FUNDACJA PANOPTYKON

Warszawa, 11 maja 2026 r.

„Demokracja na podsłuchu" – Panoptykon publikuje raport o Pegasusie i braku kontroli nad inwigilacją przez służby

„Oprogramowanie szpiegujące jest jak broń atomowa – może rozstrzygnąć o wyniku wojny, ale przy tym narobić gigantycznych szkód. Czas wyciągnąć wnioski z »afery Pegasusa« i stworzyć ramy prawne, które pozwolą służbom skutecznie działać, a przy tym będą gwarantowały ochronę dla praw i wolności" – ostrzega Fundacja Panoptykon w najnowszym raporcie „Demokracja na podsłuchu. Polska wobec Pegasusa i oprogramowania szpiegującego".

Oprogramowanie szpiegujące (*spyware*) to możliwość totalnej inwigilacji obywateli i obywatelek przez rząd. Pozwala prześwietlić zawartość każdego zakamarka telefonu, a nawet podrzucić sfabrykowany „dowód" niepopełnionego przestępstwa. To także – jak twierdzą służby – niezbędne narzędzie pracy i gwarant bezpieczeństwa kraju.

W Polsce zostało użyte wobec setek osób: sędziów, aktywistek, przedsiębiorców, a także polityków i polityczek. PiS mógł użyć służb do politycznej rozgrywki, bo nikt nie ma realnej kontroli nad ich działaniami.

Koalicja Obywatelska obiecała przed wyborami, że zabezpieczy Polskę przed podobnymi aferami. Do dziś służby i oprogramowanie szpiegujące są poza kontrolą, podatne na nadużycia.

W najnowszym raporcie Panoptykon proponuje zestaw reguł, które pozwolą służbom realizować ich zadania w obszarze kontroli operacyjnej, a przy tym zabezpieczą prawa i wolności obywatelskie.

Pegasus nielegalny i niebezpieczny dla demokracji i praw człowieka

„Oprogramowanie szpiegujące pozwala nie tylko na podsłuchiwanie rozmów czy kontrolę korespondencji. Daje też pełen dostęp do cyfrowej aktywności osoby inwigilowanej – zarówno do informacji przechowywanych na telefonie, takich jak zdjęcia czy konwersacje, ale też do aplikacji. Służby mogą zajrzeć do bankowości elektronicznej, na facebookowy feed i do historii zakupów online" – tłumaczy Wojciech Klicki, wiceprezes Fundacji Panoptykon, współautor raportu.

„Każda inwigilacja, bez względu na jej sposób i zasięg, pozbawia człowieka prywatności i poczucia bezpieczeństwa" – zauważa sędzia Beata Morawiec, była prezeska Stowarzyszenia Sędziów Themis, pokrzywdzona w aferze Pegasusa. „Najgorzej, gdy inwigilowany jest świadomy podejmowanych wobec niego działań i całkowicie bezradny. Nikomu tego nie życzę".

Nie da się technicznie zabezpieczyć oprogramowania szpiegującego

Na zagrożenia, jakie tworzy niekontrolowane wykorzystywanie oprogramowania szpiegującego przez służby, zwraca uwagę Adam Haertle, specjalista ds. cyberbezpieczeństwa, redaktor naczelny Zaufanej Trzeciej Strony, który jako jeden z pierwszych ujawnił, że CBA korzystała z Pegasusa.

„Oprogramowanie szpiegujące to potrzebne, ale też i potężne narzędzie, którego potencjalne możliwości są praktycznie niemożliwe do skutecznego ograniczenia po stronie technicznej" – uważa Haertle. „To powoduje, że absolutnie konieczne stają się konkretne ograniczenia proceduralne i niezależne mechanizmy kontrolne, zapewniające ich przestrzeganie".

Obietnice rządzących bez pokrycia

Zagrożenia związane z wykorzystaniem Pegasusa dostrzegli też politycy i polityczki. W kampanii przed wyborami do Parlamentu w 2023 r. opozycja obiecywała rozliczyć aferę i zmienić prawo w taki sposób, żeby zapobiegało nadużyciom z wykorzystaniem oprogramowania szpiegującego.

Chociaż od tego czasu minęły prawie trzy lata, niewiele się zmieniło.

„Sądzimy, że polskie służby są obecnie w posiadaniu oprogramowania szpiegującego. Ale jeśli z niego korzystają, robią to wbrew przepisom, bo nie przewidują one tak głębokiej ingerencji w prywatność, jaką daje oprogramowanie szpiegujące" – zwraca uwagę Wojciech Klicki. „Brakuje też adekwatnych gwarancji dla ochrony praw człowieka".

Mimo obietnic nie stworzono mechanizmu kontroli działań służb już w trakcie prowadzenia przez nie inwigilacji. A istniejący dziś model wyrażania zgody przez sądy nadal jest fikcyjny. Po „aferze Pegasusa" sądy nadal akceptują 99,5% wniosków o kontrolę operacyjną.

Nie zmieniło się też nic, jeśli chodzi o prawa osób niesłusznie inwigilowanych.

„Co mogą ofiary? Jakie mają narzędzia obrony i co mogą zrobić, żeby walczyć o swoje prawa?" – pyta retorycznie Sylwia Gregorczyk-Abram, adwokatka reprezentująca przed Europejskim Trybunałem Praw Człowieka osoby pokrzywdzone w aferze Pegasusa. Jak dodaje: „dziś osoba inwigilowana w Polsce nie jest informowana o działaniach służb i w praktyce nie ma możliwości ich zakwestionowania".

Rozliczenia „afery Pegasusa" również nie zostały zamknięte. Sejmowa Komisja Śledcza nie opublikowała jeszcze raportu podsumowującego jej prace, a Prokuratura nie przedstawiła nikomu aktu oskarżenia.

„Głównym problemem w braku rozliczeń z Pegasusem po 2023 r. jest przekonanie w Ministerstwie Sprawiedliwości, Prokuraturze i u Ministra Koordynatora, że Pegasus był czasami dobry, a czasami zły" – uważa gen. Krzysztof Bondaryk, były szef Agencji Bezpieczeństwa Wewnętrznego, obecnie Dyrektor Departamentu Bezpieczeństwa i Spraw Obronnych Ministerstwa Spraw Wewnętrznych i Administracji. „Podczas gdy jego zakup i użycie było od początku przestępstwem" – podkreśla.

Potrzebne zmiany – Panoptykon proponuje dwie warstwy

Raport Fundacji Panoptykon nie podważa, że służby mogą potrzebować oprogramowania szpiegującego do skutecznego działania. Przekonuje jednak, że niezbędne są zmiany w prawie, które uregulują jego wykorzystywanie.

Proponowane przez Panoptykon zmiany mają dwie warstwy. Pierwsza dotyczy generalnych zasad stosowania kontroli operacyjnej, przede wszystkim wzmocnienia i urealnienia nadzoru sądu oraz przyznania inwigilowanym prawa do informacji, że byli przedmiotem zainteresowania służb. Druga odnosi się konkretnie do oprogramowania szpiegującego, w tym do określenia, jakie formy jego użycia powinny być zakazane.

„Tylko w ten sposób można zapewnić równowagę pomiędzy koniecznością zapewnienia skuteczności działania służb a zminimalizowaniem ryzyka nadużyć" – podsumowuje Klicki.

Raport można pobrać ze strony Fundacji Panoptykon: https://panoptykon.org/demokracja-na-podsluchu-raport.