DOI: 10.17951/glosa.2025.4.47-55

GLOSA

dr hab. Adam Taracha, prof. UMCS
ORCID: 0000-0001-8630-2496

adam.taracha@mail.umcs.pl
Zespół Badawczy Kryminalistyki i Prawa Dowodowego
Instytut Prawa UMCS
Uniwersytet Marii Curie-Skłodowskiej w Lublinie

Program „Pegasus" to legalny środek techniczny stosowany w czasie kontroli operacyjnej – glosa do wyroku Sądu Apelacyjnego we Wrocławiu z dnia 11 maja 2023 r., II AKa 480/21

Słowa kluczowe: *kontrola operacyjna; Pegasus; środki techniki; czynności operacyjne*

Autor krytycznie ocenia stanowisko Sądu Apelacyjnego we Wrocławiu z dnia 11 maja 2023 r. (II AKa 480/21), w którym Sąd uznaje za nielegalne stosowanie w ramach kontroli operacyjnej środków techniki o cechach programu „Pegasus". Autor uważa, że ustawodawstwo policyjne (w tym ustawa o CBA) nie wprowadza żadnych ograniczeń w zakresie środków techniki, i zgadza się z prezentowanym przez Trybunał Konstytucyjny stanowiskiem, że środki techniki stosowane w ramach kontroli operacyjnej muszą być oparte na najnowszych technologiach pozwalających na pozyskiwanie i utrwalanie informacji.

Teza
Posłużenie się oprogramowaniem szpiegowskim w ramach kontroli operacyjnej nie może być uznane za zgodny z ustawą, legalny sposób pozyskania informacji.

Stan faktyczny przedstawiał się następująco: „R.J. został oskarżony o to, że: w okresie od 16 listopada 2018 roku do 29 marca 2019 roku w T.W. i innych miejscach na terenie Polski, działając w krótkich odstępach czasu w wykonaniu z góry powziętego zamiaru, wiedząc, że K.T. jest funkcjonariuszem Agencji Bezpieczeństwa Wewnętrznego, chcąc aby przekroczyła ona, w celu osiągnięcia korzyści majątkowej, swoje uprawnienia funkcjonariusza publicznego poprzez ujawnienie mu informacji niejawnych, swoim zachowaniem nakłaniał ją, między innymi za pośrednictwem komunikatora internetowego (…) i (…) do ujawnienia informacji niejawnych o klauzuli «tajne» dotyczących prowadzonych lub planowanych przez ABW czynności operacyjnych, w tym dotyczących obserwacji na podstawie art. 23 ust. 1 pkt 6 ustawy o ABW, wobec jego osoby, a nadto M.M. i M.S., a następnie ww. informacje niejawne wykorzystywał wbrew przepisom ustawy, m.in. poprzez przekazywanie ich dalej M.M. za pośrednictwem komunikatora (…), a nadto do modyfikacji własnych działań to jest o czyn z art. 18 § 2 k.k. w zw. z art. 231 § 1 i 2 k.k. w zw. z art. 265 § 1 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 12 § 1 k.k. w zw. z art.21 § 2 k.k.".

K.T. została oskarżona o to, że „w okresie od 16 listopada 2018 roku do 29 marca 2019 roku w K.L. i innych miejscach na terenie Polski, działając w krótkich odstępach czasu w wykonaniu z góry powziętego zamiaru, przekroczyła swoje uprawnienia funkcjonariusza Agencji Bezpieczeństwa Wewnętrznego w celu osiągnięcia korzyści majątkowej w postaci obietnicy przyszłego zatrudnienia w prywatnej firmie, w ten sposób, że ujawniła R.J. (1) za pośrednictwem komunikatora internetowego (…) i (…) informacje niejawne o klauzuli «tajne» dotyczące prowadzonych lub planowanych przez ABW czynności operacyjnych, w tym dotyczących obserwacji na podstawie art. 23 ust. 1 pkt 6 ustawy o ABW, wobec wyżej wymienionego R.J. (1), a nadto M.M. i M.S., czym działała na szkodę interesu publicznego, to jest o czyn z art. 231 § 1 i 2 k.k. w zw. z art. 265 § 1 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 12 § 1 k.k.”.

Sąd Okręgowy we Wrocławiu wyrokiem z dnia 10 września 2021 roku (III K 63/21):

a) uznał oskarżonego R.J. (1) za winnego popełnienia zarzucanego mu czynu opisanego w pkt I części dyspozytywnej wyroku, tj. za winnego popełnienia przestępstwa z art. 18 § 2 k.k. w zw. z art. 231 § 1 i 2 k.k. w zw. z art. 265 § 1 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 12 § 1 k.k. w zw. z art. 21 § 2 k.k., i za to przestępstwo wymierzył mu na podstawie art. 19 § 1 k.k. w zw. z art. 231 § 2 k.k. w zw. z art. 11 § 3 k.k. w zw. z art. 12 § 1 k.k. w zw. z art. 4 § 1 k.k. karę 1 roku pozbawienia wolności;

b) uznał oskarżoną K.T. za winną popełnienia zarzucanego jej czynu opisanego w pkt II części dyspozytywnej wyroku, tj. za winną popełnienia przestępstwa z art. 231 § 1 i 2 k.k. w zw. z art. 265 § 1 k.k. w zw. z art. 11 § 2 k.k. w zw. z art. 12 § 1 k.k., i za to przestępstwo wymierzył jej na podstawie art. 231 § 2 k.k. w zw. z art. 11 § 3 k.k. w zw. z art. 12 § 1 k.k. w zw. z art. 4 § 1 k.k. karę 1 roku pozbawienia wolności[1].

Wyrok ten zaskarżyli w całości obrońcy obojga oskarżonych.

Sąd apelacyjny zmienił zaskarżony wyrok w ten sposób, że:

a) uniewinnił R.J. (1) od popełnienia zarzucanego mu czynu, kosztami postępowania w tej części obciążając Skarb Państwa;

b) w zakresie czynu przypisanego oskarżonej K.T. w pkt II części rozstrzygającej ustalił, że 27 i 28 marca 2019 r. w K.L. jako funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego przekroczyła swoje uprawnienia w ten sposób, że ujawniła R.J. (1) za pośrednictwem komunikatora internetowego informacje niejawne o klauzuli „tajne” o prowadzonych wobec niego i M.M. przez funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego czynnościach operacyjno-rozpoznawczych polegających na obserwacji w trybie art. 23 ust. 1 pkt 6 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j. Dz.U. 2022, poz. 557 ze zm.), czym działała na szkodę interesu publicznego, i kwalifikuje przypisany jej czyn z art. 231 § 1 k.k. i art. 265 § 1 k.k. w zw. z art. 11 § 2 k.k., przyjmując przepis art. 265 § 1 k.k. w zw. z art. 11 § 3 k.k. za podstawę wymiaru kary, obniża wysokość wymierzonej oskarżonej K.T. w pkt V części rozstrzygającej grzywny do 50 stawek dziennych, w pozostałej części zaskarżony wyrok utrzymał w mocy.

Zdaniem sądu apelacyjnego rozważania na temat prawidłowości dokonanej przez sąd okręgowy oceny dowodów poprzedzać musi odniesienie się do zarzutów dotykających problemu legalności przeprowadzonej kontroli operacyjnej oraz tego, czy uzyskane w jej toku materiały zostały w sposób prawidłowy wprowadzone do procesu. Sąd apelacyjny zauważa, że dane

[1] SO we Wrocławiu orzeczone wobec oskarżonego R.J. (1) i oskarżonej K.T. kary pozbawienia wolności warunkowo zawiesił na 3 lata okresu próby. Ponadto orzekł wobec oskarżonego R.J. (1) karę grzywny w wymiarze 100 stawek dziennych przy przyjęciu wysokości jednej stawki na kwotę 100 zł, a wobec oskarżonej K.T. karę grzywny w wymiarze 100 stawek dziennych przy przyjęciu wysokości jednej stawki na kwotę 50 zł. Zobowiązał oskarżonego R.J. (1) oraz oskarżoną K.T. – w okresie próby – do informowania sądu o przebiegu okresu próby.

pozyskane w toku tej kontroli – przedstawione jako materiał dowodowy w sprawie – wykraczały poza ramy czasowe wynikające z postanowień Sądu Okręgowego w Warszawie (obejmowały także dane za okres poprzedzający zarządzenie kontroli – z kilku miesięcy sprzed października 2018 r.). Sąd apelacyjny stawia pytanie o znaczenie tej okoliczności z punktu widzenia legalności czynności operacyjnych – ich zgodności z warunkami ustawowymi określonymi w art. 17 ustawy o CBA. Zdaniem sądu apelacyjnego rysują się dwie możliwości. Pierwsza (zdaniem sądu apelacyjnego najprostsza) to taka, że czynności operacyjne wobec oskarżonego zostały wdrożone przez służby na długo przed tym, jak Sąd Okręgowy w Warszawie wydał postanowienie na podstawie art. 17 ust. 2 ustawy o CBA, i były one prowadzone przy braku tej decyzji procesowej przez okres kilku miesięcy. Następnie były kontynuowane (na mocy orzeczeń sądu) przez kolejne niespełna 6 miesięcy. Drugą możliwość stwarza wykorzystanie do pozyskania treści rozmów prowadzonych za pośrednictwem komunikatorów internetowych takiego środka technicznego, który umożliwiał dostęp do szerokiego spektrum danych z telefonu oskarżonego, w tym historycznych, bez jego wiedzy, ale także bez wiedzy operatora komunikatora, za pomocą którego oskarżony prowadził rozmowy pozostające w zainteresowaniu służb.

Należy podzielić pogląd sądu apelacyjnego, że pierwsza z tych sytuacji oznaczałaby nielegalność tej czynności, ale w tej sprawie nie mieliśmy z tym do czynienia – gdyby miała ona miejsce, sąd apelacyjny powinien złożyć zawiadomienie o popełnieniu przestępstwa (a tego nie uczynił). Jeśli chodzi o drugą z możliwości, sąd apelacyjny stwierdza, że również ona nie może być uznana za legalny sposób pozyskania w wyniku kontroli operacyjnej materiałów mających stanowić dowód w procesie. W dalszych wywodach sąd apelacyjny odnosi się do informacji, które pojawiły się w przestrzeni publicznej, o wykorzystywaniu przez służby specjalne różnych państw, m.in. europejskich, w tym w Polsce, oprogramowania do cybernetycznej inwigilacji. Następnie sąd apelacyjny podaje dość szczegółowo opis możliwości technicznych tego oprogramowania, które z uwagi na ich wyjątkowość są określane jako broń cybernetyczna, ofensywne narzędzie klasy wojskowej[2].

Zdaniem sądu apelacyjnego podniesione w toku postępowania odwoławczego poważne zastrzeżenia co do legalności użycia takiego środka techniki operacyjnej powodują konieczność ich rozważenia i obligują do zajęcia stanowiska w tym względzie, zważywszy na ich znaczenie dla rozstrzygnięcia sprawy. Sąd apelacyjny, formując pogląd o nielegalności środka techniki o cechach programu „Pegasus", w swoim uzasadnieniu opiera się głównie na ekspertyzie przygotowanej przez pracowników Katedry Prawa Karnego UJ (wielokrotnie się na nią powołując) zatytułowanej *Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych (casus Pegasusa)*[3]. Autorzy tej ekspertyzy ustalili[4], że w odniesieniu do stosowania systemu „Pegasus" doszło do złamania dyspozycji art. 48 ustawy z dnia 5 sierp-

[2] Sąd apelacyjny opisuje to oprogramowanie jako szpiegujące (typu *spyware*), umożliwiające pełną zdalną inwigilację jednostki. Przeznaczone jest ono do infekowania urządzeń mobilnych. Po zainstalowaniu przejmuje kontrolę nad telefonem, omijając wbudowane zabezpieczenia sprzętowe i programowe, łącznie z systemami szyfrowania danych. Daje pełen dostęp do wszystkich informacji znajdujących się na urządzeniu, m.in. wgląd w treść wiadomości tekstowych, pozwala na przechwytywanie połączeń głosowych, zapewnia dostęp do lokalizacji urządzenia, przechowywanych na nim filmów, zdjęć, notatek. Za pomocą tego oprogramowania możliwe jest włączenie w dowolnym momencie kamery i mikrofonu bez wiedzy użytkownika telefonu.

[3] A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zontek, *Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych (casus Pegasusa)*, Kraków 2022.

[4] Podobny pogląd wyrazili autorzy *Raportu końcowego Komisji Nadzwyczajnej do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych*, opublikowanego 6 września 2023 r. Senat RP X kadencji, druk nr 1090.

nia 2010 r. o ochronie informacji niejawnych[5] (oraz wydanego na mocy art. 49 ust. 9 tej ustawy rozporządzenia Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego[6]), bowiem zgodnie z art. 48 ust. 1 cytowanej ustawy systemy teleinformatyczne, w których mają być przetwarzane informacje niejawne, podlegają akredytacji bezpieczeństwa teleinformatycznego. Używanie systemu „Pegasus" jest niezgodne z prawem, ponieważ nie mógłby on uzyskać świadectwa akredytacji informatycznej, wymaganej zgodnie z cytowanym wyżej przepisem ustawy o ochronie informacji niejawnych[7]. Uzasadnienie wyroku sądu apelacyjnego jest wiernym powtórzeniem tych poglądów.

W swoim uzasadnieniu sąd apelacyjny nie używa określenia „Pegasus" w odniesieniu do środka techniki, który został zastosowany w czasie kontroli operacyjnej w tej sprawie, ale stwierdził, że „silne przesłanki zdają się wskazywać, że tego rodzaju system mógł zostać użyty"[8].

Z poglądem sądu apelacyjnego, że stosowanie w ramach kontroli operacyjnej środków technicznych o takich właściwościach (cechach) jak program „Pegasus" jest nielegalne, nie można się zgodzić. Zgodnie z dyrektywami wykładni prawa przyjmuje się zasadę pierwszeństwa wykładni językowej przed wykładnią systemową i funkcjonalną. Zasada pierwszeństwa wykładni językowej i subsydiarności wykładni systemowej i funkcjonalnej oznacza, że w sytuacji, gdy wykładnia językowa prowadzi do jasnego i jednoznacznego rezultatu, to w zasadzie tekst nie wymaga już dalszych zabiegów interpretacyjnych. Do wykładni systemowej i funkcjonalnej należy się odwołać tylko wtedy, gdy wykładnia językowa nie usunęła wszelkich wątpliwości[9]. Sąd apelacyjny wbrew zasadom wykładni prawa oparł się na wykładni systemowej i funkcjonalnej z pominięciem wykładni językowej przepisu art. w art. 17 ust. 1 ustawy o CBA.

Z punktu widzenia wykładni językowej kluczowe znaczenia dla rozstrzygnięcia kwestii legalności stosowania „Pegasusa" ma wyznaczenie zakresu znaczeniowego terminu „środek techniczny" użytego w przepisach dotyczących kontroli operacyjnej (art. 17 ustawy o CBA). W całym ustawodawstwie policyjnym nie znajdziemy definicji pojęcia „środek techniczny", o którym mowa w przepisach regulujących instytucję kontroli operacyjnej[10]. Wnikliwą analizę zakresu pojęcia „środki techniczne" (użytego w przepisach dotyczących kontroli operacyjnej) na gruncie prawa policyjnego w oparciu o wykładnię językową przeprowadził Trybunał Konstytucyjny w wyroku z dnia 30 lipca 2014 r.[11] Zdaniem Trybunału z wykładni językowej przepisów odnoszących się do pojęcia „środki techniczne" (Trybunał wymienia wszystkie przepisy dotyczące kontroli operacyjnej zawarte w ustawach kompetencyjnych) wynika, że środek taki musi, po pierwsze, mieć charakter techniczny, czyli być w jakiś sposób oparty na nowych technologiach, a po drugie – powinien pozwalać nie tylko pozyskiwać informacje, ale równocześnie je utrwalać[12]. Ten pogląd z uwagi na jego lakoniczność *prima facie* może rodzić wrażenie, że Trybunał Konstytucyjny nie zajmuje się szerzej możliwością wykorzystania nowych technologii w stosowaniu kontroli operacyjnej. Tak lakoniczna wypowiedź Trybunału (w tym miejscu) jest jednak uzasadniona w świetle wcześniejszych obszernych rozważań

[5] Dz.U. 2024, poz. 632.
[6] Dz.U. nr 159, poz. 948.
[7] *Raport końcowy*…, s. 33; A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zontek, *Dopuszczalność nabycia*…, s. 11–14.
[8] Uzasadnienie, s. 14.
[9] L. Morawski, *Zasady wykładni prawa*, Toruń 2006, s. 67–75 i cytowana tam literatura.
[10] Polskie ustawodawstwo policyjne nakłada na przedsiębiorcę telekomunikacyjnego, operatora pocztowego oraz usługodawcę świadczącego usługi drogą elektroniczną obowiązek zapewnienia na własny koszt warunków technicznych i organizacyjnych umożliwiających prowadzenie przez Policję kontroli operacyjnej. Jest to jedyna regulacja zawarta w ustawodawstwie policyjnym odnosząca się do warunków technicznych przeprowadzania kontroli operacyjnej.
[11] Wyrok TK z dnia 30 lipca 2014 r., K 23/11, Dz.U. poz. 1055.
[12] L. Morawski, *Zasady wykładni*…, s. 79–80.

zawartych w uzasadnieniu wyroku, które należy przytoczyć *in extenso*, aby rozwiać wszelkie wątpliwości co do stanowiska Trybunału w tej, jak już wspomniałem, kluczowej kwestii:

„Trybunał Konstytucyjny przyjmuje, że zasygnalizowana wyżej specyfika nowych technologii i ocena zagrożeń z nimi związanych uzasadnia powierzenie wyspecjalizowanym organom władzy publicznej, jakimi są służby policyjne i służby ochrony państwa (vide: art. 103 ust. 2 Konstytucji), adekwatnych uprawnień, dzięki którym będą one w stanie zapobiegać przestępstwom i je wykrywać, ścigać ich sprawców, a także dostarczać informacji na temat zagrożeń dóbr prawnie chronionych. Demokratyczne państwo prawne nie może bowiem ignorować rosnącego znaczenia nowych technologii, a ponadto skali ich wykorzystywania, niekiedy również w celu naruszania prawa. Wymaga to wyposażenia tych służb w stosowne uprawnienia i stworzenia im warunków finansowych i organizacyjnych, umożliwiających efektywną walkę z naruszeniami prawa. Organy władzy publicznej powinny dysponować prawną i faktyczną możliwością wykrywania popełnianych przestępstw i działalności skierowanej przeciwko państwu czy jego konstytucyjnym organom. Powinny one też móc wyprzedzać działania osób naruszających prawo, nie dopuszczając do wystąpienia zagrożeń. W warunkach globalnej przestępczości i przekraczającego granice państw terroryzmu czy przestępczości zorganizowanej istotna jest także prewencja zagrożeń, których wystąpienie może wyrządzić nieodwracalne straty dla dóbr prawnie chronionych. Zdaniem Trybunału brak wyposażenia służb policyjnych oraz służb ochrony państwa w możliwość korzystania ze zdobyczy nowoczesnej techniki, a nawet wyposażenie ich w taką możliwość, lecz w niewystarczającym zakresie, może oznaczać niewywiązanie się państwa z jego konstytucyjnego zadania strzeżenia niepodległości i nienaruszalności terytorium Rzeczypospolitej Polskiej, a także zapewnienia bezpieczeństwa obywateli (art. 5 Konstytucji), czy naruszać zasadę sprawności działania instytucji publicznych (wstęp do Konstytucji). Niekiedy może powodować naruszenie obowiązków wiążących Polskę umów międzynarodowych zobowiązujących do współdziałania w walce z międzynarodową przestępczością i terroryzmem"[13].

Ponadto Trybunał Konstytucyjny wskazał, że niezbędne jest sprecyzowanie sposobu niejawnego wkroczenia w sferę prywatności jednostki. Nie jest przy tym konieczne wskazanie w przepisach prawa konkretnych środków techniki operacyjnej ani tym bardziej zdefiniowanie ich parametrów. Trybunał podkreślił natomiast, że istotne jest określenie w przepisach prawa zamkniętego rodzajowo katalogu środków i metod działania, za pomocą których władze publiczne mogą w sposób niejawny gromadzić informacje o jednostkach. Zdaniem Trybunału Konstytucyjnego nie chodzi o wskazanie parametrów technicznych, ale rodzajowych nazw poszczególnych środków i informacji możliwych do pozyskania za ich pomocą (np. podsłuch rozmów telefonicznych, podsłuch i podgląd pomieszczeń i osób, podsłuch techniczny środków łączności przewodowej i radiowej, nadzór elektroniczny osób, miejsc i przedmiotów oraz środków transportu, nadzór elektroniczny środków łączności przewodowej lub radiowej). Trybunał trafnie wskazuje: „Mając na uwadze ogromną liczbę środków stosowanych przez organy państwa przydatnych w pracy operacyjno-rozpoznawczej, ustawowy ich katalog musiałby być rozbudowany, a co za tym idzie norma prawna musiałaby być kazuistyczna"[14]. Rozwiązanie to mogłoby kolidować z wymogiem abstrakcyjności normy prawnej.

Jak wielokrotnie wskazywał Trybunał, również w perspektywie określoności przepisów represyjnych przestrzeganie wymogów wynikających z zasady dostatecznej określoności prawa nie może prowadzić do kazuistyki unormowania[15]. Podobnie uznał Trybunał

[13] *Ibidem*, s. 52.
[14] *Ibidem*, s. 72.
[15] Zob. wyroki TK z dnia: 26 listopada 2003 r., SK 22/02, OTK ZU 2003, nr 9A, poz. 97, cz. III, pkt 4; 5 maja 2004 r., P 2/03, OTK ZU 2004, nr 5A, poz. 39, cz. III, pkt 3.5; 13 stycznia 2005 r., P 15/02, OTK ZU

w wyroku dotyczącym przepisów regulujących prowadzenie kontroli operacyjnej przez wywiad skarbowy[16], akceptując – po spełnieniu kilku warunków – pewien stopień ogólności unormowania sposobów kontroli operacyjnej prowadzonej przez wywiad skarbowy.

Należy podzielić pogląd Trybunału Konstytucyjnego, że na państwie spoczywa obowiązek zapewnienia służbom policyjnym i służbom ochrony państwa prawnej i faktycznej (w tym finansowej i organizacyjnej) możliwości wykonywania ich zadań z wykorzystaniem najnowszych środków techniki. Trybunał trafnie podnosi, że wyposażenie odpowiednich służb w te uprawnienia, jeśli okaże się niewystarczające, oznacza również niewywiązanie się państwa z jego konstytucyjnego zadania strzeżenia niepodległości i nienaruszalności terytorium Rzeczypospolitej Polskiej, a także zapewnienia bezpieczeństwa obywateli.

Podstawowym zarzutem do argumentacji sądu apelacyjnego jest zastosowanie wykładni systemowej w sytuacji, gdy wykładnia językowa (której sąd apelacyjny w odróżnieniu od Trybunału Konstytucyjnego nie zastosował) prowadzi do jasnego i jednoznacznego rezultatu (i w zasadzie tekst nie wymaga już dalszych zabiegów interpretacyjnych). Krytycznie ocenić należy również sposób przeprowadzenia wykładni systemowej. Zasadniczym zarzutem wobec wywodów sadu apelacyjnego co do nielegalności stosowania systemu typu „Pegasus" jest to, że opierają się one na braku możliwości uzyskania przez ten system akredytacji w zakresie przetwarzania danych w trybie 48 u.o.i.n. Oprócz trafnych uwag Norberta Loby, że ustawa ta odnosi się do innej sytuacji faktycznej niż w sprawie rozpoznawanej przez sąd apelacyjny – trzeba zauważyć, że czynność operacyjno-rozpoznawcza określana jako kontrola operacyjna (ustawa o CBA w art. 17 ust. 1) polega na uzyskaniu i utrwaleniu dowodów tzw. przestępstw katalogowych. Zgodnie z tym przepisem (a także przepisami innych tzw. ustaw policyjnych) w zakres kontroli operacyjnej nie wchodzi czynność przetwarzania danych. W ustawach policyjnych uprawnienie do przetwarzania danych regulują inne przepisy niż te dotyczące kontroli operacyjnej (np. art. 18 i 18b ustawy o CBA).

Z wywodem sądu apelacyjnego nie można się zgodzić. Z treści art. 51 ust. 1 u.o.i.n. wynika tylko tyle, że materiały niejawne uzyskane w trakcie wszystkich czynności operacyjno-rozpoznawczych (nie tylko kontroli operacyjnej, ale też inne, np. dane billingowe) przetwarzane być muszą na urządzeniach certyfikowanych, natomiast pozyskiwanie i utrwalanie informacji w trakcie realizacji czynności operacyjno-rozpoznawczych nie wymaga certyfikowanych urządzeń, programów itp. Materiały pozyskane przy użyciu „Pegasusa" uzyskane zostały leganie (u.i.o.n. pozwala na pozyskiwanie danych przy użyciu niecertyfikowanej sieci telekomunikacyjnej) i legalnie przy użyciu niecertyfikowanej sieci mogą zostać przekazane do dalszych prac (przetwarzania na urządzeniach i programach certyfikowanych).

Dodatkowym argumentem przemawiającym za tym, że brak uprawnienia do przetwarzania danych na urządzeniach niecertyfikowanych nie pozbawia uprawnionych służb możliwości posługiwania się takimi urządzeniami, jest treść art. 51 ust. 2 u.o.i.n. Przepis ten zwalnia z obowiązku akredytacji ABW, AW, SKW i SWW także w zakresie przetwarzania danych. Skoro zdaniem sądu apelacyjnego brak tego uprawnienia w art. 51 ust. 1 decyduje o konieczności uzyskania akredytacji dla programu „Pegasus", to odnosić się to może tylko do pozostałych służb policyjnych i specjalnych (poza ABW, AW, SKW i SWW), które mają uprawnienia do prowadzenia czynności operacyjno-rozpoznawczych[17]. Odnosząc się do treści

2005, nr 1A, poz. 4, cz. III, pkt 2; 28 czerwca 2005 r., SK 56/04, OTK ZU 2005, nr 6A, poz. 67, cz. V, pkt 1; 17 grudnia 2008 r., P 16/08, OTK ZU 2008, nr 10A, poz. 181, cz. IV, pkt 8.2.2; 22 czerwca 2010 r., SK 25/08, OTK ZU 2010, nr 5A, poz. 51, cz. III, pkt 4.1–4.2; 1 grudnia 2010 r., K 41/07, OTK ZU 2010, nr 10A, poz. 127, cz. III, pkt 3.2.

[16] Wyrok TK z dnia 20 czerwca 2005 r., K 4/04, cz. V, pkt 2.6.

[17] W sytuacji, gdyby zaistniała taka konieczność, w obecnym stanie prawnym CBA musiałaby skorzystać

art. 51 ust. 1 i twierdzenia, że nie zwalnia on z konieczności uzyskania akredytacji dla programów typu „Pegasus", sąd apelcyjny używa określenia „wydaje się". Natomiast w konkluzji rozważań w uzasadnieniu stwierdza już kategorycznie, że stosowanie takich programów (jak „Pegasus") jest w polskim systemie prawnym nielegalne. Teza ta nie jest prawdziwa w świetle treści przepisów art. 51 u.o.i.n. i przedstawionej powyżej argumentacji.

Nie można się też zgodzić z poglądem sądu apelacyjnego co do tzw. danych historycznych, czyli danych (przedstawionych jako materiał dowodowy w sprawie) obejmujących okres poprzedzający zarządzenie kontroli (kilku miesięcy sprzed października 2018 r.). Sąd apelacyjny pomija oczywisty fakt, że zgodnie z polskim ustawodawstwem kontrola operacyjna prowadzona jest niejawnie i polega na: 1) uzyskiwaniu i utrwalaniu treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych; 2) uzyskiwaniu i utrwalaniu obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne; 3) uzyskiwaniu i utrwalaniu treści korespondencji, w tym korespondencji prowadzonej za pomocą środków komunikacji elektronicznej; 4) uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych; 5) uzyskiwaniu dostępu i kontroli zawartości przesyłek (art. 17 ust. 5 ustawy o CBA)[18]. Trzy pierwsze punkty istotnie ograniczają możliwość pozyskiwania danych do okresu po zarządzeniu kontroli, natomiast dwa ostatnie dotyczą danych, które w momencie zarządzenia kontroli operacyjnej już są zgromadzone w poddanych kontroli miejscach, z istoty swojej mają więc walor historyczny. Oczywiste jest, że zawartość przesyłki została w niej umieszczona przed zarządzeniem kontroli, a nie po jej zarządzeniu. To samo dotyczy danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych. Ten rodzaj informacji był objęty postanowieniem o zarządzeniu kontroli operacyjnej w tej sprawie, w związku z tym również „dane historyczne" uzyskane zostały legalnie.

Do zagadnienia tego sąd apelacyjny odnosi się, stawiając pytanie o to, czy zmiana art. 17 ust. 5 ustawy o CBA dokonana w 2016 r. rzeczywiście odpowiada głównym tezom wyroku Trybunału, czy też paradoksalnie nie poszła dużo dalej, otwierając drogę do nieograniczonej inwigilacji. Zdaniem sądu apelacyjnego odpowiedź na to pytanie nie jest możliwa bez odczytania treści tego przepisu, jego pkt 4, w kontekście standardów konwencyjnych i konstytucyjnych wypracowanych na gruncie art. 8 Europejskiej Konwencji Praw Człowieka oraz art. 47 i 49 Konstytucji RP, te zaś nie pozwalają uznać za dopuszczalne stosowanie przez służby takich środków kontroli operacyjnej, które wiążą się z omijaniem i przełamaniem zabezpieczeń urządzeń mobilnych oraz uzyskiwaniem w ten sposób dostępu do szerokiego spektrum danych, w tym historycznych, wykraczających poza ramy czasowe zarządzonej kontroli operacyjnej.

W tym krótkim fragmencie uzasadnienia sąd apelacyjny wyraźnie przekracza kompetencje władzy sędziowskiej. Nie jest rolą sądu ocena, czy ustawodawca w procesie legislacyjnym wypełnił zalecenia zawarte w wyroku Trybunału Konstytucyjnego, a tym bardziej nie jest on uprawniony do stwierdzenia, że określony przepis ustawy nie spełnia standardów konstytucyjnych i w związku z tym sąd nie jest nim związany. W polskim systemie prawnym rolą sądów powszechnych jest stosowanie prawa, a nie rozstrzyganie, które przepisy ustawy obowiązują, a które nie. Ponadto wbrew temu,

z systemu posiadającego akredytację, natomiast ABW, AW, SKW i SWW mogłyby się posłużyć systemem, który nie posiada akredytacji także w zakresie przetwarzania danych.

[18] Przepisy dotyczące kontroli operacyjnej zawarte w innych ustawach policyjnych mają identyczne regulacje (zob. m.in. art. 19 ustawy o Policji, art. 27 ustawy o ABW oraz AW, art. 31 ustawy o ŻW, art. 31 ustawy o SKW oraz SWW).

co twierdzi sąd apelacyjny, w cytowanym wyroku Trybunału Konstytucyjnego z 2014 r. możemy wskazać podstawę do takiej regulacji prawnej. Trybunał uważa, że ustawy policyjne powinny zawierać wskazanie rodzajowych nazw poszczególnych środków technicznych i informacji możliwych do pozyskania za ich pomocą (np. podsłuch rozmów telefonicznych, podsłuch i podgląd pomieszczeń i osób itd.). Kwestionowany przez sąd apelacyjny przepis art. 17 ust. 5 pkt 1–5 ustawy o CBA zawiera zamknięty katalog rodzajów informacji możliwych do uzyskania w wyniku stosowania kontroli operacyjnej. Oczywiste jest, że uzyskanie w sposób niejawny określonego rodzaju informacji będzie wymagało zastosowanie odpowiedniego środka technicznego. Na przykład inny środek będzie zastosowany do uzyskania treści rozmowy telefonicznej, inny – do uzyskania i utrwalenia obrazu, inny – do uzyskania i utrwalenia dźwięku, a jeszcze inny – do rejestracji obrazu i dźwięku. Również zupełnie inny środek będzie zastosowany do tajnego przeszukania bagażu. Do uzyskiwania i utrwalania danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych (art. 17 ust. 5 pkt 4 ustawy o CBA) służą właśnie programy komputerowe takie jak „Pegasus". Sąd apelacyjny stwierdza, że „w czasie, gdy przepis ten był nowelizowany, gdy ten dodatkowy środek czy metoda kontroli operacyjnej wprowadzane były do ustawy o CBA [art. 17 ust. 5 pkt 4 ustawy o CBA – przyp. A.T.], w przestrzeni publicznej nie było jeszcze informacji o oprogramowaniu szpiegującym (…) oraz o możliwościach, jakie ono daje. Informacje takie po raz pierwszy pojawiły się dużo później", i podnosi wątpliwość, czy ustawodawca istotnie chciał wprowadzić do ustawy o CBA tego rodzaju możliwość uzyskiwania informacji w drodze kontroli operacyjnej. Argument ten nie zasługuje na aprobatę. Fakt, że w opinii publicznej nie było powszechnej wiedzy na temat aspektów technicznych jakiejś metody czy środka technicznego przewidzianego w ustawie, nie ma wpływu na obowiązywanie czy też nie określonego przepisu. Dopuszczenie takiej możliwości wprowadziłoby zupełny chaos prawny.

Konkludując, należy stwierdzić, że sąd apelacyjny, uznając, że kontrola operacyjna zastosowana przy użyciu programu typu „Pegasus" jest nielegalna, nie posłużył się argumentami wynikającymi z treści art. 17 ust. 5 pkt 4 ustawy o CBA, a raczej skoncentrował się na wykazaniu, że przepis ten nie spełnia standardów konstytucyjnych. Tezę swą uzasadniał, stosując w sposób wadliwy wykładnię systemową w oparciu o przepisy innych ustaw, które nie odnoszą się do kontroli operacyjnej (więc nie mają zastosowania w tej sprawie). Czynność rozpoznawczo-operacyjna określana jako kontrola operacyjna polega na uzyskaniu i utrwaleniu dowodów tzw. przestępstw katalogowych, a nie na przetwarzaniu danych. W związku z tym wykazywanie przez sąd apelacyjny, że program o cechach „Pegasusa" nie uzyskałby akredytacji (i w związku z tym nie mógł być legalnie zastosowany w ramach kontroli operacyjnej), jest zabiegiem zupełnie chybionym. Należy przypomnieć, że ustawodawstwo policyjne nie zawiera przepisów ograniczających zakres pojęcia „środki techniczne".

Abstract

The 'Pegasus' program as a legal technical measure used in the course of operational surveillance – commentary on the judgment of the Court of Appeal in Wrocław of 11 May 2023, II AKa 480/21

Keywords: *operational surveillance; Pegasus; technical means; operational activities*

The author critically evaluates the position of the Court of Appeal in Wrocław expressed in the judgment of 11 May 2023 (II AKa 480/21), in which the Court deemed the use of technical measures resembling the Pegasus software in operational surveillance as illegal. The author argues that police legislation (including the Act on the Central Anti-Corruption Bureau) does not impose any limitations regarding the types of technical measures used. He concurs with the position of the Constitutional Tribunal that the technical measures employed in operational surveillance must be based on the latest technologies enabling the acquisition and recording of information.

Bibliografia

Literatura

Barczak-Oplustil A., Małecki M., Tarapata S.,Behan A., Zontek W., *Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych (casus Pegasusa)*, Kraków 2022.

Morawski L., *Zasady wykładni prawa*, Toruń 2006.

Akty prawne

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz.U. 2010, nr 182, poz. 1228).

Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz.U. 2011, nr 159, poz. 948).

Orzecznictwo

Wyrok TK z dnia 30 lipca 2014 r., K 23/11, Dz.U. poz. 1055.

Wyrok TK z dnia 26 listopada 2003 r., SK 22/02, OTK ZU 2003, nr 9A, poz. 97.

Wyrok TK z dnia 5 maja 2004 r., P 2/03, OTK ZU 2004, nr 5A, poz. 39.

Wyrok TK z dnia 13 stycznia 2005 r., P 15/02, OTK ZU 2005, nr 1A, poz. 4.

Wyrok TK z dnia 28 czerwca 2005 r., SK 56/04, OTK ZU 2005, nr 6A, poz. 67.

Wyrok TK z dnia 17 grudnia 2008 r., P 16/08, OTK ZU 2008, nr 10A, poz. 181.

Wyrok TK z dnia 22 czerwca 2010 r., SK 25/08, OTK ZU 2010, nr 5A, poz. 51.

Wyrok TK z dnia 1 grudnia 2010 r., K 41/07, OTK ZU 2010, nr 10A, poz. 127.

Wyrok TK z dnia 20 czerwca 2005 r., K 4/04.

Inne

Raport końcowy Komisji Nadzwyczajnej do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych, Senat RP X kadencji, druk nr 10.