Informacja w Sprawach	Czytelnia Akt	Biuro Podawcze
Pn.- Pt. 8^{00}-16^{00}	Pn.- Pt. 8^{30} - 15^{30}	Pn.- Pt. 8^{00}-16^{00}
22 553 70 70	**System rezerwacji akt - bip.warszawa.wsa.gov.pl**	Lokalizacja BP patrz „Czytelnia Akt"
Radom 48 368 99 08	Wydz. I, II, IV, VII - ul. Jana Kazimierza 10, tel. 22 553 78 21	**ePUAP** /wsa_waw/SkrytkaESP
informacja@warszawa.wsa.gov.pl	Wydz. III - ul. Jasna 2/4, tel. 22 553 78 23	
	Wydz. V, VI - ul. Jana Pankiewicza 4, tel. 22 553 70 37	
	Wydz. VIII Radom - ul. J. Słowackiego 7 tel. 48 368 99 18	

NIP 525-228-33-65 | REGON 015608709 | Numer rachunku bankowego Sądu – **96 1010 1010 0078 1022 3100 0000**

E – TERMINARZ – wykaz posiedzeń Sądu oraz ich wyniki (bip.warszawa.wsa.gov.pl).

Wojewódzki Sąd Administracyjny
w Warszawie
WYDZIAŁ II
ul. Jana Kazimierza 10
01-248 Warszawa

Dnia **10 października 2024 r.**

Sygn. akt **II SA/Wa 2336/23**

W odpowiedzi należy podać sygnaturę akt sądu

r. pr. Adam Kuczyński
Kancelaria Radcy Prawnego
Pełnomocnik Stowarzyszenia Sieć Obywatelska-Watchdog Polska z siedzibą w Warszawie
ul. Modzelewskiego 23/373
02-679 Warszawa

DORĘCZENIE ODPISU WYROKU

W wykonaniu zarządzenia z dnia 9 października 2024 r. sekretariat Wydziału II Wojewódzkiego Sądu Administracyjnego w Warszawie doręcza Panu – jako Pełnomocnikowi skarżącego – odpis wyroku z dnia 26 kwietnia 2024 r. wraz z uzasadnieniem.

Marta Stec
referent

Sygn. akt II SA/Wa 2336/23

ODPIS

WYROK
W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 26 kwietnia 2024 r.

Wojewódzki Sąd Administracyjny w Warszawie
w składzie następującym:

Przewodniczący Sędzia WSA	Sławomir Antoniuk
Sędzia WSA	Piotr Borowiecki (spr.)
Sędzia WSA	Ewa Radziszewska-Krupa
Protokolant starszy specjalista	Ewa Kielak-Niedźwiedzka

po rozpoznaniu na rozprawie w dniu 26 kwietnia 2024 r.
sprawy ze skargi Stowarzyszenia Sieć Obywatelska Watchdog Polska z siedzibą w Warszawie
na decyzję Ministra Sprawiedliwości
z dnia 16 października 2023 r. nr BK-IV.082.270.2022
w przedmiocie odmowy udostępnienia informacji publicznej

oddala skargę

WOJEWÓDZKI SĄD ADMINISTRACYJNY W WARSZAWIE

Na oryginale właściwe podpisy
Za zgodność z oryginałem

Marta Stec
referent

Sygn. akt II SA/Wa 2336/23

UZASADNIENIE

Minister Sprawiedliwości decyzją z 16 października 2023 r nr BK-IV.082.270.2022, na podstawie art. 5 ust.1 i 2 w zw. z art. 16 ust. 1 i 2 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902); zwanej dalej u.d.i.p. w zw. z art. 4 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756, z późn. zm.); zwanej dalej u.o.i.n i art. 13 ust. 1 i 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących działania publiczne (Dz. U. z 2023 r. poz. 57, z późn. zm.) oraz w zw. z art. 5 ust. 1 i 2, art. 24 i art. 32 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 t. 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, Dz. Urz. UE L 119 z 4.05.2016 r.); dalej jako RODO i art. 104 K.p.a., po rozpatrzeniu wniosku Stowarzyszenia Sieć Obywatelska Watchdog Polska z siedzibą w Warszawie; zwane dalej „Stowarzyszeniem", odmówił udostępnienia kodu źródłowego oprogramowania o nazwie System Losowego Przydziału Spraw; zwanego dalej SLPS.

W uzasadnieniu rozstrzygnięcia organ wskazał, że wnioskiem z 30 października 2017 r. Stowarzyszenie zwróciło się do Ministra Sprawiedliwości o udostępnienie informacji w postaci kodu źródłowego programu SLPS.

Minister Sprawiedliwości, po przeprowadzeniu analizy charakteru żądanej informacji uznał, że kod źródłowy programu komputerowego nie stanowi informacji publicznej w rozumieniu art. 1 ust. 1 u.d.i.p.

Na skutek postępowania zainicjowanego przez Stowarzyszenie, Naczelny Sąd Administracyjny w wyroku z 26 maja 2022 r. sygn. akt III OSK 1189/21 zakwestionował stanowisko organu (a także sądu pierwszej instancji) uznając, że kod źródłowy SLPS stanowi informację publiczną. Sąd odstąpił od wcześniejszego stanowiska Naczelnego Sądu Administracyjnego, wyrażonego m.in. w wyroku z 27 lutego 2014 r. sygn. akt I OSK 2014/13.

Po ponownym rozpatrzeniu wniosku Stowarzyszenia z 30 października 2017 r., Minister Sprawiedliwości decyzją z 4 sierpnia 2022 r. nr BK-IV.082.270.2022 odmówił udostępnienia kodu źródłowego SLPS.

Powyższe rozstrzygnięcie Stowarzyszenie zaskarżyło do Wojewódzkiego Sądu Administracyjnego w Warszawie, który wyrokiem z 24 lutego 2023 r. sygn. akt II SA/Wa 1785/22 uchylił zaskarżoną decyzję. Sąd wskazał na potrzebę rozbudowania argumentacji

na rzecz odmowy udostępnienia wnioskowanej informacji. Zwrócił uwagę m.in. na przesłankę wynikającą z art. 5 ust. 1 u.d.i.p. w zw. z art. 4 ust. 1 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756, z późn. zm.) wyjaśniając, że „dla takiej ochrony informacji niejawnych wystarczy element materialny, tzn. istnienie takiej cechy, przez którą stanowi ona informację, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo, byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania".

Organ wyjaśnił, że wskazane wyroki sądów administracyjnych są wiążące w niniejszej sprawie. Dotyczy to zarówno prawnej oceny kodu źródłowego, jako informacji publicznej, jak również wytycznych w zakresie dalszego postępowania. Z tych względów należało przystąpić do ponownego rozpatrzenia wniosku Stowarzyszenia.

W pierwszej kolejności analizie poddano oprogramowanie o nazwie SLPS, którego kod źródłowy jest przedmiotem wniosku. Jest to program komputerowy, który działa w oparciu o generator liczb losowych i jest używany we wszystkich sądach powszechnych w celu losowego i równomiernego przydziału spraw sędziom, asesorom sądowym i referendarzom sądowym w ramach poszczególnych kategorii spraw sądowych. To rozbudowany i skomplikowany system teleinformatyczny, który we wszystkich sądach jednocześnie realizuje zarówno zasadę losowości przydziału, jak i zasadę proporcjonalności przydziału do dni pracy i wskaźników przydziału poszczególnych referentów. Jest systemem strategicznym dla wymiaru sprawiedliwości. Do chwili obecnej system wykonał ponad 23 mln losowań. System został zaprojektowany w taki sposób, aby udostępnione w nim funkcjonalności umożliwiały prawidłowe uwzględnienie szeregu zagadnień organizacyjno-zarządczych w poszczególnych wydziałach sądów powszechnych (liczba orzeczników, podział czynności, wakaty, nieobecności etc.). W celu prawidłowego działania, SLPS został ściśle połączony z innymi systemami teleinformatycznymi i infrastrukturą, z których korzystają sądy powszechne. Dotyczy to m.in. Zintegrowanego Systemu Rachunkowości i Kadr (ZSRK). W tym systemie gromadzone są dane osobowe około 56 tysięcy sędziów i innych pracowników sądów powszechnych (przede wszystkim numer PESEL, adres zamieszkania, dane o wynagrodzeniach, dane o kontach bankowych, dane o zwolnieniach lekarskich, urlopach, przebiegu zatrudnienia, dane ubezpieczeniowe, dane o niepełnosprawności etc.). Z kolei ZSRK jest połączony z innymi systemami, w tym z systemem bankowym NBP oraz platformą e-Płatności Resortu Sprawiedliwości. SLPS jest

systemem w pełni transparentnym. Jego sposób działania szczegółowo opisują następujące dokumenty publiczne:

1. ustawa z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych (Dz. U. z 2023 r. poz. 217, z późn. zm. - art. 47a),
2. rozporządzenie Ministra Sprawiedliwości z dnia 18 czerwca 2019 r. - Regulamin urzędowania sądów powszechnych (Dz. U. z 2022 r. poz. 2514, z późn. zm. - § 43 i n.),
3. uzasadnienie do rozporządzenia Ministra Sprawiedliwości z dnia 28 grudnia 2017 r. zmieniającego rozporządzenie - Regulamin urzędowania sądów powszechnych (Dz.U. z 2017 r. poz. 2481; str. 35 i n.).

Ponadto Minister Sprawiedliwości wskazał, że opublikował w Biuletynie Informacji Publicznej algorytm SLPS, tj. szczegółowy opis, w jaki sposób SLPS losuje składy orzekające do spraw sądowych (https://www.gov.pl/web/sprawiedliwość/algorytm). Udostępnił też on-line wyszukiwarkę raportów z SLPS wraz z wyjaśnieniem treści raportu pełnego z przydziału sprawy przez SLPS: https: / / www.gov.pl/web /sprawiedliwosc/wyszukiwarka-raportow-z-systemu-losowego-przydzialu-spraw, co pozwala każdej zainteresowanej osobie pobranie raportu z losowania przeprowadzonego w dowolnej sprawie sądowej i zapoznanie się z wynikiem i parametrami losowania.

Minister zaznaczył, że zadania z zakresu administrowania SLPS realizuje Sąd Apelacyjny w Białymstoku zapewniając też wsparcie użytkownikom SLPS we wszystkich sądach (§ 2 zarządzenia Ministra Sprawiedliwości z dnia 29 lipca 2022 r. w sprawie powierzenia sądom apelacyjnym wykonywania czynności związanych z projektowaniem, wdrażaniem i utrzymywaniem systemów teleinformatycznych - Dz. Urz. Min. Sprawiedliwości z 2022 r. poz. 155).

Użytkownikami SLPS są upoważnieni pracownicy poszczególnych sądów powszechnych, którzy działają w rolach Administratora Lokalnego (organizacyjnie powiązany z funkcją przewodniczącego wydziału) i Pracownika Sekretariatu (organizacyjnie powiązany z funkcją kierownika sekretariatu) w poszczególnych wydziałach sądów. Pozostali (wszyscy) pracownicy sądów powszechnych, załogowani do SLPS z komputera pracującego w sieci sądowej („Podgląd SLPS") mają z kolei możliwość bezpośredniego zweryfikowania wszystkich wpisów w SLPS, w tym zastosowanych parametrów, w każdym wydziale każdego sądu w Polsce oraz nieograniczony dostęp do raportów pełnych z losowania.

Prezesi sądów sprawują nadzór nad pracą ww. osób, w szczególności badają prawidłowość przydzielania sędziom, asesorom sądowym i referendarzom sądowym spraw oraz równomiernego obciążenia ich pracą (art. 37 b § 1 pkt 3 ustawy - Prawo o ustroju sądów powszechnych Dz. U. z 2023 r. poz. 217, z późn. zm.).

Organ podał, że według słownika pojęć informatycznych, kod źródłowy, często nazywany „źródłem" programu, zawiera deklaracje zmiennych, instrukcje, funkcje, pętle i inne instrukcje, które informują program, jak ma działać (https://tech-lib.net/definition/sourcecode.html). Innymi słowy kod źródłowy to szczegółowe instrukcje napisane przez programistę przy wykorzystaniu danego języka programowania, których wykonanie przez komputer prowadzi do prezentacji wyników operacji na dostępnych danych.

Programiści (podmioty tworzące oprogramowanie) na całym świecie chronią kody źródłowe, jako swoją tajemnicę i własność. Wyjątkiem są oprogramowania typu open source, tj. oprogramowania, których kod źródłowy jest dostępny dla użytkowników, którzy mogą go w dowolny sposób analizować, modyfikować oraz dalej rozpowszechniać.

Dostęp do kodu źródłowego pozwala na poznanie dokładnej budowy wszystkich elementów systemu, a przede wszystkim na wykonywanie w nim zmian np. poprzez dodanie nowych elementów lub usunięcie dotychczasowych fragmentów, modyfikację sposobu działania programu i jego funkcjonalności, kontrolowanie sposobu używania programu przez innych użytkowników, jego dowolnego rozpowszechniania, modyfikację mechanizmów zapewniających bezpieczeństwo programu.

Kod źródłowy SLPS składa się z sekwencji blisko trzech milionów linijek instrukcji, poleceń i innego rodzaju informacji technicznych, w tym haseł i loginów użytkowników systemu zapisanych w języku programowania.

Wysoki stopień skomplikowania kodu jest adekwatny do stopnia zaawansowania technologicznego aplikacji SLPS.

Kod źródłowy SLPS jest dostępny wyłącznie dla upoważnionych administratorów SLPS. „Szeregowi" pracownicy sądów, a także osoby trzecie spoza sądów nie mają do niego dostępu. Programiści i administratorzy SLPS ocenili, że nie istnieje bezpieczny sposób na udostępnienie kodu źródłowego podmiotowi zewnętrznemu w trybie dostępu do informacji publicznej (Stowarzyszenie oczekuje udostępnienia kodu poprzez e-mail).

Specjaliści wskazali na bardzo poważne ryzyko bezpośrednie i ryzyko pośrednie ewentualnego udostępnienia kodu źródłowego, tj. o powstanie niedopuszczalnej sytuacji, w której organy państwa nie są w stanie zagwarantować autentyczności, bezpieczeństwa i rzetelności programu informatycznego, który służy celom publicznym. Dostęp do kodu

źródłowego w połączeniu ze znajomością algorytmu SLPS (algorytm został opublikowany w BIP) oznacza możliwość zdalnego wejścia do tego programu bez konieczności dostępu do infrastruktury SLPS. Takie niekontrolowane wejście zostałoby rozpoznane przez systemy bezpieczeństwa, jako wejście użytkownika z wewnątrz organizacji (a nie jako atak z zewnątrz) i potencjalnie nie zostałoby w związku z tym powstrzymane.

Podmiot zewnętrzny mógłby w sposób nieograniczony zmieniać kod, co także mogłoby nie zostać zasygnalizowane administratorom. Następnie SLPS ze zmienionym kodem mógłby być dalej rozpowszechniany (w kraju i za granicą) pod pozorem, że jest to autentyczny program, z którego korzystają polskie sądy.

Modyfikacje mogłyby objąć obszar sposobu losowania przez program składów orzekających, a zatem wpłynąć na przebieg konkretnych postępowań sądowych.

Żaden z dostępnych mechanizmów prawnych, czy faktycznych nie pozwala na kontrolowanie przez organ sposobu postępowania z kodem źródłowym po jego udostępnieniu. Ministerstwo nie mogłoby zatem interweniować w przypadku niewłaściwego przechowywania kodu np. na urządzeniach, które nie zostały wyposażone w odpowiednie systemy bezpieczeństwa, czy w przypadku przesyłania kodu kanałami podatnymi na ataki hakerskie.

W związku z powyższym udostępnienie kodu źródłowego może doprowadzić do skutecznego cyberataku na SLPS (także całkowicie poza świadomością wnioskodawcy, który byłby w posiadaniu kodu). W kodzie oprócz logiki działania SLPS, jego architektury i konfiguracji, a także integracji z innymi systemami sądowymi, zapisane zostały również mechanizmy zapewniające bezpieczeństwo aplikacji, a więc m.in. zabezpieczenia, z których korzysta system w celu prawidłowej autoryzacji/uwierzytelnienia użytkowników podczas logowania do systemu. Z tego względu ryzyko potencjalnego nieuprawnionego ataku na SLPS specjaliści określili jako realne i bardzo wysokie.

W ich ocenie potencjalne ułatwienie osobom atakującym zrozumienia kodu źródłowego SLPS i wykorzystania tej wiedzy do poszukiwania podatności systemu na atak niesie m.in. ryzyko manipulowania działaniem SLPS w celu wpłynięcia na losowy proces przydziału spraw, a w konsekwencji umożliwienie kontrolowania przebiegu postępowań sądowych.

Oznacza również możliwość wprowadzenia zmian w programie, które zdestabilizują albo zablokują jego działanie, wprowadzając zakłócenia w pracy sądów.

Potencjalna identyfikacja podatności w infrastrukturze sieciowej lub protokołach komunikacyjnych, które są wykorzystywane przez program, może prowadzić do ataków

powodujących zakłócenie, opóźnienie lub całkowite zawieszenie przeprowadzania spraw sądowych, w szczególności poprzez wprowadzanie złośliwego kodu, tj. skryptów lub instrukcji do przesyłanych danych, co może prowadzić do uruchomienia nieautoryzowanych operacji lub naruszenia bezpieczeństwa systemu.

Realną pozostaje także możliwość celowego przeciążania SLPS tzw. atak DDoS, gdy atakujący może konfigurować automaty\roboty i wysyłać automatycznie ogromne ilości żądań do programu, co prowadzi do przeciążenia sieci i uniemożliwia prawidłowe funkcjonowanie systemu lub całkowitą jego niedostępność i może doprowadzić do sparaliżowania funkcjonowania wymiaru sprawiedliwości.

Atakujący mogliby również podjąć próbę przechwycenia danych w trakcie komunikacji tzw. atak typu Man-in-the-Middle, tj. przechwycenie i manipulowanie komunikacją między dwiema stronami, w tym podmiany przesyłanych danych lub wprowadzanie zmian, które zakłócą prawidłowe funkcjonowanie SLPS.

Ryzyka pośrednie związane z udostępnieniem kodu źródłowego wynikają z faktu, że SLPS w celu prawidłowego działania został zintegrowany (ściśle połączony) z innymi systemami teleinformatycznymi wymiaru sprawiedliwości.

Taka konfiguracja systemów informatycznych powoduje, że potencjalny atak na jeden z nich otwiera możliwość ataku na pozostałe. Sytuację tę można zobrazować poprzez metaforę budynku, przy założeniu, że budynkiem jest infrastruktura teleinformatyczna resortu sprawiedliwości, a pomieszczeniami są poszczególne systemy/aplikacje. Jeżeli podmiot nieuprawniony wejdzie do sieci wewnętrznej, to tak jakby znalazł się wewnątrz budynku, a tym samym miał ułatwiony dostęp do poszczególnych pomieszczeń (systemów/aplikacji). Chodzi przede wszystkim o Zintegrowany System Rachunkowości i Kadr (ZSRK), w którym przechowywane są dane osobowe, w tym dane wrażliwe wszystkich osób zatrudnionych w sądach powszechnych (ok. 56 tysięcy osób). Z kolei ZSRK jest połączony m.in. z systemem bankowym NBP oraz platformą e-płatności Resortu Sprawiedliwości. Przedostanie się do infrastruktury sieciowej za pośrednictwem SLPS, przez ZSRK i e-Płatności może umożliwić przejęcie kontroli nad takimi systemami jak Krajowy Rejestr Sądowy, Księgi Wieczyste, Rejestr Zastawów, Krajowy Rejestr Zadłużonych, Elektroniczne Postępowanie Upominawcze, Aplikacja Funduszu Sprawiedliwości, Nieodpłatna Pomoc Prawna i wiele innych oraz całkowicie sparaliżować ich działanie, a także uzyskać nieuprawniony dostęp do danych osobowych milionów obywateli. Zwłaszcza, że ww. systemy są powiązane z Bazą PESEL, której administratorem jest Ministerstwo Cyfryzacji.

Udostępnienie kodu źródłowego SLPS oznacza zatem realny i najwyższy stopień zagrożenia infrastruktury teleinformatycznej resortu sprawiedliwości i państwa.

Organ zaznaczył, że opisane zagrożenia mogą w przyszłości dotyczyć także kolejnych olbrzymich baz danych, ponieważ w planach rozwoju SLPS znajduje się integracja SLPS z systemami repertoryjno-biurowymi (SRB), które funkcjonują w sądach powszechnych i zapewniają obsługę biurową wszystkich postępowań sądowych. W SRB znajdują się dane osobowe stron postępowań (miliony obywateli), dokumenty wewnętrzne, projekty orzeczeń (jeszcze przed publikacją), informacje finansowe dotyczące postępowania itp.

Potencjalny atak na opisane systemy teleinformatyczne państwa jest tym bardziej realny, że na dzień wydania niniejszej decyzji na terenie całego kraju obowiązuje podwyższony stopień alarmowy. Obecnie jest to trzeci stopień alarmowy CRP (CHARLIE-CRP) oraz drugi stopień alarmowy BRAVO. Stopnie alarmowe CRP dotyczą zagrożenia w cyberprzestrzeni. CHARLIE-CRP jest trzecim z czterech stopni alarmowych określonych w ustawie o działaniach antyterrorystycznych i jest wprowadzany w przypadku wystąpienia zdarzenia potwierdzającego prawdopodobny cel ataku o charakterze terrorystycznym w cyberprzestrzeni albo uzyskania wiarygodnych informacji o planowanym zdarzeniu. Stopień alarmowy BRAVO (drugi w czterostopniowej skali) wprowadza się w przypadku zaistnienia zwiększonego i przewidywalnego zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym. Oznacza to, że służby mają informację o potencjalnym zagrożeniu, a w związku z tym administracja publiczna jest zobowiązana do zachowania szczególnej czujności (https: / Zwww.gov.pl/web/rcb/przedluzenie-obowiazywania- stopni-alarmowych-do-30-listopada-2023-r).

Z uwagi na znaczenie SLPS dla bezpieczeństwa systemów teleinformatycznych państwa oraz potrzebę zapewnienia prawidłowej realizacji ustawowego zadania losowego przydziału spraw sądowych, zarówno kod źródłowy, jak i infrastruktura związana z SLPS zostały objęte najwyższą ochroną.

Źródeł tej ochrony, zarówno systemowej, jak i fizycznej, należy poszukiwać zarówno w aktach prawnych powszechnie obowiązujących, jak i aktach wewnętrznych wprowadzonych specjalnie w celu ochrony systemów teleinformatycznych wymiaru sprawiedliwości. Przepisy te nakładają na Ministra Sprawiedliwości i inne podmioty zaangażowane w obsługę SLPS konkretne obowiązki.

W pierwszej kolejności wskazać należy na ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących działania publiczne określającą

wymagania dla systemów teleinformatycznych, które służą do realizacji zadań publicznych i obliguje podmioty publiczne, które używają tych systemów, aby zapewniały spełnienie i utrzymanie tych wymagań (art. 13 ust. 1 i 2). Systemy teleinformatyczne podlegają kontroli pod względem spełniania wymogów ustawowych. Kontrola odbywa się w trybie i na zasadach określonych w ustawie z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. z 2020 r. poz. 224).

Aktem wykonawczym do ww. ustawy jest rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2017 r. poz. 2247), zgodnie z którym systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk (§ 15 ust. 1). Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej (§16 ust. 1). Podmiot realizujący zadania publiczne jest zobowiązany zapewnić poufność, dostępność i integralność informacji przetwarzanych w systemach teleinformatycznych z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. W tym celu m.in. opracowuje i doskonali system zarządzania bezpieczeństwem informacji (§20 ust. 1). Podmiot publiczny jest również zobowiązany m.in. do zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami oraz do zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach, teleinformatycznych, polegającego w szczególności na zapewnieniu bezpieczeństwa plików systemowych, redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych, a także na ochronie systemów teleinformatycznych przed ich utratą i nieuprawnioną modyfikacją (§20 ust. 2 pkt 7 i 12).

Jeśli w systemie informatycznym odbywa się przetwarzanie danych osobowych (tak jak w przypadku SLPS) do ich ochrony znajduje zastosowanie ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) oraz 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, Dz. Urz. UE L119 z 4.05.2016 r.; RODO).

W myśl art. 5 ust. 1 i 2 rozporządzenia, dane osobowe m.in. muszą być przetwarzane zgodnie z prawem, w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. Administrator danych osobowych jest odpowiedzialny za przestrzeganie ww. zasad i musi być w stanie wykazać ich przestrzeganie.

Uwzględniając charakter, zakres, kontekst, i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać (art. 24 rozporządzenia).

Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku szyfrowanie danych osobowych, zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego oraz regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych (art. 32 ust. 1 i 2 rozporządzenia).

Niezależnie od aktów prawnych powszechnie obowiązujących, organ jest zobowiązany do stosowania szeregu zasad bezpieczeństwa wprowadzonych przez uregulowania wewnętrzne. Do najważniejszych należą: Polityka Bezpieczeństwa Informacji Ministerstwa Sprawiedliwości, Polityka Bezpieczeństwa Systemów Teleinformatycznych Ministerstwa Sprawiedliwości, Regulamin użytkownika Systemów Teleinformatycznych

Ministerstwa Sprawiedliwości, Polityka Bezpieczeństwa Danych Osobowych Ministerstwa Sprawiedliwości. Przewidują one szczegółowe zasady postępowania w zakresie fizycznej ochrony infrastruktury informatycznej (wydzielenie bezpiecznych pomieszczeń, w których zlokalizowana jest infrastruktura systemów teleinformatycznych, całodobowy monitoring pomieszczeń, fizyczna kontrola dostępu pracowników do ww. pomieszczeń etc.), kontrolę dostępu do systemów (w tym zabezpieczenia kryptograficzne, zarządzanie uprawnieniami użytkowników, dostęp administracyjny, zasady dostępu zdalnego etc.), zarządzanie incydentami bezpieczeństwa, zarządzanie ciągłością działania itd.

Wojewódzki Sąd Administracyjny w Warszawie w wyroku wydanym w niniejszej sprawie zwrócił uwagę także na brzmienie art. 4 ust. 1 ustawy o ochronie informacji niejawnych, zgodnie z którym informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo wykonywania czynności zleconych.

Sąd podkreślił, że wymóg ten odnosi się do informacji niejawnych w ogóle, a nie tylko tych, którym nadano klauzulę tajności. Wystarczy zatem element materialny, tzn. istnienie takiej cechy, przez którą stanowi ona informację, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo, byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania.

W pełni podzielając pogląd Sądu należy zauważyć, że w świetle przedstawionej powyżej charakterystyki SPS oraz jego kodu źródłowego, a także zważywszy na skomplikowany system powiązań SLPS z innymi systemami teleinformatycznymi wymiaru sprawiedliwości i państwa, nie może budzić wątpliwości, iż posiadają one wszystkie cechy, z powodu których, zgodnie z ustawą, ich nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne. To pozwala uznać kod za informację podlegającą reżimowi przewidzianemu dla ochrony informacji niejawnych (por. m.in. wyroki NSA: z 19 października 2017 r. sygn. akt I OSK 1822/16, z 28 kwietnia 2016 r. sygn. akt I OSK 2620/14).

Udostępnienie kodu źródłowego byłoby zagrożeniem realnym najwyższego stopnia, stanowiącym możliwość wyrządzenia szkody określonej w ustawie o ochronie informacji niejawnych.

Już samo ryzyko związane z przechowywaniem przez wnioskodawcę kodu na urządzeniach, które nie posiadają zabezpieczeń wymaganych dla infrastruktury krytycznej

państwa, powoduje, że osoby potencjalnie zainteresowane kompleksowym rozpoznaniem systemów teleinformatycznych RP (cyberprzestępcy) będą w stanie pozyskać kod. Tak, jak wyjaśniono, dostęp do kodu w połączeniu ze znajomością jawnego algorytmu pozwala na wejście do oprogramowania SLPS, a za jego pośrednictwem do innych systemów państwa, w tym Krajowego Rejestru Sądowego, Ksiąg Wieczystych, systemu e-Płatności i bazy PESEL. Daje to też możliwość ingerencji w prace polskiego wymiaru sprawiedliwości, a nawet jego paraliż poprzez całkowite zablokowanie SLPS, czy ZSRiK.

W sytuacji więc, gdy ujawnienie żądanej informacji godziłoby w interes wymiaru sprawiedliwości i bezpieczeństwo publiczne, uprawnienie jednostki do dostępu do informacji publicznej musi podlegać ograniczeniu.

Prawna podstawa ograniczenia prawa do informacji publicznej wynika zarówno z Konstytucji RP, jak i u.d.i.p.

W myśl art. 5 ust. 1 i 2 u.d.i.p., prawo do informacji publicznej podlega ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych. Prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. W obliczu zagrożeń jakie niosą współcześnie dla państwa i obywateli organizacje terrorystyczne, organizacje przestępcze, hakerzy etc., kwalifikacja wniosku Stowarzyszenia przez pryzmat ww. norm wymaga szczególnego podejścia, uwzględniającego nie tylko wiedzę powszechną, ale również specjalistyczną.

Jak w niniejszej sprawie wskazał Wojewódzki Sąd Administracyjny w Warszawie, art. 5 u.d.i.p. nie zawiera wyczerpującego katalogu przyczyn, które w konkretnej sprawie mogą uzasadniać konieczność ograniczenia dostępu do informacji wytworzonych, odnoszących się, czy będących w posiadaniu podmiotów publicznych. Istnieją bowiem również inne, niż wymienione w tym przepisie ustawowym, wartości, których ochrona uzasadnia - w świetle art. 61 ust. 3 Konstytucji RP - zastosowanie tego typu ograniczeń.

Jak wyjaśniono powyżej kod źródłowy podlega reżimowi ochrony przewidzianemu dla informacji niejawnych (art. 5 ust. 1 u.d.i.p.). Kod źródłowy, ale też oprogramowanie SLPS i inne zintegrowane z nim systemy teleinformatyczne wymiaru sprawiedliwości i państwa przetwarzają miliony danych osobowych polskich obywateli, w tym danych wrażliwych. Zatem otwarcie dostępu do kodu stanowiłoby poważne naruszenie zasad związanych z przetwarzaniem danych osobowych, a tym samym naruszałoby prawo do prywatności tych osób (art. 5 ust. 2 u.d.i.p.). Kod źródłowy, jako autorski projekt Ministerstwa Sprawiedliwości, spełnia również wszelkie przesłanki pozwalające na zakwalifikowanie go, poprzez analogię,

jako tajemnicę w rozumieniu art. 5 ust. 2 u.d.i.p. Przypomnieć należy, że norma ta dotyczy informacji technicznych, technologicznych, organizacyjnych lub innych informacji posiadających wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności (art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji Dz. U. z 2022 r. poz. 1233).

Ministerstwo Sprawiedliwości podejmuje wszelkie prawem przewidziane działania zorientowane na utrzymanie bezpieczeństwa kodu źródłowego i jego poufności, co zostało wyjaśnione powyżej. Ponadto SLPS jest systemem transparentnym dla obywateli. Zasady jego działania zostały opisane w dokumentach powszechnie dostępnych (wymienionych na wstępie), a w domenie publicznej dostępny jest algorytm aplikacji, zaś każda zainteresowana osoba może za pośrednictwem wyszukiwarki on-line pobierać raporty z losowań przeprowadzonych przez SLPS we wszystkich sprawach.

W ocenie Ministra kod źródłowy SLPS spełnia wszystkie prawem przewidziane przesłanki do uznania, iż prawo do jego udostępnienia podlega ograniczeniu z uwagi na dobro wymiaru sprawiedliwości i bezpieczeństwo publiczne. U.d.i.p. nie przewiduje mechanizmu, który pozwoliłyby czuwać nad bezpieczeństwem informacji po jej udostępnieniu. W konsekwencji organ odpowiedzialny za bezpieczeństwo, integralność i nienaruszalność SLPS utraciłyby jakąkolwiek kontrolę nad tym kto aktualnie posiada dostęp do kodu źródłowego i jakie operacje na nim przeprowadza. Z kolei próba „pozbawienia" kodu, na potrzeby udostępnienia, wszystkich niezbędnych z punktu widzenia bezpieczeństwa fragmentów (m.in. zapisanych w kodzie loginów i haseł użytkowników systemu) byłaby zadaniem niewykonalnym z uwagi na jego złożoną strukturę (blisko 3 min linijek kodu). Kod stałby się całkowicie nieczytelny, utraciłby walor nośnika wiarygodnych informacji o SLPS.

W związku z powyższym w czasie podwyższonego zagrożenia atakami o charakterze terrorystycznym w cyberprzestrzeni, należało wydać decyzję o odmowie udostępnienia kodu źródłowego.

Pismem z dnia 22 listopada 2023 r. Stowarzyszenie skierowało do Wojewódzkiego Sądu Administracyjnego w Warszawie skargę na decyzję Ministra Sprawiedliwości z 16 października 2023 r. nr BK-IV.082.270.2022 o odmowie udostępnienia informacji publicznej wnosząc o stwierdzenie jej nieważności, ewentualnie o uchylenie oraz

o zasądzenie kosztów postępowania, w tym kosztów zastępstwa procesowego, wedle norm przepisanych.

Zaskarżonemu rozstrzygnięciu zarzuciło naruszenie:

1) przepisów postępowania, co mogło mieć istotny wpływ na wynik sprawy:
   a) art. 10 § 1 K.p.a. poprzez zaniechanie zapewnienia czynnego udziału w każdym stadium postępowania i wypowiedzenia się co do zebranych dowodów i materiałów i zgłoszonych żądań,
   b) art. 84 § 1 K.p.a. poprzez zaniechanie powołania biegłego z zakresu architektury programów komputerowych oraz cyberbezpieczeństwa,
   c) art. 7 K.p.a., art. 77 § 1 K.p.a., art. 80 K.p.a. i art. 107 § 3 K.p.a. poprzez zaniechanie przez organ dokonania prawdziwych ustaleń faktycznych co do treści i charakteru wnioskowanej informacji publicznej,
   d) art., 107 § 1 pkt 4 K.p.a. poprzez podanie nieznanej prawu podstawy prawnej,
2) przepisów prawa materialnego:
   a) art. 5 ust. 1 u.d.i.p. w związku z art. 13 ust. 1 i 2 ustawy o informatyzacji działalności podmiotów realizujących działania publiczne poprzez ich zastosowanie, chociaż nie stanowią one przepisów o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych, a więc nie mogą stanowić podstawy do odmowy udostępnienia informacji publicznej,
   b) art. 5 ust. 1 i 2 u.d.i.p. w związku z art. 5 ust. 1 i 2 RODO, 24 RODO i art. 32 ust. 1 i 2 RODO poprzez ich zastosowanie, chociaż nie stanowią one przepisów o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych ani samodzielnej podstawy do odmowy udostępnienia informacji publicznej, a więc nie mogą stanowić podstawy do odmowy udostępnienia informacji publicznej,
   c) art. 5 ust. 1 i 2 u.d.i.p. poprzez odmówienie udostępnienia informacji publicznej w sytuacji, gdy żadna z przesłanek wymienionych w powołanych przepisach nie zaistniała.

W uzasadnieniu skargi Stowarzyszenie wskazało, że organ przedłużył termin na rozpoznanie wniosku powołując się na konieczność pogłębionej analizy wytycznych Wojewódzkiego Sądu Administracyjnego w Warszawie zawartych w uzasadnieniu wyroku z 24 lutego 2023 r. sygn. akt II SA/Wa 1785/22. Skoro zatem Minister prowadził analizy, to powinien był umożliwić stronie skarżącej zapoznanie się ze zgromadzonym w sprawie materiałem dowodowym, zgodnie z art. 10 § 1 K.p.a. Wymóg ten w niniejszej sprawie ma

o tyle istotne znaczenie, że w toku postępowania przed Wojewódzkim Sądem Administracyjnym w Warszawie w sprawie o sygn. akt II SA/Wa 1785/22 strona skarżąca składała do akt prywatną ekspertyzę dotyczącą kluczowych w postępowaniu kwestii technicznych związanych z kodem źródłowym. Ze znanych sobie względów organ odstąpił od powiadomienia Stowarzyszenia o możliwości zapoznania się ze zgromadzonym materiałem dowodowym.

W ocenie strony skarżącej fakt złożenia na etapie postępowania sądowoadministracyjnego ekspertyzy dotyczącej złożonych kwestii technicznych powinna skłonić organ do powołania w toku postępowania biegłego z zakresu architektury programów komputerowych oraz cyberbezpieczeństwa. Do wyjaśnienia sprawy potrzebne są wiadomości specjalne, których organ nie posiada, bowiem nie ma w tym zakresie stosownej wiedzy technicznej.

Stowarzyszenie podkreśliło, że organ odmawiając udostępnienia wnioskowanej informacji publicznej powołuje się na fakt, iż kod źródłowy programu komputerowego jest integralnie połączony z innymi krytycznymi dla funkcjonowania Państwa programami i systemami komputerowymi. Jest to twierdzenie jeśli nie gołosłowne, to przynajmniej nieuzasadnione. Nie wskazuje jednak, które części kodu źródłowego odpowiadają za takie połączenia. Co więcej, Minister pomija dotychczasowy przebieg postępowania w sprawie i popada w sprzeczność ze swoim wcześniejszym stanowiskiem. Otóż, jak zauważył Naczelny Sąd Administracyjny w wyroku w sprawie sygn. akt III OSK 1189/21, organ twierdził, iż już ujawnienie algorytmu SLPS stanowi zagrożenie dla cyberbezpieczeństwa państwa. Tymczasem nie tylko algorytm został opublikowany bez szkód dla cyberbezpieczństwa państwa, ale i organ zaczął wskazywać fakt jego publikacji jako przemawiający za zasadnością odmowy udostępnienia kodu źródłowego. Przypomnieć też należy, co nie umknęło Naczelnemu Sądowi Administracyjnemu w sprawie sygn. akt III OSK 1189/21, że kod źródłowy stanowi realizację algorytmu w języku zrozumiałym dla komputerów. Innymi słowy w kodzie źródłowym programu komputerowego nie ma miejsca dla jakichkolwiek dodatków w rodzaju loginów, haseł czy danych osobowych, jak próbuje to przedstawić organ. W ramach informatyki istnieją takie pojęcia jak biblioteki, czy bazy danych, do których poszczególne programy komputerowe (zapisane kodem źródłowym) mogą „sięgać". Kod źródłowy opisuje w jaki sposób program komputerowy „sięga" do takiej bazy danych, jak zapisuje pobrane dane i w jaki sposób je przetwarza, natomiast sam tych danych nie zawiera. Równocześnie opisanie w kodzie źródłowym i ujawnienie tego sposobu importowania danych nie przesądza samo w siebie o zagrożeniu cyberbezpieczeństwa,

bowiem, jak można przypuszczać, krytyczne dla państwa systemy komputerowe są fizycznie oddzielone od ogólnodostępnego Internetu, zaś same bazy danych są zabezpieczone przed nieuprawnionym dostępem.

Ponadto Stowarzyszenie zaznaczyło, że decyzja została wydana z rażącym naruszeniem prawa, względnie bez podstawy prawnej, co powinno skutkować stwierdzeniem jej nieważności. W sentencji jako podstawę jej wydania podano art. 5 ust. 1 i 2 u.d.i.p. i art. 16 ust. 1 i 2 u.d.i.p. oraz przepisy ustawy o informatyzacji działalności podmiotów realizujących działania publiczne i RODO. Przepis art. 5 ust. 1 u.d.i.p. jest przepisem odsyłającym i nie może stanowić samodzielnej podstawy do wydania decyzji o odmowie udostępnienia informacji publicznej. Powołane przez organ przepisy prawa materialnego nie stanowią o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych, a zatem nie stanowią podstawy do odmowy udostępnienia informacji publicznej. Organ w uzasadnieniu rozstrzygnięcia nie wskazał prywatność jakich to osób fizycznych lub jakie to tajemnice przedsiębiorcy usprawiedliwiałyby wydanie decyzji odmownej. Wniosek o rozpoznanie sprawy poza kolejnością wynika z dwóch okoliczności. Po pierwsze, zgodnie z art. 21 pkt 2 u.d.i.p. skargi dotyczące dostępu do informacji publicznej rozpoznaje się w terminie 30 dni od wpływu skargi wraz z odpowiedzią na skargę. Terminu tego, przy obecnym obłożeniu Sądu, nie sposób dochować przy zachowaniu zwykłej kolejności rozpoznawania spraw. Po drugie, sprawa dotyczy wniosku sprzed 6 lat, co winno skutkować jej priorytetowym potraktowaniem.

W odpowiedzi na skargę Minister Sprawiedliwości wniósł o oddalenie skargi, podtrzymując argumentację zawartą w zaskarżonej decyzji.

Wojewódzki Sąd Administracyjny w Warszawie zważył, co następuje:

Stosownie do treści art. 1 ustawy z dnia 25 lipca 2002 r. – Prawo o ustroju sądów administracyjnych (t.j. Dz. U. z 2024 r. poz. 1267), sądy administracyjne sprawują wymiar sprawiedliwości poprzez kontrolę działalności administracji publicznej pod względem zgodności z prawem zaskarżonej decyzji administracyjnej. Jest więc to kontrola legalności rozstrzygnięcia zapadłego w postępowaniu administracyjnym, z punktu widzenia jego zgodności z prawem materialnym i procesowym.

Oceniając przedmiotową decyzję według powyższych kryteriów, uznać należy, że skarga nie zasługuje na uwzględnienie.

W pierwszej kolejności zwrócić należy uwagę, iż Minister Sprawiedliwości, mając na względzie obowiązek wynikający z art. 153 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz. U. z 2024 r. poz. 935); dalej jako P.p.s.a., był związany oceną prawną dokonaną przez Wojewódzki Sąd Administracyjny w Warszawie z 24 lutego 2023 r. sygn. akt II SA/Wa 1785/22 33/22 w uzasadnieniu wyroku, w którym stwierdzono, że Minister nie wykazał przesłanek ograniczających dostęp do wnioskowanej informacji publicznej wynikających z przepisów o ochronie informacji niejawnych, jak też przepisów o ochronie innych tajemnic ustawowo chronionych, o których mowa w art. 5 ust. 1 u.d.i.p. Również nie wyjaśnił powodów ograniczenia prawa do wnioskowanej informacji, które by wynikały z art. 5 ust. 2 u.d.i.p. Tym samym naruszył przepisy prawa materialnego i procesowego, w szczególności poprzez skonstruowanie uzasadniania decyzji w sposób nieopowiadający wymogom art. 107 § 3 K.p.a.

Realizując powyższe wytyczne Sądu organ w uzasadnieniu zaskarżonej decyzji w sposób przekonywujący przedstawił argumentację, która legła u podstaw podjętego rozstrzygnięcia.

Oceniając zaskarżoną decyzję pod względem jej zgodności z prawem należy wyjść od tego, że Konstytucja Rzeczypospolitej Polskiej w art. 61 ust. 1 gwarantuje obywatelowi prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Prawo to obejmuje również uzyskiwanie informacji o działalności organów samorządu gospodarczego i zawodowego, a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa. Prawo do uzyskiwania informacji obejmuje dostęp do dokumentów oraz wstęp na posiedzenia kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów, z możliwością rejestracji dźwięku lub obrazu (art. 61 ust. 2 Konstytucji RP). Ograniczenie prawa, o którym mowa w ust. 1 i 2, może nastąpić wyłącznie ze względu na określone w ustawach ochronę wolności i praw innych osób i podmiotów gospodarczych oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa (art. 61 ust. 3 Konstytucji RP).

Dostęp do informacji publicznej nie ma charakteru absolutnego i może być ograniczony, gdyby ujawnienie pewnych informacji zagrażałoby interesom państwa, a pośrednio także interesom wszystkich obywateli. Z tej przyczyny w art. 5 u.d.i.p. zostały wskazane ograniczenia w dostępie do informacji publicznej.

W sprawie tej, wbrew zarzutom skargi, nie doszło do naruszenia przepisu art. 5 ust. 1 u.d.i.p. i art. 61 Konstytucji RP.

Zgodnie z art. 5 ust. 1 u.d.i.p. prawo do informacji publicznej podlega ograniczeniu w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych. Zgodnie z art. 4 ust. 1 u.o.i.n, informacje niejawne mogą być udostępnione wyłącznie osobie dającej rękojmię zachowania tajemnicy i tylko w zakresie niezbędnym do wykonywania przez nią pracy lub pełnienia służby na zajmowanym stanowisku albo wykonywania czynności zleconych. Wymóg ten odnosi się do informacji niejawnych w ogóle, a nie tylko tych, którym nadano klauzulę tajności.

Podkreślenia wymaga, że dla takiej ochrony wystarczy element materialny, tzn. istnienie takiej cechy, przez którą stanowi ona informację, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania (art. 1 u.o.i.n.).

W orzecznictwie sądowoadministracyjnym ugruntowany jest pogląd, iż informacja niejawna chroniona jest bez względu na to, czy oznaczona została odpowiednią klauzulą. Informacja jest bowiem niejawna z uwagi na zagrożenia wynikające z jej treści lub sposobu jej uzyskania, a nie w wyniku klasyfikacji i klauzulowania (patrz wyroki NSA: z 21 września 2012 r. sygn. akt I OSK 1393/12, z 18 sierpnia 2015 r. sygn. akt I OSK 1679/14, publik. orzeczenia.nsa.gov.pl). Sąd rozpatrujący niniejszą sprawę pogląd ten podziela.

Raz jeszcze podkreślenia wymaga, że istnienie elementu materialnego informacji niejawnych można ustalić na podstawie art. 1 ust. 1 u.o.i.n., bez potrzeby odnoszenia się do art. 5 tej ustawy, albowiem poszczególne przepisy tego artykułu, nie tworzą dodatkowej definicji pojęcia informacji niejawnych, lecz stanowią szczegółowe rozwinięcie zdefiniowanego w art. 1 ust. 1 u.o.i.n. tego pojęcia, służące celom odpowiedniego zakwalifikowania w zakresie stopnia ochrony tychże informacji, a nie samej potrzeby ich ochrony (v. wyrok NSA z 2 lutego 2018 r. sygn. akt I OSK 668/16, orzeczenia.nsa.gov.pl).

Sąd, po zapoznaniu się z aktami sprawy stwierdził, że organ uprawniony był w tej sprawie do zastosowania art. 5 ust. 1 u.d.i.p. i ograniczenia dostępu do kodu źródłowego oprogramowania o nazwie System Losowego Przydziału Spraw (SLPS) z powołaniem się na ochronę informacji niejawnych.

Minister trafnie wskazał, że spełniony został w tej sprawie element materialny, tj. żądany dokument posiada cechy informacji, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby

z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania (art. 1 u.o.i.n.). W obszernej argumentacji decyzji organ przedstawił zasady działania oprogramowania o nazwie SLPS, środowisko teleinformatyczne i infrastrukturalne w jakim funkcjonuje ten program, dostępności do programu i zasady sprawowania nadzoru nad korzystaniem programu, podkreślając przy tym, iż kod źródłowy jest wyłącznie dostępny dla upoważnionych administratorów SLPS. Pracownicy sądów nieodpowiadających za bezpieczeństwo systemów informatycznych oraz osoby postronne nie mają dostępu do przedmiotowego kodu. Programiści i administratorzy SLPS ocenili, że nie istnieje bezpieczny sposób na udostępnienie kodu źródłowego podmiotowi zewnętrznemu w trybie dostępu do informacji publicznej. Dostęp do kodu źródłowego w połączeniu ze znajomością algorytmu SLPS (ujawnionego w BIP) umożliwiłby niekontrolowane zdalne wejścia do tego programu bez konieczności dostępu do infrastruktury SLPS. Nieautoryzowane wejście zostałoby rozpoznane przez systemy bezpieczeństwa, jako wejście użytkownika z wewnątrz organizacji (a nie jako atak z zewnątrz) i potencjalnie nie zostałoby w związku z tym powstrzymane. Wiązałoby się z ryzykiem zmiany kodu, utratą jego autentyczności, bezpieczeństwa i rzetelności programu informatycznego, który służy celom publicznym. Potencjalny cyberatak, przy znajomości kodu źródłowego, umożliwiłby ingerowanie w SLPS, łącznie z wprowadzeniem zmian w programie, jego zablokowanie i zakłócenie pracy sądów powszechnych w skali całego kraju (SLPS został zintegrowany z innymi systemami teleinformatycznymi wymiaru sprawiedliwości). Zatem udostępnienie kodu źródłowego w przestrzeni publicznej stwarzałoby realne zagrożenie infrastruktury teleinformatycznej resortu sprawiedliwości i państwa.

Stanowisko organu koresponduje z poglądem wyrażonym przez NSA w powołanym powyżej wyroku o sygn. akt III OSK 1189/21, którym organ i Sądy są związane, iż: „Nie ulega wątpliwości, że dysponowanie kodem źródłowym pozwala na całościową analizę funkcjonowania programu komputerowego, w tym także na ocenę możliwości nadużycia lub ingerencji w sposób funkcjonowania programu. Zwraca na to uwagę Sąd pierwszej instancji, wskazując, że udostępnienie informacji technicznych (kodu źródłowego) może prowadzić do ujawnienia danych mających istotny wpływ na bezpieczeństwo danego narzędzia informatycznego".

W świetle przedstawionej argumentacji organ bezspornie miał podstawy do stwierdzenia, że żądany kod źródłowy zawiera informacje istotne dla bezpieczeństwa infrastruktury teleinformatycznej o szczególnym znaczeniu dla prawidłowego

funkcjonowania sądownictwa publicznego i całości aparatu państwowego. Niebagatelne znaczenie ma tu zagrożenie atakami cybernetycznymi (w kontekście obowiązującego obecnie stopnia alarmowego CHARLI-CRP i BRAVO), a zapobieganie tym zagrożeniom jest szczególnie istotne z punktu widzenia sprawnego działania państwa. Wobec tego dane mające znaczenie dla bezpieczeństwa teleinformatycznego instytucji publicznych, powinny podlegać specjalnej ochronie nie tylko technicznej, ale i prawnej. Sąd nie znalazł w tej sprawie podstaw do podważenia stanowiska organu, że powszechna dostępność danych tego rodzaju zagraża bezpieczeństwu państwa i porządkowi publicznemu, które zgodnie z art. 61 ust. 3 Konstytucji RP stanowią podstawę ograniczenia prawa do informacji.

Z tej też przyczyny, w ocenie składu orzekającego, odmowa udostępnienia wnioskowanej informacji na podstawie art. 5 ust. 1 u.d.i.p. w zw. z art. 4 ust. 1 u.o.i.n. stała się w pełni uzasadniona.

Trzeba mieć też na uwadze, że nieautoryzowana przy użyciu kodu źródłowego ingerencja w program SLPS narażałaby poufność danych osobowych zawartych w tym programie. Danych osobowych nie tylko pracowników sądów, prokuratury, ale i stron postępowania, uczestników postępowania, świadków, biegłych, itp. Na administratorze danych i podmiocie je przetwarzającym spoczywa zaś obowiązek zabezpieczenia przetwarzanych danych osobowych. W świetle art. 32 ust. 1 lit. b RODO, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Zasadność ujawnienia kodu źródłowego programu SLPS w przestrzeni publicznej, w kontekście zagrożeń związanych z aktywnością cyberprzestępczą, jawi się jako wątpliwa jeśli się zwróci uwagę na wskazane przez organ zagrożenia związane z możliwością ujawnienia danych milionów obywateli. W tym kontekście również ograniczenie dostępu do żądanej informacji na podstawie art. 5 ust. 2

u.d.i.p. w zw. z art. 24 i art. 32 ust. 1 i 2 RODO, Sąd ocenia jako uzasadnione i zgodne z prawem.

Sąd nie podziela natomiast poglądu organu, iż kod źródłowy, jako autorski projekt Ministerstwa Sprawiedliwości, poprzez analogię powinien podlegać ochronie z art. 5 ust. 2 u.d.i.p. jako „tajemnica przedsiębiorcy", bowiem nie ma ku temu podstaw na gruncie art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczeniu nieuczciwej konkurencji (Dz. U. z 2022 r. poz. 1233).

Niemniej jednak konfrontując interes obywatela do uzyskania informacji publicznej z interesem bezpieczeństwa państwa (przejawiający się w zapewnieniu odpowiedniego zabezpieczenia publicznych systemów teleinformatycznych w celu przeciwdziałania atakom cyberprzestępczym) i obowiązkiem należytego zabezpieczenia danych osobowych obywateli przed ich administratora, w realiach niniejszej sprawy należy dać prymat interesowi podmiotu publicznego. Tym samym nie sposób podzielić zarzutów skargi mówiących o naruszeniu przez organ przepisów prawa materialnego.

W ocenie Sądu, organ wypełnił obowiązek uzasadnienia decyzji odmawiającej udostępnienia żądanej informacji w sposób wystarczający dla dokonania oceny jej zgodności z prawem. Minister przede wszystkim w wystarczającym stopniu wykazał, że spełniony został element materialny pozwalający zakwalifikować kod źródłowy SLPS jako podlegający ochronie przewidzianej dla informacji niejawnych. Nie budzi wątpliwości stwierdzenie organu, że tego rodzaju informacja mogłaby być wykorzystana w przypadku działań nakierowanych przeciwko integralności systemu teleinformatycznego Ministerstwa, co wzmacnia stwierdzenie przez organ, iż mamy do czynienia z informacją, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne.

Prawo do poszukiwania i rozpowszechniania informacji może podlegać ograniczeniom w określonych przypadkach, co miało miejsce w niniejszej sprawie. W wyroku z 11 stycznia 2018 r. sygn. akt I OSK 549/16 (orzeczenia.nsa.gov.pl) Naczelny Sąd Administracyjny wskazał, że „(...) przepis art. 61 ust. 3 Konstytucji RP jest adresowany nie tylko do ustawodawcy, umożliwiając wprowadzanie ustawami generalnych i abstrakcyjnych ograniczeń prawa do informacji, lecz również do sądów, które - na podstawie analizy okoliczności konkretnej sprawy - są upoważnione do uznania, że z uwagi na potrzebę ochrony wolności i praw, porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa istnieje w określonym przypadku konieczność odmówienia udostępnienia informacji. Zastosowanie ww. regulacji konstytucyjnej w procesie stosowania

ustawy o dostępie do informacji publicznej może - w okolicznościach konkretnej sprawy - prowadzić do wniosku, że określona treść (dokument, pismo) stanowi co prawda informację publiczną w rozumieniu art. 1 ust. 1 tej ustawy, ale ze względu na wskazane w Konstytucji ograniczenie nie podlega udostępnieniu. Może tu chodzić o informacje, których udostępnianie godziłoby w ochronę tych wartości konstytucyjnych, wymienionych w art. 61 ust. 3 Konstytucji, do których nie znajduje bezpośredniego zastosowania ograniczenie ustawowe, zawarte w art. 5 u.d.i.p.".

W wyroku tym Naczelny Sąd Administracyjny podniósł też, że „Jedną z przesłanek uzasadniających ograniczenie prawa do informacji publicznej w rozumieniu art. 1 ust. 1 u.d.i.p. jest konieczność ochrony „porządku publicznego i bezpieczeństwa państwa" (art. 61 ust. 3 Konstytucji). W pojęciu tym mieści się m.in. postulat zapewnienia organom władzy publicznej prawidłowego funkcjonowania w celu wykonywania ich kompetencji. Treść pojęcia „porządek publiczny" należy interpretować w związku z zasadą rzetelności i sprawności działania instytucji publicznych, sformułowaną w preambule Konstytucji. Zasada ta nakazuje m.in. stworzenie organom władzy publicznej warunków technicznych i proceduralnych sprzyjających możliwości wszechstronnego gromadzenia danych i materiałów, które w ocenie organu są niezbędne do prawidłowego i praworządnego realizowania zadań i kompetencji. Natomiast dla potrzeb niniejszej sprawy, pojęcie „bezpieczeństwo państwa" należy postrzegać w umożliwieniu organom państwa i podmiotom wykonującym zadania publiczne zapewnienia bezpieczeństwa obywateli oraz mienia publicznego i prywatnego".

Organ wskazał w decyzji na możliwość spowodowania szkód dla Rzeczypospolitej Polskiej w sytuacji udostępnienia żądanej informacji publicznej. Minister w stopniu wystarczającym uzasadnił swoje stanowisko co do zaistnienia przesłanek wyłączających dostęp do żądanej informacji publicznej, co czyni zawarte w skardze zarzuty naruszenia art. 7 i art. 107 § 3 K.p.a. niezasadnymi.

Za bezpodstawny należy uznać także zarzut naruszenia art. 10, art. 77 § 1, art. 80 K.p.a. i art. 84 K.p.a. bowiem w sprawie te przepisy nie miały zastosowania. Postępowanie w sprawie udostępnienia informacji publicznej jest postępowaniem odformalizowanym i uproszczonym, w którym przepisy Kodeksu postępowania administracyjnego znajdują zastosowanie dopiero na etapie wydania decyzji w trybie art. 16 u.d.i.p. Wobec tego aktywność procesowa strony jest w tym postępowaniu ograniczona, zwłaszcza w postępowaniu o udostępnienie informacji publicznej nie przeprowadza się postępowania dowodowego z udziałem strony. NSA w wyroku z 21 lutego 2024 r. sygn. akt III OSK 6933/21 (publik. LEX nr 3705278) stwierdził, że przepisy K.p.a. stosuje się jedynie do decyzji

o odmowie udostępnienia informacji publicznej oraz umorzeniu postępowania o udostępnienie informacji publicznej. „Na tle u.d.i.p. wskazuje się, że jest to ustawa szczególna, regulująca w sposób kompleksowy kwestie związane z prawem dostępu do informacji publicznej (...). Sprawa o dostęp do informacji publicznej nie jest sprawą administracyjną w rozumieniu art. 1 pkt 1 K.p.a., a zawarte w niej odesłanie do przepisów kodeksu jest bardzo wąskie i dotyczy wyłącznie wydania decyzji o odmowie udostępnienia informacji i decyzji o umorzeniu postępowania (art. 16 ust. 2 u.d.i.p.)".

Reasumując, Sąd dokonując oceny zgodności z prawem zaskarżonej decyzji o odmowie udostępnienia informacji publicznej nie stwierdził naruszenia prawa materialnego, jak i procesowego w stopniu mającym wpływ na końcowy wynik sprawy.

Z tych względów, Wojewódzki Sąd Administracyjny w Warszawie, na podstawie przepisu art. 151 P.p.s.a. orzekł, jak w wyroku.

WOJEWÓDZKI SĄD ADMINISTRACYJNY * W WARSZAWIE * 2 *

Na oryginale właściwe podpisy
Za zgodność z oryginałem

Marta Stec
referent

Wojewódzki Sąd Administracyjny w Warszawie
Wydział II
ul. Jana Kazimierza 10
01-248 WARSZAWA

1793

OPŁATA POBRANA
TAXE PERCUE-POLOGNE
Umowa z Pocztą Polską SA
ID Nr 497858/W

WARSZAWA 42
11 10 2024
OC

WARSZAWA 121
14 10 2024
TI

Awizowano powtórnie
.....
.....

II SA/Wa 2336/23

1590612 10.10.2024 03 POLECONA ZPO

R (00)659007734367406696

r. pr. Adam Kuczyński r. pr. Adam Kuczyński
Modzelewskiego 23/373
02-679 Warszawa

10.10.2024

2024

Poczta Polska
Opłata pobrana _____ zł ___ gr

Awizowano powtórnie
dnia .....
podpis 22-10-2024

WARSZAWA 121
22 10 2024
TI

172

1289955

2024-10-28