23.10.2023

RZECZPOSPOLITA POLSKA
MINISTER SPRAWIEDLIWOŚCI

Warszawa, 16 października 2023 r.

BK-IV.082.270.2022

DECYZJA

Działając na postawie art. 5 ust. 1 i 2 w zw. z art. 16 ust. 1 i 2 ustawy z dnia 6 września 2001r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902) 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 ze zm.) 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 ze 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 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 L 119 z 4.05.2016 r.) i art. 104 k.p.a., po rozpatrzeniu wniosku Stowarzyszenia Sieć Obywatelska Watchdog Polska

odmawiam
udostępnienia kodu źródłowego oprogramowania
o nazwie System Losowego Przydziału Spraw

UZASADNIENIE

I.
Przebieg postępowania

Stowarzyszenie Sieć Obywatelska Watchdog Polska (w dalszej treści: **Stowarzyszenie**) zwróciło się do Ministra Sprawiedliwości z wnioskiem o udostępnienie informacji publicznej w postaci kodu źródłowego oprogramowania o nazwie System Losowego Przydziału Spraw (**w** dalszej treści: **SLPS**).

Minister Sprawiedliwości, po przeprowadzeniu analizy charakteru żądanej informacji, w oparciu o dotychczasowe orzecznictwo sądów administracyjnych uznał, że kod źródłowy programu komputerowego nie stanowi informacji publicznej w rozumieniu art. 1 ust. 1 *ustawy z dnia 6 września 2001r. o dostępie do informacji publicznej* (Dz. U. z 2022 r. poz. 902; w dalszej treści: **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 I instancji) uznając, że kod źródłowy SLPS stanowi informację publiczną.

Naczelny Sąd Administracyjny przyznał, że odstępuje tym samym od wcześniejszego stanowiska Naczelnego Sądu Administracyjnego, wyrażonego m.in. w wyroku z 27 lutego 2014 r. sygn. akt I OSK 2014/13.

Minister Sprawiedliwości wykonał wyrok Naczelnego Sądu Administracyjnego poprzez wydanie decyzji z 4 sierpnia 2022 r. nr BK-IV.082.270.2022 o odmowie udostępnienia kodu źródłowego SLPS.

Stowarzyszenie zaskarżyło tę decyzję do Wojewódzkiego Sądu Administracyjnego w Warszawie. Sąd w wyroku z 24 lutego 2023 r. sygn. akt II SA/Wa 1785/22 uchylił decyzję organu. W uzasadnieniu wyroku Sąd wskazał na potrzebę rozbudowania argumentacji na rzecz odmowy udostępnienia wnioskowanej informacji. Sąd 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 ze 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".

II.

System Losowego Przydziału Spraw

Wskazane wyroki sądów administracyjnych pozostają wiążące dla organu 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 System Losowego Przydziału Spraw, którego kod źródłowy jest przedmiotem wniosku.

System Losowego Przydziału Spraw jest programem komputerowym, który działa w oparciu o generator liczb losowych. 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.

SLPS jest rozbudowanym i skomplikowanym systemem teleinformatycznym, który w czasie rzeczywistym we wszystkich sądach jednocześnie realizuje zarówno zasadę losowości przydziału, jak i zasadę proporcjonalności przydziału do dni pracy i wskaźników przydziału poszczególnych referentów.

SLPS 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 ze zm. – art. 47a);

2. rozporządzenie Ministra Sprawiedliwości z dnia 18 czerwca 2019 r. Regulamin urzędowania sądów powszechnych (Dz. U. z 2022 r. poz. 2514 ze 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.).

Dodatkowo, Minister Sprawiedliwości 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/sprawiedliwosc/algorytm).

Minister 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. Narzędzie to pozwala każdej zainteresowanej osobie pobranie raportu z losowania przeprowadzonego w dowolnej sprawie sądowej i zapoznanie się z wynikiem i parametrami losowania.

Zadania z zakresu administrowania SLPS realizuje Sąd Apelacyjny w Białymstoku. Sąd zapewnienia 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. Sprawiedl. 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, zalogowani 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 ze zm.).

III.

Kod źródłowy Systemu Losowego Przydziału Spraw

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 por. m.in.
https://www.nytimes.com/2023/03/26/technology/twitter-source-code-leak.html
https://biznes24.pl/zuchwala-kradziez-w-apple/
https://spidersweb.pl/2023/01/league-of-legends-i-teamfight-tactics-z-wykradzionym-kodem-zrodlowym-czarna-seria-trwa.html

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 Systemu Losowego Przydziału Spraw 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. Poniżej przykładowy fragment kodu:

```
private async Task DrawForDepartment(Department department, int scheduledDrawId)
{
using (var nestedContainer = UnityContainer.GetNewContainer(true))
{
InitializeRNGEngine(nestedContainer);
var drawForDepartmentHelper = nestedContainer.GetInstance<DrawForDepartmentHelper>();
List<Category> categoryList = await
drawForDepartmentHelper.GetCategoriesFromDepartmentList(department.Id);
List<Judge> judges = drawForDepartmentHelper.GetJudgesFromDepartment(department.Id);
await judgesInCategoriesCreator.Create(judges, categoryList);
foreach (Category category in categoryList)
{
await courtCaseContainer.LoadUnresolvedCasesFromDepartment(department, category);
int courtCasesCount = courtCaseContainer.NoLocalCases();
for (int i = 0; i < courtCasesCount; i++)
{
CourtCaseInDraw courtCaseInDraw = courtCaseContainer.GetAndRemoveRandomLocalCase();
try
{
var option = new TransactionOptions()
{
IsolationLevel = IsolationLevel.ReadCommitted
};
using (var scope = new TransactionScope(TransactionScopeOption.Required, option,
TransactionScopeAsyncFlowOption.Enabled))
{
using (var courtCaseInDrawHelper = nestedContainer.GetInstance<CourtCaseInDrawHelper>())
{
CourtCase courtCase = courtCaseInDrawHelper.GetCourtCase(courtCaseInDraw.CourtCaseId);
if (courtCase.IsCourtCaseInInactiveCategory()) continue;
List<LayJudge> layJudgesFromRegion = await
courtCaseInDrawHelper.GetAllFromDefaultGroupInDepartment(department.Id);
List<int> excludedJudgesIds = await
courtCaseInDrawHelper.GetAllExcludedFromCourtCaseJudgesIds(courtCase);
List<JudgeInCategory> judgesInCategory = await
courtCaseInDrawHelper.GetAllAvailableJudgesInCategory(courtCase, department.Id, category.Id);
await courtCaseInDrawHelper.CreateCourtCaseInDraw(courtCaseInDraw, scheduledDrawId);
if (courtCase.Status != CourtStatus.StaffExtentionNeeded)
{
IEnumerable<JudgeInCourtCase> judgesInCourtCase = await
judgeInCourtCaseRepository.GetAllRelatedToCourtCase(courtCaseInDraw.CourtCaseId);
int layJudgesFromRegionCount = layJudgesFromRegion.Where(x => !x.IsExcludedFromCase(courtCase))
.ToList()
.Count;
int triosAmount = await courtCaseInDrawHelper.GetTriosAmount(department, courtCase.IsCurrentTrio);
var judgesForPresidingJudges = judgesInCategory.Where(x => !excludedJudgesIds.Contains(x.JudgeId) &&
!judgesInCourtCase.Select(j => j.JudgeId).Contains(x.JudgeId) &&
((x.Judge.DelegatedUnderSpecialProcedure && x.CourtCasesToDrawCount.HasValue &&
x.CourtCasesToDrawCount.Value - x.CurrentDrawnCourtCasesCount > 0) ||
(!x.Judge.DelegatedUnderSpecialProcedure && !x.Judge.IsExcludedFromAllDraws &&
!x.JudgeExcludedFromDrawInCategory && x.JudgeDutiesPercentage > 0))).ToList();
var judgesForPresidingJudgesExcludedByAbsence = await
courtCaseInDrawHelper.GetJudgesListWithoutAbsentJudges(judgesForPresidingJudges);
if (triosAmount == 0 && autoTriosGenetratorEnabled)
{
bool isGenerated = GenerateIfNoTrios(department, courtCase);
if (isGenerated)
{
triosAmount = await courtCaseInDrawHelper.GetTriosAmount(department, courtCase.IsCurrentTrio);
```

```
}
}
if (!(await courtCaseInDrawHelper.DoesCourtCaseMeetRequirementsForDraw(layJudgesFromRegionCount,
courtCaseInDraw, judgesForPresidingJudgesExcludedByAbsence.Count,
judgesInCategory.Count, triosAmount)))
{
scope.Complete();
continue;
}
}
await courtCaseInDrawHelper.Process(courtCaseInDraw, judgesInCategory, layJudgesFromRegion);
scope.Complete();
}
}
}
catch (Exception e)
{
Log4Net.Error(
$"Error occured in DrawProcessManager.Draw.DrawForDepartment. CourtCaseId:
{courtCaseInDraw.CourtCaseId}",
e);
}
}
}
await drawForDepartmentHelper.UpdateUnassignedCourtCases(department, categoryList);
}
}
```

Wysoki stopień skomplikowania kodu jest adekwatny do stopnia zaawansowania technologicznego aplikacji System Losowego Przydziału Spraw, co wyjaśniono na wstępie.

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 (należy przypomnieć, że Stowarzyszenie oczekuje udostępnienia kodu poprzez e-mail).

Specjaliści wskazali na bardzo poważne ryzyko bezpośrednie i ryzyko pośrednie ewentualnego udostępnienia kodu źródłowego.

Chodzi przede wszystkim 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, o czym wspomniano na wstępie) 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 co za tym idzie 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 podmiana 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 (o czym wspomniano na wstępie).

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). Tak, jak podano na wstępie, w tym systemie 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.

Podkreślenia wymaga, 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. 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://www.gov.pl/web/rcb/przedluzenie-obowiazywania-stopni-alarmowych-do-30-listopada-2023-r).

Powyższa okoliczność jest bardzo istotnym elementem stanu faktycznego w niniejszej sprawie.

IV.

Prawne podstawy ochrony kodu źródłowego Systemu Losowego Przydziału Spraw

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.

Wskazane przepisy 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 (Dz. U. z 2023 r. poz. 57 ze zm.). Ustawa określa 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 rozporządzeniem, 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 L 119 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 z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2023 r. poz. 756 ze zm.). W myśl tej normy 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. W ocenie Sądu 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.

W pełni podzielając pogląd Sądu należy zauważyć, że w świetle przedstawionej powyżej charakterystyki Systemu Losowego Przydziału Spraw 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.

Przedstawione stanowisko znajduje odzwierciedlenie w utrwalonej linii orzeczniczej Naczelnego Sądu Administracyjnego (por. m.in. wyrok z 19.10.2017 r. sygn. akt I OSK 1822/16, wyrok z 28.04.2016 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, a szczegółowo przedstawionej w pkt. II i III niniejszej decyzji.

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 Zintegrowanego Systemu Rachunkowości i Kadr.

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 z ustawy z dnia 6 września 2001r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902).

Stosownie do art. 61 ust. 3 Konstytucji RP, ograniczenie prawa do informacji może nastąpić 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.

Ww. dyspozycję wykonuje m.in. art. 5 ust. 1 i 2 ustawy o dostępie do informacji publicznej. 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, którą przedstawiono w pkt. II i III niniejszej decyzji.

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 (por. wyrok NSA z dnia 11 stycznia 2018 r., sygn. akt I OSK 549/16).

Jak wyjaśniono, 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.

Na podkreślenie zasługuje fakt, że 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.

Podsumowując zatem stanowisko organu podkreślenia wymaga, że kod źródłowy Systemu Losowego Przydziału Spraw spełnia wszystkie prawem przewidziane przesłanki do uznania, iż prawo do jego udostępnienia podlega ograniczeniu z uwagi na dobro wymiaru sprawiedliwości i bezpieczeństwo publiczne.

Ustawa o dostępie do informacji publicznej nie przewiduje mechanizmu, który pozwoliłyby czuwać nad bezpieczeństwem informacji po jej udostępnieniu. W konsekwencji, co zostało już zasygnalizowane, 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 mln linijek kodu). Kod stałby się całkowicie nieczytelny, utraciłby walor nośnika wiarygodnych informacji o Systemie Losowego Przydziału Spraw.

Z powyższych względów, w czasie podwyższonego zagrożenia atakami o charakterze terrorystycznym w cyberprzestrzeni, należało wydać decyzję o odmowie udostępnienia kodu źródłowego.

z upoważnienia
MINISTRA SPRAWIEDLIWOŚCI
Damian Bess
ZASTĘPCA DYREKTORA
Biura Komunikacji i Promocji

Informacja:

W związku z obowiązkiem, nałożonym przez art. 16 ust. 2 pkt 2 u.d.i.p., informuję, że w toku postępowania zajął stanowisko Dyrektor Departamentu Informatyzacji i Rejestrów Sądowych, Dyrektor Biura Cyberbezpieczeństwa, Dyrektor Biura Bezpieczeństwa i Dyrektor Departamentu Kadr i Organizacji Sądów Powszechnych i Wojskowych. Ich dane osobowe znajdują się w Biuletynie Informacji Publicznej, pod adresem: https://www.gov.pl/web/sprawiedliwosc/struktura-organizacyjna

Pouczenie:

Strona niezadowolona z niniejszej decyzji może zwrócić się do Ministra Sprawiedliwości z wnioskiem o ponowne rozpatrzenie sprawy w terminie 14 dni od dnia jej doręczenia.
W myśl art. 127a k.p.a. w trakcie biegu terminu do wniesienia odwołania (wniosku o ponowne rozpatrzenie sprawy) strona może zrzec się prawa do wniesienia odwołania wobec organu administracji publicznej, który wydał decyzję. Z dniem

doręczenia organowi administracji publicznej oświadczenia o zrzeczeniu się w/w prawa decyzja staje się ostateczna i prawomocna.
Stosownie do art. 52 § 3 ustawy Prawo o postępowaniu przed sądami administracyjnymi, jeżeli stronie przysługuje prawo do zwrócenia się do organu, który wydał decyzję z wnioskiem o ponowne rozpatrzenie sprawy, strona może wnieść skargę na tę decyzję bez skorzystania z tego prawa.

Otrzymuje:
Stowarzyszenie Sieć Obywatelska Watchdog Polska

Ministerstwo Sprawiedliwości

Biuro Komunikacji i Promocji

OPŁATA POBRANA
TAXE PERÇUE - POLOGNE
Urząd Pocztowy Polska S.A. ID 460277/W

WARSZAWA 132
17102023
DAR

POLECONY
za potwierdzeniem odbioru

23.10.2023

459007734204610282

)459007734204610282

2023

a Polska

pobrana ___ zł ___ gr

BK-IV.082.270.2022

2192388 2023-10-16 03 POLECONA ZPO

Sieć Obywatelska Watchdog Polska
ul. Ursynowska 22/2
02-605 Warszawa

2023-10-16