był on powiązany z funkcją danego rozwiązania. Przykładowo, kryptonim FOXACID odnosił się do serwera wykorzystywanego do infiltracji przeglądarek, natomiast EGOTISTICALGIRAFFE używany był w kontekście ataków na sieci TOR[14]. W odróżnieniu od praktyk NSA, Snowden nie opracowywał technik kryptograficznych mających na celu ukrycie systemów odpowiedzialnych za tworzenie kopii zapasowych. Pierwsza zastosowana przez niego nazwa kodowa EPICSHELTER, zyskała szczególne znaczenie w momencie, gdy w późniejszym okresie NSA wdrożyła ten system pod nazwą „Plan Modernizacji Magazynu Danych". W ciągu dwóch lat rozwiązanie to, w zmodyfikowanej formie, zostało zaadaptowane do użytku operacyjnego. System EPICSHELTER stanowi punkt wyjścia dla zrozumienia kierunku działań NSA. Rozwijany był on w ramach programu finansowanego przez Joint Counterintelligence Training Academy (JCITA, pol. Wspólna Akademia Szkolenia Kontrwywiadowczego), współpracującą z Defense Intelligence Agency (DIA, pol. Agencja Wywiadowcza Departamentu Obrony) oraz innymi służbami specjalizującymi się w prowadzeniu tajnych operacji[15].

[13] Tamże, s. 222-223.

[14] *The Onion Router* (sieć TOR) – to usługa działająca w Internecie, która zapewnia wyższą anonimowość, niż ma to miejsce w przypadku zwykłej sieci. Zob. S*ieć Tor, anonimizacja ruchu*, https://home.agh.edu.pl/~pmarynow/pliki/2021zima/tor.pdf, [dostęp: 8 grudnia 2025].

[15] E. Snowden, *Pamięć*..., s. 222-223.

Podczas konferencji specjalistów służb wywiadowczych (w tym przedstawicieli NSA, CIA, FBI oraz wywiadu wojskowego) omawiano zagadnienia związane z metodami przeciwdziałania atakom prowadzonym przez chińskich hakerów przeciwko Stanom Zjednoczonym. Snowden postanowił w tym kontekście przygotować prezentację poświęconą przenikaniu się tradycyjnego kontrwywiadu z nową dziedziną, jaką stał się cyberwywiad. Na potrzeby wystąpienia zgromadził materiały z zasobów NSA i CIA, obejmujące raporty oraz analizy dotyczące tzw. *intrusion sets*, czyli zestawów danych opisujących zaawansowane operacje cyberprzestępcze. Dążąc do pełniejszego zrozumienia problematyki, Snowden szczegółowo zapoznał się z dokumentacją dotyczącą elektronicznego śledzenia agentów amerykańskich działających na terenie Chińskiej Republiki Ludowej. Choć początkowo postrzegał Chiny jako typowy reżim autorytarny, jego uwagę stopniowo zaczęły przyciągać analogie między tamtejszym systemem nadzoru, a mechanizmami stosowanymi przez Stany Zjednoczone. Analizując chińskie rozwiązania w obszarze inwigilacji, dostrzegł, że wiele z nich opiera się na technologiach i założeniach, które mogą być równie dobrze wykorzystywane w systemie amerykańskim. Kluczowe znaczenie zyskała dla niego zasada, zgodnie z którą „jeśli da się coś zrobić, to najprawdopodobniej ktoś to zrobi albo już zrobił", a państwo dysponujące największym dostępem do informacji – takie jak Stany Zjednoczone, nie mogło stanowić wyjątku. Snowden wskazywał na podobieństwa w metodach kontroli informacji, szczególnie w odniesieniu do „Wielkiego Firewalla" (zapory sieciowej) oraz technik cenzury stosowanych przez władze w Pekinie, zestawiając je z praktykami amerykańskich służb w zakresie cyberbezpieczeństwa i nadzoru. Refleksje te doprowadziły go do głębokich wątpliwości, co do rzeczywistej granicy między systemem demokratycznym, a rozbudowanym aparatem kontroli[16].

Podejmując w 2009 roku zatrudnienie w NSA, Snowden dysponował zaledwie nieznacznie szerszą wiedzą na temat jej działalności, niż przeciętny obywatel Stanów Zjednoczonych. Z dostępnych wówczas doniesień prasowych wynikało, że NSA realizowała liczne programy wywiadowcze, zatwierdzone przez prezydenta George'a W. Busha po ataku na World Trade Center. Szczególną uwagę zwracała prezydencka inicjatywa tzw. President's Surveillance Program (pol. Program Nadzoru Prezydenckiego) [dalej: PSP], która stała się przedmiotem ostrej krytyki opinii publicznej. Chodziło o podsłuchy prowadzone bez uprzedniego nakazu sądowego, stanowiące element PSP. Istnienie tego programu zostało ujawnione w 2005 roku dzięki demaskatorom z NSA oraz Departamentu Sprawiedliwości, o czym poinformował dziennik „The New York Times". Po ujawnieniu tych informacji PSP formalnie zamknięto w 2007 roku. Jak się jednak okazało, deklaracje dotyczące zakończenia praktyk podsłuchowych miały pozorny charakter. W ostatnich latach prezydentury Busha juniora, Kongres uchwalił dwie ustawy – *Protect American* w 2007 roku oraz *FISA Amendments Act* w 2008

[16] Tamże, s. 225-226.

roku, które w istocie zalegalizowały działania NSA oraz zapewniły immunitet dostawcom Internetu i operatorom telekomunikacyjnym uczestniczącym w PSP[17].

Sytuacja prawna programów inwigilacyjnych prowadzonych przez NSA została omówiona w raporcie opublikowanym w lipcu 2009 roku przez inspektoraty generalne pięciu agencji federalnych: Departamentu Obrony, Departamentu Sprawiedliwości, CIA, NSA oraz Biura Dyrektora Krajowego Wywiadu. Dokument *Unclassified Report on the President's Surveillance Program* (niejawny raport poświęcony programowi inwigilacyjnemu prezydenta), miał w założeniu zastąpić postępowanie dochodzeniowe Kongresu dotyczące działań NSA. Choć raport zawierał istotne informacje, w ocenie Snowdena jego wartość analityczna była ograniczona. Wiele kwestii pominięto, a odpowiedzialność za podejmowane decyzje została rozproszona. Sam dokument w istocie bronił legalności opisywanych programów. Dążąc do zrozumienia motywów, które skłoniły pracowników Departamentu Sprawiedliwości do ujawnienia informacji o PSP, Snowden postanowił odnaleźć poufną wersję raportu. Po przeszukaniu szerokiego zbioru dokumentów początkowo przerwał swoje działania, jednak po pewnym czasie natrafił na poszukiwany materiał. Okazał się nim raport objęty najwyższym poziomem tajności sklasyfikowany jako *Exceptionally Controlled Information* (ECI). Zawierał on treści, których brakowało w publicznie dostępnych raportach – szczegółowe informacje dotyczące najbardziej kontrowersyjnych programów inwigilacyjnych prowadzonych przez NSA. Programy te realizowano przy współudziale Departamentu Sprawiedliwości oraz z wykorzystaniem technologii amerykańskich korporacji, nierzadko z naruszeniem obowiązujących przepisów prawa[18].

Szczególną uwagę Edwarda Snowdena zwróciło porównanie treści jawnej i tajnej wersji raportu. Choć formalnie odnosiły się one do tych samych zagadnień, wersja niejawna zawierała szereg dodatkowych informacji, które ujawniły skalę oraz strukturę amerykańskich operacji inwigilacyjnych. Część jawna koncentrowała się na działaniach podjętych po atakach na World Trade Center, uzasadniając je koniecznością pozyskiwania informacji wywiadowczych. Natomiast wersja tajna ukazywała rozległy proces gromadzenia danych oraz systematyczne poszerzanie uprawnień operacyjnych NSA. Dla Snowdena stanowiło to potwierdzenie, że faktyczna działalność NSA w znacznym stopniu wykracza poza to, co przedstawiono opinii publicznej. Dane zaczęto gromadzić już od 2001 roku, a każda administracja kolejnego prezydenta zyskiwała możliwość objęcia inwigilacją praktycznie każdej osoby posiadającej telefon lub komputer. Umożliwiało to szczegółową analizę tożsamości, aktywności, lokalizacji, sieci kontaktów oraz przeszłości danej jednostki. Z upływem czasu Snowden docierał do coraz większej liczby informacji dotyczących skali i mechanizmów inwigilacji[19].

[17] Tamże, s. 227-228.
[18] Tamże, s. 229-230.
[19] Tamże, s. 232-233, 235-236.

Na początku 2013 roku Edward Snowden objął stanowisko w firmie doradczej Booz Allen Hamilton na Hawajach, co otworzyło mu dostęp do najbardziej wrażliwych zasobów informacyjnych NSA. Jako jeden z około tysiąca administratorów systemów, dysponował uprawnieniami pozwalającymi na przeglądanie rozległych zbiorów danych wywiadowczych w sposób, który nie pozostawiał po sobie żadnych śladów. Dodatkowo, dzięki różnicy czasu miał możliwość zdalnego logowania się do systemów NSA w godzinach nocnych. W tym okresie Snowden systematycznie kopiował wybrane dokumenty na nośniki zewnętrzne typu pendrive. Z racji pełnionej funkcji administratora mógł to uzasadnić potrzebą tworzenia kopii zapasowych lub wykonywania czynności serwisowych. Po upływie około czterech tygodni zatrudnienia zgłosił problemy zdrowotne i wystąpił o udzielenie urlopu bezpłatnego. 20 maja 2013 roku opuścił terytorium Stanów Zjednoczonych[20].

W grudniu 2012 roku nawiązał kontakt z dziennikarzem „The Guardian" Glennem Greenwaldem, posługując się pseudonimem „Cincinnatus" i zwrócił się do niego z prośbą o zainstalowanie oprogramowania szyfrującego PGP. Greenwald początkowo zlekceważył tę korespondencję. Do sprawy powrócił 18 kwietnia 2013 roku, kiedy otrzymał e-mail od dokumentalistki Laury Poitras. W wiadomości Poitras podkreślała konieczność niezwłocznego spotkania. Greenwald odpowiedział na wiadomość zaraz po przylocie do Stanów Zjednoczonych, informując, gdzie aktualnie przebywa. Podczas rozmowy w restauracji, mimo pozornej swobody, obie strony zachowywały dyskrecję. Poitras wyjaśniła, że otrzymała anonimową wiadomość od osoby posiadającej dostęp do wysoce tajnych dokumentów, kompromitujących rząd Stanów Zjednoczonych, dotyczących działań wywiadowczych, w tym inwigilacji obywateli amerykańskich. Zaproponowała Greenwaldowi współpracę przy publikacji tych materiałów. Informator nalegał, aby rozmowy na tematy wrażliwe były prowadzone wyłącznie po uprzednim wyjęciu baterii z telefonów, w celu zminimalizowania ryzyka podsłuchu. Zalecił również, by Poitras nie rozdzielała dokumentów i stale przechowywała je przy sobie, ponieważ odgrywały one kluczową rolę w ujawnieniu prawdy[21].

Po pewnym czasie Laura Poitras była przygotowana, by ujawnić posiadane informacje. W tym celu udała się do Hongkongu, gdzie przebywał Edward Snowden. Na tydzień przed spotkaniem z Poitras i Greenwaldem, Snowden opracował podsumowanie swojej działalności, które miało posłużyć jako materiał briefingowy dla dziennikarzy. Jego zamiarem było przekonanie ich, że rząd Stanów Zjednoczonych prowadzi rzeczywistą, globalną inwigilację oraz wyjaśnienie mechanizmów i metod stosowanych w tym procesie. W związku z tym przygotował słownik terminów związanych z technologią wywiadowczą, mający ułatwić szybkie i przejrzyste zrozumienie przedstawianych zagadnień. Prioryte-

[20] L. Harding, *How Edward Snowden*…

[21] G. Greenwald, *Snowden. Nigdzie*…, s. 18-21.

tem było uporządkowanie najpoważniejszych nadużyć w sposób logiczny oraz ich klarowne zaprezentowanie[22].

Dnia 2 czerwca 2013 roku Glenn Greenwald i Laura Poitras przybyli do Hongkongu. Zgodnie z uprzednio ustalonymi instrukcjami spotkali się z Edwardem Snowdenem, po czym wspólnie udali się do jego pokoju hotelowego. Poitras zarejestrowała ich spotkanie za pomocą kamery cyfrowej. W tym czasie Snowden szczegółowo przedstawił Greenwaldowi strukturę, zasady funkcjonowania oraz cele kluczowych programów inwigilacyjnych, prowadzonych przez NSA. Zwracał szczególną uwagę na udział prywatnych przedsiębiorstw technologicznych, które zarówno świadomie, jak i pod presją władz państwowych, uczestniczyły w przekazywaniu danych. Podkreślał, że informacje trafiające do NSA pochodziły bezpośrednio z centrów przetwarzania danych największych korporacji technologicznych i obejmowały m.in. wiadomości e-mail, historię wyszukiwania oraz treści przesyłane za pośrednictwem komunikatorów internetowych. Programy takie jak *Planning Tool For Resource Integration, Synchronization and Management* (PRISM) umożliwiły masowy dostęp do danych użytkowników bez ich wiedzy i zgody. W dniach 3-9 czerwca 2013 roku Edward Snowden pozostawał w pokoju hotelowym w towarzystwie Laury Poitras, Glenna Greenwalda, Ewena MacAskilla z „The Guardian", a zdalnie dołączył do nich Barton Gellman z „The Washington Post". Poitras pracowała w tym czasie nad dokumentacją filmową dotyczącą programów NSA, podczas gdy pozostali przygotowywali artykuły prasowe[23]. 6 czerwca 2013 roku w dzienniku „The Guardian" ukazał się pierwszy artykuł autorstwa Glenna Greenwalda poświęcony problematyce inwigilacji. Tekst ujawniał, że administracja prezydenta Baracka Obamy kontynuowała praktyki masowej inwigilacji obywateli, zapoczątkowane po 11 września 2001 roku przez administrację George'a W. Busha. Działania te opierały się na szerokiej interpretacji przepisów ustawy USA PATRIOT Act, która umożliwiła gromadzenie danych bez konieczności wskazania konkretnych podejrzanych. Ponadto, na mocy tajnego nakazu sądu FISA z kwietnia 2013 roku, firma Verizon Wireless – największy operator telefonii komórkowej w USA[24], została zobowiązana do codziennego przekazywania NSA metadanych wszystkich połączeń telefonicznych, zarówno krajowych, jak i międzynarodowych. Przekazywane informacje obejmowały m.in. numery telefonów, czas trwania połączeń oraz dane dotyczące lokalizacji rozmówców, przy czym nie rejestrowano treści rozmów[25].

Następnego dnia w „The Guardian" ukazał się kolejny artykuł, w którym poinformowano, że NSA uzyskała bezpośredni dostęp do systemów, takich firm jak Google, Facebook, Apple czy Microsoft w ramach programu PRISM. Program

[22] E. Snowden, *Pamięć...*, s. 370-371.

[23] Tamże, s. 372-374.

[24] *Verizon Wireless*, w: *Wikipedia*, https://pl.wikipedia.org/wiki/Verizon_Wireless, [dostęp: 8 grudnia 2025].

[25] G. Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, [dostęp: 1 grudnia 2025].

ten umożliwiał inwigilację osób, które „z dużym prawdopodobieństwem" przebywały poza terytorium Stanów Zjednoczonych. Ujawnione dokumenty wskazały jednak, iż w rzeczywistości gromadzono również dane osób znajdujących się na obszarze USA. Przedstawiciele Apple i Google oświadczyli, że nie przekazują danych rządowi bez uprzedniego nakazu sądowego, oraz że nigdy wcześniej nie słyszeli o programie PRISM[26].

Program PRISM został uruchomiony w 2007 roku. Do 2012 roku dołączyły do niego m.in. Microsoft, Yahoo, Google, Facebook, YouTube, Skype, AOL oraz Apple, a NSA planowała rozszerzenie współpracy o kolejne podmioty, w tym Dropbox. Z ujawnionych dokumentów wynikało, że FBI pełniło rolę pośrednika między NSA a firmami technologicznymi. Pozyskiwane w ramach programu dane obejmowały m.in. wiadomości e-mail, pliki, fotografie, rozmowy audio i wideo, a także informacje pochodzące z komunikatorów internetowych oraz serwisów społecznościowych. NSA określała PRISM jako „jedno z najcenniejszych i najbardziej produktywnych narzędzi operacyjnych". Ówczesny szef NSA gen. Keith Alexander twierdził natomiast, że dzięki PRISM udało się zapobiec około 50 „spiskom terrorystycznym", dlatego ujawnienie informacji na temat tego narzędzia „stanowi olbrzymią, niemożliwą do naprawienia szkodę dla USA i ich sojuszników"[27].

Dnia 11 czerwca 2013 roku w „The Guardian" opublikowano artykuł przedstawiający sylwetkę Edwarda Snowdena, co oznaczało jego publiczne ujawnienie jako sygnalisty. Snowden podkreślał, że jego działania nie były motywowane względami osobistymi, lecz wynikały z potrzeby zachowania wierności własnym zasadom. Jego celem było ujawnienie nadużyć systemu, a nie wyrządzenie szkody konkretnym osobom. Snowden zrezygnował z anonimowości, aby pokazać, że nie ma nic do ukrycia. Zdawał sobie sprawę z ryzyka, w tym możliwości oskarżenia o szpiegostwo, jednak, jak sam wskazywał, decyzja ta była w pełni świadoma. Doświadczenia zdobyte podczas pracy w CIA i NSA, a także obserwacja praktyk wywiadowczych skłoniły go do krytycznej refleksji nad funkcjonowaniem państwa amerykańskiego. W jego ocenie powszechna inwigilacja prowadzi do destrukcji prywatności oraz ograniczenia przestrzeni dla wolności intelektualnej. Snowden zaznaczył, że ujawnił wyłącznie te dokumenty, które miały znaczenie publiczne i przekazał je dziennikarzom, ufając ich odpowiedzialności w zakresie doboru materiałów do publikacji. Jego dalsze losy pozostawały niepewne. Liczył na uzyskanie azylu (w szczególności rozważał Islandię), jednocześnie mając świadomość, że jego decyzja oznacza długotrwałą izolację oraz życie pod stałym nadzorem. Pomimo tego był przekonany, że podjęte przez niego działania mogą

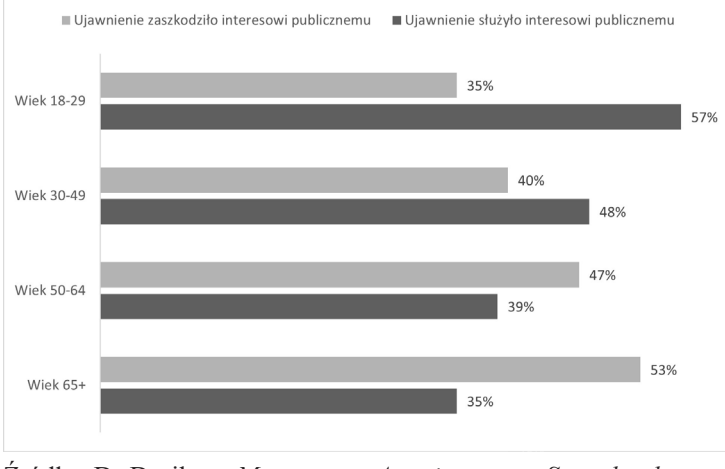
[26] G. Greenwald, E. MacAskill, *NSA Prism program taps in to user data of Apple, Google and others*, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, [dostęp: 1 grudnia 2025].

[27] Tamże; M. Grzelak, *Skutki sprawy Edwarda Snowdena dla prywatności danych w cyberprzestrzeni*, „Bezpieczeństwo Narodowe" 2015, nr 1, s. 192.

zainicjować globalną debatę na temat granic wolności, ochrony prywatności oraz zakresu odpowiedzialności państwa[28].

Po upublicznieniu przez Edwarda Snowdena dokumentów przeprowadzono szereg badań opinii publicznej, koncentrujących się m.in. na obawach przed nadmierną kontrolą ze strony instytucji państwowych oraz na ewentualnych zmianach w sposobie korzystania z technologii. Z badania zrealizowanego przez bezstronny ośrodek analityczny Pew Research Center we współpracy z gazetą „USA Today" wynika, że młodzi dorośli wykazują wyższy poziom poparcia zarówno dla samego Snowdena, jak i dla ujawnionych przez niego informacji dotyczących nadzoru telefonicznego i internetowego prowadzonych przez NSA, niż ma to miejsce w starszych grupach wiekowych[29]. Wyniki tych badań zob. wykr. 1.

Wykres 1. Ocena ujawnionych przez Edwarda Snowdena programów inwigilacyjnych



Źródło: D. Desilver, *Most young Americans say Snowden has served the public interest*, https://www.pewresearch.org/short-reads/2014/01/22/most-young-americans-say-snowden-has-served-the-public-interest/, [dostęp: 1 grudnia 2025].

Z przedstawionych danych wynika, że młodzi dorośli w wieku 18-29 lat zdecydowanie częściej postrzegają działania Edwarda Snowdena jako służące interesowi publicznemu (57%), podczas gdy wśród osób powyżej 65. roku życia odsetek ten wynosi jedynie 35%. Odwrotna zależność widoczna jest w przypadku ocen negatywnych – aż 53% najstarszych ankietowanych, uważa że ujawnienie dokumentów zaszkodziło interesowi publicznemu, w porównaniu z 35%

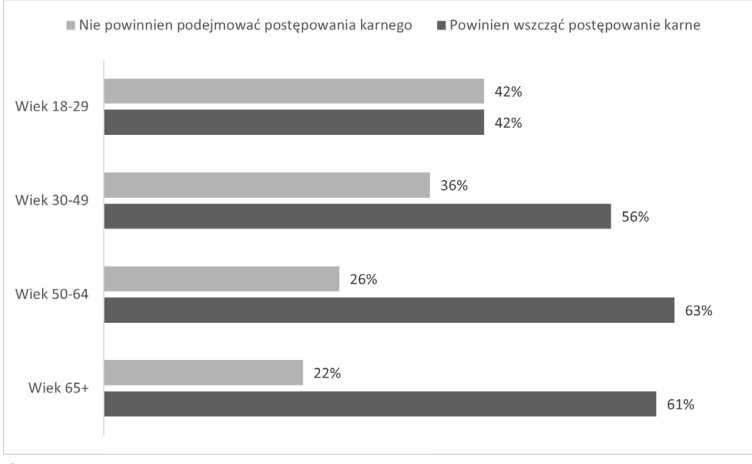
[28] G. Greenwald, E. MacAskill, L. Poitras, *Edward Snowden. The whistleblower behind the NSA surveillance revelations*, https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance, [dostęp: 1 grudnia 2025].

[29] D. Desilver, *Most young Americans say Snowden has served the public interest*, https://www.pewresearch.org/short-reads/2014/01/22/most-young-americans-say-snowden-has-served-the-public-interest/, [dostęp: 1 grudnia 2025].

w grupie najmłodszej. Wraz z wiekiem rośnie zatem odsetek osób krytycznie oceniających działania Snowdena.

Poglądy opinii publicznej dotyczące zasadności postawienia Edwarda Snowdena przed sądem zob. wykr. 2.

Wykres 2. Opinia publiczna w sprawie zasadności wszczęcia postępowania karnego przeciwko Edwardowi Snowdenowi

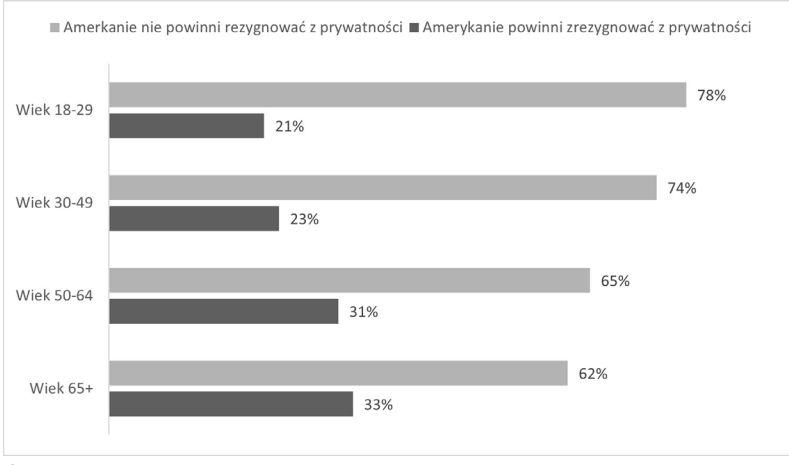


Źródło: D. Desilver, *Most young Americans say Snowden has served the public interest*, https://www.pewresearch.org/short-reads/2014/01/22/most-young-americans-say-snowden-has-served-the-public-interest/, [dostęp: 1 grudnia 2025].

W grupie młodych dorosłych w wieku 18-29 lat odpowiedzi były najbardziej zróżnicowane. 42% uważało, że Snowden powinien zostać oskarżony, natomiast taki sam odsetek sprzeciwiał się postępowaniu karnemu wobec niego. W grupie wiekowej 30-49 lat, 56% respondentów opowiadało się za wszczęciem postępowania karnego, podczas gdy 36% było temu przeciwnych. Wśród osób w wieku 50-64 lat oraz 65+ dominowało poparcie dla działań karnych (odpowiednio 63% i 61%), przy czym sprzeciw wyrażało jedynie 26% i 22% ankietowanych. Dane te wskazują, że wraz z wiekiem rośnie odsetek osób popierających pociągnięcie Snowdena do odpowiedzialności karnej. Najmłodsza grupa respondentów jest zarazem najbardziej spolaryzowana i najmniej skłonna do jednoznacznego potępienia jego działań.

Kolejne pytanie dotyczyło gotowości Amerykanów do rezygnacji z części swojej prywatności, czyli zaakceptowania wzmożonej inwigilacji w imię walki z terroryzmem oraz podniesienia poziomu bezpieczeństwa państwa. Struktura udzielonych odpowiedzi zob. wykr. 3.

Wykres 3. Postawy Amerykanów wobec ograniczania prywatności i wolności na rzecz zwiększenia bezpieczeństwa przed terroryzmem



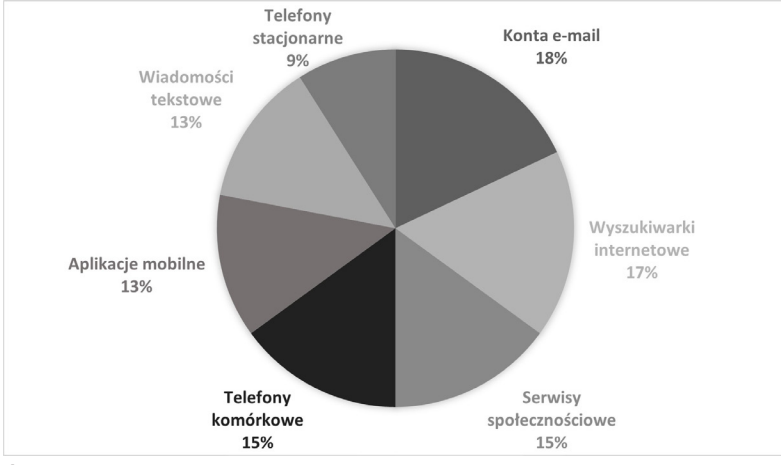
Źródło: D. Desilver, *Most young Americans say Snowden has served the public interest,* https://www.pewresearch.org/short-reads/2014/01/22/most-young-americans-say-snowden-has-served-the-public-interest/, [dostęp: 1 grudnia 2025].

W grupie najmłodszych respondentów aż 78% badanych odrzucało możliwość rezygnacji z prywatności w zamian za bezpieczeństwo. W kolejnych kategoriach wiekowych odsetek osób akceptujących takie rozwiązanie stopniowo wzrastał. W grupie 65+ na tego rodzaju poświęcenie godziło się 33% ankietowanych, przy czym nadal przeważały postawy sprzeciwu (62%). Uzyskane wyniki wskazują, że młodsze pokolenia Amerykanów są w większym stopniu przywiązane do wartości związanych z ochroną prywatności oraz wolności obywatelskich niż osoby starsze.

Badanie zrealizowane przez Pew Research Center miało ukazać, czy i w jaki sposób obywatele Stanów Zjednoczonych zmodyfikowali sposoby korzystania z nowych technologii komunikacyjnych pod wpływem afery Snowdena. Zestawienie wyników zob. wykr. 4.

Wśród 87% dorosłych Amerykanów, którzy słyszeli o omawianych programach inwigilacyjnych, 25% zadeklarowało, że zmieniło swoje nawyki korzystania z co najmniej jednej technologii. Najczęściej modyfikacje dotyczyły poczty elektronicznej: 18% badanych korzysta z e-maila rzadziej lub z większą ostrożnością, np. rezygnując z przesyłania tą drogą informacji wrażliwych. 17% respondentów zmieniło sposób korzystania z wyszukiwarek internetowych, unikając wyszukiwania określonych treści, bądź wybierając wyszukiwarki oferujące wyższy poziom ochrony prywatności. Kolejne obszary wskazane przez ankietowanych to media społecznościowe (15%), gdzie użytkownicy publikują mniej informacji osobistych lub modyfikują ustawienia prywatności. Również 15% respondentów zmieniło sposób korzystania z telefonów komórkowych i nie rozmawia na tematy wrażliwe. Ankietowani rzadziej deklarowali zmianę sposobu

Wykres 4. Wpływ ujawnienia programów inwigilacyjnych na sposób korzystania z technologii przez użytkowników (respondenci mogli wskazać więcej niż jedną odpowiedź)



Źródło: A.W. Geiger, *How Americans have viewed goverment surveillance and privacy since Snowden leaks*, https://www.pewresearch.org/short-reads/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/, [dostęp: 1 grudnia 2025].

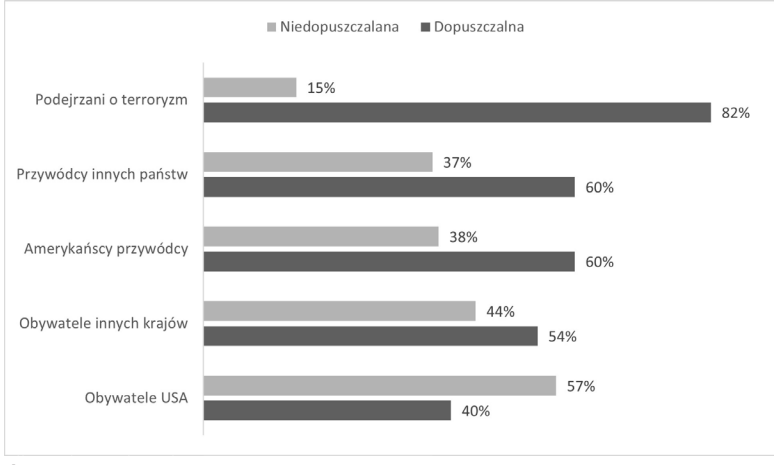
korzystania z aplikacji mobilnych (13%), między innymi rezygnując z instalacji aplikacji, które gromadzą dane, oraz wiadomości tekstowych SMS (13%), gdzie unikają przekazywania określonych treści. Najmniejszy odsetek badanych (9%) zmienił sposób korzystania z telefonów stacjonarnych, ograniczając prowadzenie za ich pośrednictwem rozmów o charakterze poufnym[30].

W ramach tego samego badania zapytano Amerykanów, czy uznają inwigilację wybranych osób za dopuszczalną. Ich odpowiedzi zob. wykr. 5.

Wśród ankietowanych dominuje przekonanie, że inwigilacja osób podejrzanych o terroryzm mieści się w granicach dopuszczalności – taką opinię wyraziło 82% respondentów. Zbliżony poziom akceptacji odnotowano w odniesieniu do nadzoru nad przywódcami Stanów Zjednoczonych oraz liderami innych państw (po 60%). Bardziej zróżnicowany obraz widać w odniesieniu do obywateli innych krajów. 54% ankietowanych dopuszcza możliwość ich inwigilacji, natomiast 44% ocenia takie działania jako niedopuszczalne. Największy sprzeciw wywołuje nadzór nad obywatelami Stanów Zjednoczonych – jedynie 40% badanych akceptuje tego rodzaju praktyki, podczas gdy 57% wyraża wobec nich dezaprobatę. Dane te wskazują, że dopuszczalność inwigilacji jest w opinii publicznej uzależniona od statusu i przynależności obywatelskiej osób objętych nadzorem, przy czym największy zakres ochrony prywatności przypisywany jest obywatelom USA.

[30] L. Rainie, M. Madden, *Americans' Privacy Strategies Post-Snowden*, https://www.pewresearch.org/internet/2015/03/16/americans-privacy-strategies-post-snowden, [dostęp: 1 grudnia 2025].

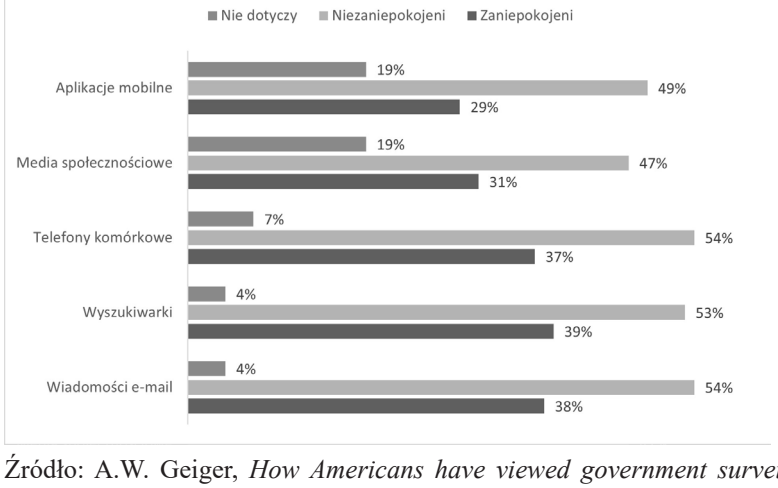
Wykres 5. Poziom akceptacji inwigilacji wśród Amerykanów w zależności od przynależności do grupy osób objętych nadzorem



Źródło: A.W. Geiger, *How Americans have viewed goverment surveillance and privacy since Snowden leaks*, https://www.pewresearch.org/short-reads/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/, [dostęp: 2 grudnia 2025].

Z kolei ogólny stosunek dorosłych Amerykanów do działań inwigilacyjnych ilustruje wykres 6, prezentujący poziom ich zaniepokojenia możliwością monitorowania aktywności przez władze państwowe.

Wykres 6. Odsetek obywateli USA deklarujących, że odczuwają bądź nie odczuwają niepokoju w związku z rządową inwigilacją ich danych oraz komunikacji elektronicznej

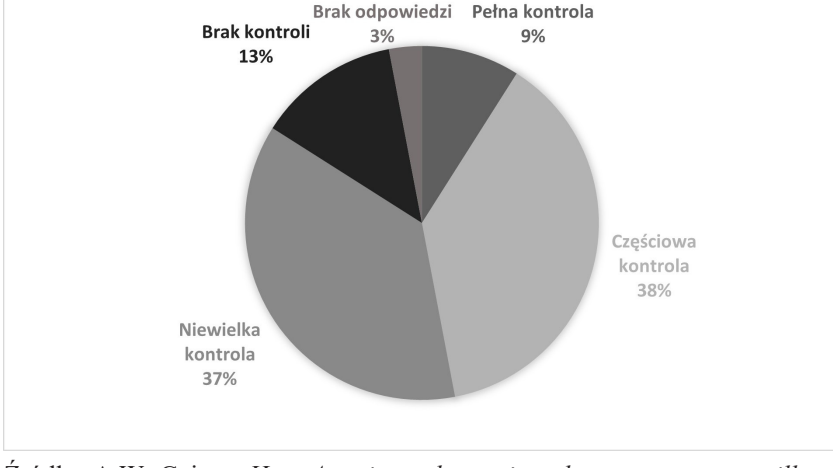


Źródło: A.W. Geiger, *How Americans have viewed government surveillance and privacy since Snowden leaks*, https://www.pewresearch.org/short-reads/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/, [dostęp: 2 grudnia 2025].

Badani oceniali poziom swoich obaw w odniesieniu do pięciu kategorii aktywności cyfrowej. Największe zaniepokojenie budziła inwigilacja wyszukiwarek internetowych (39%), korespondencji e-mail (38%) oraz połączeń telefonicznych (37%). Najniższy poziom obaw odnotowano w przypadku aplikacji mobilnych (29%) oraz mediów społecznościowych (31%). Jednocześnie w odniesieniu do każdej z form aktywności większość respondentów nie deklarowała poważniejszych obaw. Przykładowo 54% ankietowanych nie obawiała się monitorowania poczty elektronicznej, a 53% wyszukiwarek internetowych. Część badanych wskazała, że nie korzysta z określonych technologii. Uzyskane wyniki sugerują, że pomimo szerokiej świadomości możliwości inwigilacyjnych ze strony rządu, poziom obaw społeczeństwa amerykańskiego wobec monitorowania ich osobistej aktywności cyfrowej pozostaje umiarkowany.

W 2015 roku Pew Research Center zapytało Amerykanów o subiektywne poczucie kontroli nad informacjami dotyczącymi ich codziennej egzystencji. Ich odpowiedzi ilustruje wykres 7.

Wykres 7. Odsetek dorosłych obywateli USA deklarujących poziom kontroli nad informacjami gromadzonymi na temat ich codziennego życia

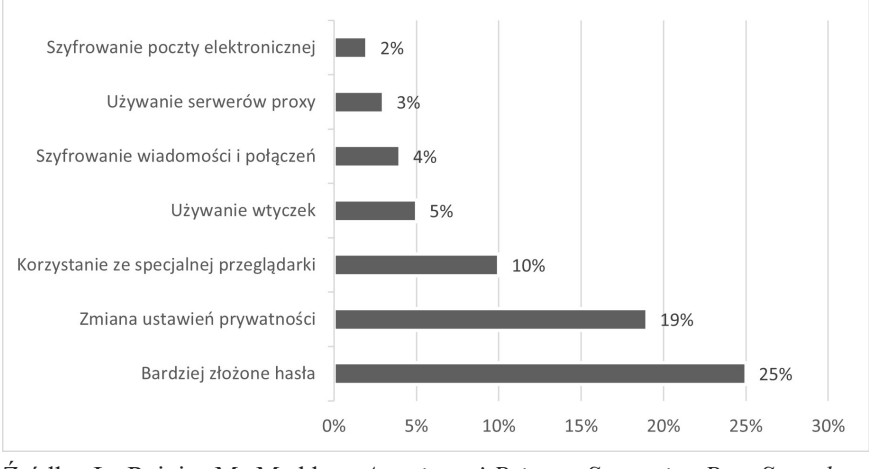


Źródło: A.W. Geiger, *How Americans have viewed government surveillance and privacy since Snowden leaks*, https://www.pewresearch.org/short-reads/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/, [dostęp: 2 grudnia 2025].

Z przedstawionego wykresu wynika, że jedynie 9% badanych uważa, że ma pełną kontrolę nad tym, jakie informacje są o nich gromadzone. 38% respondentów deklaruje posiadanie częściowej kontroli. Natomiast 37% ocenia, że ma nad tym procesem niewielką kontrolę. Z kolei 13% badanych stwierdza, że nie ma żadnej kontroli nad zbieraniem informacji dotyczących ich codziennego życia, a 3% odmówiło udzielenia odpowiedzi na to pytanie.

Pew Research Center zapytało również obywateli Stanów Zjednoczonych, czy stosują jakiekolwiek techniki ochrony przed inwigilacją. Wyniki tego badania zob. wykr. 8.

Wykres 8. Strategie ochrony prywatności stosowane przez użytkowników w odpowiedzi na ujawnienie informacji o rządowych programach nadzoru



Źródło: L. Rainie, M. Madden, *Americans' Privacy Strategies Post-Snowden*, https://www.pewresearch.org/internet/2015/03/16/americans-privacy-strategies-post-snowden, [dostęp: 3 grudnia 2025].

Najczęściej wdrażano działania stosunkowo proste, niewymagające zaawansowanej wiedzy informatycznej, takie jak stosowanie „silniejszych" haseł (25%) oraz modyfikacja ustawień prywatności w serwisach społecznościowych (19%). Zdecydowanie rzadziej wybierano bardziej złożone rozwiązanie, m.in. korzystanie z przeglądarek niewyświetlających historii wyszukiwania (10%), wtyczek zwiększających poziom prywatności (5%), szyfrowanie wiadomości (4%), używanie serwerów proxy (3%) czy też szyfrowanie korespondencji e-mail (2%).

Reakcje rządów i mediów Stanów Zjednoczonych oraz innych państw

Po wyjeździe z Hongkongu Edward Snowden udał się do Rosji. Część przedstawicieli amerykańskiej sceny politycznej, m.in. kongresmen Mike Rogres, interpretowała ten fakt jako przejaw braku odpowiedzialności oraz zagrożenie dla bezpieczeństwa narodowego. Władze Stanów Zjednoczonych unieważniły mu paszport, co uniemożliwiło Snowdenowi dalszą podróż i doprowadziło do przymusowego pozostania na terytorium Federacji Rosyjskiej. W następstwie tej decyzji szereg państw, takich jak Kuba, Niemcy, Wielka Brytania, Brazylia, a nawet Polska, odmówiło udzielenia mu azylu. Równocześnie w mediach zaczęły pojawiać się niezweryfikowane doniesienia sugerujące, jakoby po przy-

byciu do Moskwy Snowden przekazał część posiadanych materiałów rosyjskim władzom. Snowden podkreślał jednak, że współpracował tylko z dziennikarzami w Hongkongu i nie miał zamiaru nikomu więcej przekazywać materiałów. Najdalej idące i pozbawione solidnych podstaw oskarżenia ukazały się na łamach „The New York Times", gdzie, powołując się na anonimowych ekspertów sugerowano, że w czasie pobytu w Hongkongu Snowden miał przekazać rządowi w Pekinie zawartość czterech laptopów[31]. Zgodnie z doniesieniami „South China Morning Post", rzekomo przekazane materiały obejmowały m.in. daty, adresy IP oraz szczegóły operacyjne dotyczące włamań, w tym wskaźniki skuteczności i bieżący status uzyskanego dostępu. Sam Snowden miał podkreślać, że dane te dotyczyły sektora cywilnego. Jednocześnie eksperci zwracali uwagę, iż w warunkach chińskich, granica między sektorem publicznym a prywatnym jest płynna, a przedsiębiorstwa państwowe nierzadko pełnią funkcje o strategicznym charakterze[32].

W udzielonym wywiadzie dla „The Guardian" Snowden kategorycznie zaprzeczył, jakoby przekazał jakiekolwiek informacje władzom Chińskiej Republiki Ludowej czy Federacji Rosyjskiej, a także temu, by którakolwiek z tych stron uzyskała dostęp do danych znajdujących się w jego laptopach. Doniesienia o rzekomym skopiowaniu zawartości jego urządzeń były jednak szeroko rozpowszechniane w innych mediach, stając się narzędziem kampanii mającej na celu podważenie wiarygodności Snowdena. Dotychczas nie przedstawiono żadnych dowodów potwierdzających prawdziwość tych oskarżeń, a jedynym udokumentowanym stanowiskiem pozostaje zaprzeczenie samego Snowdena. Ponadto, badania opinii publicznej, w tym sondaż przeprowadzony przez Quinnipiac University, wskazują, że większość obywateli Stanów Zjednoczonych postrzega Edwarda Snowdena jako sygnalistę, a nie zdrajcę[33].

Po ukazaniu się wspomnianego artykułu w „The New York Times" został on poddany krytyce przez Margaret Sullivan, ówczesną redaktorkę odpowiedzialną za standardy redakcyjne w tym periodyku. W rozmowie z szefem działu zagranicznego, Josephem Kahnem wskazała, że priorytetem jest umożliwienie czytelnikom zapoznania się z różnymi punktami widzenia, tak aby mogli formułować własne wnioski. Sullivan zwróciła jednak uwagę, że tekst opiera się przede wszystkim na domysłach ekspertów, a nie na faktach czy bezpośrednich dowodach. Redakcja ostatecznie przyznała, że nie dysponowała żadnymi potwierdzonymi informacjami, wskazującymi, że dane z nośników Edwarda Snowdena zostały rzeczywiście przejęte przez służby innych państw. Jednocześnie Lucie Liu, specjalistka z zakresu bezpieczeństwa informatycznego stwier-

[31] G. Greenwald, *Snowden. Nigdzie…*, s. 276.

[32] NYT, *Snowden's Leaks on China Cloud Affect Its Role in His Fate*, https://www.nytimes.com/2013/06/15/world/asia/ex-nsa-contractors-disclosures-could-complicate-his-fate.html, [dostęp: 5 grudnia 2025].

[33] G. Greenwald, *Snowden. I never gave any information to Chinese or Russian governments*, https://www.theguardian.com/commentisfree/2013/jul/10/snowden-denies-information-russia-china, [dostęp: 5 grudnia 2025].

działa jednoznacznie, że Edward Snowden zabezpieczył informacje przy użyciu silnych mechanizmów kryptograficznych oraz odłączył nośnik USB od sieci, co uniemożliwiło przechwycenie jakichkolwiek danych[34].

Chińskie Ministerstwo Spraw Zagranicznych odrzuciło pojawiające się spekulacje, jakoby Edward Snowden działał w interesie władz w Pekinie, określając tego rodzaju twierdzenia jako „całkowicie bezpodstawne", jednocześnie wzywając USA do złożenia wyjaśnień w sprawie prowadzonych działań inwigilacyjnych. Stanowiło to reakcję na narastającą falę komentarzy, w tym wypowiedź byłego wiceprezydenta Dicka Cheneya, który określił Edwarda Snowdena mianem zdrajcy i zasugerował jego potencjalne związki z Chińską Republiką Ludową. Chińskie media, a w szczególności „Global Times", zaznaczyły, że ewentualna ekstradycja Snowdena oznaczałaby „utratę twarzy", zarówno dla władz Hongkongu, jak i rządu centralnego, a jego działania interpretowano jako ujawnienie naruszeń praw obywatelskich dokonanych przez administrację w Waszyngtonie[35].

W 2013 roku Frank La Rue – sprawozdawca ONZ ds. wolności słowa wskazał, że sposób, w jaki rząd brytyjski zareagował na ujawnienia tajnych materiałów przez Edwarda Snowdena, podważa międzynarodową reputację Wielkiej Brytanii jako państwa stojącego na straży wolności mediów oraz dziennikarstwa śledczego. Frank La Rue wyrażał szczególne zaniepokojenie groźbami kierowanymi pod adresem dziennika „The Guardian", który wspólnie z „The New York Times" i „The Washington Post" ujawnił działania brytyjskiego Government Communications Headquarters (GCHQ, pol. Kwatera Główna Łączności Rządowej) oraz amerykańskiej NSA. Potępił zarówno propozycje pociągnięcia redakcji do odpowiedzialności za rzekomą zdradę stanu, jak i presję polityczną wywieraną na redaktora naczelnego Alana Rusbridgera. Jego stanowisko zbiegło się w czasie z zapowiedzią przyjazdu międzynarodowej delegacji redaktorów i wydawców, zorganizowanego przez World Association of News Publishers (WAN-IFRA, pol. Światowe Stowarzyszenie Wydawców Prasy), którego celem było wyrażenie sprzeciwu wobec ingerencji rządu w system regulacji prasowych oraz niezależność brytyjskich mediów. Dyrektor generalny WAN-IFRA Vincent Payrègne podkreślił, że działania władz Wielkiej Brytanii nie tylko niszczą jej reputację jako obrońcy wolności prasy, lecz także dostarczają autorytarnym reżimom wygodny pretekst do stosowania represji wobec mediów. W artykule „The New York Times" również wyrażono obawy o przyszłość wolności prasy w Wielkiej Brytanii, zwracając uwagę na brak konstytucyjnych gwarancji w tym zakresie oraz wskazując, że działania parlamentarzystów i policji wobec „The Guardian" mają charakter zastraszający i mogą skutkować wszczęciem postępowania karnego[36].

[34] G. Greenwald, *Snowden. Nigdzie…*, s. 277.

[35] T. Branigan, *Edward Snowden 'not a Chinese spy' – Beijing*, https://www.theguardian.com/world/2013/jun/17/edward-snowden-not-chinese-spy-beijing, [dostęp: 5 grudnia 2025].

[36] M. Taylor, N. Hopkins, P. Maynard, *UK's reputation is damaged by reaction to Edward Snowden, says UN official*, https://www.theguardian.com/world/2013/nov/15/uk-reputation-edward-snowden-un, [dostęp: 6 grudnia 2025].

Dnia 6 czerwca 2013 roku dziennik „The Washington Post" zwrócił się z prośbą o komentarz do Apple, Facebook, Google, Yahoo oraz innych podmiotów technologicznych, po ujawnieniu przez Glenna Greenwalda i Laurę Poitras informacji o programie PRISM. Przedsiębiorstwa te niezwłocznie zaprzeczały, jakoby przekazywały dane bez stosownych nakazów sądowych. Pomimo że dostęp do materiałów był ograniczony ze względu na klauzule poufności o charakterze prawnym, to formułowane przez firmy odpowiedzi często oceniano jako niejednoznaczne i wymijające. Prezydent Barack Obama usiłował uspokoić opinię publiczną, deklarując, że program nie obejmował obywateli Stanów Zjednoczonych. Wymienione wyżej korporacje zaczęły wdrażać zaawansowane mechanizmy szyfrowania, oparte m.in. na technologiach typu *Perfect Forward Secrecy*. Najistotniejszym skutkiem afery okazał się jednak spadek zaufania na arenie międzynarodowej. Państwa, takie jak Brazylia, zaczęły wymagać lokalnego przechowywania danych, co rodziło ryzyko postępującej fragmentyzacji Internetu oraz zwiększenia kosztów prowadzenia działalności gospodarczej[37].

Po upublicznieniu materiałów przez Edwarda Snowdena, ponad 450 organizacji oraz setki tysięcy osób prywatnych na całym świecie, w tym także z Polski, poparło postulat wdrożenia 13 zasad mających na celu ograniczenie masowej inwigilacji. W odróżnieniu od instytucji międzynarodowych, takich jak ONZ czy Unia Europejska, polskie władze nie zajęły oficjalnego, jednoznacznego stanowiska wobec amerykańskich praktyk nadzorczych. Fundacja Panoptykon, Helsińska Fundacja Praw Człowieka oraz Amnesty International Poland wielokrotnie podejmowały próby zmierzające do uzyskania informacji na temat oficjalnej oceny tych działań przez polskie organy państwowe. Mimo tych starań, odpowiedzi ze strony instytucji publicznych były ogólne i ograniczone. Szczególnie widoczne stało się to w czasie wizyty prezydenta Baracka Obamy w 2014 roku, kiedy w debacie publicznej koncentrowano się raczej na motywach, jakimi kierował się Edward Snowden, niż na znaczeniu ujawnionych przez niego informacji. Fundacja Panoptykon sformułowała hasło „inwigilacja to nie wolność", akcentując rosnącą rozbieżność między społecznymi oczekiwaniami w zakresie przejrzystości działań władz i ochrony praw jednostki, a faktycznym brakiem adekwatnej reakcji państwa[38].

W październiku 2013 roku wyżej wspomniane organizacje pozarządowe wraz z Helsińską Fundacją Praw Człowieka, skierowały do kluczowych przedstawicieli władz państwowych (premiera Donalda Tuska, ministra spraw zagranicznych Radosława Sikorskiego, ministra spraw wewnętrznych Bartłomieja Sienkiewicza, ministra sprawiedliwości Marka Biernackiego oraz prokuratora generalnego Andrzeja Seremeta) zestaw 100 pytań dotyczących potencjalnego

[37] S. Levy, *How the NSA nearly destroyed the internet*, https://www.wired.com/story/how-the-us-almost-killed-the-internet/, [dostęp: 6 grudnia 2025].

[38] A. Obem, *Rok po ujawnieniu masowej inwigilacji. Polskie władze nadal nie widzą problemu*, https://panoptykon.org/wiadomosc/rok-po-ujawnieniu-masowej-inwigilacji-polskie-wladze-nadal-nie-widza-problemu, [dostęp: 6 grudnia 2025].

udziału Polski w działaniach NSA oraz sposobu reakcji instytucji publicznych na informacje ujawnione przez Edwarda Snowdena. Pytania dotyczyły m.in. znajomości programu PRISM, stosowania takich narzędzi, jak system XKeyscore[39] oraz ewentualnego uczestnictwa Polski w transatlantyckiej grupie ds. nadzoru. Z udzielonych odpowiedzi wynikało, że podjętą w sposób formalny inicjatywą było wysłanie noty dyplomatycznej z prośbą o wyjaśnienie zaistniałej sytuacji. Kancelaria prezydenta Bronisława Komorowskiego również poinformowała, że „nie posiada informacji" na temat programu PRISM[40].

W sytuacji, gdy przedstawiciele polskich władz konsekwentnie milczeli, organizacje społeczne zdecydowały się wnieść skargi do sądu administracyjnego. Jedną z takich skarg złożyło m.in. Centralne Biuro Antykorupcyjne (CBA). Dotyczyła ona odmowy udzielenia informacji o ewentualnym wykorzystaniu systemu XKeyscore oraz zarzucanej bezczynności prezesowi Rady Ministrów, a także ministrom spraw wewnętrznych i zagranicznych. Kolejne materiały ujawnione przez Edwarda Snowdena w następnych miesiącach – w tym dokumenty wskazujące na możliwą bezpośrednią współpracę Polski z NSA, również nie skłoniły władz naszego kraju do przedstawienia oficjalnego stanowiska. Na płaszczyźnie parlamentarnej ograniczono się jedynie do przeprowadzenia zamkniętego posiedzenia Komisji ds. Służb Specjalnych, którego przebiegu nie upubliczniono. Taki brak przejrzystości oraz niewielkie zaangażowanie organów państwa w wyjaśnienie potencjalnych naruszeń praw obywatelskich, rodziły poważne wątpliwości co do realnego respektowania standardów demokratycznego państwa. W odpowiedzi organizowano akcje społeczne, takie jak „Inwigilacja to nie wolność!" Celem akcji było zwrócenie uwagi opinii publicznej na konieczność rzetelnego rozliczenia zarzutów[41].

W raporcie opublikowanym w 2014 roku przez organizacje Human Rights Watch oraz American Civil Liberties Union wskazano, że prowadzona w Stanach Zjednoczonych przez NSA masowa inwigilacja w istotny sposób zakłóciła wykonywanie pracy, zarówno przez dziennikarzy zajmujących się tematyką bezpieczeństwa narodowego, jak i przez prawników reprezentujących swoich klientów. Na podstawie wywiadów przeprowadzonych z 46 dziennikarzami, 42 adwokatami i 5 byłymi urzędnikami państwowymi, autorzy raportu opisali sytuacje, w których sam lęk przed elektronicznym śledzeniem zniechęcał potencjalnych informatorów do kontaktów z mediami nawet, kiedy poruszane kwestie

[39] XKeyscore to system zbierający i pozwalający analitykom NSA na przeglądanie praktycznie wszystkich informacji wytwarzanych i gromadzonych przez internautów. XKeyscore pozwala np. na analizowanie zawartości poczty elektronicznej, informacji wymienianych za pośrednictwem *social mediów* (w tym czatów) oraz historii wyszukiwania. Zob. W. Smol, *XKeyscore. PRISM to nie wszystko! [Aktualizacja]*, https://sekurak.pl/xkeyscore-prism-to-nie-wszystko/, [dostęp: 9 grudnia 2025].

[40] W. Klicki, *12 miesięcy ze Snowdenem – 100 pytań wciąż bez odpowiedzi*, https://panoptykon.org/wiadomosc/12-miesiecy-ze-snowdenem-100-pytan-wciaz-bez-odpowiedzi, [dostęp: 6 grudnia 2025].

[41] Tamże.

nie dotyczyły tajemnicy państwowej. Podkreślono ponadto, że wzrosła nieufność i pogłębiający się strach przez restrykcyjną polityką administracji Baracka Obamy. Jeden z obrońców stwierdził wręcz: „Nie chcę działać jak diler narkotykowy, by chronić tajemnicę adwokacką”[42]. Mimo tych sygnałów rząd USA utrzymywał, że prowadzony nadzór nie narusza ani wolności mediów, ani poufności komunikacji między adwokatem a klientem. Autorzy raportu opowiedzieli się za ograniczeniem skali inwigilacji, wzmocnieniem ochrony sygnalistów, zwiększeniem przejrzystości działań władz oraz zmianą procedur tzw. „minimalizacji”, które mają służyć ochronie prywatności obywateli amerykańskich. Dokument został opublikowany na kilka dni przed przedstawieniem w Senacie projektu ustawy USA Freedom Act, mającej zmienić programy inwigilacyjne NSA[43].

W Niemczech ujawnienia dokonane przez Snowdena stały się impulsem do intensywnej debaty publicznej. Opozycja polityczna oraz media oskarżyły Bundesnachrichtendienst (pol. Federalną Służbę Wywiadowczą) [dalej: BND] o współudział europejskich polityków, instytucji unijnych i międzynarodowych korporacji w inwigilacji, zwracając uwagę na wykorzystanie w tym celu amerykańskiej stacji nasłuchowej w Bawarii. W centrum sporu politycznego znalazł się minister spraw wewnętrznych Thomas de Maizière, któremu zarzucono zaniechanie stosowanych działań oraz wprowadzenie w błąd członków Bundestagu. Opozycja domagała się ujawnienia tzw. listy selektorów wykorzystywanych przez BND. Jednak ówczesna kanclerz Angela Merkel broniła współpracy z NSA, uzasadniając to koniecznością przeciwdziałania międzynarodowemu terroryzmowi. Jednocześnie ujawnienia Snowdena stały się czynnikiem skłaniającym do ponownego przemyślenia i częściowej weryfikacji tej współpracy[44].

Na międzynarodowej konferencji zorganizowanej w 2015 roku przez Ditchley Foundation z udziałem przedstawicieli amerykańskich i brytyjskich służb wywiadowczych, podkreślono, że ostra reakcja obu rządów na ujawnienia Snowdena jedynie spotęgowała społeczną nieufność wobec agencji wywiadowczych. Dziennikarz śledczy Duncan Campbell podkreślił, że działania Edwarda Snowdena trwale odmienią sposób postrzegania nadzoru. Na pierwszy plan w debacie publicznej wysunięty został problem nadużyć i braku przejrzystości. Podczas konferencji zaznaczono, że konieczne jest zwiększenie transparentności, zarówno w odniesieniu do metod operacyjnych, jak i zasad dostępu do danych gromadzonych przez podmioty prywatne, takie jak Google czy Twitter. Uczestnicy dyskusji, w tym dyrektor Government Communications Headquarters (GCHW, pol. Agencja Wywiadu Sygnałowego i Kryptografii) – Robert Hannigan i były szef dowództwa antyterrorystycznego londyńskiej policji metropolitalnej – Peter

[42] D. Nicks, *Government Spying Hurts Journalists and Lawyers, Report Says*, https://time.com/3048380/government-spying-hurts-journalists-and-lawyers-report-says/, [dostęp: 6 grudnia 2025].

[43] Tamże.

[44] *Snowden dla „Spiegla”. USA uprawiają szpiegostwo gospodarcze*, https://www.radiopik.pl/3,30572,snowden-dla-spiegla-usa-uprawiaja-szpiegostwo-gospodarcze&s=1778&si=1778&sp=1778, [dostęp: 6 grudnia 2025].

Clarke, zgodzili się, że rządy powinny częściej prowadzić otwarte debaty na temat inwigilacji, ponieważ strategia „milczenia i uniku" jedynie nasiliła nieufność obywateli. Zwrócono przy tym uwagę, że w trakcie dyskusji żaden z uczestników nie określił Edwarda Snowdena mianem zdrajcy[45].

Podsumowanie

Celem artykułu była analiza sprawy Edwarda Snowdena jako punktu zwrotnego w ujawnieniu skali i zasięgu współczesnych programów masowej inwigilacji oraz jej konsekwencji dla porządku demokratycznego. W artykule omówiono rolę mediów w nadaniu ujawnieniom globalnego wymiaru oraz zrekonstruowano debatę nad relacją między bezpieczeństwem narodowym, a prawem do prywatności i ukazano brak przejrzystości w funkcjonowaniu służb specjalnych. Szczególny nacisk położono na świadomość obywateli USA w zakresie elektronicznej inwigilacji oraz ich oddziaływania na debatę publiczną.

W Polsce zagadnienie inwigilacji oraz ujawnienie tego procederu przez Snowdena było przedstawiane w prasie[46] m.in. na łamach „Polityki"[47], „Newsweeka Polska"[48], „Gazety Wyborczej"[49] oraz przez portale informacyjne, takie jak Onet czy Wirtualna Polska. Początkowo relacje opierały się głównie na materiałach z prasy zagranicznej, z czasem jednak uzupełniano je o analizy odnoszące się do polskich uwarunkowań. W polskim kontekście ujawnienia dokonane przez Edwarda Snowdena przyczyniły się do wzrostu świadomości społecznej w zakresie skali i technik elektronicznej inwigilacji. Stały się również impulsem do szeroko zakrojonej debaty o dopuszczalnych granicach nadzoru oraz skłoniły część obywateli do sięgania po narzędzia zwiększające bezpieczeństwo komunikacji elektronicznej.

Od 2013 roku Edward Snowden przebywa na terytorium Rosji. W 2022 roku uzyskał obywatelstwo tego państwa i został włączony do tamtejszego systemu podatkowego. Zajmuje się przede wszystkim działalnością edukacyjną oraz publicystyką w obszarze ochrony prywatności i bezpieczeństwa cyfrowego, występując na konferencjach oraz w mediach, głównie w formie zdalnej.

[45] A. Travis, *Snowden leak. Governments' hostile reaction fuelled public's distrust of spies*, https://www.theguardian.com/world/2015/jun/15/snowden-files-us-uk-government-hostile-reaction-distrust-spies, [dostęp: 11 lipca 2025].

[46] Szerzej zob. K. Świtała, *Orwellowski system nadzoru. Inwigilacja społeczeństwa w sieci a ochrona prywatności. Analiza „afery Snowdena" w polskiej prasie*, w: *Amerykański system ochrony praw człowieka. Aksjologia, instytucje, efektywność*, red. nauk. J. Jaskiernia, Toruń 2015, s. 411-437.

[47] Zob. np. A. Leszczyński, *Efekt Snowdena*, „Polityka" 2015, nr 25, s. 50-52.

[48] Zob. np. P. Milewski, *Wujek Sam patrzy*, „Newsweek Polska" 2013, nr 25, s. 58-61.

[49] Zob. np.: E. Snowden, *Snowden. Nie jestem szpiegiem Rosji*, rozm. przepr. S. Aust, Ch. Krüger, M. Scjolz, „Gazeta Wyborcza" 2019, nr 215, s. 6-7; E. Lucas, *Zdrada naiwnych krzyżowców. Snowden: męczennik, głupiec czy zdrajca?*, „Gazeta Wyborcza" 2014, nr 26, s. 17; R. Imielski, *Sekrety misji Edwarda Snowdena*, „Gazeta Wyborcza" 2014, nr 112, s. 12-13; M. Zawadzki, *Rozhulał się Wielki Brat. Afera Snowdena. Jak to się zaczęło*, „Gazeta Wyborcza" 2013, nr 156, s. 15.

Bibliografia:

Bamford James, *The most Wanted Man in the World*, https://interactive.wired.com/www-wired-com__2014__08__edward-snowden/index.html#ch-5.

Branigan Tania, *Edward Snowden 'not a Chinese spy' – Beijing*, https://www.theguardian.com/world/2013/jun/17/edward-snowden-not-chinese-spy-beijing.

Desilver Drew, *Most young Americans say Snowden has served the public interest*, https://www.pewresearch.org/short-reads/2014/01/22/most-young-americans-say-snowden-has-served-the-public-interest/.

Geiger A.W., *How Americans have viewed goverment surveillance and privacy since Snowden leaks*, https://www.pewresearch.org/short-reads/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/.

Greenwald Glenn, *NSA collecting phone records of millions of Verizon customers daily*, https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Greenwald Glenn, *Snowden. I never gave any information to Chinese or Russian governments*, https://www.theguardian.com/commentisfree/2013/jul/10/snowden-denies-information-russia-china.

Greenwald Glenn, *Snowden. Nigdzie się nie ukryjesz*, Warszawa 2014.

Greenwald Glenn, MacAskill Ewen, *NSA Prism program taps in to user data of Apple, Google and others*, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

Greenwald Glenn, MacAskill Ewen, Poitras Laura, *Edward Snowden. The whistleblower behind the NSA surveillance revelations*, https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

Grzelak Michał, *Skutki sprawy Edwarda Snowdena dla prywatności danych w cyberprzestrzeni*, „Bezpieczeństwo Narodowe" 2015, nr 1, s. 191-211.

Harding Luke, *How Edward Snowden went from loyal NSA contractor to whistleblower*, https://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leak-nsa-contractor-extract.

Harding Luke, *Polowanie na Snowdena*, Warszawa cop. 2014.

Imielski Roman, *Sekrety misji Edwarda Snowdena*, „Gazeta Wyborcza" 2014, nr 112, s. 12-13.

Jasiński Karol, *Główne idee libertarianzimu*, „Studia Warmińskie" 2022, vol. 59, s. 7-24.

Klicki Wojciech, *12 miesięcy ze Snowdenem – 100 pytań wciąż bez odpowiedzi*, https://panoptykon.org/wiadomosc/12-miesiecy-ze-snowdenem-100-pytan-wciaz-bez-odpowiedzi.

Leszczyński Adam, *Efekt Snowdena*, „Polityka" 2015, nr 25, s. 50-52.

Levy Steven, *How the NSA nearly destroyed the internet*, https://www.wired.com/story/how-the-us-almost-killed-the-internet/.

Lucas Edward, *Zdrada naiwnych krzyżowców. Snowden: męczennik, głupiec czy zdrajca?*, „Gazeta Wyborcza" 2014, nr 26, s. 17.

Milewski Piotr, *Wujek Sam patrzy*, „Newsweek Polska" 2013, nr 25, s. 58-61.

Nicks Denver, *Government Spying Hurts Journalists and Lawyers, Report Says*, https://time.com/3048380/government-spying-hurts-journalists-and-lawyers-report-says/.

NYT, *Snowden's Leaks on China Cloud Affect Its Role in His Fate*, https://www.nytimes.com/2013/06/15/world/asia/ex-nsa-contractors-disclosures-could-complicate-his-fate.html.

Obem Anna, *Rok po ujawnieniu masowej inwigilacji. Polskie władze nadal nie widzą problemu*, https://panoptykon.org/wiadomosc/rok-po-ujawnieniu-masowej-inwigilacji-polskie-wladze-nadal-nie-widza-problemu.

Rainie Lee, Madden Mary, *Americans' Privacy Strategies Post-Snowden*, https://www.pewresearch.org/internet/2015/03/16/americans-privacy-strategies-post-snowden.

Sieć Tor, anonimizacja ruchu, https://home.agh.edu.pl/~pmarynow/pliki/2021zima/tor.pdf.

Smol Wojciech, *XKeyscore. PRISM to nie wszystko! [Aktualizacja]*, https://sekurak.pl/xkeyscore-prism-to-nie-wszystko/.

Snowden dla „Spiegla". USA uprawiają szpiegostwo gospodarcze, https://www.radiopik.pl/3,30572,snowden-dla-spiegla-usa-uprawiaja-szpiegostwo-gospodarcze&s=1778&si=1778&sp=1778.

Snowden Edward, *Pamięć nieulotna*, Kraków 2019.

Snowden Edward, *Snowden. Nie jestem szpiegiem Rosji*, rozm. przepr. Stefan Aust, Charlotte Krüger, Martin Scjolz, „Gazeta Wyborcza" 2019, nr 215, s. 6-7.

Świtała Karolina, *Orwellowski system nadzoru. Inwigilacja społeczeństwa w sieci a ochrona prywatności. Analiza „afery Snowdena" w polskiej prasie*, w: *Amerykański system ochrony praw człowieka. Aksjologia, instytucje, efektywność*, red. nauk. Jerzy Jaskiernia, Toruń 2015, s. 411-437.

Taylor Matthew, Hopkins Nick, Maynard Phil, *UK's reputation is damaged by reaction to Edward Snowden, says UN official*, https://www.theguardian.com/world/2013/nov/15/uk-reputation-edward-snowden-un.

Travis Alan, *Snowden leak. Governments' hostile reaction fuelled public's distrust of spies*, https://www.theguardian.com/world/2015/jun/15/snowden-files-us-uk-government-hostile-reaction-distrust-spies.

Zawadzki Mariusz, *Rozhulał się Wielki Brat. Afera Snowdena. Jak to się zaczęło*, „Gazeta Wyborcza" 2013, nr 156, s. 15.

Karolina Czarnecka

Edward Snowden jako bohater debaty publicznej o nadzorze państwowym i ochronie prywatności w erze Internetu

Edward Snowden, jako sygnalista ujawniający w 2013 roku tajne dokumenty amerykańskich służb wywiadowczych, stał się jedną z centralnych postaci współczesnej debaty o granicach nadzoru państwowego, prawie do prywatności oraz dopuszczalnym zakresie ingerencji władz w życie obywateli w erze cyfrowej. Ujawnione przez niego materiały odsłoniły rozległy system elektronicznej inwigilacji prowadzonej przez NSA i jej zagranicznych partnerów, obejmujący masowe pozyskiwanie danych bez wiedzy i zgody osób, których one dotyczyły. Zaburzyło to zaufanie do instytucji państwowych oraz korporacji technologicznych. W centrum rozważań znajduje się zarówno biografia Snowdena i ewolucja jego poglądów na temat roli państwa i praw obywatelskich, jak i analiza ujawnionych dokumentów, które wywołały globalną dyskusję nad relacją między bezpieczeństwem a prywatnością. Analizie poddano reakcje polityczne i społeczne w USA oraz w wybranych państwach, a także zwrócono uwagę na rolę mediów w tej dys-

kusji. Szczególną uwagę poświęcono zróżnicowanym ocenom działań Snowdena oraz temu, w jaki sposób stały się one punktem odniesienia w sporze o transparentność działań służb i miejsce sygnalistów w systemach demokratycznych.

Słowa kluczowe: Edward Snowden, inwigilacja, nadzór państwowy, prawo do prywatności, rola mediów, sygnalista

Edward Snowden as a hero of the public debate on state surveillance and privacy protection in the internet age

Edward Snowden, as a whistleblower who in 2013 disclosed classified Documents of the U.S. intelligence services, has become one of the central figures in the contemporary debate on the limits of state surveillance, the right to privacy, and permissible scope of govermental interference in citizens' lives in the digital era. Revealed by him materials exposed an extensive system of electronic surveillance conducted by the NSA and its foreign partners, involving the mass collection of data without the knowledge or consent of the individuals concerned. This undermined trust in state institutions and technology corporations. The analysis focuses both on Snowden's biography and the evolution of his views on the role of the state and civil rights, and on the examination of the disclosed Documents, which sparked a global discussion on the relationship between security and privacy. The study also considers political and social reaction in the United States and selected other countries, as well as the role of the media in this debate. Particular attention was paid to the diverse assessments of Snowden's actions and how they became a point of reference in the dispute over the transparency of services' activities and the place of whistleblowers in democratic systems.

Key words: Edward Snowden, surveillance, state surveillance, right to privacy, role of the media, whistleblower

Data zgłoszenia tekstu: 09.01.2026
Data akceptacji tekstu: 24.02.2026