



Górki-Sypniewo, 10.04.2025 r.

Fundacja Cyber-Complex
Górki-Sypniewo 1, 18-421 Piątnica
KRS: 0000866262
NIP: 7182156130 REGON: 387361152
fundacja@cybercomplex.net
www.cybercomplex.net

Adresat wniosku: Komisja do Spraw Petycji
Sejm Rzeczypospolitej Polskiej
ul. Wiejska 4/6/8
00-902 Warszawa

Wnoszący wniosek: Fundacja Cyber-Complex
Górki-Sypniewo 1
18-421 Piątnica

WNIOSEK

O CZĘŚCIOWE UZNANIE ZA ZASADNĄ PETYCJĘ **BKSP-155-X-411/25** W SPRAWIE ZMIANY USTAWY Z
DNIA 6 WRZEŚNIA 2001 R. O DOSTĘPIE DO INFORMACJI PUBLICZNEJ (**Dz.U. z 2022 R. POZ. 902**)

Fundacja Cyber-Complex (dalej FCC) częściowo uznaje za zasadne obawy dotyczące możliwości pozyskiwania informacji w ramach zapytania o informację w trybie całkowicie anonimowym. Mimo wpłynięcia do Sejmu Rzeczypospolitej Polskiej wniosku¹ z dnia 26 marca 2025 r., którego nadawcą jest Stowarzyszenie Sieć Obywatelska Watchdog Polska o uznanie petycji za bezzasadną FCC uważa, że problematyka wymaga znacznie dogłębniejszej analizy i nie można na podstawie wykazanej argumentacji jej jednoznacznie rozstrzygnąć. Całkowicie liberalny i anonimowy dostęp do informacji publicznych ma także swoje negatywne konsekwencje, co powinno być brane pod uwagę.

UZASADNIENIE

W petycji BKSP-155-X-411/25 postulowano zmianę prowadzącą do uniemożliwienia składania anonimowych wniosków o udzielenie informacji publicznej

¹ https://siecobywatelska.pl/wp-content/uploads/2025/03/54_SOWP_2025_PR-Kancelaria-Sejmu-RP-WNIOSEK-o-uznanie-petycji-za-bezzasadna.pdf

oraz wyłączeniu z obowiązku publikowania w Biuletynie Informacji Publicznej (BIP) dokumentacji przebiegu kontroli.

FCC jest stanowiska, że jeżeli chodzi o drugi postulat (obowiązek publikowania dokumentacji przebiegu kontroli) to jest on bezzasadny. Jednakże pierwszy postulat usunięcia anonimowego dostępu do informacji ma swoje uzasadnienie.

Fundacja Cyber-Complex zdaje sobie sprawę, że prawo dostępu do informacji publicznej jest jednym z fundamentów demokratycznego państwa prawa i stanowi istotną gwarancję jawności życia publicznego. Niemniej jednak, w aktualnych realiach geopolitycznych oraz w świetle rosnących zagrożeń o charakterze hybrydowym, w tym terrorystycznym, konieczne jest nowoczesne wyważenie wartości: **wolności i bezpieczeństwa**.

Problematyka ta dotyczy równowagi między wolnością a bezpieczeństwem, czyli klasycznego dylematu w nowoczesnych demokracjach. Z punktu widzenia naukowego oraz akademickiego zagadnienie to jest doskonale znane i opisywane w renomowanych oraz recenzowanych czasopismach naukowych^{2,3,4}.

W polskim systemie prawnym obecnie możliwe jest składanie wniosków o informację publiczną całkowicie anonimowo. Choć zwiększa to swobodę działania obywateli i organizacji społecznych, równocześnie pozostawia otwartą furtkę dla nadużyć, które – w najgorszym przypadku – mogą zostać wykorzystane do celów zagrażających bezpieczeństwu państwa.

Zwracamy uwagę, że w wielu państwach Unii Europejskiej (m.in. Francji, Niemczech, Hiszpanii, Włoszech⁵) identyfikacja wnioskodawcy jest standardową praktyką i nie stoi w sprzeczności z zasadą transparentności. Wręcz przeciwnie – wprowadzenie takiego obowiązku może zwiększyć odpowiedzialność wnioskodawców oraz przeciwdziałać działaniom o charakterze wywiadowczym⁶, sabotażowym lub dezinformacyjnym.

- 2 Wyporska-Frankiewicz, Joanna Beata, and Ewa Cisowska-Sakrajda. "Dostęp do informacji publicznej a bezpieczeństwo państwa." *Wiedza Obronna* 278.1 (2022): 109-141.
<https://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-3d14433e-dc36-468e-9c20-79949bd23edc>
- 3 Cisowska-Sakrajda, Ewa. "Dostęp do informacji publicznej w warunkach normalnego funkcjonowania państwa a zagrożenia dla bezpieczeństwa zewnętrznego państwa." *Wiedza Obronna* 282.1 (2023): 211-251.
<https://wiedzaobronna.edu.pl/index.php/wo/article/view/219>
- 4 Kogut, Bogulaw, et al. "Information security in Poland and in the European Union: Administrative and legal conditions." (2021).
<https://www.um.edu.mt/library/oar/handle/123456789/81854>
- 5 We Włoszech czasem wymagana jest nawet weryfikacja wnioskodawcy za pomocą podpisu cyfrowego.
- 6 OSINT (Open Source Intelligence) – to termin określający biały wywiad, czyli pozyskiwanie i analiza informacji pochodzących z ogólnodostępnych, legalnych źródeł. W odróżnieniu od tradycyjnego wywiadu, OSINT nie wymaga stosowania metod tajnych ani łamania zabezpieczeń – opiera się wyłącznie na tym, co jest publicznie dostępne.

Co więcej, identyfikacja nie musi prowadzić do ograniczenia praw obywatelskich. Wnioski nadal mogą być składane elektronicznie, a dane osobowe wykorzystywane wyłącznie do celów proceduralnych. W przypadku zapytań o charakterze rutynowym – jak budżet gminy czy wynagrodzenia urzędników – dane te nie muszą być nawet analizowane pod kątem bezpieczeństwa. Natomiast przy zapytaniach nietypowych (np. o systemy monitoringu, plany ochrony obiektów, schematy sieci energetycznych) organy będą miały znacznie większe możliwości śledcze podczas analizy nawet w ujęciu „post factum”⁷.

Oczywiście dane bardziej krytyczne dla funkcjonowania państwa są chronione w ramach przepisów dotyczących informacji niejawnych tj. głównie ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2019 poz. 742). Informacje tego typu nie podlegają udostępnianiu zgodnie z informacją publiczną. Jednakże każdy z nas będąc elementem społeczeństwa informacyjnego powinien, być świadom tego, że w świecie jakim żyjemy może być wiele informacji potencjalnie wrażliwych, a nie wszystkie z nich muszą być formalnie zakwalifikowane jako informacje niejawne⁸.

Stowarzyszenie Sieć Obywatelska Watchdog Polska w swoim wniosku zawarło argumentację, że usunięcie możliwości wnioskowania o informację w trybie anonimowym może spowodować, że osoby podpisujące się pod dokumentem mogą doświadczyć reperkusji, ponieważ urzędnicy mogą tą informację wykorzystać celowo jako pretekst do wyciągnięcia negatywnych konsekwencji.

Można tutaj odnieść się do zasady „dobrej woli”^{9,10} (ang. *good faith*, łac. *bona fides*), która jest jedną z fundamentalnych zasad prawa i jest obecna niemal we wszystkich systemach prawnych – zarówno w prawie cywilnym, administracyjnym, jak i międzynarodowym. Jest jak niewidzialna nić łącząca strony w stosunkach prawnych i wymagająca od nich uczciwego, lojalnego działania.

W istocie zakładając na samym początku nieuczciwe działania to w procesie tym zarówno osoby wnioskujące o informację publiczną mogą zaznać reperkusji, jak i pozyskane w sposób anonimowy informacje mogą być wykorzystane przeciwko instytucjom publicznym oraz państwu. Wykorzystywanie tego typu informacji do działań wywiadowczych, sabotażowych lub terrorystycznych i jest powszechnie znane¹¹.

7 Analiza z perspektywy czasu, już po zaistnieniu sytuacji.

8 W ramach Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2019 poz. 742)

9 Lis, Edyta. "Zasada dobrej wiary w prawie międzynarodowym." *Studia Iuridica Lublinensia* 25.1 (2016): 17-46.
<https://www.ceeol.com/search/article-detail?id=414041>

10 Mazzota, F. "Good Faith Principle: Vexata Quaestio." *International sales law: a global challenge*. Cambridge University Press, Cambridge (2014).

11 Raport Amerykańskiej Federalnej Agencji Zarządzania Kryzysowego (FEMA) "Planning Considerations: Complex Coordinated Terrorist Attacks" wskazuje, że skoordynowane ataki terrorystyczne często wykorzystują zsynchronizowane zespoły działające niezależnie w wielu lokalizacjach, co wymaga szczegółowego planowania i wykorzystywania w pełnym spektrum z informacji publicznych.
https://www.fema.gov/sites/default/files/2020-07/planning-considerations-complex-coordinated-terrorist-attacks.pdf?utm_source=chatgpt.com





Wprowadzenie wymogu prawnego podawania danych (imienia i nazwiska) nie eliminuje definitywnie wyżej wskazanego problemu systemowego. Tak jak jednak wspomniano może zwiększyć świadomość oraz odpowiedzialność wnioskodawców, a także jeżeli zajdzie takowa potrzeba zwiększyć możliwości analityczne służb bezpieczeństwa.

Wspomniana w petycji kwestia sztucznej inteligencji (AI – ang. *Artificial intelligence*) nie jest także bez znaczenia. W obecnym momencie jednakże FCC nie posiada konkretnych informacji statystycznych czy faktycznie dochodzi w niektórych miejscach do zwiększonego obciążenia urzędów ze względu na wykorzystanie narzędzi AI. W przyszłości jest bardzo prawdopodobne, że może dojść do znacznego nasilenia takiego trendu wykorzystania sztucznej inteligencji.

Reasumując wierzymy, że wprowadzenie racjonalnych ograniczeń anonimowości przy zachowaniu transparentności instytucji publicznych będzie wyrazem dojrzałego i odpowiedzialnego podejścia do ochrony interesu państwa oraz jego obywateli. Ufamy także w świadomość rozgraniczenia wolności i bezpieczeństwa, a także w to, że bilans tych dwóch wartości nie musi wcale zakłócić wymaganej transparentności.

Ostatecznie chcielibyśmy ponownie podkreślić, że w naszym mniemaniu postulowana zmiana prowadząca do uniemożliwienia składania anonimowych wniosków o udzielenie informacji publicznej nie jest bezzasadna.

Fundacja Cyber-Complex
Górki-Sypniewo 1, 18-421 Piątnica
KRS: 0000866262
NIP: 7182156130 REGON: 387361152
fundacja@cybercomplex.net
www.cybercomplex.net

Z wyrazami szacunku,
w imieniu Fundacji Cyber-Complex

Ewa Maria Tęcza
Kierownik Zespołu
Zespół Operacyjny ds. Archiwizacji
Fundacja Cyber-Complex
e-mail: etecza@cybercomplex.net
Telefon: (+48) 728 569 998

Ewa Tęcza

Łukasz Świerczewski
Dyrektor Zarządu
Fundacja Cyber-Complex
e-mail: lswierczewski@cybercomplex.net
telefon: (+48) 720 770 024

Łukasz Świerczewski