Warszawa, 12 października 2026 r.

REKOMENDACJE FUNDACJI PANOPTYKON[1] w sprawie ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości

Obszar ochrony danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości regulują: dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WsiSW (**dalej: dyrektywa, dyrektywa LED**)[2], a także ustawa z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (**dalej: ustawa, ustawa wdrożeniowa**).

Konieczność wprowadzenia zmian w tym obszarze wynika z zainicjowania przez Komisję Europejską postępowania naruszeniowego przeciwko Polsce (INFR(2026)2130). O prawidłowe wdrożenie w polskim systemie dyrektywy LED wielokrotnie wnioskował także Prezes Urzędu Ochrony Danych Osobowych[3].

Poniżej przedstawiamy najważniejsze, w naszej ocenie, obszary dotyczące przetwarzania danych osobowych w związku z zapobieganiem i zwalczaniem przestępczości, które wymagają zmian. Rekomendacje zilustrowane są historiami konkretnych osób, których prawa zostały ograniczone w związku z niewłaściwym działaniem zasad ochrony danych osobowych w obszarze zwalczania przestępczości. Historie tych osób Fundacja Panoptykon zbierała podczas projektu „Razem dla dobrego wdrożenia dyrektywy policyjnej", realizowanego w ramach Programu Równych Praw.

[1] Rekomendacje przygotowane przez Wojciecha Klickiego i Mateusza Wrotnego.

[2] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WsiSW. Skrót LED pochodzi od angielskiej nazwy dyrektywy: Law Enforcement Directive.

[3] Por. m.in. wystąpienie Prezesa Urzędu Ochrony Danych Osobowych do Ministra Spraw Wewnętrznych i Administracji oraz do Ministra Sprawiedliwości z 16 marca 2026 r. dostępne pod adresem: https://uodo.gov.pl/pl/file/7252.

Finansowane przez Unię Europejską

1. Nadzór nad przetwarzaniem danych osobowych przez prokuraturę

1.1. Hierarchiczne podporządkowanie, a nie niezależność

W obecnie obowiązującym w Polsce modelu nadzór nad właściwym i zgodnym z prawem przetwarzaniem danych osobowych przez prokuraturę, w ramach realizowanych zadań w zakresie ścigania przestępstw, sprawują prokuratorzy nadrzędni[4]. Nad prokuraturą rejonową czuwa prokurator okręgowy, nad prokuraturą okręgową – prokurator regionalny, a nad prokuraturą regionalną i Prokuraturą Krajową – Prokurator Krajowy.

Organy te wykonują funkcje nadzorcze, stosując do tego celu polecenia służbowe (a nie decyzje administracyjne)[5]. W ramach nadzoru rozpatrują skargi osób, których dane są przetwarzane niezgodnie z prawem, prowadzą postępowania wyjaśniające i kontrolują zgodność przetwarzania z przepisami.

Dyrektywa nakłada obowiązek, aby nad monitorowaniem stosowania przepisów czuwał organ niezależny od podmiotów przetwarzających dane, co ma umożliwić obiektywną i bezstronną kontrolę ich działania. Dyrektywa dopuszcza ustanowienie innych niż organ nadzorczy podmiotów do kontrolowania przetwarzania danych przez organy sprawujące wymiar sprawiedliwości. Zostawiając na marginesie to, czym właściwie jest „sprawowanie wymiaru sprawiedliwości", kluczowe jest, czy w przyjętym modelu nadzór funkcjonuje skutecznie i czy pozostaje niezależny.

Niezależność jako niezbędny warunek sprawowania nadzoru szczegółowo wyjaśnił Trybunał Sprawiedliwości Unii Europejskiej w sprawie Prokuratuur (C-746/18)[6]. Niezależność organu kontrolującego wymaga, aby był on **oddzielony** od organu prowadzącego postępowanie. Organ ten nie może uczestniczyć w dochodzeniu ani śledztwie. Powinien również zachowywać neutralność wobec stron postępowania oraz podejmować decyzje w sposób obiektywny i wolny od wpływów zewnętrznych. Wymogu tego nie spełnia prokurator nadrzędny, który pozostaje z prokuratorem prowadzącym postępowanie w relacji podporządkowania służbowego, a tym samym nie ma statusu niezależnej strony trzeciej. Problem ten jest szczególnie jaskrawy w przypadku przetwarzania danych przez Prokuraturę Krajową, w której nie ma zewnętrznego podmiotu odpowiadającego za kontrolę przetwarzania danych. Ilustruje to poniższy przykład.

[4] Art. 191a § 1 ustawy Prawo o prokuraturze.

[5] Tamże, art. 191a § 1a.

[6] Wyrok TSUE z 2 marca 2021 r., LEX nr 312592.

1.2. Przychodzi obywatel do prokuratora

Z próbą wyegzekwowania przysługujących mu uprawnień związanych z przetwarzaniem danych osobowych przez prokuraturę zmierzył się pewien aktywista. W marcu 2024 r. Prokuratura Krajowa ujawniła, że była w posiadaniu izraelskiego oprogramowania Hermes. System przeznaczony jest do gromadzenia i analizowania ogromnych ilości danych z różnych źródeł. O tym, że został poddany analizie z wykorzystaniem Hermesa, nasz rozmówca dowiedział się przypadkowo od dziennikarza, który przygotowywał na ten temat artykuł.

Pełnomocnik aktywisty skierował do Prokuratury Krajowej wniosek o udostępnienie informacji, jakie dane osobowe aktywisty ona przetwarza. Z odpowiedzi Prokuratury wynikało, że wniosek ten potraktowany został jako… zawiadomienie o podejrzeniu popełnienia przestępstwa.

> „Złożyliśmy z pełnomocnikiem do Prokuratora Krajowego wniosek z pytaniem, jakie informacje na mój temat były przetwarzane przez prokuraturę. Po terminie ustawowym[7] otrzymaliśmy zdawkową odpowiedź. Było w niej napisane, że powinniśmy wystąpić o akta sprawy. Szło to w stronę postępowania karnego, którego przepisy odrębnie regulują przetwarzanie danych osobowych. A nam przecież chodziło o skorzystanie z uprawnień przewidzianych w ustawie o ochronie danych przetwarzanych przez organy ścigania”[8, 9].

Nasz rozmówca próbował uzyskać informacje o przetwarzanych danych, kierując wniosek do Prokuratury Krajowej, a więc do tego samego podmiotu, który te dane gromadził i wykorzystywał. Otrzymana odpowiedź była nie tylko spóźniona, lecz także ogólnikowa i nie odnosiła się do istoty pytania.

Kluczowe jest to, że nadzór nad przetwarzaniem danych osobowych w Prokuraturze Krajowej prowadzi Prokurator Krajowy. Zabrakło zatem zewnętrznego i niezależnego organu, który mógłby zweryfikować prawidłowość przetwarzania danych i zapewnić rzeczywistą ochronę praw jednostki, np. realizację prawa do informacji na temat tego, jakie dane są przetwarzane.

Nadzór nad przetwarzaniem danych osobowych w prokuraturze należy powierzyć niezależnemu organowi, zamiast utrzymywać nieefektywny mechanizm nadzoru wewnętrznego.

[7] Na podstawie odesłania z art. 191a § 4 Prokuratura Krajowa powinna udzielić odpowiedź bez zbędnej zwłoki, nie później niż w terminie miesiąca od dnia wpływu.

[8] Chodzi o ustawę z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

[9] Wypowiedź aktywisty dla Fundacji Panoptykon, 11 marca 2026 r.

2. Postępowanie karne wyłączone spod działania ustawy

2.1. Dane osobowe a akta sprawy karnej

Przepisy ustawy wdrożeniowej (art. 3 ust. 1) wyłączają stosowanie jej przepisów do danych osobowych zawartych w aktach sprawy oraz do czynności prowadzonych na podstawie wskazanych w tym przepisie ustaw (w tym m.in. Kodeksu postępowania karnego)[10]. W praktyce oznacza to, że dane osobowe zgromadzone w toku postępowania przygotowawczego, a także dane zgromadzone w postępowaniu sądowym są pozbawione ochrony przewidzianej w tej ustawie.

Już na etapie prac nad ustawą wdrażającą dyrektywę LED Ministerstwo Spraw Zagranicznych zwracało uwagę, że takie wyłączenie sprzeciwia się celowi dyrektywy, jakim jest objęcie ochroną danych osobowych przetwarzanych w celu zwalczania przestępczości. W ocenie Ministerstwa przy tak szeroko ujętym wyłączeniu poza zakresem dyrektywy znalazłaby się większość danych osobowych (przecież postępowanie karne opiera się na aktach sprawy)[11].

Ta uwaga pozostaje aktualna.

2.2. Służby kontra pacjentki

Z problemem nadmiernego przetwarzania danych osobowych w toku postępowania przygotowawczego spotkała się skarżąca w sprawie A.G.-Ś. przeciwko Polsce[12]. W związku ze śledztwem prowadzonym przeciwko jej mężowi Prokuratura pozyskała z Narodowego Funduszu Zdrowia dokumentację medyczną kobiety. Były to informacje wykraczające poza zakres niezbędny do prowadzenia śledztwa. Mimo braku ich znaczenia dla sprawy prokuratura przez wiele lat przechowywała je w aktach i udostępniała szerokiemu kręgowi podmiotów. Skarżąca nie została przy tym poinformowana o pozyskaniu i wykorzystaniu tych danych ani nie miała realnej możliwości zakwestionowania tej sytuacji.

Europejski Trybunał Praw Człowieka orzekł, że skarżąca nie dysponowała żadnym skutecznym mechanizmem ograniczenia zakresu przetwarzania danych, przez co naruszone zostało jej prawo do poszanowania życia prywatnego.

Innym przykładem są czynności funkcjonariuszy Centralnego Biura Antykorupcyjnego. Na podstawie postanowienia prokuratora Prokuratury Regionalnej w Szczecinie CBA przeprowadziło przeszukanie w gabinecie ginekologicznym i zabezpieczyło dokumentację

[10] Art. 3 ust. 1 ustawy wdrożeniowej.

[11] Opinia Ministerstwa Spraw Zagranicznych z 14 sierpnia 2018 r. dostępna pod adresem: https://legislacja.gov.pl/docs//2/12310605/12502724/12502726/dokument355779.PDF.

[12] Wyrok Europejskiego Trybunał Praw Człowieka z 13 listopada 2025 r. w sprawie A.G.-Ś. przeciwko Polsce (skarga nr 10685/18).

medyczną pacjentek gromadzoną od 1996 r.[13]. Po włączeniu tej dokumentacji do akt prowadzonej przez CBA sprawy **pacjentki utraciły kontrolę** nad najbardziej intymnymi informacjami o swoim życiu. Rodzi to pytanie, gdzie przebiegają granice dopuszczalnego gromadzenia i przetwarzania tak szerokiego zakresu danych.

Prawo w sytuacji, w której dane osobowe nie mają znaczenia dla postępowania karnego albo przestają być dla niego istotne, powinno zapewnić jednostce możliwość kontroli. Prokuratorzy powinni dokonywać bardziej wnikliwej oceny zakresu materiałów włączanych do akt sprawy. Zgodnie z dyrektywą LED w odniesieniu do danych znajdujących się w aktach sprawy przetwarzanych na potrzeby postępowania przygotowawczego lub sądowego w sprawie karnej przepisy krajowe powinny zapewniać osobie, której dane dotyczą, możliwość korzystania ze swoich podstawowych uprawnień[14], w tym prawa dostępu do danych osobowych[15] i prawa do ich sprostowania lub usunięcia[16].

3. Służby specjalne bez kontroli (przetwarzania danych)

3.1. Bezpieczeństwo narodowe jako wytrych

Obowiązujące w Polsce przepisy wyłączają stosowanie zasad ochrony danych osobowych m.in. w odniesieniu do danych „przetwarzanych w związku z zapewnieniem bezpieczeństwa narodowego, **w tym w ramach realizacji zadań ustawowych** Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego oraz Centralnego Biura Antykorupcyjnego”[17].

To wyłączenie jest nieprecyzyjne, ponieważ pojęcie bezpieczeństwa narodowego nie zostało wprost zdefiniowane w przepisach prawa. Bezpieczeństwo narodowe należy do wyłącznej kompetencji państw członkowskich[18], co nie oznacza jednak, że państwa członkowskie dysponują całkowitą swobodą w definiowaniu tego pojęcia. Jego stosowanie powinno podlegać ścisłej wykładni i kontroli proporcjonalności[19].

Polski ustawodawca przyjął dyskusyjne założenie, że całość działalności służb specjalnych mieści się w tym pojęciu. W szczególności w przypadku CBA trudno uznać, że wszystkie jego zadania

[13] Sieć Obywatelska Watchdog Polska, *CBA i dokumentacja medyczna – ciąg dalszy sprawy ze Szczecina*, https://siecobywatelska.pl/cba-i-dokumentacja-medyczna-ciag-dalszy-sprawy-ze-szczecina/.

[14] Art. 13 dyrektywy LED.

[15] Tamże, art. 14.

[16] Tamże, art. 16.

[17] Art. 3 pkt. 2 ustawy wdrożeniowej.

[18] Art. 4 ust. 2 Traktatu o Unii Europejskiej.

[19] Wyrok Trybunału Sprawiedliwości z 6 października 2020 r., C-511/18, La Quadrature du Net i in. przeciwko Premier Ministre i in., LEX nr 3095381.

(np. zwalczanie przestępstw związanych z korupcją w sporcie) mają bezpośredni związek z bezpieczeństwem narodowym.

Jednocześnie w przepisach sektorowych dotyczących bezpośrednio działania konkretnych służb specjalnych brak jest jasnych regulacji określających sposób nadzoru nad przetwarzaniem danych osobowych w tych służbach i zakres przysługujących jednostce w związku z tym uprawnień.

3.2. Czy służby zawsze powinny podlegać wyłączeniu

W 2008 r. Marta Lempart ubiegała się o pracę w Agencji Bezpieczeństwa Wewnętrznego. Agencja nigdy nie odpowiedziała na jej zgłoszenie i liderka Strajku Kobiet pewnie zapomniałaby o sprawie, gdyby nie stała się ona tematem medialnym w czasie protestów przeciwko zaostrzeniu przepisów dotyczących aborcji w Polsce w 2020 r.

> „Wyciągnęli rzeczy sprzed kilkunastu lat. Wtedy było dla mnie jasne, że czesali wszystko, co mogło być. Myślę, że udostępnili te informacje, żeby mi zaszkodzić, bo to było w czasie protestów w 2020 r."[20].

Sprawę podjął z urzędu Rzecznik Praw Obywatelskich[21]. To jednak niewiele dało, a aktywistka nie dysponowała skutecznym środkiem odwoławczym, bo **całość zadań ustawowych** ABW została wyłączona spod działania ustawy wdrażającej LED. Z uwagi na to szerokie wyłączenie nie jest do końca jasne nawet to, w jaki sposób służby mogą przetwarzać dane osobowe ani czego im nie wolno. Służby powinny mieć możliwość przetwarzania danych do wykonywania swych zadań, ale nie oznacza to, że wszystkie procesy przetwarzania danych (w tym rekrutacja do służby) powinny pozostawać poza jakąkolwiek kontrolą.

Dlatego konieczne jest stworzenie w służbach spójnych i kompleksowych zasad ochrony danych osobowych, które wyeliminują istniejące luki oraz zapobiegną nadmiernej dowolności działania służb w tym obszarze.

[20] Wypowiedź Marty Lempart dla Fundacji Panoptykon, 11 marca 2026 r.

[21] Rzecznik Praw Obywatelskich, *Z ABW wyciekły dane nt. Liderki Strajku Kobiet. Rzecznik prosi Agencję o wyjaśnienia*, https://bip.brpo.gov.pl/pl/content/z-abw-wyciekly-dane-nt-liderki-strajku-kobiet-rpo-prosi-o-wyjasnienia.

4. Ograniczenie praw osoby, której dane dotyczą (czyli mam twoje dane i co mi zrobisz?)

4.1. Prawo dostępu do danych

Jednym z podstawowych praw jednostki, wynikających zarówno z ogólnego rozporządzenia o ochronie danych (RODO)[22], jak i dyrektywy LED[23], jest prawo dostępu do danych osobowych. To uprawnienie na gruncie regulacji dotyczących zwalczania i zapobiegania przestępczości jest w pewien sposób ograniczane. Zgodnie z motywem 44 dyrektywy LED państwa członkowskie mogą ograniczyć prawo do informacji i dostępu do danych. Jest to dopuszczalne tylko w sytuacji, gdy jest to „konieczne i proporcjonalne w społeczeństwie demokratycznym".

Każda decyzja o ograniczeniu praw – zgodnie z przywołanym wyżej motywem – powinna być oceniana indywidualnie[24]. Administrator powinien zatem każdorazowo przeprowadzić test proporcjonalności polegający na wyważeniu interesów osoby, której dane dotyczą, z potrzebą zapewnienia prawidłowego toku postępowań prowadzonych przez służby.

Ustawa wdrożeniowa w art. 26 przewiduje takie wyłączenia, które mają charakter elastyczny i podlegają indywidualnej ocenie (np. można odmówić udostępnienia informacji, jeśli w konkretnym przypadku ich udostępnienie mogłoby utrudnić lub uniemożliwić rozpoznawanie, zapobieganie, wykrywanie lub zwalczanie czynu zabronionego)[25].

W tym samym art. 26 znalazły się jednak także ograniczenia, które wyraźnie wykraczają poza ramy dyrektywy. Największe wątpliwości budzi zasada odmowy udostępnienia informacji w sytuacji, w której „mogłoby to prowadzić do ujawnienia informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych"[26]. Takie ogólne wyłączenie jest sprzeczne z dyrektywą LED.

4.2. Czynności operacyjno-rozpoznawcze jako wyjątek

Zgodnie z ustawą wdrożeniową nie podlegają ujawnieniu informacje pozyskane w toku czynności operacyjno-rozpoznawczych. Oznacza to tyle, że kryterium odmowy realizacji praw jednostki jest pochodzenie danych. Takie podejście budzi wątpliwości, ponieważ fakt uzyskania danych

[22] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), art. 15 ust. 1.

[23] Art. 14 dyrektywy.

[24] „Administrator powinien dokonywać oceny – badając konkretnie i indywidualnie każdy przypadek – czy prawo dostępu powinno zostać częściowo lub całkowicie ograniczone" – motyw 44 dyrektywy LED.

[25] Art. 26 ust. 1 pkt 2. ustawy wdrożeniowej.

[26] Tamże, art. 26 ust. 1.

w ramach tych czynności nie zawsze odpowiada przesłankom dopuszczającym ograniczenie praw przewidzianym w dyrektywie.

Czynności operacyjno-rozpoznawcze to zespół metod, dzięki którym służby mogą pozyskiwać informacje w sposób niejawny. Do ich uzyskiwania wykorzystywane są np. kontrola operacyjna czy obserwacja. Osoba nie ma świadomości, że jej dane zostały zebrane, a tym bardziej – jakie konkretnie dane są przetwarzane. Może to dotyczyć także sytuacji, w której osoba postronna rozmawia przez telefon z kimś objętym podsłuchem. Choć sama nie była przedmiotem kontroli, jej dane również zostają utrwalone i trafiają do materiałów zgromadzonych przez służby.

4.3. Informacje niejawne jako wyjątek

Kolejny wyjątek uniemożliwiający uzyskanie informacji o przetwarzanych danych osobowych wynika z ochrony informacji niejawnych. W art. 84 ustawy wdrożeniowej wskazano bowiem, że do danych osobowych stanowiących informacje niejawne nie stosuje się przepisów o ochronie danych osobowych[27].

Klauzulę informacji niejawnej (tajnej, ściśle tajnej, poufnej lub zastrzeżonej) może nadać osoba, która wytworzyła lub podpisała dokument[28]. Ustawa o ochronie informacji niejawnych (art. 9) nie zawiera natomiast efektywnych mechanizmów pozwalających podmiotowi danych zakwestionować nadanie klauzuli. Osoba, której dane dotyczą, w praktyce nie ma możliwości skorzystania ze swoich uprawnień ani doprowadzenia do merytorycznej kontroli decyzji o nadaniu klauzuli odbierającej jej tę możliwość.

4.4. Pan tu nie stał, czyli krótka historia o odmowie wejścia do instytucji publicznych

Osoba, która nie wie, jakie dane osobowe na jej temat są przetwarzane ani w jaki sposób są one wykorzystywane, nie ma możliwości skorzystania z innych uprawnień przewidzianych w dyrektywie. Przykładem jest wynikające z art. 52 dyrektywy prawo do wniesienia skargi do organu nadzorczego na niezgodne z prawem przetwarzanie danych.

W takiej sytuacji znaleźli się dziennikarz radiowy i fotoreporter, których praca polega na relacjonowaniu konferencji prasowych odbywających się w budynkach należących do administracji rządowej. Pierwszy z przedstawicieli mediów, pracujący dla jednej ze stacji radiowych, w czerwcu 2025 r. otrzymał od pracowniczki Ministerstwa Edukacji Narodowej informację, że nie zostanie wpuszczony na konferencję prasową ze względu na negatywną opinię Służby Ochrony Państwa. Nie wskazała, czego konkretnie dotyczyła opinia SOP ani na jakiej podstawie została sporządzona. Wcześniej nazwisko dziennikarza widniało w systemie akredytacji medialnych, a on sam regularnie uczestniczył w konferencjach prasowych, w tym w Kancelarii

[27] Art. 84 ustawy wdrożeniowej stanowił nowelizację art. 1 ustawy o ochronie informacji niejawnych.

[28] Art. 6 ust. 1 ustawy o ochronie informacji niejawnych.

Prezesa Rady Ministrów oraz w poszczególnych ministerstwach. Po tym zdarzeniu okazało się, że ma zablokowany dostęp do systemu akredytacyjnego i nie może wejść do niektórych budynków instytucji publicznych (do innych nadal miał wstęp).

Dziennikarz zwrócił się do KPRM z prośbą o wyjaśnienia. Został odesłany do SOP-u, który poinformował go, że decyzja jest skutkiem informacji niejawnych i nie może mu zostać udostępniona.

> „Całe szczęście redakcja wykazała się zrozumieniem i stanęła po mojej stronie, ale prawdziwa zgroza tej sytuacji dotarła do mnie w momencie, kiedy zacząłem się zastanawiać, co by było, gdybym chciał zmienić pracę. Moja praca jest bezpośrednio związana z tym, że muszę chodzić np. do ministerstw. Gdybym powiedział o tych blokadach nowemu potencjalnemu pracodawcy, to myślę, że bym tej pracy nie dostał”[29].

Z kolei fotoreporter, z którym rozmawialiśmy, w latach 2019–2026 napotykał powtarzające się problemy z akredytacją do Pałacu Prezydenckiego, choć do innych instytucji publicznych zazwyczaj miał wstęp. W grudniu 2025 r. jego login zniknął z systemu akredytacyjnego. Mogło to być skutkiem wydania przez SOP negatywnej opinii na jego temat. SOP odmówił wyjaśnień, jedynie nieoficjalnie funkcjonariusz powiedział mu, że „powinien wiedzieć, co zrobił”[30].

Podobne doświadczenie miała jedna z aktywistek organizacji propalestyńskich, która na zaproszenie jednej z posłanek chciała wejść do budynku Sejmu. Straż Marszałkowska nie wydała jej jednak przepustki, nie wskazując przy tym przyczyny ani podstawy decyzji. Od posłanki aktywistka dowiedziała się, że odmowa wynika z umieszczenia jej na „czarnej liście ABW”. Nasza rozmówczyni nie otrzymała wcześniej żadnej informacji o wpisie na listę ani wyjaśnienia podstawy działania służb.

> „Wydaje mi się, że to Straż Marszałkowska zadzwoniła do posłanki, żeby skonsultować, dlaczego zaprasza osoby będące na czarnej liście ABW. Posłanka nie wiedziała, że na niej jesteśmy. Nie wiem nawet, czy ona faktycznie cofnęła to zaproszenie, czy nie. Dostaliśmy po prostu informację, że nie zostaniemy wpuszczeni”[31].

[29] Wypowiedź dziennikarza dla Fundacji Panoptykon, 6 marca 2026 r.

[30] Wypowiedź fotoreportera dla Fundacji Panoptykon, 9 kwietnia 2026 r.

[31] Wypowiedź aktywistki dla Fundacji Panoptykon, 3 marca 2026 r.

Aktywistka zwróciła się następnie do Straży Marszałkowskiej z wnioskiem o udostępnienie danych osobowych, jakie na jej temat przetwarza. Otrzymała odpowiedź, zgodnie z którą jedyną informacją na jej temat jest fakt, że zgłosiła zamiar wejścia na teren Sejmu.

Choć aktywistka nie poniosła konsekwencji prawnych, zdarzenie wywołało u niej stres i poczucie arbitralności decyzji.

> „Gdybym miała robić coś, co mogłoby zaszkodzić, to rozumiem, że służby mogłyby interweniować, ale ja nie uważam, że jestem niebezpieczną osobą i nie uważam, że ktoś miałby powód, żeby mnie tak traktować. Czy gdybym chciała zostać posłanką – bo nie wykluczam takiej możliwości – to czy nie będę mogła?”[32].

***

W opisanych powyżej sytuacjach służby takie jak SOP, ABW i Straż Marszałkowska, dysponowały danymi osobowymi osób, z którymi rozmawialiśmy, i na ich podstawie podejmowały decyzje. Osoby, których dane dotyczyły, nie otrzymały informacji o tym, jakie to dane ani co wpłynęło na odmowę wstępu do instytucji publicznych. Nie do końca było również jasne, na jakiej podstawie odmawia się im dostępu do samych danych.

Dlatego ustawodawca powinien uchylić przepisy, które pozwalają na nadmierne ograniczenie prawa do udostępniania danych osobowych (w tym te dotyczące czynności operacyjno-rozpoznawczych oraz ochrony informacji niejawnych), a następnie dostosować je do wymogów stawianych przez dyrektywę LED.

5. Brak wdrożenia do polskiej ustawy kontroli pośredniej organu nadzorczego

5.1. Nie tylko skarga. Organ nadzorczy na straży praw

Dyrektywa LED przewiduje możliwość przyjmowania przepisów ograniczających informowanie osoby, której dane dotyczą[33], ale jednocześnie, by osiągnąć równowagę między prawami jednostki a skutecznym zwalczaniem przestępstw, wprowadza mechanizm tzw. pośredniej kontroli organu nadzorczego[34].

[32] Tamże.

[33] W dyrektywie te regulacje znajdują się w art. 13 ust. 3, art. 15 ust. 3 i art. 16 ust. 4

[34] Art. 17 ust. 1-3 dyrektywy LED.

Zgodnie z tym mechanizmem jednostka może wykonywać swoje uprawnienia za pośrednictwem organu nadzorczego, zamiast bezpośrednio wobec administratora. W takiej sytuacji to wyznaczony organ nadzorczy działa jako niezależny gwarant ochrony praw jednostki, dokonując weryfikacji zgodności z prawem przetwarzania danych i oceniając zasadność ewentualnych ograniczeń. Mechanizm ten ma kluczowe znaczenie nie tyle w sytuacji naruszenia ochrony danych osobowych, ile wtedy, gdy odmowa udzielenia informacji wynika z ustawowych ograniczeń wskazanych w poprzednim rozdziale.

Osoba, której dane dotyczą, powinna zostać poinformowana o możliwości skorzystania z tej ścieżki. Po przeprowadzeniu kontroli organ nadzorczy powinien przekazać jej informację o wynikach weryfikacji.

5.2. Niejednoznaczne wdrożenie art. 17 dyrektywy LED

Jeśli służby odmawiają osobie, której dane dotyczą, udzielenia informacji na temat ich przetwarzanych, powołując się np. na to, że zostały one pozyskane w wyniku czynności operacyjno-rozpoznawczych lub objęte są klauzulą tajności, to takie działania wciąż powinny być objęte kontrolą. Dziennikarze, których historie przedstawiliśmy wyżej, powinni mieć możliwość zwrócenia się do organu nadzorczego z wnioskiem o sprawdzenie zarówno tego, czy ograniczenie ich prawa do informacji było zgodne z prawem, jak i tego, czy służby przetwarzały ich dane zgodnie z przepisami.

Oprócz opisanej wyżej możliwości wykonywania praw jednostki za pośrednictwem organu nadzorczego dyrektywa LED przewiduje też prawo złożenia skargi do organu nadzorczego[35].

Te dwa uprawnienia na gruncie polskiej ustawy wdrożeniowej miały być realizowane przez art. 50. Jednak wykonywanie uprawnień za pośrednictwem organu nadzorczego jest odrębną instytucją prawną od skargi. W polskiej ustawie wdrażającej mechanizm pośredniej kontroli organu nadzorczego nie został w pełni zaimplementowany. Prezes UODO może w wyniku skargi podjąć kontrolę, ale jednostka nigdy nie pozna jej wyników, a w konsekwencji nie będzie mogła ich zaskarżyć. W ten sposób osoba, której dane dotyczą, ma znacząco ograniczoną możliwość wykorzystania swoich uprawnień wynikających z dyrektywy.

Konieczne jest zatem pełne wdrożenie mechanizmu pośredniego wykonywania praw jednostki przewidzianego w art. 17 dyrektywy LED, w tym wprowadzenie wyraźnych przepisów umożliwiających skuteczne korzystanie z tych uprawnień za pośrednictwem Prezesa UODO.

[35] Art. 52 dyrektywy LED zaimplementowany w art. 50 ust. 5 ustawy wdrożeniowej.

Rekomendacje powstały w ramach projektu „Razem dla dobrego wdrożenia dyrektywy policyjnej" finansowanego przez Komisję Europejską w ramach Programu Równych Praw realizowanego ze środków programu CERV finansowanego ze środków Komisji Europejskiej w ramach programu „Obywatele, Równość, Prawa i Wartości" na lata 2021–2027.

Wyrażone poglądy i opinie są jedynie opiniami autora lub autorów i niekoniecznie odzwierciedlają poglądy i opinie Unii Europejskiej lub Komisji Europejskiej. Unia Europejska ani organ przyznający nie ponoszą za nie odpowiedzialności.

Finansowane przez Unię Europejską