Rada
Unii Europejskiej

Bruksela, 10 października 2024 r.
(OR. en)

14403/24

DATAPROTECT 299
JAI 1489
RELEX 1262
USA 42

PISMO PRZEWODNIE

Od:	Sekretarz generalna Komisji Europejskiej (podpisała dyrektor Martine DEPREZ)
Data otrzymania:	9 października 2024 r.
Do:	Thérèse BLANCHET, sekretarz generalna Rady Unii Europejskiej
Nr dok. Kom.:	COM(2024) 451 final
Dotyczy:	SPRAWOZDANIE KOMISJI DLA PARLAMENTU EUROPEJSKIEGO I RADY w sprawie pierwszego okresowego przeglądu funkcjonowania decyzji stwierdzającej odpowiedni stopień ochrony zapewniony w ramach ochrony danych UE–USA

Delegacje otrzymują w załączeniu dokument COM(2024) 451 final.

Zał.: COM(2024) 451 final

KOMISJA
EUROPEJSKA

Bruksela, dnia 9.10.2024 r.
COM(2024) 451 final

SPRAWOZDANIE KOMISJI DLA PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie pierwszego okresowego przeglądu funkcjonowania decyzji stwierdzającej odpowiedni stopień ochrony zapewniony w ramach ochrony danych UE–USA

1. PIERWSZY PRZEGLĄD OKRESOWY – KONTEKST, PRZYGOTOWANIE I PRZEBIEG

W decyzji z 10 lipca 2023 r. („decyzja stwierdzająca odpowiedni stopień ochrony”) Komisja stwierdziła, że ramy ochrony danych UE–USA (DPF) zapewniają odpowiedni poziom ochrony danych osobowych przekazywanych z Unii Europejskiej do podmiotów w Stanach Zjednoczonych Ameryki[1]. W decyzji stwierdzającej odpowiedni poziom ochrony nałożono na Komisję obowiązek przeprowadzania okresowych przeglądów, z których pierwszy należy przeprowadzić po upływie roku od daty powiadomienia państw członkowskich o decyzji stwierdzającej odpowiedni stopień ochrony. W niniejszym sprawozdaniu podsumowano pierwszy przegląd.

Zgodnie z wymogiem zawartym w motywie 211 decyzji stwierdzającej odpowiedni stopień ochrony pierwszy przegląd, mający miejsce po pierwszym roku funkcjonowania nowych ram, koncentrował się na sprawdzeniu, czy wszystkie elementy przewidziane w tych ramach zostały wdrożone i czy funkcjonują skutecznie. Przegląd obejmował wszystkie aspekty funkcjonowania ram, w tym w świetle zmian prawnych, które miały miejsce od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony.

Przygotowując roczny przegląd, Komisja zebrała informacje od zainteresowanych stron, w szczególności od organizacji pozarządowych posiadających wiedzę specjalistyczną w zakresie praw cyfrowych i ochrony prywatności[2], podmiotów posiadających certyfikację DPF (za pośrednictwem ich stowarzyszeń branżowych[3]), a także od organów Stanów Zjednoczonych zaangażowanych we wdrażanie ram. Ponadto Komisja zebrała również informacje zwrotne od ogółu społeczeństwa za pośrednictwem specjalnego zaproszenia do zgłaszania uwag na portalu „Wyraź swoją opinię”[4].

W dniach 18–19 lipca 2024 r. w Waszyngtonie odbyło się spotkanie przeglądowe. Otworzyli je komisarz UE ds. sprawiedliwości i konsumentów Didier Reynders oraz amerykańska sekretarz ds. handlu Gina Raimondo[5].

---

[1] Decyzja wykonawcza Komisji (UE) 2023/1795 z dnia 10 lipca 2023 r. na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679, stwierdzająca odpowiedni stopień ochrony danych osobowych zapewniony w ramach ochrony danych UE–USA.

[2] Komisja przesłała kwestionariusz do dziewięciu organizacji pozarządowych (Human Rights Watch, American Civil Liberties Union, Consumer Federation of America, Center for Digital Democracy, New America Open Technology Institute, Access Now, Electronic Frontier Foundation, Electronic Privacy Information Center, Center for Democracy and Technology). Pytania koncentrowały się na istotnych zmianach amerykańskich ram prawnych, mechanizmach nadzoru i egzekwowania przepisów oraz funkcjonowaniu mechanizmów dochodzenia roszczeń. 9 lipca 2024 r. służby Komisji i przedstawiciele EROD spotkali się również online z tymi organizacjami pozarządowymi.

[3] Komisja przesłała kwestionariusz dziewięciu stowarzyszeniom branżowym (Software & Information Industry Association, U.S. Chamber of Commerce, Information Technology Industry Council, Software Alliance, Centre for Information Policy Leadership, Interactive Advertising Bureau, United States Council for International Business, Computer and Communications Industry Association, Engine). Pytania koncentrowały się na doświadczeniach przedsiębiorstw posiadających certyfikację DPF, w szczególności na procesie certyfikacji, działaniach podjętych w celu przestrzegania zasad DPF, mechanizmach rozpatrywania wniosków i skarg osób fizycznych itp.

[4] Otrzymane informacje zwrotne można znaleźć pod następującym adresem: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14379-EU-US-Data-Privacy-Framework-report-of-the-Commission-on-how-the-framework-is-functioning_pl.

[5] Spotkanie przeglądowe zorganizowano według tematów, a każdy punkt porządku obrad został przedstawiony w formie krótkiej prezentacji przez właściwy organ Stanów Zjednoczonych, przedstawiciela UE lub podmiot, po

Po stronie UE przegląd przeprowadzili przedstawiciele Dyrekcji Generalnej Komisji Europejskiej ds. Sprawiedliwości i Konsumentów, wraz z pięcioma przedstawicielami wyznaczonymi przez Europejską Radę Ochrony Danych (EROD) i reprezentującymi różne krajowe organy ochrony danych i Europejskiego Inspektora Ochrony Danych[6]. Po stronie USA w przeglądzie uczestniczyli przedstawiciele Departamentu Handlu (DoC), Departamentu Stanu, Federalnej Komisji Handlu (FTC), Departamentu Transportu (DoT), Urzędu Dyrektora Krajowych Służb Wywiadowczych (ODNI), Departamentu Sprawiedliwości (DoJ), Inspektora Generalnego Wspólnoty Wywiadowczej, a także członkowie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi (PCLOB). Ponadto na posiedzeniach poświęconych omawianemu przeglądowi informacji udzielali przedstawiciele organizacji oferujących usługi niezależnego rozstrzygania sporów oraz Amerykańskiego Stowarzyszenia Arbitrażowego. Źródłem informacji dla przeglądu były także prezentacje podmiotów posiadających certyfikację DPF na temat wypełniania przez przedsiębiorstwa wymogów określonych w ramach.

Ustalenia Komisji uzupełniono o publicznie dostępne materiały, w tym orzeczenia sądowe, przepisy wykonawcze i procedury właściwych organów Stanów Zjednoczonych, sprawozdania i badania organizacji pozarządowych, sprawozdania na temat przejrzystości udostępniane przez przedsiębiorstwa posiadające certyfikację DPF, roczne sprawozdania dostarczane przez niezależne organy nadzoru oraz doniesienia medialne.

2. USTALENIA

2.1. Aspekty handlowe

2.1.1. Proces certyfikacji

Aby móc otrzymywać dane osobowe przekazywane z UE na podstawie DPF, amerykańskie przedsiębiorstwo musi dokonać w DoC certyfikacji pod kątem przestrzegania określonych wymogów dotyczących ochrony danych („zasady DPF”), a następnie co roku ją ponawiać. Certyfikacja wymaga, aby przedsiębiorstwo podlegało uprawnieniom dochodzeniowym i wykonawczym FTC lub DoT, publicznie zadeklarowało swoje zobowiązanie do przestrzegania zasad DPF oraz publicznie ujawniło swoją politykę ochrony prywatności i w pełni wdrożyło takie wymogi[7]. Przed sfinalizowaniem certyfikacji DoC sprawdza, czy przedsiębiorstwo spełniło wszystkie wymogi certyfikacyjne[8].

Podczas spotkania przeglądowego DoC wyjaśnił, że w pierwszym roku funkcjonowania DPF nacisk położono na wprowadzenie procesu certyfikacji, w tym na opracowanie specjalnych narzędzi informatycznych, aktualizację procedur, współpracę z przedsiębiorstwami oraz prowadzenie innych działań informacyjnych/związanych z podnoszeniem świadomości. Do dnia spotkania przeglądowego certyfikację DPF uzyskało ponad 2 800 przedsiębiorstw. Oznacza to, że liczba przedsiębiorstw, które uzyskały certyfikację DPF, zwiększyła się w porównaniu z pierwszym rokiem funkcjonowania poprzednich ram, tzn. Tarczy

czym odbyła się szczegółowa sesja pytań i odpowiedzi. Pierwszego dnia omówiono „aspekty handlowe” ram (tj. stosowanie i egzekwowanie wymogów mających zastosowanie do przedsiębiorstw certyfikowanych w ramach DPF), natomiast drugiego dnia omówiono kwestie związane z dostępem rządu do danych osobowych.

[6] Przedstawiciele Komisji i EROD spotkali się 12 czerwca i 10 lipca 2024 r., aby przygotować się do przeglądu, omówić otrzymane uwagi i określić, które aspekty wymagają zebrania dodatkowych informacji i wyjaśnień.

[7] Sekcja I pkt 2 załącznika I do decyzji stwierdzającej odpowiedni stopień ochrony.

[8] Załącznik III do decyzji stwierdzającej odpowiedni stopień ochrony.

Prywatności”[9]. Zgodnie z informacjami przekazanymi przez DoC 70 % uczestników to MŚP, a duża liczba przedsiębiorstw objętych DPF (47 %) działa w sektorze informacji, technologii i komunikacji (ICT). Ponadto 60 % przedsiębiorstw posiada certyfikację wyłącznie w odniesieniu do danych innych niż dane o zasobach ludzkich, 2,5 % przedsiębiorstw posiada certyfikację wyłącznie w odniesieniu do danych o zasobach ludzkich, a 37,5 % posiada certyfikację zarówno w odniesieniu do danych o zasobach ludzkich, jak i danych innych niż dane o zasobach ludzkich.

DoC przyjął niezbędne procedury rozpatrywania wniosków składanych przez przedsiębiorstwa. Przedsiębiorstwa muszą składać wnioski o certyfikację na stronie internetowej DoC dotyczącej DPF (https://www.dataprivacyframework.gov/). Znajdują się tam informacje o tym, jak przystąpić do DPF[10] oraz o obowiązkach przedsiębiorstwa wynikających z tych ram[11]. Za wszystkie aspekty związane z zarządzaniem i administrowaniem DPF, w tym za proces certyfikacji i monitorowanie zgodności, odpowiada specjalny zespół w DoC, podlegający dyrektorowi ds. ramy ochrony danych. Każdym wnioskiem zajmuje się konkretny pracownik, który pozostaje odpowiedzialny za dane przedsiębiorstwo przez cały czas trwania procesu certyfikacji.

Aby uzyskać certyfikację na podstawie ram, przedsiębiorstwa składają wniosek, w tym projekt polityki ochrony prywatności. DoC sprawdza, czy jest on zgodny z odpowiednimi wymogami DPF. W przypadku, gdy podmioty chcą uzyskać certyfikację poszczególnych podmiotów niższego szczebla w ramach grupy przedsiębiorstw (np. poszczególnych jednostek zależnych), DoC zwraca się o jedną kompleksową politykę ochrony prywatności, która wyraźnie wskazuje wszystkie podmioty niższego szczebla, które mają być objęte tą polityką, oraz dokonuje jej przeglądu, albo o odrębną politykę dla każdego podmiotu niższego szczebla. DoC weryfikuje również za pomocą niezależnego mechanizmu ochrony prawnej (IRM)[12] wskazanego we wniosku, czy podmiot rzeczywiście się w tym mechanizmie zarejestrował. W przypadku przedsiębiorstw, które wybrały panel organów ochrony danych (np. ponieważ przetwarzają dane o zasobach ludzkich), DoC sprawdza, czy przedsiębiorstwo uiściło opłaty wymagane, aby mogło skorzystać z panelu. W razie potrzeby DoC weryfikuje również, czy wnioskodawca podlega jurysdykcji FTC lub DoT (a zatem kwalifikuje się do przystąpienia do DPF).

Jeżeli wszystkie warunki są spełnione, DoC informuje podmiot, że może opublikować na własnej stronie internetowej swoją politykę ochrony prywatności odnoszącą się do DPF. Po opublikowaniu polityki ochrony prywatności, DoC potwierdza certyfikację i umieszcza przedsiębiorstwo w wykazie DPF na swojej stronie internetowej. Od daty umieszczenia podmiotu w wykazie[13] przez DoC można powoływać się na DPF w celu otrzymywania danych osobowych z UE.

Jak wyjaśniono podczas spotkania przeglądowego, kontrole przeprowadzone dotychczas przez DoC doprowadziły do odrzucenia 33 wniosków, ponieważ nie spełniały one wymogów DPF. Zasadniczo DoC współpracuje z przedsiębiorstwem w celu wyeliminowania wszelkich

[9] W równoważnym okresie certyfikację w ramach Tarczy Prywatności uzyskało 2 400 przedsiębiorstw.
[10] https://www.dataprivacyframework.gov/program-articles/How-to-Join-the-Data-Privacy-Framework-(DPF)-Program-(part%E2%80%931).
[11] https://www.dataprivacyframework.gov/key-requirements.
[12] Mechanizmy rozstrzygania sporów w sektorze prywatnym, za pomocą których bada się i szybko rozstrzyga skargi oraz spory osób fizycznych, bez konieczności ponoszenia przez te osoby jakichkolwiek kosztów.
[13] Sekcja I pkt 3 załącznika I do decyzji stwierdzającej odpowiedni stopień ochrony.

uchybień. W przypadku, gdy DoC stwierdzi uchybienia, informuje przedsiębiorstwo o konieczności ich usunięcia oraz o tym, że brak odpowiedzi w określonym terminie lub inne niespełnienie wymogu samocertyfikacji zgodnie z procedurami DoC doprowadzą do uznania wniosku za zaniechany. Jeśli wstępna certyfikacja nie zostanie zakończona/poprawiona w ciągu 12 miesięcy, DoC uzna ją za zaniechaną.

Termin corocznej ponownej certyfikacji jest określony w wykazie DPF dla każdego przedsiębiorstwa. Aby przypomnieć przedsiębiorstwom o konieczności złożenia wniosku o ponowną certyfikację, DoC stworzył system przypominający o zbliżającym się wygaśnięciu certyfikacji. Podmioty otrzymują przypomnienia na miesiąc, dwa tygodnie oraz jeden dzień przed terminem wygaśnięcia certyfikacji. Podmioty, których certyfikacja wygasła, są usuwane z wykazu DPF. Jak opisano w załączniku III do decyzji stwierdzającej odpowiedni stopień ochrony, na stronie internetowej DoC znajduje się specjalna sekcja zawierająca wykaz amerykańskich podmiotów, które nie są już aktywnymi uczestnikami, wraz z informacjami o powodach ich usunięcia z wykazu (np. wygaśnięcie lub wycofanie się) („wykaz nieaktywnych podmiotów"). Gdy powodem usunięcia podmiotów z wykazu DPF jest to, że pozwoliły one na wygaśnięcie certyfikacji, DoC kontaktuje się z tymi podmiotami, aby potwierdzić, czy zamierzają się wycofać albo czy planują uzyskać ponowną certyfikację. W tym drugim przypadku DoC weryfikuje, czy w okresie wygaśnięcia podmioty stosowały zasady DPF wobec danych osobowych otrzymanych w ramach DPF, oraz wyjaśnia, jakie kroki podejmą w celu rozwiązania nierozstrzygniętych kwestii opóźniających ponowną certyfikację. Jeżeli przedsiębiorstwa powiadomią DoC o chęci wycofania się z DPF, DoC wymaga od nich potwierdzenia, czy zwrócą lub usuną dane otrzymane w ramach DPF, czy zatrzymają je i będą nadal stosować zasady DPF do takich danych (co należy potwierdzać corocznie) albo czy zatrzymają je i wprowadzą inne zabezpieczenia (takie jak standardowe klauzule umowne przyjęte przez Komisję Europejską).

Z informacji zwrotnych otrzymanych od stowarzyszeń branżowych i przedsiębiorstw wynika, że przedsiębiorstwa posiadające certyfikację DPF podjęły szereg kroków w celu zapewnienia zgodności z zasadami DPF. Na przykład w celu zapewnienia zgodności z *zasadą dotyczącą ochrony prawnej, egzekwowania prawa oraz odpowiedzialności* podmioty przeprowadziły kontrole wewnętrzne w formie samooceny lub zewnętrznego przeglądu zgodności. Przedstawiciele dwóch niezależnych mechanizmów ochrony prawnej sektora prywatnego, którzy uczestniczyli w spotkaniu przeglądowym, wyjaśnili, że mechanizmy zapewniają zewnętrzny przegląd zgodności poprzez analizę polityki ochrony prywatności. W przypadku jednego z tych mechanizmów wyjaśniono dodatkowo, że w jego ramach przeprowadza się audyty oraz wyrywkowe kontrole, koncentrując się na zasadach *dostępu, wyboru i dalszego przekazywania danych*. Ponadto certyfikowane przedsiębiorstwa opracowały wewnętrzne programy zgodności i mechanizmy nadzoru, przeszkoliły pracowników, wdrożyły mechanizmy umożliwiające osobom fizycznym korzystanie z przysługujących im praw, przeprowadziły oceny wpływu na prywatność oraz dokonały przeglądu istniejących umów.

2.1.2. Monitorowanie zgodności, fałszywe oświadczenia o uczestnictwie i egzekwowanie przepisów

W ramach DPF DoC jest odpowiedzialny za monitorowanie zgodności z zasadami DPF przy użyciu różnych narzędzi, w tym kontroli z urzędu (z własnej inicjatywy), kontroli wyrywkowych *ad hoc* i kwestionariuszy dotyczących zgodności. Działania te obejmują

wyszukiwanie fałszywych oświadczeń o uczestnictwie w przedmiotowych ramach, na przykład poprzez wyszukiwanie w internecie[14], i reagowanie na takie fałszywe oświadczenia.

Aby monitorować przestrzeganie zasad przez przedsiębiorstwa objęte DPF, DoC polegał głównie na doraźnych wyszukiwaniach w internecie i kontrolach mediów (społecznościowych) w ciągu ostatniego roku. DoC poinformował, że w tym pierwszym roku nie wykrył problemów związanych z przestrzeganiem zasad DPF i nie zgłosił żadnych przedsiębiorstw do FTC lub DoT w celu podjęcia ewentualnych czynności służących egzekwowaniu przepisów. Utworzył również specjalny punkt kontaktowy w celu ułatwienia współpracy z organami ochrony danych oraz przyjmowania skarg od osób fizycznych i zgłoszeń od innych organów (np. organów ochrony danych lub FTC). W ciągu ostatniego roku nie wpłynęły jednak żadne zgłoszenia ani skargi. Podczas gdy w pierwszym roku funkcjonowania DPF skoncentrowano się na ustanowieniu ram i procesie certyfikacji, DoC wyjaśnił podczas spotkania przeglądowego, że planuje przeprowadzać kontrole zgodności w sposób zautomatyzowany, aby były bardziej systematyczne, i obecnie opracowuje niezbędne do tego narzędzia informatyczne.

Komisja przyjmuje do wiadomości, że w pierwszym roku DoC musiał skoncentrować swoje wysiłki na ustanowieniu ram i procesu certyfikacji. W przyszłości ważne jest, aby DoC zintensyfikował działania mające na celu monitorowanie i sprawdzanie zgodności z zasadami, co jest konieczne do zapewnienia stałego wysokiego poziomu zgodności z ramami i wykrywania przypadków wymagających dalszych czynności służących egzekwowaniu przepisów, w tym ewentualnych fałszywych oświadczeń przedsiębiorstw o uczestnictwie. W związku z tym Komisja z zadowoleniem przyjmuje fakt, że DoC potwierdził swój zamiar opracowania i stosowania (zautomatyzowanych) narzędzi w celu skuteczniejszego i bardziej systematycznego identyfikowania kwestii związanych ze zgodnością i fałszywych oświadczeń, oraz jest zdania, że działanie to powinno stanowić część szerszych wysiłków na rzecz większego wykorzystania różnych narzędzi, którymi dysponuje (np. kontroli wyrywkowych, kwestionariuszy dotyczących przeglądu zgodności, wniosków o udzielenie informacji itp.), w tym w celu weryfikacji zgodności z określonymi wymogami w ramach DPF[15].

Podmioty objęte DPF podlegają jurysdykcji FTC i DoT. Podczas spotkania przeglądowego DoT potwierdził, że wdrożono wszystkie procesy, aby umożliwić podjęcie odpowiednich czynności służących egzekwowaniu przepisów. Wyjaśnił również, że do DPF przystąpiło bardzo niewiele przedsiębiorstw podlegających jego jurysdykcji (tj. kilku pośredników sprzedaży biletów, ale ani jedna linia lotnicza). FTC potwierdziła, że systematycznie kontroluje naruszenia DPF w każdym ze swoich dochodzeń w zakresie ochrony prywatności. Do tej pory FTC nie otrzymała żadnych zgłoszeń od innych organów. FTC otrzymała kilka skarg, w których wspomniano DPF, chociaż dwie z nich dotyczyły przedsiębiorstw znajdujących się w „wykazie nieaktywnych podmiotów", dwie dotyczyły przedsiębiorstw, które nie uczestniczyły w ramach, a jedna nie dotyczyła danych osobowych przekazywanych z UE. Do czasu powstania niniejszego sprawozdania FTC nie wydała decyzji służących egzekwowaniu

[14] Zob. załącznik III do decyzji stwierdzającej odpowiedni stopień ochrony. Fałszywe oświadczenia mogą pojawić się na przykład wtedy, gdy przedsiębiorstwo twierdzi, że uczestniczy w DPF i albo nigdy nie rozpoczęło procesu certyfikacji, albo rozpoczęło go, ale nie zakończyło lub pozwoliło na wygaśnięcie swojej certyfikacji.

[15] Na przykład w odniesieniu do dalszego przekazywania danych, korzystając z możliwości przewidzianej w zasadzie DPF 3 lit. b), aby zwrócić się o streszczenie lub poświadczoną kopię odpowiednich postanowień dotyczących prywatności zawartych w umowach dotyczących dalszego przekazywania danych.

zgodności z DPF, chociaż potwierdziła, że kilka przedsiębiorstw posiadających certyfikację DPF jest obecnie objętych dochodzeniem.

Komisja z zadowoleniem przyjmuje fakt, że FTC systematycznie kontroluje naruszenia DPF we wszystkich dochodzeniach w zakresie ochrony prywatności. Ponieważ stała skuteczność DPF zależy od ich solidnego egzekwowania, oczekuje się, że FTC będzie w dalszym ciągu wykonywać swoje uprawnienia dochodzeniowe w ramach DPF, w tym poprzez proaktywne prowadzenie akcji kontrolnych koncentrujących się na przestrzeganiu określonych wymogów DPF lub na niektórych sektorach.

2.1.3. Rozpatrywanie skarg

DPF zapewniają osobom fizycznym z UE różne możliwości skorzystania z mechanizmu ochrony prawnej w przypadku nieprzestrzegania zasad DPF przez certyfikowane podmioty[16]. Działania te obejmują dążenie do rozwiązania sprawy poprzez bezpośredni kontakt z podmiotem objętym DPF, który musi udzielić odpowiedzi pokrzywdzonej osobie w ciągu 45 dni. Osoby fizyczne mogą również wnieść skargę do niezależnego mechanizmu ochrony prawnej wyznaczonego przez podmiot w celu zbadania i rozstrzygnięcia skarg. W zależności od okoliczności może to być organ zajmujący się alternatywnym rozstrzyganiem sporów albo organ ochrony danych[17]. Ponadto w przypadku, gdy żaden z pozostałych dostępnych środków odwoławczych nie przyniósł zadowalającego rozstrzygnięcia skargi osoby, której dane dotyczą, osoby fizyczne mogą poddać sprawę pod arbitraż panelu DPF UE–USA w ramach mechanizmu ochrony prawnej ostatniej szansy.

2.1.3.1. Rozpatrywanie skarg przez przedsiębiorstwa

Z odpowiedzi udzielonych przez stowarzyszenia branżowe i przedsiębiorstwa na kwestionariusze przesłane przez Komisję wynika, że przedsiębiorstwa posiadające certyfikację DPF otrzymały bardzo niewiele skarg od osób fizycznych dotyczących nieprzestrzegania zasad DPF, a niektóre nie otrzymały ich wcale. Jednocześnie przedsiębiorstwa wprowadziły różne mechanizmy i narzędzia umożliwiające osobom fizycznym korzystanie z przysługujących im praw i składanie skarg, w tym za pośrednictwem formularzy internetowych, poczty elektronicznej i telefonu.

2.1.3.2. *Niezależne mechanizmy ochrony prawnej (IRM)*

Informacje zwrotne otrzymane podczas spotkania przeglądowego oraz informacje przekazane przez stowarzyszenia branżowe wskazują, że złożono bardzo niewielką liczbę skarg do niezależnych mechanizmów rozstrzygania sporów. Niezależne mechanizmy ochrony prawnej wybrane przez przedsiębiorstwa to BBB National Programs, JAMS, TRUSTe i VeraSafe. W DPF wymaga się, aby niezależne mechanizmy ochrony prawnej publikowały roczne sprawozdanie zawierające zagregowane dane statystyczne dotyczące korzystania z ich usług rozstrzygania sporów. W momencie przyjmowania niniejszego sprawozdania wszystkie zainteresowane niezależne mechanizmy ochrony prawnej opublikowały swoje sprawozdania roczne[18].

---

[16] Zob. sekcja 2.4 decyzji stwierdzającej odpowiedni stopień ochrony.

[17] Podmioty objęte DPF są zobowiązane do współpracy przy badaniu i rozstrzyganiu skarg przez organ ochrony danych, jeżeli dotyczą one przetwarzania danych o zasobach ludzkich gromadzonych w kontekście stosunku pracy albo jeżeli dany podmiot dobrowolnie poddał się nadzorowi organów ochrony danych.

[18] ANA – https://www.ana.net/content/show/id/accountability-dpf-consumers;
BBB National Programs – https://assets.bbbprograms.org/docs/default-source/eu-privacy-

Ponadto podczas spotkania przeglądowego BBB i VeraSafe przedstawiły szczegółowe prezentacje swojej działalności w ostatnim roku. Zgłosiły, że liczba uczestników biznesowych wybierających ich usługi wzrosła w porównaniu z poprzednimi ramami, i wspomniały, że otrzymały pewną liczbę skarg, chociaż zdecydowana większość z nich nie kwalifikowała się do rozstrzygnięcia. Przykładowo, mechanizm BBB otrzymał 87 skarg od osób fizycznych z UE, przy czym tylko dwie z nich kwalifikowały się do rozstrzygnięcia. Choć zgodnie z wyjaśnieniem BBB skargi są rozpatrywane średnio w ciągu 5 dni roboczych, te dwie skargi zostały ostatecznie zamknięte z powodu braku odpowiedzi ze strony osób fizycznych. Mechanizm VeraSafe otrzymał 26 skarg, z których sześć kwalifikowało się do rozstrzygnięcia. Dwie z nich, dotyczące wniosków o dostęp do danych oraz ich usunięcie, rozpatrzono je pozytywnie, dwie nadal oczekują na rozpatrzenie, a dwie ostatnie wycofano lub zamknięto z powodu braku odpowiedzi ze strony osoby fizycznej. Oba niezależne mechanizmy ochrony prawnej wyjaśniły, że dążą do udzielenia odpowiedzi na skargi w języku danej osoby fizycznej.

Przedsiębiorstwa objęte DPF, które przetwarzają dane o zasobach ludzkich przekazywane z UE, muszą wybrać organy ochrony danych UE jako swoje niezależne mechanizmy ochrony prawnej dla tych danych, podczas gdy w przypadku innych rodzajów danych osobowych przekazywanych w oparciu o DPF przedsiębiorstwo objęte DPF może dobrowolnie wybrać unijne organy ochrony danych jako swoje niezależne mechanizmy ochrony prawnej. W istocie ponad połowa przedsiębiorstw certyfikowanych na podstawie DPF opowiedziała się w czasie przeglądu za tym rozwiązaniem[19], co daje powody do zadowolenia. Od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony EROD przyjęła regulamin wewnętrzny „nieformalnego panelu unijnych organów ochrony danych". Panel jest odpowiedzialny za udzielanie wiążących wskazówek amerykańskim podmiotom w związku z nierozstrzygniętymi skargami osób fizycznych dotyczącymi posługiwania się danymi osobowymi, które zostały przekazane z UE w ramach DPF. Zgodnie z regulaminem panel składa się z jednego organu ochrony danych działającego jako główny organ ochrony danych oraz innych wyznaczonych organów ochrony danych działających jako podmioty wspólnie dokonujące przeglądu[20]. Panel udziela wiążących wskazówek w ciągu 60 dni od otrzymania skargi w ramach DPF. EROD opublikowała również wzór formularza skargi na potrzeby

shield/dpf_periodicalreport_072024.pdf; ICDR – AAA – https://go.adr.org/rs/294-SFS-516/images/Data%20Privacy%20Framework%20IRM%20Program%20Report%202023-2024%20FINAL.pdf?version=0;
Insights Association – https://www.insightsassociation.org/Portals/INSIGHTS/Insights%20Association%20DPF%20Services%20Program%202024%20Annual%20Report_Final_1.pdf;
JAMS – https://www.jamsadr.com/files/Uploads/Documents/2024-Annual-Report-DPF-Cases.pdf;
Privacy Trust DPF Services – https://privacytrust.com/fserve/PrivacyTrust_Dispute_Resolution_Report_2023_2024.pdf;
TRUSTe Dispute Resolution –https://trustarc.com/wp-content/uploads/2024/07/2024-Independent-Recourse-Mechanism-Annual-Report.pdf;
Verasafe – https://verasafe.com/wp-content/uploads/2020/06/VeraSafe-DPF-Dispute-Resolution-Program-Annual-Report-2024.pdf.

[19] Wkrótce po dacie spotkania przeglądowego na stronie internetowej DPF wskazano, że dla 1 511 z 2 892 uczestników funkcję mechanizmu ochrony prawnej pełni unijny organ ochrony danych.

[20] 17 kwietnia 2024 r. EROD przyjęła regulamin wewnętrzny „nieformalnego panelu unijnych organów ochrony danych" zgodnie z ramami ochrony danych UE–USA. Jest on dostępny pod adresem: https://www.edpb.europa.eu/system/files/2024-04/dpf_rules-of-procedure_informal-panel-dpas_en.pdf.

składania skarg do organów ochrony danych[21], a także odpowiedzi na pytania w sprawie DPF, które są często zadawane przez osoby fizyczne[22] i przedsiębiorstwa[23] z UE. Do czasu przeglądu panel nie otrzymał żadnych skarg.

2.1.3.3. Wiążący mechanizm arbitrażowy

Do zarządzania wiążącym mechanizmem arbitrażowym DoC wybrał Międzynarodowe Centrum Rozstrzygania Sporów (ICDR), które jest międzynarodowym oddziałem Amerykańskiego Stowarzyszenia Arbitrażowego. Po przyjęciu decyzji stwierdzającej odpowiedni stopień ochrony DoC wraz z Komisją wybrał 11 arbitrów posiadających doświadczenie w dziedzinie ochrony prywatności, reprezentujących różne sektory, w tym sądownictwo polubowne, sądownictwo państwowe, środowisko akademickie oraz społeczeństwo obywatelskie[24]. Przyjęto także regulamin arbitrażowy[25] panelu DPF oraz kodeks postępowania arbitrów[26], które są dostępne na stronie internetowej ICDR. Do czasu przeglądu żadna osoba fizyczna z UE nie uruchomiła jeszcze mechanizmu arbitrażowego.

2.1.4. Wytyczne, współpraca i podnoszenie świadomości

Od czasu wejścia w życie DPF DoC prowadzi różne działania związane z podnoszeniem świadomości, organizując seminaria wyjazdowe, webinaria i konferencje, docierając do stowarzyszeń branżowych i nawiązując bezpośrednie kontakty z ponad 3 000 przedsiębiorstw w celu przekazania informacji na temat DPF. Opublikował również wytyczne, w tym w formie odpowiedzi na najczęściej zadawane pytania, skierowane do osób fizycznych, a także do przedsiębiorstw z UE i USA[27]. EROD opracowała z kolei formularze skarg i odpowiedzi na najczęściej zadawane pytania osób fizycznych i przedsiębiorstw. Również Komisja opublikowała odpowiedzi na pytania oraz arkusz informacyjny na temat DPF, gdy przyjęła decyzję stwierdzającą odpowiedni stopień ochrony[28].

Jednocześnie ze spotkania przeglądowego wynika, że konieczne są dalsze działania w celu zwiększenia świadomości wśród osób fizycznych i przedstawienia wytycznych przedsiębiorstwom. Informacje otrzymane od przedsiębiorstw i niezależnych mechanizmów ochrony prawnej oraz bardzo mała liczba skarg wskazują, że osoby fizyczne nie zawsze są świadome swoich praw lub mechanizmów umożliwiających korzystanie z nich. Podczas spotkania przeglądowego DoC wyraził zainteresowanie współpracą z unijnymi organami ochrony danych w celu zwiększenia świadomości na temat ram wśród osób fizycznych z UE. Komisja zachęca do podejmowania takich inicjatyw, a także podejmuje kroki w celu lepszego informowania osób fizycznych, w tym zamieszcza na swojej stronie internetowej dodatkowe

[21] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-template-complaint-form_pl.
[22] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-individuals_pl.
[23] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/eu-us-data-privacy-framework-faq-european-businesses_pl.
[24] https://go.adr.org/DPF_Arbitrator_Bios.html.
[25] https://go.adr.org/rs/294-SFS-516/images/IC.DR-AAA_EU-US_DPF_AnnexI_Arbitration_Rules.pdf.
[26] https://go.adr.org/rs/294-SFS-516/images/Code_of_Conduct_for_Arbitrators_Appointed_to_EU-US_DPF_AnnexI_Arbitrations.pdf.
[27] Zob. np. https://www.dataprivacyframework.gov/US-Businesses.
[28] https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_pl.

informacje na temat DPF, na przykład w postaci linków i odniesień do odpowiednich wytycznych przyjętych przez EROD, DoC i inne organy Stanów Zjednoczonych.

Jeżeli chodzi o wytyczne dotyczące zasad DPF, przedstawiciele EROD uzgodnili podczas spotkania przeglądowego, że w nadchodzących miesiącach będą współpracować w celu doprecyzowania pojęcia „danych o zasobach ludzkich" w ramach DPF oraz szczegółowych obowiązków mających zastosowanie do przetwarzania takich danych. Przeanalizowano różne elementy, które należy uwzględnić w takich wytycznych. Na przykład wytyczne te mogłyby dotyczyć realnych scenariuszy, w których dane pracowników mają być przetwarzane w ramach DPF (np. przez dostawcę usług w chmurze), i wyjaśniać na ich przykładzie, które obowiązki związane z DPF mają zastosowanie. Ponadto wytyczne mogłyby sugerować przedsiębiorstwom, które otrzymują dane pracowników będących osobami fizycznymi z UE (ale niekoniecznie wykorzystują takie dane w kontekście stosunku pracy), aby wybrały panel organu ochrony danych jako swój niezależny mechanizm ochrony prawnej. Dzięki temu takie osoby fizyczne będą mogły zwrócić się do organu, który jest im bliski i – w stosownych przypadkach – lepiej zaznajomiony z obowiązującymi przepisami krajowymi mającymi zastosowanie do danych o zasobach ludzkich.

Ponadto szczególnym aspektem, w przypadku którego celowe jest wydanie większej liczby wytycznych (co wynika m.in. z informacji otrzymanych od stowarzyszeń branżowych), są wymogi DPF dotyczące dalszego przekazywania danych. DoC wskazał również, że warto byłoby zbadać, czy niektóre sektory mogą skorzystać z dodatkowych wytycznych dotyczących stosowania zasad DPF w ich działalności, np. w badaniach z dziedziny zdrowia i w usługach finansowych.

Komisja z zadowoleniem przyjmuje gotowość obu stron do opracowania wytycznych i oczekuje, że prace nad wyżej wymienionymi zagadnieniami rozpoczną się wkrótce.

Jeżeli chodzi o kwestie ogólne, ustanowiono szereg mechanizmów w celu zapewnienia wymiany informacji i współpracy między organami Stanów Zjednoczonych a organami ochrony danych, w tym poprzez wyznaczenie specjalnych punktów kontaktowych w ramach FTC i DoC w celu rozpatrywania zapytań i zgłoszeń ze strony organów ochrony danych.

2.1.5. Istotne zmiany w systemie prawnym Stanów Zjednoczonych

Od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony zaszedł szereg zmian w amerykańskich ramach prawnych w dziedzinie ochrony prywatności: legislacyjnych, regulacyjnych i w orzecznictwie. Zasadniczo wskazują one na większą zbieżność między podejściem UE i USA do niektórych wyzwań związanych z ochroną prywatności, w tym poprzez stosowanie podobnych pojęć prawnych. Niektóre z tych zmian są w toku i będą wymagały dalszego monitorowania.

Na szczeblu federalnym prezydent wydał szereg rozporządzeń wykonawczych, które są istotne dla wykorzystywania danych osobowych. W szczególności rozporządzenie wykonawcze 14117 z dnia 28 lutego 2024 r.[29] zakazuje transakcji obejmujących niektóre kategorie wrażliwych danych osobowych (np. dane dotyczące zdrowia, identyfikatory biometryczne, dane genomowe człowieka) z podmiotami w niektórych „państwach budzących

[29] https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related.

obawy”[30] lub ogranicza takie transakcje. Nakazano w nim prokuratorowi generalnemu przedstawienie wniosku dotyczącego regulacji – którego w chwili przyjęcia niniejszego sprawozdania jeszcze nie wydano – określających szczegółowo sposób wdrożenia tego rozporządzenia wykonawczego. Ponadto rozporządzenie wykonawcze 14110 z dnia 30 października 2023 r. w sprawie sztucznej inteligencji[31] kładzie nacisk na rozwój bezpiecznej i godnej zaufania sztucznej inteligencji. Zobowiązano w nim kilka agencji federalnych do opracowania norm bezpieczeństwa związanych ze sztuczną inteligencją i wytycznych w tym zakresie, dotyczących m.in. konkretnych zagrożeń dla ochrony prywatności i technik ochrony prywatności w kontekście sztucznej inteligencji.

Jeżeli chodzi o prace legislacyjne, chociaż w ostatnich latach w Kongresie przedstawiono projekty federalnych ustaw o ochronie prywatności, od lipca 2024 r. 20 stanów USA przyjęło kompleksowe ustawy dotyczące ochrony prywatności, a w ośmiu stanach ustawy te weszły w życie: w Kalifornii, Kolorado, Oregonie, Wirginii, Connecticut, Utah, Teksasie i Florydzie. Ponadto 17 stanów USA przyjęło przepisy dotyczące zautomatyzowanego przetwarzania (lub przynajmniej niektórych jego form) i ogólnie dopuszczające możliwość korzystania z klauzuli *opt-out* w odniesieniu do niektórych rodzajów podejmowania decyzji w oparciu o „profilowanie”[32].

Jeżeli chodzi o zmiany w orzecznictwie, kilku przedstawicieli społeczeństwa obywatelskiego zwróciło uwagę na niedawny wyrok Sądu Najwyższego w sprawie Loper Bright Enterprises przeciwko Raimondo (z 28 czerwca 2024 r.). Wyrok ten jest sprzeczny z wcześniejszym orzecznictwem dotyczącym doktryny „Chevron”, zgodnie z którą sądy stosują zasadę poszanowania uzasadnionej interpretacji prawa przez organ regulacyjny w przypadku niejednoznaczności prawa egzekwowanego przez ten organ. W szczególności niektóre organizacje pozarządowe wyraziły obawy co do wpływu tego orzeczenia Sądu Najwyższego na uprawnienia decyzyjne FTC w dziedzinie ochrony prywatności, uznając jednocześnie, że orzeczenie to może nie mieć wpływu lub mieć ograniczony wpływ na uprawnienia wykonawcze FTC. Na spotkaniu przeglądowym FTC poinformowała, że jest jeszcze za wcześnie, aby poznać dokładne konsekwencje wydania tego wyroku. Jednocześnie wyjaśniła, że tworzenie przepisów przez FTC odbywa się na podstawie ustawy o FTC, której przepisy

[30] Wśród nich znalazły się – zgodnie z propozycją prokuratora generalnego zawartą w wydanym 3 maja 2024 r. obwieszczeniu – Chiny, Kuba, Hongkong i Makau, Iran, Korea Północna i Wenezuela. Zob. https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and.

[31] https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

[32] Pomimo różnic w rozumieniu tego pojęcia w poszczególnych stanach „profilowanie” jest zasadniczo definiowane jako dowolna forma zautomatyzowanego przetwarzania danych osobowych w celu oceny, analizy lub przewidywania osobistych aspektów związanych z sytuacją ekonomiczną, zdrowiem, osobistymi preferencjami, zainteresowaniami, wiarygodnością, zachowaniem, lokalizacją lub przemieszczaniem się zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Zazwyczaj konsumenci mogą zrezygnować z profilowania. Następujące stany opracowały przepisy dotyczące profilowania: Kolorado (Colo. Rev. Stat. Ann. § 6-1-1306), Connecticut (Conn. Gen. Stat. Ann. § 42-518), Delaware (Del. Code Ann. tit. 6, § 12D-104), Floryda (Fla. Stat. Ann. § 501.705), Indiana (Ind. Code Ann. § 24-15-3-1), Kentucky (Ky. Rev. Stat. Ann. § 367.3615), Maryland (Maryland Online Data Privacy Act of 2024, uchwalona 9 maja 2024 r.), Minnesota (Minn. Stat. Ann. § 325O.07), Montana (Mont. Code Ann. § 30-14-2808), Nebraska (Neb. Rev. Stat. Ann. § 87-1107), New Hampshire (N.H. Rev. Stat. Ann. § 507-H:4), New Jersey (N.J. Stat. Ann. § 56:8-166.8), Oregon (Or. Rev. Stat. Ann. § 646A.574), Rhode Island (Rhode Island Data Transparency and Privacy Protection Act, uchwalona 29 czerwca 2024 r.), Tennessee (Tenn. Code Ann. § 47-18-3304), Teksas (Tex. Bus. & Com. Code Ann. § 541.051) oraz Virginia (Va. Code Ann. § 59.1-577).

różnią się od tych obowiązujących inne organy administracyjne, a doktryna „Chevron" ma w ich przypadku mniejsze znaczenie. W związku z tym niedawny wyrok może mieć ograniczony wpływ na ten obszar.

Ponadto FTC poinformowała o ostatnich zmianach w swoim podejściu do zautomatyzowanego przetwarzania i sztucznej inteligencji. Chodzi tu między innymi o przyjęcie, wspólnie z innymi organami egzekwowania prawa, oświadczenia przeciwko dyskryminacji i stronniczości w zautomatyzowanych systemach[33], a także o szereg czynności służących egzekwowaniu przepisów, w których FTC skupia się między innymi na przejrzystości, uczciwości zautomatyzowanego przetwarzania i możliwości kwestionowania wyników przez osoby fizyczne. Najbardziej znaczącym przypadkiem w tym kontekście jest decyzja FTC przeciwko Rite Aid z marca 2024 r., w której nałożono pięcioletni zakaz wykorzystywania przez tę firmę technologii rozpoznawania twarzy do celów bezpieczeństwa[34]. W szczególności FTC stwierdziła, że Rite Aid nie podjęła racjonalnych środków w celu zapobieżenia błędnym wynikom i poinformowania konsumentów o stosowanej technologii. Jeżeli chodzi o kwestie ogólne, podczas spotkania przeglądowego FTC omówiła swoje bieżące priorytety, a zwłaszcza obszary, które jej zdaniem zasługują na bardziej proaktywne podejście do egzekwowania prawa w przyszłości. Są to ochrona danych wrażliwych (np. danych dotyczących zdrowia, danych biometrycznych, geolokalizacji)[35], ochrona dziecka[36] i nieletnich w internecie oraz bezpieczeństwo danych[37].

Komisja będzie nadal uważnie śledzić te i inne wydarzenia w USA, w szczególności wszelkie dalsze działania na rzecz kompleksowej federalnej ustawy o ochronie prywatności oraz ewentualny wpływ niedawnego orzecznictwa Sądu Najwyższego na rolę FTC w obszarze ochrony prywatności.

Komisja z zadowoleniem przyjmuje informacje przekazane przez FTC na temat jej ostatnich czynności służących egzekwowaniu przepisów, a także bieżących priorytetów, które w dużej mierze odpowiadają trendom i priorytetom w zakresie egzekwowania ochrony danych w Europie. FTC bierze również aktywny udział w sieci zrzeszającej państwa korzystające z unijnej decyzji stwierdzającej odpowiedni stopień ochrony, którą Komisja zainicjowała w marcu 2024 r.[38] Taka zwiększona zbieżność działań powinna zachęcać i ułatwiać ściślejszą

[33] https://files.consumerfinance.gov/f/documents/cfpb_joint-statement-enforcement-against-discrimination-bias-automated-systems_2023-04.pdf.

[34] https://www.ftc.gov/legal-library/browse/cases-proceedings/2023190-rite-aid-corporation-ftc-v.

[35] Zob. np. niedawne zarządzenie FTC przeciwko X-Mode za sprzedaż i udostępnianie wrażliwych informacji o lokalizacji (https://www.ftc.gov/system/files/ftc_gov/pdf/X-ModeSocialDecisionandOrder.pdf) oraz przeciwko Monument w sprawie ujawniania wrażliwych danych dotyczących zdrowia stronom trzecim w celach marketingowych (https://www.ftc.gov/system/files/ftc_gov/pdf/MonumentOrderFiled.pdf).

[36] Na przykład FTC ogłosiła niedawno dochodzenie, które doprowadziło do złożenia pozwu przeciwko TikTokowi i jego spółce dominującej, Bytedance, w związku z domniemanym naruszeniem prawa o ochronie prywatności dzieci. Zarzuca się, że obie spółki nie spełniły wymogu powiadomienia i uzyskania zgody rodziców przed zebraniem i wykorzystaniem danych osobowych od dzieci poniżej 13. roku życia (https://www.ftc.gov/news-events/news/press-releases/2024/08/ftc-investigation-leads-lawsuit-against-tiktok-bytedance-flagrantly-violating-childrens-privacy-law).

[37] Zob. przegląd ostatnich czynności służących egzekwowaniu przepisów w publikacji FTC z 2023 r. „Privacy and Data Security Update". https://ec.europa.eu/commission/presscorner/detail/en/mex_24_1307.

[38] Zob. https://ec.europa.eu/commission/presscorner/detail/pl/mex_24_1307. Rezultatem spotkania w marcu 2024 r. była decyzja o zorganizowaniu serii sesji tematycznych. Pierwsza z nich odbyła się w lipcu 2024 r. i koncentrowała się na opracowaniu narzędzi, które mogą pomagać małym i średnim przedsiębiorstwom w przestrzeganiu przepisów dotyczących ochrony prywatności.

współpracę między organami ochrony prywatności po obu stronach Atlantyku, zwłaszcza w kwestiach istotnych dla funkcjonowania DPF.

2.2. Aspekty związane z dostępem do danych osobowych przekazywanych na podstawie ram ochrony danych UE-USA i ich wykorzystywaniem przez amerykańskie organy publiczne

Decyzja stwierdzająca odpowiedni stopień ochrony zawiera szczegółową ocenę przepisów regulujących gromadzenie i wykorzystywanie danych osobowych przekazywanych z UE do przedsiębiorstw posiadających certyfikację DPF przez amerykańskie organy publiczne, w szczególności do celów egzekwowania prawa karnego i bezpieczeństwa narodowego. Od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony, co potwierdziły władze USA podczas spotkania przeglądowego, w pierwszym roku obowiązywania DPF nie nastąpiły żadne istotne zmiany w zakresie ram prawnych mających zastosowanie do dostępu do danych do celów egzekwowania prawa lub do celów regulacyjnych. Z tego powodu poniższe ustalenia dotyczą jedynie zmian w dziedzinie bezpieczeństwa narodowego.

Wnioski wyciągnięte w decyzji stwierdzającej odpowiedni stopień ochrony w zakresie dostępu agencji wywiadowczych do danych opierają się na analizie warunków i ograniczeń mających zastosowanie do operacji rozpoznania radioelektronicznego prowadzonych przez kilka odpowiednich organów prawnych – w szczególności na podstawie sekcji 702 ustawy o kontroli wywiadu (FISA) i rozporządzenia wykonawczego 12333[39] – uzupełnionych i wzmocnionych rozporządzeniem wykonawczym 14086 w sprawie wzmocnienia zabezpieczeń w odniesieniu do działań Stanów Zjednoczonych w zakresie rozpoznania radioelektronicznego (rozporządzenie wykonawcze 14086) przyjętym przez prezydenta Stanów Zjednoczonych 7 października 2022 r. Zabezpieczenia określone w rozporządzeniu wykonawczym 14086 mają zastosowanie do wszystkich działań Stanów Zjednoczonych w zakresie rozpoznania radioelektronicznego, niezależnie od uprawnień, na podstawie których takich działania są prowadzone, i od miejsca ich prowadzenia, oraz chronią dane osób niebędących obywatelami ani rezydentami Stanów Zjednoczonych (w tym Europejczyków)[40]. W rozporządzeniu wykonawczym 14086 ustanowiono również nowy mechanizm dochodzenia roszczeń, za pomocą którego osoby fizyczne mogą powoływać się na te wiążące zabezpieczenia i je egzekwować w UE.

W kolejnych sekcjach opisano kroki podjęte przez organy Stanów Zjednoczonych od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony w celu zapewnienia zgodności z rozporządzeniem wykonawczym 14086, a także istotne zmiany w odniesieniu do wyżej wymienionych ram prawnych.

2.2.1. Istotne zmiany w amerykańskich ramach prawnych

[39] Inne środki, które można podjąć na mocy ustawy o kontroli wywiadu w odniesieniu do danych przekazywanych z UE, to zindywidualizowany nadzór elektroniczny (sekcja 105 ustawy o kontroli wywiadu), przeszukanie fizyczne (sekcja 302 ustawy o kontroli wywiadu), korzystanie z urządzeń rejestrujących wybierane numery oraz urządzeń śledzących (sekcja 402 ustawy o kontroli wywiadu) oraz gromadzenie dokumentacji dotyczącej prowadzonej działalności od niektórych przedsiębiorstw (przewoźników publicznych, publicznych obiektów noclegowych, wypożyczalni pojazdów lub obiektów magazynowych, sekcja 501 ustawy o kontroli wywiadu). Wspomniane różne podstawy prawne szczegółowo przeanalizowano w decyzji stwierdzającej odpowiedni stopień ochrony (motywy 142–152).

[40] Więcej informacji można znaleźć w sekcji 3.2.1.2 decyzji stwierdzającej odpowiedni stopień ochrony.

2.2.1.1. Wdrożenie rozporządzenia wykonawczego 14086 przez agencje wywiadowcze

Ograniczenia i zabezpieczenia wprowadzone rozporządzeniem wykonawczym 14086 uzupełniają ograniczenia i zabezpieczenia przewidziane w sekcji 702 ustawy o kontroli wywiadu i rozporządzeniu wykonawczym 12333. Są one wiążące dla wszystkich agencji wywiadowczych i dodatkowo wdrożono je za pomocą polityk i procedur przyjętych przez każdą agencję.

W ramach pierwszego przeglądu władze Stanów Zjednoczonych potwierdziły, że od czasu jego przyjęcia nie wprowadzono żadnych zmian w rozporządzeniu wykonawczym 14086. Ponadto wyjaśniono, że prezydent Stanów Zjednoczonych nie skorzystał z uprawnienia przewidzianego w sekcji 2 lit. b) pkt (i) ppkt B i sekcji 2 lit. b) pkt (ii) ppkt C rozporządzenia wykonawczego 14086 w celu aktualizacji wykazu uzasadnionych celów, w jakich można gromadzić dane w wyniku rozpoznania radioelektronicznego, lub wykazu celów, do których można wykorzystywać dane gromadzone hurtowo[41]. Aby określić bardziej szczegółowe priorytety wywiadowcze, w odniesieniu do których można faktycznie gromadzić dane z rozpoznania radioelektronicznego, w rozporządzeniu wykonawczym 14086 wprowadzono specjalną procedurę. W szczególności należy skonsultować się z urzędnikiem ds. ochrony wolności obywatelskich Urzędu Dyrektora Krajowych Służb Wywiadowczych (ODNI CLPO), aby ocenić każdy priorytet pod kątem tego, czy 1) przyczynia się on do realizacji co najmniej jednego uzasadnionego celu wymienionego w rozporządzeniu wykonawczym; 2) nie został on zaprojektowany z myślą o gromadzeniu danych w wyniku rozpoznania radioelektronicznego, ani nie przewiduje się, że spowoduje on gromadzenie danych w wyniku rozpoznania radioelektronicznego na potrzeby realizacji zakazanego celu wymienionego w rozporządzeniu wykonawczym oraz 3) został on określony po odpowiednim uwzględnieniu prywatności i wolności obywatelskich wszystkich osób[42]. Podczas spotkania przeglądowego ODNI CLPO potwierdził, że dokonał przeglądu priorytetów zaproponowanych przez Dyrektora Krajowych Służb Wywiadowczych w ramach krajowych priorytetów wywiadowczych z 2023 r., stwierdził, że spełniają one powyższe wymogi, i przekazał swoje wnioski Dyrektorowi Krajowych Służb Wywiadowczych (DNI), który z kolei przedłożył prezydentowi priorytety do zatwierdzenia. ODNI CLPO zorganizował również szkolenia na temat wymogów rozporządzenia wykonawczego 14086 dla części wspólnoty wywiadowczej zaangażowanej w opracowywanie priorytetów wywiadowczych.

Ponadto w ubiegłym roku organy Stanów Zjednoczone podjęły dalsze praktyczne kroki w celu wdrożenia rozporządzenia wykonawczego 14086 w swojej codziennej działalności. W szczególności agencje wywiadowcze wprowadziły dalsze wewnętrzne polityki i wytyczne dotyczące stosowania rozporządzenia wykonawczego, na przykład procesy wewnętrzne (poprzez wewnętrzne wymogi dotyczące zezwoleń, udokumentowane kontrole dostępu, tak aby dostęp do informacji miały wyłącznie osoby, które zostały odpowiednio przeszkolone i spełniają niezbędne wymogi dotyczące misji, itp.) w celu zapewnienia, aby wymogów dotyczących konieczności i proporcjonalności przestrzegano zarówno w kontekście

[41] Te uzasadnione cele obejmują na przykład ochronę przed szpiegostwem, sabotażem, zamachem lub innymi działaniami wywiadowczymi prowadzonymi przez rząd innego państwa, podmiot lub osobę z innego państwa bądź w ich imieniu lub z ich pomocą; ochronę przed terroryzmem, braniem zakładników i przetrzymywaniem w niewoli osób przez rząd innego państwa, podmiot lub osobę z innego państwa bądź w ich imieniu.

[42] Sekcja 2 lit. b) pkt (iii) rozporządzenia wykonawczego 14086.

ukierunkowanego, jak i hurtowego gromadzenia danych[43]. Ponadto przeprowadzono szkolenia na temat rozporządzenia wykonawczego 14086 dla pracowników różnych agencji wywiadowczych (np. NSA, CIA, FBI), w tym coroczne i doraźne sesje szkoleniowe organizowane przez ODNI CLPO oraz obowiązkowe szkolenia dla wszystkich nowych pracowników rozpoczynających pracę w Urzędzie Dyrektora Krajowych Służb Wywiadowczych.

Komisja z zadowoleniem przyjmuje różne środki wprowadzone w celu wdrożenia i zapewnienia zgodności z rozporządzeniem wykonawczym 14086. Jako że zdobyto więcej doświadczeń w zakresie praktycznego stosowania zabezpieczeń przewidzianych w rozporządzeniu wykonawczym, Komisja byłaby wdzięczna za możliwość omówienia w przyszłych przeglądach konkretnych przykładów stosowania rozporządzenia wykonawczego w praktyce (przy jednoczesnym poszanowaniu mających zastosowanie względów poufności).

2.2.1.2. Ponowne zatwierdzenie sekcji 702 ustawy o kontroli wywiadu

Zgodnie z przepisami sekcji 702 ustawy o kontroli wywiadu dopuszcza się możliwość namierzania osób niebędących obywatelami ani rezydentami Stanów Zjednoczonych, co do których istnieje uzasadnione podejrzenie, że przebywają poza terytorium Stanów Zjednoczonych w celu pozyskiwania zagranicznych danych wywiadowczych. Uzyskiwanie danych odbywa się na podstawie certyfikatów wydawanych corocznie i zatwierdzanych przez Sąd ds. Kontroli Wywiadu (FISC). W certyfikatach tych określono konkretne kategorie zagranicznych danych wywiadowczych, które mają być gromadzone. 21 lipca 2023 r. ODNI ogłosił, że wyróżnia się trzy zatwierdzone certyfikacje na podstawie sekcji 702 ustawy o kontroli wywiadu, obejmujące następujące kategorie danych wywiadowczych: 1) rządy obcych państw i podmioty powiązane, 2) zwalczanie terroryzmu oraz 3) zwalczanie proliferacji[44]. Certyfikacje muszą również zawierać procedury „namierzania” oraz „minimalizacji”, które zostały zatwierdzone przez Sąd ds. Kontroli Wywiadu[45]. W szczególności „namierzanie” odbywa się poprzez zwrócenie się do amerykańskich przedsiębiorstw, które spełniają definicję „dostawcy usług łączności elektronicznej” zawartą w ustawie o kontroli wywiadu, o ujawnianie danych pochodzących z łączności elektronicznej w odniesieniu do komunikatów wysyłanych do lub z „selektorów”, które identyfikują konkretne konto komunikacyjne, np. numer telefonu lub adres e-mail. Rząd Stanów Zjednoczonych opublikował szereg materiałów dotyczących sekcji 702 ustawy o kontroli wywiadu w celu poinformowania opinii publicznej o funkcjonowaniu programów nadzoru, mających zastosowanie wymogach i ochronie prywatności, a także o roli Sądu ds. Kontroli Wywiadu[46].

Ze względu na klauzulę wygaśnięcia sekcja 702 ustawy o kontroli wywiadu miała wygasnąć z końcem 2023 r., chyba że ponownie zatwierdzi ją Kongres. Po tymczasowym ponownym

[43]Zob. komunikat prasowy https://www.intel.gov/ic-on-the-record-database/results/oversight/1278-odni-releases-ic-procedures-implementing-new-safeguardsin-executive-order-14086, opublikowany 3 lipca 2023 r.
[44] https://www.intelligence.gov/ic-on-the-record-database/results/1307-release-of-documents-related-to-the-2023-fisa-section-702-certifications.
[45] Takie procedury ograniczają gromadzenie danych w odniesieniu do konkretnego celu wywiadu zagranicznego, ograniczają dostęp do baz danych, w których przechowywane są informacje uzyskane na podstawie sekcji 702 ustawy o kontroli wywiadu (w tym poprzez kontrole dostępu) oraz nakładają ograniczenia dotyczące wykorzystywania, zatrzymywania i rozpowszechniania takich informacji.
[46] https://www.intel.gov/foreign-intelligence-surveillance-act.

zatwierdzeniu bez żadnych zmian Kongres przyjął 19 kwietnia 2024 r. ustawę o reformie wywiadu i bezpieczeństwu Ameryki (RISAA), ponownie zatwierdzając sekcję 702 ustawy o kontroli wywiadu na okres 2 lat i wprowadzając kilka zmian. Zmiany te można zasadniczo podzielić na dwie kategorie: 1) zmiany zakresu działań w zakresie nadzoru dozwolonych na podstawie sekcji 702 ustawy o kontroli wywiadu oraz 2) zmiany instytucjonalne i proceduralne.

Zmiany zakresu działań w zakresie nadzoru dozwolonych na podstawie sekcji 702 ustawy o kontroli wywiadu

Ustawa o reformie wywiadu i bezpieczeństwu Ameryki wprowadziła trzy główne zmiany zakresu działań w zakresie nadzoru, które można przeprowadzić na podstawie sekcji 702 ustawy o kontroli wywiadu.

Po pierwsze, zbieranie danych na temat „miejsca pobytu" zostało ostatecznie zakazane[47]. Termin ten odnosi się do zbioru komunikatów, w których selektor sekcji 702 (taki jak adres e-mail) nie znajduje się w polu „do" lub „od" komunikatu, ale raczej zawiera odniesienie do takiego selektora w komunikacie (np. wiadomości e-mail, które nie są wysyłane na wybrany adres e-mail lub z wybranego adresu e-mail, ale zawierają wybrany adres e-mail w tekście lub treści wiadomości e-mail). Pomimo że takie gromadzenie danych zostało już wykluczone w następstwie zmiany ustawy o kontroli wywiadu w 2018 r., ustawa o kontroli wywiadu nadal przewidywała możliwość ponownego rozpoczęcia gromadzenia danych w przyszłości po przeprowadzeniu specjalnej procedury potwierdzenia z udziałem Sądu ds. Kontroli Wywiadu i Kongresu. Ostatnia zmiana wprowadzona przez ustawę o reformie wywiadu i bezpieczeństwu Ameryki zniosła tę możliwość.

Po drugie, rozszerzono definicję zagranicznych informacji wywiadowczych o informacje dotyczące zwalczania narkotyków[48]. Podczas spotkania przeglądowego władze USA wyjaśniły, że wprowadzono takie rozwiązanie w świetle obecnego kryzysu związanego z fentanylem i rosnącego zagrożenia dla bezpieczeństwa narodowego ze strony międzynarodowych handlarzy i producentów narkotyków. W tym kontekście potwierdzono, że pojęcie to wchodzi w zakres kilku uzasadnionych celów wymienionych w rozporządzeniu wykonawczym 14086, tj. zrozumienia lub oceny możliwości, zamiarów lub działań podmiotów zagranicznych, które stwarzają faktyczne lub potencjalne zagrożenie dla bezpieczeństwa narodowego USA lub ich sojuszników; zrozumienia lub oceny transgranicznych zagrożeń, które wpływają na bezpieczeństwo globalne, w tym zagrożeń dla zdrowia publicznego oraz ochrony przed transgranicznymi zagrożeniami przestępstwami[49].

Po trzecie, ustawa o reformie wywiadu i bezpieczeństwu Ameryki poszerzyła definicję „dostawcy usług łączności elektronicznej", rozszerzając tym samym zakres przedsiębiorstw, które mogą być zobowiązane do dostarczania informacji zgodnie z sekcją 702 ustawy o kontroli wywiadu[50]. Definicja obejmuje obecnie „innych usługodawców mających dostęp do urządzeń, które są lub mogą być wykorzystywane do transmisji lub przechowywania komunikatów przekazywanych za pomocą łączności kablowej lub elektronicznej", z wyraźnym wyłączeniem publicznych obiektów noclegowych, lokali mieszkalnych, obiektów użyteczności publicznej i obiektów gastronomicznych. W piśmie skierowanym do Kongresu

[47] Sekcja 22 ustawy o reformie wywiadu i bezpieczeństwu Ameryki.
[48] Sekcja 23 ustawy o reformie wywiadu i bezpieczeństwu Ameryki.
[49] Sekcja 2 lit. b) pkt (ii) lit. (A) ppkt 2, ppkt 3 i ppkt 10 rozporządzenia wykonawczego 14086.
[50] Sekcja 25 ustawy o reformie wywiadu i bezpieczeństwu Ameryki.

DoJ odniósł się do tej poprawki jako do zmiany technicznej mającej na celu objęcie „bardzo małej" liczby przedsiębiorstw technologicznych, które zgodnie z niedawnymi decyzjami Sądu ds. Kontroli Wywiadu i Sądu Apelacyjnego ds. Kontroli Wywiadu (FISCR) nie zostały uwzględnione w poprzedniej definicji „dostawcy usług łączności elektronicznej"[51]. W tym samym piśmie DoJ zobowiązał się do zawężenia zakresu poprzez zastosowanie tej definicji wyłącznie do usługodawców będących przedmiotem sporu sądowego, w wyniku którego Sąd ds. Kontroli Wywiadu wydał decyzję. W związku z tym przedsiębiorstwa, których to dotyczy, zostały wymienione w niejawnym załączniku dla Kongresu. Kilka organizacji pozarządowych, w tym organizacje, które przekazały informacje zwrotne w ramach przeglądu, wyraziło obawy dotyczące tego rozszerzenia definicji, argumentując, że może ono potencjalnie objąć wiele amerykańskich przedsiębiorstw (ponieważ wiele z nich świadczy pewien rodzaj usług i ma dostęp do sprzętu komunikacyjnego). W świetle tych obaw w projekcie ustawy o autoryzacji wywiadu na rok budżetowy 2025, który jest obecnie rozpatrywany przez Kongres, zaproponowano kolejną poprawkę przy poparciu wspólnoty wywiadowczej. Zmiana ta, jeśli przyjmie ją Kongres, zapewni, by dodatkowe przedsiębiorstwa objęte definicją „dostawcy usług łączności elektronicznej" były ograniczone jedynie do tych, o których mowa w wyżej wymienionych orzeczeniach Sądu ds. Kontroli Wywiadu. Projekt przewiduje również, że każda dyrektywa skierowana do takiego przedsiębiorstwa musiałaby zostać zgłoszona do Sądu ds. Kontroli Wywiadu, aby ten mógł sprawdzić, czy przedsiębiorstwo rzeczywiście mieści się w jej zakresie. W piśmie skierowanym do Kongresu DoJ zobowiązał się do składania Kongresowi co sześć miesięcy sprawozdań dotyczących stosowania zaktualizowanej definicji, aby umożliwić Kongresowi sprawowanie odpowiedniego nadzoru w odniesieniu do wąskiego stosowania definicji.

Co ważne, podczas spotkania przeglądowego władze Stanów Zjednoczonych i Rada Nadzoru nad Prywatnością i Wolnościami Obywatelskimi potwierdziły, że wszystkie zabezpieczenia przewidziane w rozporządzeniu wykonawczym 14086 nadal mają pełne zastosowanie do gromadzenia i wykorzystywania danych zgodnie z sekcją 702 ustawy o kontroli wywiadu, w tym po wprowadzeniu tych zmian. W związku z tym, chociaż ustawa o reformie wywiadu i bezpieczeństwu Ameryki w pewnym stopniu rozszerza zakres przedsiębiorstw, które mogą otrzymać zarządzenie, nie ogranicza korzystania z praw. Niemniej jednak ważne będzie monitorowanie dalszych zmian (legislacyjnych i sprawozdawczych) oraz otrzymywanie informacji na temat stosowania tych nowych przepisów w praktyce. Mowa tu na przykład o wpływie rozszerzenia definicji „wywiadu zagranicznego" i „dostawcy usług łączności elektronicznej" na liczbę osób namierzanych zgodnie z sekcją 702 ustawy o kontroli wywiadu (podawaną corocznie przez Urząd Dyrektora Krajowych Służb Wywiadowczych, zob. poniższe informacje na temat przejrzystości). Wiele informacji na ten temat będzie można znaleźć w przyszłym sprawozdaniu z działań następczych uzupełniającym niedawne sprawozdanie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące sekcji 702 ustawy o kontroli wywiadu (zob. poniżej).

Zmiany instytucjonalne i proceduralne

[51] https://www.justice.gov/opa/media/1348621/dl?inline. Zob. decyzja Sądu ds. Kontroli Wywiadu z 2022 r. (https://www.intel.gov/assets/documents/702%20Documents/declassified/2022-FISC-ECSP-OPINION.pdf) oraz orzeczenie Sądu ds. Kontroli Wywiadu podtrzymujące tę decyzję (https://www.intel.gov/assets/documents/702%20Documents/declassified/2023_FISC-R_ECSP_Opinion.pdf).

Jeżeli chodzi o zmiany instytucjonalne i proceduralne, ustawa o reformie wywiadu i bezpieczeństwu Ameryki skodyfikowała kilka procedur, które były już stosowane w praktyce, i wprowadziła nowe zabezpieczenia. Chociaż niektóre z nich dotyczą wyłącznie osób będących obywatelami lub rezydentami Stanów Zjednoczonych, kilka zmian zwiększa ochronę zarówno osób będących obywatelami lub rezydentami Stanów Zjednoczonych, jak i osób niebędących obywatelami ani rezydentami Stanów Zjednoczonych, których dane mogą być gromadzone na podstawie sekcji 702 ustawy o kontroli wywiadu[52], a zatem mają znaczenie dla funkcjonowania DPF.

Po pierwsze, wprowadzono szereg dodatkowych wymogów w zakresie odpowiedzialności, nadzoru i sprawozdawczości. W szczególności personel FBI musi obecnie przechodzić coroczne szkolenie w zakresie przepisów stosowanych przy wyszukiwaniu informacji uzyskanych na podstawie sekcji 702 ustawy o kontroli wywiadu[53]. FBI jest również zobowiązane do składania Kongresowi sprawozdań na temat swoich działań w zakresie zapytań (np. liczby zapytań wykorzystujących „technologie zadań partii", tj. uruchamianie wielu zapytań w ramach jednego zapytania) oraz na temat środków odpowiedzialności wprowadzonych w celu zapewnienia zgodności z wymogami prawnymi dotyczącymi zapytań (sekcje 11-12 ustawy o reformie wywiadu i bezpieczeństwu Ameryki). Ponadto Inspektora Generalnego DoJ poinstruowano, aby sporządził sprawozdanie na temat przestrzegania przez FBI wymogów dotyczących zapytań (sekcja 9 ustawy o reformie wywiadu i bezpieczeństwu Ameryki). Jeżeli chodzi o kwestie ogólne, aby zwiększyć przejrzystość procedur przed Sądem ds. Kontroli Wywiadu, ODNI i Prokurator Generalny są obecnie zobowiązani do zakończenia przeglądu odtajnienia decyzji Sądu ds. Kontroli Wywiadu w terminie 180 dni (sekcja 7 ustawy o reformie wywiadu i bezpieczeństwu Ameryki). Ponadto stenogramy wszystkich przesłuchań przed Sądem ds. Kontroli Wywiadu i Sądem Apelacyjnym ds. Kontroli Wywiadu (gdzie można odwoływać się od decyzji tego pierwszego sądu) należy przechowywać i przekazywać Kongresowi (sekcja 8 ustawy o reformie wywiadu i bezpieczeństwu Ameryki).

Po drugie, ustawa o reformie wywiadu i bezpieczeństwu Ameryki wprowadziła dalsze ograniczenia dotyczące wykorzystywania przez FBI danych zgromadzonych na podstawie sekcji 702 ustawy o kontroli wywiadu. Sekcja 2 lit. d) ustawy o reformie wywiadu i bezpieczeństwu Ameryki stanowi, że zapytania z wykorzystaniem „technologii partii" można dokonać wyłącznie po uzyskaniu zgody pełnomocnika FBI, chyba że zachodzą wyjątkowe okoliczności. Ponadto FBI nie może teraz automatycznie sprawdzać niezminimalizowanych informacji uzyskanych na podstawie sekcji 702 ustawy o kontroli wywiadu, a zamiast tego musi dopilnować, aby analitycy potwierdzili wybór wyszukiwania takich informacji. Ustawa o reformie wywiadu i bezpieczeństwu Ameryki zakazała również FBI przeprowadzania zapytań, które mają na celu wyłącznie znalezienie i wydobycie dowodów działalności przestępczej (chyba że istnieje uzasadnione przekonanie, że mogą one pomóc w złagodzeniu

[52] Ponadto ustawa o reformie wywiadu i bezpieczeństwu Ameryki wprowadziła pewne zmiany w odniesieniu do tradycyjnego zindywidualizowanego nadzoru elektronicznego zgodnie z sekcją 105 ustawy o kontroli wywiadu (na podstawie nakazu wydanego przez Sąd ds. Kontroli Wywiadu, jeżeli występuje uzasadnione podejrzenie). Złożenie przez agencję wywiadowczą do prokuratora generalnego wniosku o wydanie nakazu przeprowadzenia zindywidualizowanego nadzoru elektronicznego wymaga obecnie złożenia pod przysięgą oświadczenia uzasadniającego przekonanie, że spełnione są warunki określone w sekcji 105 ustawy o kontroli wywiadu (sekcja 6 lit. a) ustawy o reformie wywiadu i bezpieczeństwu Ameryki). Dopuszczalny czas trwania nadzoru elektronicznego w odniesieniu do obcego państwa lub agentów obcych państw przedłużono z 120 dni do 1 roku (sekcja 6 lit. g) ustawy o reformie wywiadu i bezpieczeństwu Ameryki).

[53] Sekcja 2 lit. d) ustawy o reformie wywiadu i bezpieczeństwu Ameryki.

lub wyeliminowaniu zagrożenia życia lub poważnego uszkodzenia ciała, lub gdy jest to konieczne do wypełnienia obowiązków związanych z ujawnieniem informacji w postępowaniu sądowym)[54]. Ponadto FBI nie może wprowadzać niezminimalizowanych danych do repozytoriów analitycznych, chyba że osoba namierzana jest związana z prowadzonym dochodzeniem w sprawie bezpieczeństwa narodowego[55].

Po trzecie, niektóre przepisy dotyczące statusu i roli stron niebędących stroną sporu przed Sądem ds. Kontroli Wywiadu zostały zmienione[56]. Strony takie wyznacza się jako ekspertów w celu wspierania Sądu (i Sądu Apelacyjnego ds. Kontroli Wywiadu) w sprawach związanych z prywatnością i wolnościami obywatelskimi lub w celu wyjaśnienia kwestii technologicznych przy rozpatrywaniu konkretnego wniosku rządu. Chociaż wcześniej ustawa o kontroli wywiadu wymagała, aby strony niebędące stroną sporu posiadały wiedzę fachową w zakresie prywatności i wolności obywatelskich, gromadzenia danych wywiadowczych, technologii komunikacyjnych lub innych istotnych dziedzin, obecnie wymaga ona, co do zasady, wiedzy fachowej w zakresie prywatności i wolności obywatelskich oraz gromadzenia danych wywiadowczych. Sąd miał bowiem już wcześniej możliwość wyznaczania takiej strony w każdym przypadku, który uznał za stosowny, i był do tego zobowiązany, gdy miał do czynienia z nową lub istotną interpretacją prawa. Po ponownym zatwierdzeniu Sąd ds. Kontroli Wywiadu jest obecnie również zobowiązany do wyznaczenia strony niebędącej stroną sporu za każdym razem, gdy otrzyma wniosek o zatwierdzenie określonych w sekcji 702 ustawy o kontroli wywiadu certyfikacji i procedur towarzyszących (np. procedur w zakresie namierzania), chyba że stwierdzi, że nie byłoby to właściwe lub prawdopodobnie spowodowałoby nadmierne opóźnienie[57]. Ponadto zamiast wyznaczyć tylko jedną osobę, Sąd może teraz zdecydować o wyznaczeniu jednej lub kilku stron niebędących stroną sporu. Wyjaśniono również, że informacje, które mają przekazywać strony niebędące stroną sporu, muszą być „ograniczone do konkretnych kwestii wskazanych przez sąd", chociaż obszary, w których strony te mogą się wypowiadać, pozostały szerokie (tj. argumenty prawne i informacje związane z ochroną prywatności i wolności obywatelskich osób będących obywatelami lub rezydentami Stanów Zjednoczonych, gromadzeniem danych wywiadowczych i technologiami komunikacyjnymi lub wszelkimi innymi istotnymi obszarami).

Ponadto w sekcji 18 ustawy o reformie wywiadu i bezpieczeństwu Ameryki ustanowiono „Komisję ds. reform FISA" – składającą się m.in. z członków Kongresu, przewodniczącego Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi, głównego zastępcy dyrektora wywiadu narodowego i zastępcy prokuratora generalnego oraz dodatkowych członków mianowanych przez Kongres[58] – w celu zalecenia dodatkowych reform ustawy o kontroli wywiadu.

Komisja będzie ściśle monitorować dalsze zmiany w odniesieniu do sekcji 702 ustawy o kontroli wywiadu, w tym w kontekście działań nadzorczych Rady Nadzoru nad

[54] Sekcja 3 lit. a) ustawy o reformie wywiadu i bezpieczeństwu Ameryki.

[55] Sekcja 3 lit. b) ustawy o reformie wywiadu i bezpieczeństwu Ameryki. W razie konieczności wynikającej z wyjątkowych okoliczności, dyrektor FBI może podjąć decyzję o odstąpieniu od tego przepisu, o czym należy poinformować Kongres.

[56] Dla jasności, zmiany te nie mają wpływu na status i rolę rzeczników specjalnych przed Sądem ds. Kontroli Ochrony Danych (DPRC), co potwierdziły Stany Zjednoczone na spotkaniu przeglądowym.

[57] Sekcja 5 lit. b) ustawy o reformie wywiadu i bezpieczeństwu Ameryki.

[58] Sekcja 18 wyraźnie wymaga reprezentacji spoza Kongresu.

Prywatnością i Wolnościami Obywatelskimi (zob. poniżej), prac komisji ds. reform oraz zbliżającego się przeglądu ustawy o kontroli wywiadu po dwóch latach.

2.2.1.3. Działania nadzorcze w praktyce: dane liczbowe i tendencje

W rocznym sprawozdaniu ODNI na temat przejrzystości statystycznej dotyczącym wykorzystania przez wspólnotę wywiadowczą krajowych organów nadzoru bezpieczeństwa w roku kalendarzowym 2023 (opublikowanym w kwietniu 2024 r.)[59] wykazano, że liczba osób namierzanych zgodnie z sekcją 702 ustawy o kontroli wywiadu, wzrosła z 245 073 w roku kalendarzowym 2022 do 268 590 w roku kalendarzowym 2023. W sprawozdaniu wyjaśniono, że wahania liczba osób namierzanych mogą być związane z różnymi przyczynami, w tym ze zmianami w priorytetach operacyjnych, wydarzeniami światowymi, możliwościami technicznymi, zachowaniami namierzanych osób i zmianami w sektorze telekomunikacyjnym. W sprawozdaniu wskazano, że żadna osoba niebędąca obywatelem ani rezydentem Stanów Zjednoczonych (w porównaniu z jedną osobą w 2021 r. i żadną w 2022 r.) nie była namierzana zgodnie z sekcją 402 ustawy o kontroli wywiadu (urządzenia rejestrujące wybierane numery oraz urządzenia śledzące); z kolei sześć nakazów (w porównaniu z 13 w 2021 r. i 11 w 2022 r.) dotyczących sześciu osób namierzanych wydano na podstawie sekcji 501 ustawy o kontroli wywiadu (dostęp do dokumentacji dotyczącej działalności prowadzonej przez przewoźników publicznych, wypożyczalnie pojazdów lub fizyczne obiekty magazynowe) i obejmowały one 5 412 unikalnych identyfikatorów (w porównaniu z 23 157 w 2021 r. i 55 431 w 2022 r.), które wykorzystano do przekazywania informacji zgromadzonych na podstawie tych nakazów.

W rocznym sprawozdaniu Departamentu Sprawiedliwości dla Kongresu dotyczącym ustawy o kontroli wywiadu wskazano, że w roku kalendarzowym 2023 złożono do Sądu ds. Kontroli Wywiadu 327 wniosków o przeprowadzenie nadzoru elektronicznego lub przeszukań fizycznych do celów wywiadu zagranicznego na podstawie, odpowiednio, sekcji 105 i 302 ustawy o kontroli wywiadu[60]. Łączna liczba osób namierzanych wynosiła od 500 do 999. Jeżeli chodzi o wezwania do przedstawienia informacji do celów bezpieczeństwa narodowego (NSL), według sprawozdania wydano 10 115 wniosków (z wyłączeniem wyłącznie wezwań do przedstawienia informacji jedynie o abonentach) w celu uzyskania informacji na temat osób niebędących obywatelami ani rezydentami Stanów Zjednoczonych, w których zwrócono się o informacje dotyczące 3 033 różnych osób niebędących obywatelami ani rezydentami Stanów Zjednoczonych[61].

Kilka przedsiębiorstw posiadających certyfikację DPF (np. Google, Meta) korzysta z przewidzianej w prawie Stanów Zjednoczonych możliwości publikowania sprawozdań z przejrzystości, w których ogłaszana jest liczba wniosków o udzielenie informacji na podstawie ustawy o kontroli wywiadu i liczba wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego, które otrzymały w danym okresie sprawozdawczym.

[59] https://www.dni.gov/files/CLPT/documents/2024_ASTR_for_CY2023.pdf.
[60] https://www.justice.gov/nsd/media/1350236/dl?inline.
[61] Liczby te utrzymywały się na zasadniczo stabilnym poziomie w porównaniu z poprzednim rokiem sprawozdawczym (2022 r.). Dla porównania w 2022 r. w Sądzie ds. Kontroli Wywiadu złożono 317 wniosków końcowych dotyczących prowadzenia nadzoru elektronicznego lub przeszukania fizycznego do celów wywiadu zagranicznego. Łączna liczba osób namierzanych, objętych nakazami nadzoru elektronicznego wynosiła od 0 do 499. W 2022 r. FBI złożyło 9103 wezwania do przedstawienia informacji do celów bezpieczeństwa narodowego w odniesieniu do osób niebędących obywatelami ani rezydentami Stanów Zjednoczonych (z wyłączeniem wezwań do przedstawienia informacji jedynie o abonentach). Źródło: https://irp.fas.org/agency/doj/fisa/2022rept.pdf.

W momencie sporządzania niniejszego sprawozdania statystyki dotyczące wniosków o udzielenie informacji na podstawie ustawy o kontroli wywiadu po lipcu 2023 r. nie były jeszcze dostępne. Google zgłosił na przykład, że w okresie od lipca do grudnia 2023 r. otrzymało od 500 do 999 wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego, które dotyczyły od 2000 do 2499 kont[62]. Meta zgłosiła, że w tym samym okresie sprawozdawczym otrzymała od 0 do 499 wezwań do przedstawienia informacji do celów bezpieczeństwa narodowego, które dotyczyły od 500 do 999 kont[63]. W ostatnich latach liczby wniosków i wezwań utrzymywały się na dość stabilnym poziomie. Aby jeszcze bardziej zwiększyć przejrzystość, niektóre przedsiębiorstwa (np. Google) aktywnie publikują informacje o otrzymanych wezwaniach do przedstawienia informacji do celów bezpieczeństwa narodowego, po zniesieniu ograniczeń dotyczących nieujawniania informacji[64].

2.2.1.4. Inne zmiany

W kontekście przygotowań do przeglądu kilka organizacji pozarządowych zgłosiło zastrzeżenia dotyczące nowych form pozyskiwania danych przez amerykańskie agencje wywiadowcze, tzn. poprzez zakup danych od podmiotów komercyjnych, w szczególności brokerów danych. Wyjaśniły one, że chociaż dane zgromadzone na tej podstawie nadal należy przetwarzać zgodnie z innymi wymogami, w tym na przykład zgodnie z przepisami rozporządzenia wykonawczego 12333[65], takie nabycie danych odbywa się poza ramami ustawy o kontroli wywiadu i rozporządzenia wykonawczego 14086.

W tym względzie należy przypomnieć, że każdy rodzaj dobrowolnego udostępniania danych stronom trzecim podlega szeregowi szczegółowych warunków w ramach DPF. Po pierwsze, certyfikowany podmiot nie może udostępniać danych stronie trzeciej (niedziałającej w charakterze przedstawiciela/podmiotu przetwarzającego), nie stosując zasad powiadomienia i wyboru wobec zainteresowanych osób[66]. Po drugie, zgodnie z zasadą odpowiedzialności za dalsze przekazywanie może ono mieć miejsce 1) wyłącznie w ograniczonym i określonym celu, 2) na podstawie umowy między podmiotem objętym DPF UE-USA a stroną trzecią i 3) tylko wtedy, gdy umowa ta zobowiązuje stronę trzecią do zapewnienia takiego samego stopnia ochrony jak ten gwarantowany przez zasady[67].

Ponadto, jak omówiono również podczas spotkania przeglądowego, FTC podjęła czynności służące egzekwowaniu przepisów wobec brokerów danych sprzedających wrażliwe dane konsumentów. Na przykład w sprawie przeciwko *X-Mode* i jego następcy *Outlogic* FTC wydała 9 stycznia 2024 r. postanowienie zakazujące przedsiębiorstwu sprzedaży danych geolokalizacyjnych stronom trzecim oraz usuwania danych, które wykorzystało i udostępniło niezgodnie z prawem. Badanie przeprowadzone przez FTC wykazało między innymi, że przedsiębiorstwo nie poinformowało w pełni osób fizycznych o wykorzystaniu i sprzedaży ich danych geolokalizacyjnych, nie wprowadziło środków umożliwiających osobom fizycznym rezygnację ze śledzenia, zezwoliło na wykorzystanie danych do celów potencjalnie dyskryminujących i nie wprowadziło ograniczeń w wykorzystywaniu takich informacji przez

[62] https://transparencyreport.google.com/user-data/us-national-security.
[63] https://transparency.meta.com/reports/government-data-requests/country/US/.
[64] https://transparencyreport.google.com/user-data/us-national-security.
[65] Zob. np. sekcja 2.4 rozporządzenia wykonawczego 12333 dotycząca technik zbierania danych.
[66] Zob. motyw 40 decyzji stwierdzającej odpowiedni stopień ochrony.
[67] Zob. motyw 38 decyzji stwierdzającej odpowiedni stopień ochrony.

strony trzecie[68]. Komisja oczekuje, że FTC przyjmie takie samo podejście, jeżeli przedsiębiorstwa posiadające certyfikację DPF będą udostępniać dane z naruszeniem wyżej wymienionych przepisów.

Ponadto warto wspomnieć, że w maju 2024 r. ODNI wydał ramy polityki wspólnoty wywiadowczej w zakresie informacji dostępnych w handlu[69]. Ramy te określają szereg zasad i wymogów, których agencje wywiadowcze powinny przestrzegać – m.in. w celu zminimalizowania zagrożeń dla prywatności i swobód obywatelskich – przy pozyskiwaniu i wykorzystywaniu informacji w kontekście transakcji handlowej.

2.2.2. Niezależny nadzór

Działalność amerykańskich agencji wywiadowczych podlega nadzorowi różnych organów, w tym urzędników ds. prywatności i wolności obywatelskich, inspektorów generalnych, Kongresu i Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi. W szczególności, zgodnie z rozporządzeniem wykonawczym 14086 każda agencja wywiadowcza musi posiadać urzędników wysokiego szczebla ds. prawnych, nadzoru i zgodności, by zapewnić zgodność z mającym zastosowanie prawem amerykańskim. Tę funkcję nadzorczą pełnią urzędnicy, którym wyznaczono określone role w zakresie zgodności, jak również urzędnicy ds. prywatności i wolności obywatelskich oraz Inspektorzy Generalni[70]. Muszą oni prowadzić okresowy nadzór nad działaniami w zakresie rozpoznania radioelektronicznego i zapewniać usuwanie wszelkich niezgodności. Agencje wywiadowcze muszą zapewnić takim urzędnikom dostęp do wszystkich istotnych informacji, by umożliwić im wykonywanie funkcji nadzorczych, i nie mogą podejmować żadnych działań utrudniających działania nadzorcze lub w sposób niewłaściwy wpływających na takie działania.

W spotkaniu przeglądowym uczestniczył główny doradca Biura Generalnego Inspektora Wspólnoty Wywiadowczej (ICIG) w ODNI, który ma pełną jurysdykcję nad całą wspólnotą wywiadowczą i jest uprawniony do badania skarg lub informacji dotyczących zarzutów bezprawnego zachowania lub nadużycia władzy. Potwierdził on, że Generalny Inspektor Wspólnoty Wywiadowczej systematycznie sprawdza zgodność z rozporządzeniem wykonawczym 14086 w ramach swoich działań nadzorczych. Odniósł się również do niedawnych działań nadzorczych innych inspektorów generalnych wspólnoty wywiadowczej, szczegółowo opisanych w regularnych sprawozdaniach. Na przykład w półrocznym

[68] https://www.ftc.gov/news-events/news/press-releases/2024/01/ftc-order-prohibits-data-broker-x-mode-social-outlogic-selling-sensitive-location-data.

[69] https://www.dni.gov/files/ODNI/documents/CAI/Commercially-Available-Information-Framework-May2024.pdf. Agencje wywiadowcze są zobowiązane do przestrzegania ram od sierpnia 2024 r.

[70] Każda agencja wywiadowcza posiada inspektora generalnego, który jest ustawowo niezależny i odpowiedzialny za przeprowadzanie audytów i dochodzeń dotyczących działań prowadzonych przez odpowiednią agencję do celów bezpieczeństwa narodowego. Mają wgląd we wszystkie inne istotne materiały (w tym materiały niejawne), w razie potrzeby na mocy wezwania, oraz mogą odbierać zeznania. Inspektorzy generalni kierują sprawy o podejrzenie popełnienia przestępstwa do organów ścigania i formułują zalecenia dotyczące działań naprawczych skierowane do szefów agencji. Chociaż ich zalecenia nie są wiążące, ich sprawozdania, m.in. na temat działań następczych (lub braku takich działań), co do zasady są podawane do publicznej wiadomości i wysyłane do Kongresu. Zob. w tym względzie przypis 136 decyzji stwierdzającej odpowiedni stopień ochrony dotyczący roli inspektora generalnego.

sprawozdaniu dla Kongresu za okres od kwietnia do września 2023 r.[71] Inspektor Generalny Agencji Bezpieczeństwa Narodowego (NSA) poinformował o ocenie wewnętrznych ram kontroli NSA w odniesieniu do decyzji i wniosków w sprawie namierzania. Stwierdzono w nim, że ramy te funkcjonują prawidłowo, aby zapewnić zgodność z przepisami, dyrektywami i politykami, które chronią wolności obywatelskie i prywatność. W tym samym sprawozdaniu wspomniano również o dochodzeniu, które ujawniło niewłaściwe wykorzystanie narzędzia rozpoznania radioelektronicznego przez pracownika NSA do nieuprawnionych celów.

Zgodnie z rozporządzeniem wykonawczym 14086 Radzie Nadzoru nad Prywatnością i Wolnościami Obywatelskimi[72] powierzono szczególne funkcje nadzorcze[73]. Przewodnicząca i trzej członkowie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi wzięli udział w posiedzeniu przeglądowym i poinformowali, że w kwietniu 2023 r. Rada ta doradzała agencjom wywiadowczym na temat ich projektów polityk i procedur wdrażających rozporządzenie wykonawcze 14086 oraz konsultowano się z nią w sprawie mianowania sędziów i rzeczników specjalnych Sądu ds. Kontroli Ochrony Danych. Rada rozpoczęła również projekt nadzoru mający na celu (1) przegląd wdrożenia zaktualizowanych polityk i procedur przyjętych przez agencje wywiadowcze w celu zapewnienia ich zgodności z rozporządzeniem wykonawczym oraz (2) przeprowadzenie corocznego przeglądu funkcjonowania nowego mechanizmu dochodzenia roszczeń (zob. poniżej)[74]. Członkowie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi potwierdzili, że Rada planuje przeprowadzić oba przeglądy w najbliższej przyszłości. W odniesieniu do dochodzenia roszczeń wyjaśnili, że w związku z brakiem skarg przegląd Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi skupi się na polityce i procedurach wprowadzonych w celu ustanowienia mechanizmu.

Jeżeli chodzi o inne działania nadzorcze, 28 września 2023 r. Rada Nadzoru nad Prywatnością i Wolnościami Obywatelskimi opublikowała sprawozdanie dotyczące sekcji 702 ustawy o kontroli wywiadu[75]. Sprawozdanie to stanowi kontynuację wcześniejszego sprawozdania z 2014 r. i zawiera zaktualizowane informacje dotyczące okoliczności faktycznych i prawnych związanych z funkcjonowaniem programów nadzoru na mocy sekcji 702 ustawy o kontroli wywiadu. Sprawozdanie zawiera również zalecenia dotyczące przestrzegania przez agencje wywiadowcze obowiązujących wymogów oraz sugestie dla Kongresu dotyczące dalszego wzmocnienia kilku aspektów sekcji 702 ustawy o kontroli wywiadu w kontekście jej

[71] https://oig.nsa.gov/reports/Article/3609957/semiannual-report-to-congress-1-april-2023-to-30-september-2023/.

[72] Rada Nadzoru nad Prywatnością i Wolnościami Obywatelskimi jest niezależną agencją, której powierzono obowiązki w obszarze kształtowania i wdrażania polityki walki z terroryzmem, aby zapewnić ochronę prywatności i wolności obywatelskich. Ma ona dostęp do wszystkich stosownych informacji (z uwzględnieniem informacji niejawnych), może przeprowadzać przesłuchania i odbierać zeznania. Może wydawać zalecenia skierowane do organów ścigania i organów wywiadowczych oraz regularnie sporządza sprawozdania dla Kongresu i Prezydenta. Jej sprawozdania są udostępniane publicznie w możliwie największym stopniu.

[73] https://documents.pclob.gov/prod/Documents/EventsAndPress/834a1977-f420-4b2a-ae93-8a522b2c7c74/Trans-Atlantic%20Data%20Privacy%20Framework%20EO%20press%20release%20(FINAL)%20-%20Completed%20508%20-%2010202022.pdf.

[74] https://www.pclob.gov/OversightProjects/Details/1115.

[75] https://documents.pclob.gov/prod/Documents/OversightReport/8ca320e5-01d3-4d6a-8106-3384aad6ff31/2023%20PCLOB%20702%20Report%20-%20Nov%2017%202023%20-%201446.pdf.

ponownego zatwierdzenia (w tym poprzez kodyfikację uzasadnionych celów działań w zakresie nadzoru wymienionych w rozporządzeniu wykonawczym 14086)[76]. Podczas spotkania przeglądowego Rada Nadzoru nad Prywatnością i Wolnościami Obywatelskimi poinformowała, że spodziewa się otrzymać wkrótce od agencji wywiadowczych odpowiedzi na temat realizacji jej zaleceń, które zostaną uwzględnione w przyszłym sprawozdaniu z działań następczych. Inne bieżące projekty w zakresie nadzoru to m.in. projekt dotyczący zwalczania terroryzmu krajowego i jego wpływu na prywatność i wolności obywatelskie, a także gromadzenie przez FBI danych ze źródeł otwartych lub dostępnych na rynku[77].

Ponadto organizacje pozarządowe, z którymi przeprowadzono konsultacje w kontekście przeglądu, wyraziły obawę, że kadencja kilku członków Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi ma wygasnąć w niedalekiej przyszłości, co może potencjalnie pozostawić tę Radę bez kworum. Chodzi tu w szczególności o kadencję przewodniczącej, która wygasła, a okres, w którym możliwe jest pełnienie funkcji tymczasowej, kończy się w styczniu 2025 r. Jednocześnie jedno inne stanowisko jest nieobsadzone, a trzecie stanowisko zwolni się w styczniu przyszłego roku. Podczas spotkania przeglądowego członkowie wyjaśnili, że nie spodziewają się, aby Rada Nadzoru nad Prywatnością i Wolnościami Obywatelskimi straciła kworum, ponieważ przedstawiono już nominację na obecnie wolne stanowisko (która czeka na zatwierdzenie przez Senat)[78]. Podkreślili również, że nawet jeśli Rada utraci kworum, nie wpłynie to na jej zdolność do dalszego prowadzenia projektów w zakresie nadzoru. Biorąc jednak pod uwagę ważną rolę Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi w przeglądzie wdrażania rozporządzenia wykonawczego 14086, Komisja będzie ściśle monitorować status przyszłych wakatów i nominacji/powołań.

2.2.3. Dochodzenie roszczeń

Rozporządzeniem wykonawczym 14086, uzupełnionym rozporządzeniem prokuratora generalnego, ustanowiono nowy mechanizm dochodzenia roszczeń w celu rozpatrywania i rozstrzygania kwalifikujących się skarg osób fizycznych dotyczących działań Stanów Zjednoczonych w obszarze rozpoznania radioelektronicznego[79]. Każda fizyczna osoba w UE jest uprawniona do złożenia skargi w ramach mechanizmu dochodzenia roszczeń dotyczącej domniemanego naruszenia amerykańskiego prawa regulującego działania w zakresie rozpoznania radioelektronicznego (np. rozporządzenia wykonawczego 14086, sekcji 702 ustawy o kontroli wywiadu, rozporządzenia wykonawczego 12333) w odniesieniu do danych osobowych przekazywanych do USA, które negatywnie wpływa na jego interesy w zakresie ochrony prywatności i wolności obywatelskich. Osoby fizyczne mogą złożyć skargę do organu ochrony danych w państwie członkowskim UE, które – za pośrednictwem sekretariatu EROD – przekazuje skargę do mechanizmu dochodzenia roszczeń. Mechanizm ten składa się z dwóch warstw: wstępnego badania skarg prowadzonego przez ODNI CLPO oraz możliwości odwołania się od decyzji tego urzędu przed niezależnym Sądem ds. Kontroli Ochrony Danych. Po zakończeniu przeglądu przez ODNI CLPO lub Sąd ds. Kontroli Ochrony Danych osoby

[76] Komisja zauważa, że niektóre z tych zaleceń zostały włączone do ustawy o reformie wywiadu i bezpieczeństwu Ameryki, w tym zalecenie dotyczące gromadzenia danych i zalecenie w sprawie wzmocnienia roli ekspertów Sądu ds. Kontroli Wywiadu (strony niebędące stroną sporu).
[77] https://www.pclob.gov/OversightProjects.
[78] https://documents.pclob.gov/prod/Documents/EventsAndPress/deb9cd13-12af-4250-998e-a520a2419a6b/PCLOB%20nominee%20press%20release%206-13-24.pdf.
[79] Motywy 176–194 decyzji stwierdzającej odpowiedni stopień ochrony.

fizyczne są informowane za pośrednictwem organu krajowego, że „kontrola nie wykazała żadnych naruszeń objętych zakresem albo [że] ODNI CLPO / Sąd ds. Kontroli Ochrony Danych wydał decyzję nakazującą wdrożenie odpowiednich środków zaradczych". Decyzje ODNI CLPO i Sądu ds. Kontroli Ochrony Danych są wiążące dla agencji wywiadowczych.

Od czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony podjęto dalsze kroki w celu zapewnienia pełnej operacyjności mechanizmu dochodzenia roszczeń.

Jeżeli chodzi o ustanowienie Sądu ds. Kontroli Ochrony Danych, 14 listopada 2023 r. do sądu powołano ośmiu sędziów (tj. dwóch więcej sędziów niż wynosi minimalna liczba wymagana na mocy rozporządzenia wykonawczego 14086, uzupełnionego regulaminem Prokuratora Generalnego, sekcja 28 § 201.3 lit. a) C.F.R.)[80]. Zostali oni powołani na podstawie kryteriów określonych w rozporządzeniu wykonawczym 14086 i zgodnie z procedurą w nim ustanowioną, w tym po konsultacji m.in. z Radą Nadzoru nad Prywatnością i Wolnościami Obywatelskimi[81]. Wśród sędziów tych znaleźli się: byli sędziowie federalnego sądu pierwszej instancji i sądu apelacyjnego, były prokurator generalny USA i były członek Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi. Zgodnie z wymogami rozporządzenia wykonawczego co najmniej połowa sędziów ma wcześniejsze doświadczenie orzecznicze. Ponadto w kwietniu 2024 r. powołano dwóch rzeczników specjalnych – prawników posiadających wiedzę fachową zarówno w zakresie ochrony prywatności, jak i bezpieczeństwa narodowego – w celu reprezentowania interesów osób fizycznych przed Sądem ds. Kontroli Ochrony Danych. Na spotkaniu przeglądowym potwierdzono, że wszyscy sędziowie i rzecznicy specjalni otrzymali najwyższe poświadczenie bezpieczeństwa, w związku z czym mogą mieć dostęp do materiałów niejawnych podczas wykonywania swoich zadań dla Sądu ds. Kontroli Ochrony Danych. Sąd ds. Kontroli Ochrony Danych opublikował również zestaw odpowiedzi na najczęściej zadawane pytania, w których przedstawił więcej informacji na temat swojej roli, niezależności i funkcjonowania[82].

Jeżeli chodzi o rozpatrywanie skarg, ODNI przyjął 6 grudnia 2022 r. dyrektywę w sprawie wspólnoty wywiadowczej 126, która szczegółowo reguluje (poprzez określenie terminów, ustanowienie bezpiecznego repozytorium elektronicznego i bezpiecznych kanałów komunikacji, wymaganie od urzędnika ds. ochrony wolności obywatelskich (CLPO) i od wspólnoty wywiadowczej współpracy z Radą Nadzoru nad Prywatnością i Wolnościami Obywatelskimi w kontekście corocznego przeglądu mechanizmu dochodzenia roszczeń itp.) różne aspekty procesu badania i rozpatrywania skarg[83]. Dyrektywa ta ma zastosowanie do całej wspólnoty wywiadowczej Stanów Zjednoczonych i została uzupełniona o dodatkowe procedury wewnętrzne przyjęte przez poszczególne agencje wywiadowcze, dotyczące ich współpracy z ODNI CLPO w kontekście rozpatrywania skarg (np. opracowanie bezpiecznego repozytorium do wymiany skarg i wnioskowanych dokumentów oraz bezpieczna komunikacja między właściwymi agencjami). W nadchodzących miesiącach Sąd ds. Kontroli Ochrony Danych wyda również bardziej szczegółowe przepisy dotyczące rozpatrywania skarg i innych aspektów proceduralnych.

[80] https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-judges-data-protection-review-court.
[81] Sekcja 3 lit. d) ppkt A rozporządzenia wykonawczego 14086.
[82] https://www.justice.gov/opcl/dprc-resources.
[83] https://www.dni.gov/files/documents/ICD/ICD_126-Implementation-Procedures-for-SIGINT-Redress-Mechanism.pdf

W Unii Europejskiej i w Stanach Zjednoczonych podjęto szereg dodatkowych środków mających na celu informowanie ogółu społeczeństwa, a także ułatwienie składania i rozpatrywania skarg. Działania te obejmują przyjęcie przez EROD noty informacyjnej na temat nowego mechanizmu dochodzenia roszczeń[84], wzoru formularza skargi (który ma zostać przetłumaczony i opublikowany przez wszystkie organy ochrony danych w ich językach krajowych)[85] oraz regulaminu regulującego współpracę między krajowymi organami nadzoru a sekretariatem EROD[86]. ODNI opublikował również odpowiedzi na najczęściej zadawane pytania i notę informacyjną na temat nowego mechanizmu dochodzenia roszczeń, a także zaangażował się w działania podnoszące świadomość społeczną[87].

Ponadto w ciągu ostatniego roku EROD i odpowiednie organy Stanów Zjednoczonych ściśle współpracowały w kilku aspektach operacyjnych. W szczególności, jak potwierdzono podczas spotkania przeglądowego, wprowadzono szyfrowany kanał komunikacji w celu przekazywania skarg z organów krajowych w UE do sekretariatu EROD, z sekretariatu EROD do ODNI CLPO, a także do Biura Ochrony Prywatności i Wolności Obywatelskich (OPCL) Departamentu Sprawiedliwości oraz między ODNI CLPO a innymi organami po stronie USA (np. Sądem ds. Kontroli Ochrony Danych). Ponadto ODNI CLPO wyjaśnił, że wprowadzono dalsze procedury wewnętrzne dotyczące współpracy poszczególnych agencji wywiadowczych z ODNI CLPO w zakresie rozpatrywania skarg.

Ponadto Biuro Ochrony Prywatności i Wolności Obywatelskich Departamentu Sprawiedliwości (OPCL), które udziela wsparcia administracyjnego Sądowi ds. Kontroli Ochrony Danych, poinformował również, że Sąd ten działa w ramach własnej specjalnej linii budżetowej i jest wyposażony w urządzenia niezbędne do wykonywania swoich zadań, w tym bezpieczne komputery i laptopy, telefony itp. Ponadto, zgodnie z wymogami rozporządzenia wykonawczego 14086, DoC podjął niezbędne środki, w tym poprzez ustanowienie szyfrowanego kanału komunikacji z ODNI CLPO, w celu prowadzenia rejestru wszystkich otrzymanych kwalifikujących się skarg. DoC będzie okresowo kontaktować się z ODNI CLPO w celu ustalenia, czy informacje dotyczące poszczególnych skarg zostały odtajnione. Jeżeli tak, DoC powiadomi o tym zainteresowaną osobę fizyczną, aby umożliwić jej uzyskanie dostępu do takich informacji.

Do chwili spotkania przeglądowego unijne organy nadzorcze nie otrzymały żadnych skarg, w związku z czym nie uruchomiono jeszcze nowego mechanizmu dochodzenia roszczeń.

3. WNIOSKI

Na podstawie informacji zebranych podczas pierwszego przeglądu Komisja stwierdza, że organy Stanów Zjednoczonych wprowadziły niezbędne struktury i procedury w celu zapewnienia skutecznego funkcjonowania ram ochrony danych. W tym kontekście Komisja

[84] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/information-note-data-protection-framework-redress_pl.
[85] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/template-complaint-form-us-office-director-national_pl.
[86] https://www.edpb.europa.eu/our-work-tools/our-documents/other-guidance/rules-procedure-data-protection-framework-redress_pl.
[87] https://www.dni.gov/files/CLPT/documents/Fact_Sheets/The_Role_of_the_ODNI_CLPO_FAQs.pdf and https://www.dni.gov/files/CLPT/documents/Fact_Sheets/Data_Privacy_Framework.pdf.

bardzo docenia bardzo dobrą współpracę z organami Stanów Zjednoczonych w zakresie przeprowadzenia przeglądu.

Choć podczas pierwszego przeglądu skupiono się oczywiście na sprawdzeniu, czy wszystkie składowe elementy ram zostały wdrożone, to doświadczenie w praktycznym stosowaniu zabezpieczeń mających zastosowanie zarówno do przetwarzania danych przez certyfikowane przedsiębiorstwa, jak i do dostępu do danych przez organy publiczne, jest z konieczności ograniczone po zaledwie roku funkcjonowania. Komisja będzie zatem ściśle monitorować istotne zmiany w nadchodzących miesiącach i latach, zwracając szczególną uwagę na 1) przyszłe sprawozdania Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi dotyczące wdrożenia rozporządzenia wykonawczego 14086 i funkcjonowania mechanizmu dochodzenia roszczeń w ramach rozpoznania radioelektronicznego, w szczególności na Sąd ds. Kontroli Ochrony Danych; 2) możliwe dalsze zmiany sekcji 702 ustawy o kontroli wywiadu; oraz 3) nominacje i mianowanie członków Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi w celu obsadzenia przyszłych wakatów.

Ponadto, aby zapewnić stałe i skuteczne funkcjonowanie, Komisja uważa, że ważne jest, aby:

- jak zapowiedziano na spotkaniu przeglądowym, DoC wykorzystywał w większym stopniu różne narzędzia przewidziane w DPF do monitorowania przestrzegania zasad przez przedsiębiorstwa i wykrywania fałszywych oświadczeń o uczestnictwie;
- FTC dalej rozwijała swoje proaktywne podejście do badania i egzekwowania przestrzegania przez certyfikowane przedsiębiorstwa zasad DPF oraz
- DoC, FTC i unijne organy ochrony danych opracowały wspólne instrumenty zawierające wytyczne w sprawie kluczowych wymogów wynikających z zasad DPF, np. w sprawie danych o zasobach ludzkich i dalszego przekazywania danych.

W świetle tego wyników przeglądu oraz zgodnie z motywem 211 decyzji stwierdzającej odpowiedni stopień ochrony Komisja uważa, że należy przeprowadzić kolejny okresowy przegląd po trzech latach. Pozwoli to zdobyć większe doświadczenie w praktycznym stosowaniu DPF i uwzględnić wyżej wymienione nadchodzące zmiany. Zgodnie z art. 3 ust. 4 decyzji stwierdzającej odpowiedni stopień ochrony Komisja skonsultuje się w sprawie częstotliwości przyszłych przeglądów z EROD i komitetem ustanowionym na mocy art. 93 ust. 1 ogólnego rozporządzenia o ochronie danych.