

Miłosz Kościelniak-Marszał

## Wpływ oprogramowania typu Pegasus na korzystanie w procesie karnym z materiałów zabezpieczonych z urządzeń mobilnych

*The impact of Pegasus-like software on the use of materials secured from mobile devices in criminal proceedings*

### Abstract

*Pegasus-like spyware was developed as a tool for active intelligence work, where the procedural use of the collected data was of secondary importance. Its use to obtain evidence for a criminal trial triggers the need for procedural authorities to change their approach to all data obtained from terminal devices. The functionality which gives the system operator the option to interfere with the content of information contained in the device, make changes to it, or even implement it – without being able to determine who (the subject of the surveillance or the operator) placed, modified or removed the given content on, in, or from the device – means that the use of such materials as a source of incriminating findings against a defendant must lead to the conclusion that the criminal trial where such materials are used is, as a whole, not fair and violates Article 45 of the Constitution of the Republic of Poland and Article 6(1) of the European Convention on Human Rights.*

**Keywords:** surveillance, evidence, investigation, criminal trial

### Streszczenie

Oprogramowanie szpiegujące typu Pegasus powstało jako narzędzie aktywnej pracy wywiadowczej, przy której procesowe wykorzystywanie zgromadzonych danych ma znaczenie drugorzędne. Zastosowanie go w celu zdobycia dowodów na potrzeby procesu karnego wywołuje konieczność zmiany podejścia organów procesowych do wszystkich danych uzyskiwanych z urządzeń końcowych. Funkcjonalność dająca możliwość ingerowania przez operatora systemu w treść informacji znajdujących się w urządzeniu, dokonywanie w nich zmian lub nawet implementacji,

Dr Miłosz Kościelniak-Marszał, Uniwersytet Opolski, Polska, ORCID: 0000-0002-7261-3389, e-mail: kancelaria@adwokاتمilosz.pl

Data zgłoszenia tekstu przez autora: 2.10.2024 r.; data zaakceptowania do publikacji: 24.07.2025 r.

*bez możliwości ustalenia, kto (obiekt inwigilowany czy operator Pegasusa) umieścił, zmodyfikował lub usunął dane treści z urzędzenia, powoduje, że wykorzystanie takich materiałów jako źródła obciążających oskarżonego ustaleń prowadzić musi do wniosku, że proces karny jako całość nie jest sprawiedliwy i narusza art. 45 Konstytucji Rzeczypospolitej Polskiej oraz art. 6 ust. 1 Europejskiej Konwencji Praw Człowieka.*

**Słowa kluczowe:** inwigilacja, dowód, śledztwo, proces karny

## 1. Wstęp

Międzynarodową dyskusję nad prawidłowym korzystaniem przez organy państwowe z oprogramowania o nazwie Pegasus zainicjowało śledztwo przeprowadzone w 2021 r. przez dziennikarzy Forbidden Stories oraz Amnesty International, w wyniku którego ujawniono, że izraelska spółka NSO Group sprzedawała takim państwom jak Meksyk, Arabia Saudyjska, Azerbejdżan, Armenia, Indie, Maroko, Węgry oraz Polska oprogramowanie o tej nazwie, które miało służyć do zwalczania najpoważniejszych przestępstw, zwłaszcza terroryzmu.

Pierwszym klientem NSO Group był Meksyk, gdzie system przyczynił się do schwytania narkotykowego barona. Wkrótce jednak obiektami inwigilacji stali się obrońcy praw człowieka oraz osoby pozostające w opozycji do władz państwowych. W październiku 2018 r. zabito krytyka saudyjskiej rodziny królewskiej Jamala Khashoggię. Analiza jego telefonu oraz aparatów bliskich mu osób wykazała, że w miesiącach poprzedzających śmierć i po niej byli oni inwigilowani Pegasusem. W Azerbejdżanie ujawniono ponad 1000 numerów telefonicznych, które zostały zainfekowane tym programem. Wśród inwigilowanych znaleźli się m.in. dziennikarze, w tym Khadija Ismayilova z Radio Free Europe. W Armenii Pegasus był stosowany zarówno wobec dziennikarzy, jak i obrońców praw człowieka. Z kolei rząd węgierski wykorzystał go przeciwko dziennikarzom, politykom opozycji, prawnikom, wykładowcom akademickim, prokuratorom oraz działaczom społecznym. W Grecji szpiegowano w ten sposób ok. 300 osób, w tym członków Parlamentu Europejskiego i dziennikarzy. W Hiszpanii inwigilowano nim premiera, ministra obrony narodowej, ministra spraw wewnętrznych oraz innych wysokiej rangi urzędników, a także członków lokalnego rządu Katalonii, osoby należące do ruchu walczącego o niezależność Katalonii oraz członków Parlamentu Europejskiego, prawników, wykładowców akademickich, jak również przedstawicieli społeczeństwa obywatelskiego. Maroko i Rwanda inwigilowały Pegasusem m.in. prezydenta Francji, premiera, ministra obrony i ministra spraw wewnętrznych Hiszpanii, premiera Belgii, poprzedniego przewodniczącego Komisji Europejskiej, a także byłego premiera Włoch. W Polsce Pegasusa natomiast użyto wobec senatora Krzysztofa Brejzy w okresie, gdy kierował sztabem wyborczym partii opozycyjnej w 2019 r., oraz prokurator Ewy Wrzosek, która krytykowała niedemokratyczne zmiany w polskim sądownictwie, a także sprzeciwiającego się polityce rządu, a zwłaszcza ministrowi sprawiedliwości, adwokata Romana Giertycha<sup>1</sup>.

Cel i sposób wykorzystywania przez państwo polskie wspomnianego oprogramowania rozpały ogromne emocje, których eskalacji sprzyjały zbliżające się wybory parlamentarne. W trakcie kampanii nadużycia związane z Pegasusem stały się ważną kartą w rękach działaczy opozycji. W szczególności zarzucano, że tylko senator K. Brejza był inwigilowany 33 razy, a na jego telefon został wprowadzony ok. 1 GB danych, czyli zmieniono zawartość jego telefonu przez dodanie nowej zawartości<sup>2</sup>.

<sup>1</sup> M. Matusiak-Frącczak, *Konwencyjne standardy legalnej inwigilacji a zastosowanie systemu Pegasus w Polsce*, „Europejski Przegląd Sądowy” 2023/12, s. 26–28.

<sup>2</sup> M. Matusiak-Frącczak, *Konwencyjne...*, s. 28.

Zmodyfikowane materiały zostały w toku poprzedniej kampanii wyborczej pokazane widzom kontrolowanej przez rząd telewizji, co wskazywało, że użycie Pegasusa miało kontekst polityczny, a nie prawnokarny<sup>3</sup>.

W tym samym czasie Parlament Europejski powołał komisję śledczą ds. Pegasusa. Komisja opracowała raport, który został przyjęty przez Parlament zaleceniem z 15.06.2023 r. Stwierdzono w nim, że omawiana inwigilacja nie spełnia wymogów nakreślonych w orzecznictwie Europejskiego Trybunału Praw Człowieka (dalej ETPC) i Trybunału Sprawiedliwości Unii Europejskiej (dalej TSUE), w związku z czym jest sprzeczna z zasadami zawartymi w art. 2 Traktatu o Unii Europejskiej<sup>4</sup> oraz prawami podstawowymi zawartymi w art. 7 (prawo do poszanowania prywatności), art. 8 (ochrona danych osobowych), art. 11 (prawo do swobody wypowiedzi), art. 17 (prawo własności), art. 21 (zasada niedyskryminacji) i art. 47 (prawo do skutecznego środka prawnego i dostępu do bezstronnego sądu) Karty praw podstawowych Unii Europejskiej<sup>5</sup>.

Osobną płaszczyznę rozważań stanowią wątpliwości dotyczące funkcjonalności oprogramowania szpiegowskiego, w aspekcie wykorzystania zdobytych za jego pomocą materiałów w ewentualnym postępowaniu karnym.

## 2. Pegasus jako narzędzie kontroli operacyjnej

Wraz z wybuchem „afery Pegasusa” w polskim piśmiennictwie pojawiły się głosy, że tego rodzaju narzędzia są niezbędną odpowiedzią na kierunek, w jakim rozwija się współczesna przestępczość, i stanowią konieczne dziś wyposażenie służb. Podkreślano, że inne państwa wdrożyły jeszcze bardziej zaawansowane metody pracy operacyjnej aniżeli formy przewidziane w prawie polskim. Przykładowo szwedzkie służby dysponują systemem nasłuchu elektromagnetycznego, a więc przechwytywania i analizy treści komunikacji prowadzonej przez miliony obywateli. Podobne rozwiązania przewidywał brytyjski Investigatory Powers Act. Inny przykład to przejście przez służby francuskie prywatnego komunikatora EncroChat i masowe przechwytywanie wiadomości z dziesiątek tysięcy telefonów. Natomiast w Niemczech przepisy przyznają służbom prawo wykorzystania oprogramowania do przełamывania zabezpieczeń telefonów i komputerów oraz do odczytywania zawartości urządzeń użytkowanych przez osoby, którym oficjalnie nie postawiono zarzutów, a są dopiero podejrzewane o popełnienie przestępstwa. Narzędzia takie nazywane są „*Staatstrojanern*”, czyli „trojanami państwowymi”, i stosowane do szerszej grupy przestępstw aniżeli tylko terrorystyczne<sup>6</sup>. Zwrócono jednocześnie uwagę, że choć działania takie wkraczają w podstawowe prawa i wolności obywatelskie, to formy i metody realizacji czynności

<sup>3</sup> M. Matusiak-Frącczak, *Konwencyjne...*, s. 29.

<sup>4</sup> Traktat o funkcjonowaniu Unii Europejskiej z 25.03.1957 r. (Dz.U. z 2004 r. Nr 90, poz. 864/2 ze zm.).

<sup>5</sup> Karta praw podstawowych Unii Europejskiej (Dz.Urz. UE C 303 z 14.12.2007 r., s. 1); M. Matusiak-Frącczak, *Konwencyjne...*, s. 28.

<sup>6</sup> P. Opitek, *Poważnie kontrolować można nie tylko terrorystów*, „Rzeczpospolita” z 20.01.2022 r., <https://www.rp.pl/opinie-prawne/art19306701-pawel-opitek-powaznie-kontrolowac-mozna-nie-tylko-terrorystow> (dostęp: 25.04.2024 r.).

operacyjno-rozpoznawczych, a więc technika pracy służb, muszą pozostawać tajemnicą, aby były skuteczne w walce z przestępczością i aby funkcjonariusze i osoby udzielające pomocy organom ścigania czuli się bezpieczni<sup>7</sup>. Utajenie powyższych informacji nie przeszkodziło autorytatywnie zarzucić nieprawdziwość twierdzeniom, jakoby wdrożenie kontroli operacyjnej pozwalało na zarządzanie mikrofonem oraz kamerą telefonu i rejestrację zapisu audio-video z otoczenia aparatu, a więc totalną inwigilację osoby<sup>8</sup>. Nie zabrakło przy tym oskarżeń o populizm i wywoływanie powszechnej niechęci do kontroli operacyjnej, które może wywołać brak społecznej akceptacji stosowania tej formy gromadzenia dowodów i w efekcie doprowadzić do sytuacji, że w przyszłości czynności takie zostaną wyrugowane z polskiego porządku prawnego. Wówczas pojawiłoby się pytanie, za pomocą jakich innych metod uprawnione (i obowiązane) organy państwa miałyby dbać o bezpieczeństwo wewnętrzne i zewnętrzne, i w jaki to inny sposób następowałoby zbieranie dowodów popełnienia najbardziej szkodliwych społecznie czynów zabronionych, takich jak czyny związane ze zdarzeniami terrorystycznymi, funkcjonowaniem zorganizowanych grup przestępczych czy czyny korupcyjne<sup>9</sup>.

Odpowiedź na tak sformułowane pytanie, niosące w podtekście kasandryczne wizje przyszłości, nie wydaje się jednak w ogóle potrzebna, gdyż dotąd w debacie publicznej nie pojawił się nigdzie postulat rezygnacji z kontroli operacyjnych, a cała krytyka koncentruje się wokół metody realizacji takich czynności poprzez stosowanie oprogramowania szpiegującego o nieproporcjonalnie szerokim spektrum działania oraz zdobywania za jego pomocą materiałów dowodowych na potrzeby procesu karnego. W grę wchodzi bowiem szereg praw obywateli, które mogą zostać w ten sposób naruszone, w szczególności art. 47 (prawo do poszanowania prywatności), art. 49 (prawo do tajemnicy korespondencji), art. 51 (prawo do ochrony danych osobowych), art. 42 (prawo do obrony), art. 45 ust. 1 (prawo do sprawiedliwego procesu) Konstytucji Rzeczypospolitej Polskiej<sup>10</sup>.

Przytoczone rozbieżności wpisują się w spór pomiędzy zadeklarowanymi zwoleńnikami sięgania przez państwo po formy tajnego zdobywania informacji, którzy uważają, że jest to niezbędne narzędzie walki z najpoważniejszymi formami przestępczości, a ich oponentami, którzy są przekonani, że metody takie nie licują z godnością wymiaru sprawiedliwości<sup>11</sup>, a samą kontrolę operacyjną postrzegają jako źródło potencjalnych nadużyć i opresyjną aktywność państwa<sup>12</sup>. Ich obawy potęguje brak skutecznych mechanizmów kontroli nad służbami w zakresie zarówno podstaw zastosowania

<sup>7</sup> P. Opitek, *Kontrola operacyjna urzędnika końcowego*, „Prokuratura i Prawo” 2023/4, s. 37–38.

<sup>8</sup> P. Opitek, *Kontrola...*, s. 43–44.

<sup>9</sup> T. Łodziana, *Kontrola operacyjna oraz użycie systemu Pegasus w Polsce – polemika*, „Palestra” 2022/9, s. 63, <https://palestra.pl/pl/czasopismo/wydanie/9-2022/artukul/kontrola-operacyjna-oraz-uzycie-systemu-pegasus-w-polsce-polemika> (dostęp: 25.04.2024 r.).

<sup>10</sup> Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. Nr 78, poz. 483 ze zm.) – dalej Konstytucja RP;

<sup>11</sup> M. Matusiak-Frącczak, *Kontrola operacyjna oraz użycie systemu Pegasus w Polsce*, „Palestra” 2022/7–8, s. 17–18.

<sup>12</sup> A. Taracha, *Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawnodowodowe*, Lublin 2006, s. 346.

<sup>12</sup> P. Opitek, *Kontrola...*, s. 37–38.

inwigilacji, jak i korzystania przez służby z metodologii, w szczególności określonego typu oprogramowania do zdobywania materiałów, które są następnie wykorzystywane na potrzeby oskarżenia w prowadzonych postępowaniach karnych. Zwrócić tymczasem trzeba uwagę, że tajna inwigilacja jest w Polsce stosowana na ogromną skalę – w samym tylko 2022 r. sądy wydały zgody na podsłuchy w ponad 99% przypadków, a Policja zastosowała go aż 9781 razy. Jednocześnie Najwyższa Izba Kontroli, po zbadaniu okresu od 1.01.2017 r. do 31.03.2023 r., postawiła wniosek, że obowiązujący w Polsce system nadzoru, koordynacji oraz kontroli działalności służb specjalnych jest nieskuteczny i nie odpowiada standardom obowiązującym w demokratycznych państwach prawa. W szczególności nie zapewnia efektywnego nadzoru nad realizacją zadań służb oraz nie gwarantuje, że w toku ich wykonywania będą przestrzegane obowiązujące przepisy prawa oraz respektowane prawa i wolności obywatelskie<sup>13</sup>. Nie wiadomo przy tym, ile programów, które pozwalają na kontrolę urządzeń końcowych, posiadają polskie służby. Ujawniono natomiast, że w latach 2017–2022 trzy z nich wykorzystwały Pegasusa do kontroli operacyjnej urządzeń końcowych wobec 578 osób. W 2017 r. dotyczyło to 6 osób, w 2018 r. – 100 osób, w 2019 r. – 140 osób, w 2020 r. – 161 osób, w 2021 r. – 162 osób, a w 2022 r. – 9 osób<sup>14</sup>. W ogólnym rozrachunku liczby te z pewnością okazałyby się większe, gdyż Pegasus nie był jedynym tego typu systemem, jakim dysponowały polskie służby. Wskazuje na to okoliczność, że 6.03.2024 r. prokurator w Prokuraturze Regionalnej w Rzeszowie wszczął śledztwo w sprawie przekroczenia uprawnień oraz niedopełnienia obowiązków w okresie od nieustalonego dnia 2020 r. do 1.02.2023 r. w Warszawie przez funkcjonariuszy publicznych w związku z oceną zasadności przeprowadzenia zakupu za kwotę 12 503 048 zł oraz trybem nabycia przez Prokuraturę Krajową oprogramowania o nazwie handlowej Hermes, który podobnie jak Pegasus służy do zaawansowanego zbierania i analizy danych z wielu źródeł internetowych<sup>15</sup>. Niemniej to właśnie tytułowy Pegasus, z uwagi na nieznanie wcześniej funkcjonalności, stał się punktem zwrotnym w dyskusji na temat zarówno metod pozyskiwania przez organy państwa informacji, jak i procesowego wykorzystywania materiałów pochodzących z urządzeń końcowych.

Możliwości, jakie posiada aktualna wersja oprogramowania Pegasus, nie są powszechnie znane, co wynika z zakładanego przez twórców przeznaczenia systemu i z regulacji normatywnych, które ograniczają możliwość ujawnienia informacji dotyczących organizacji, form i metod pracy operacyjnej służb specjalnych. Zdaniem Naczelnego Sądu Administracyjnego (dalej NSA) informacja o posiadanych przez organy technicznych możliwościach działania wskazuje, w sposób pośredni, na metody pracy operacyjnej stosowane przez funkcjonariuszy, a także na kierunki tej działalności operacyjnej. Dla osób, które potencjalnie zainteresowane są działalnością przestępczą,

<sup>13</sup> J. Ojczyk, *Służby podsłuchują nas bez kontroli, bo pozwala na to prawo. Potwierdził to europejski trybunał*, „Business Insider” z 28.05.2024 r., <https://businessinsider.com.pl/prawo/europejski-trybunal-praw-czlowieka-wyda-wyrok-w-sprawie-inwigilacji-w-polsce/3b3e4kh> (dostęp: 4.06.2024 r.).

<sup>14</sup> M. Kowalewski, *Sąd Najwyższy zgadzał się na stosowanie Pegasusa*, <https://www.salon24.pl/newsroom/1374074,sad-najwyzszy-zgadzal-sie-na-stosowanie-pegasusa> (dostęp: 4.06.2024 r.).

<sup>15</sup> 2008-3.Ds.6.2024, <https://www.gov.pl/web/pr-rzeszow/komunikat-z-dnia-21-czerwca-2024r> (dostęp: 25.06.2024 r.).

w zakresie objętym działaniem organu, informacja o posiadanych przez organ możliwościach technicznych ma niebagatelne znaczenie. Dysponując wiedzą na ten temat, muszą się bowiem liczyć z ryzykiem tego, że organy ścigania skorzystają z posiadanych środków, a więc w efekcie osoby takie mogą próbować zabezpieczyć się przed oddziaływaniem tych środków. W konsekwencji mogłoby to utrudnić organowi wykonywanie jego ustawowych działań, a więc godziłoby w interes państwa polskiego i pośrednio w prawo wszystkich obywateli do życia w bezpiecznym kraju. Niewiedza po stronie osób łamiących prawo ma tu charakter przewencyjny, gdyż utrudnia działania przestępcze, i w interesie Rzeczypospolitej Polskiej pozostaje, aby uprawnienie jednostki do dostępu do informacji publicznej podlegało w tym zakresie ograniczeniu<sup>16</sup>.

W przestrzeni publicznej ostatnie źródłowe dane na temat tego systemu pochodzą z 2016 r., kiedy to firma NSO Group opublikowała raport zawierający wiele szczegółowych informacji przedstawiających jego możliwości. Trzeba jednak założyć, że od tego czasu Pegasus został rozwinięty o nowe funkcjonalności. Oprogramowanie – we wspomnianej wersji – stanowiło zespół zagregowanych luk *0-day* połączony z interfejsem umożliwiającym infekowanie urządzenia i następcze wykonywanie komend z poziomu administratora systemu wraz z możliwością wysyłania danych z urządzeń ofiary oraz katalogowania i opracowywania pobranych danych. System przeznaczony był do infekowania urządzeń mobilnych i posiadał wyłącznie zdolność atakowania urządzeń wyposażonych w „mobilne” systemy operacyjne, takie jak Android, iOS, BlackBerry OS czy Symbian. Jego działanie polegało na tym, że administrator systemu – używając jednej z dostępnych dla danej wersji systemu operacyjnego metod – dokonywał przesłania kodu programu klienckiego Pegasus, nazywanego „agentem”, na atakowane urządzenie końcowe (telefon/tablet atakowanego). Jego uruchomienie na tym urządzeniu otwierało kanał komunikacyjny z centralą danego operatora, co umożliwiało odbieranie poleceń i komend, które agent, posiadający pełne uprawnienia administracyjne, mógł wykonywać na urządzeniu bez wiedzy użytkownika. Jednocześnie agent, a za jego pośrednictwem administrator, uzyskiwał pełny dostęp do zasobów programowych i sprzętowych oferowanych przez dany model urządzenia, w tym: dostęp do kamery i mikrofonu, dostęp do wiadomości e-mail, SMS i komunikatorów internetowych, śledzenie lokalizacji urządzenia, dostęp do ustawień urządzenia, zgromadzonych plików (dokumentów, zdjęć, nagrań), danych wprowadzonych do kalendarza, wykazów kontaktów, połączeń telefonicznych, historii wyszukiwania w przeglądarkach internetowych oraz *social mediów* i aplikacji zainstalowanych na urządzeniu. Ulokowanie agenta dawało możliwość nieograniczonej ingerencji w urządzenie i przechowywane na nim dane, co znacznie przekraczało możliwości, jakie miał zwykły użytkownik systemu, który mógł wykonywać wyłącznie operacje dozwolone przez system operacyjny i współdziałające z nim oprogramowanie<sup>17</sup>. Początkowo zainfekowanie telefonu Pegasusem

<sup>16</sup> Wyrok NSA z 18.08.2015 r., I OSK 1679/14, LEX nr 1984363.

<sup>17</sup> A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zontek, *Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych (casus Pegasus)*, Kraków 2022, s. 7–9, <https://kipk.pl/wp-content/uploads/2022/02/ekspertyzapegasus.pdf> (dostęp: 10.05.2024 r.).

wymagało działania ze strony użytkownika telefonu. Taki użytkownik otrzymywał przez SMS, WhatsApp, Messenger itp. wiadomość zawierającą link, po którego kliknięciu program instalował się na telefonie. Z czasem technologia została ulepszona do mechanizmu określanego jako *zero-click*, przy którym nie była wymagana żadna interakcja ze strony użytkownika, gdyż wystarczy, że na urządzenie mobilne przychodzi wiadomość, a po jej odebraniu Pegasus sam się instaluje<sup>18</sup>.

### 3. Możliwości współczesnej wersji systemu Pegasus

Szersze światło na temat nowszej wersji Pegasusu rzuciły jednak prace sejmowej komisji śledczej powołanej do zbadania legalności, prawidłowości oraz celowości czynności operacyjno-rozpoznawczych podejmowanych m.in. z wykorzystaniem oprogramowania Pegasus przez członków rady ministrów, służby specjalne, Policję, organy kontroli skarbowej oraz celnoskarbowej, organy powołane do ścigania przestępstw i prokuraturę w okresie od 16.11.2015 r. do 20.11.2023 r. Podczas jej posiedzenia 15.03.2024 r. przesłuchany został Jerzy Kosiński, który brał udział w prezentacji, którą w kwietniu 2019 r. przeprowadzili dla polskich władz przedstawiciele NSO Group. Świadek, będący dyrektorem Morskiego Centrum Cyberbezpieczeństwa Wydziału Dowodzenia i Operacji Morskich Akademii Marynarki Wojennej, objaśnił, że Pegasus okazał się narzędziem informatycznym o złożonej funkcjonalności, które posiada kilka modułów. Pierwszy pozwalał na przejście kontroli nad urządzeniem mobilnym w sposób niesygnalizujący właścicielowi, że kontrola została przez niego utracona. Drugi pozwalał na zarządzanie tym, co znajduje się w zasobach telefonu. Trzeci przekazywał informacje z przejętego urządzenia na serwer, gdzie były przechowywane. Natomiast czwarty to moduł operatora, który pozwalał mu dotrzeć do tych informacji i zarządzać przejętym telefonem<sup>19</sup>. Świadek zaznaczył, że Pegasus nie był jedynym dostępnym oprogramowaniem szpiegującym i już wcześniej podobne narzędzie dla Interpolu prezentowała firma niemiecka. Pozwalało ono na przejście kontroli nad komputerem poprzez jego zainfekowanie, co dawało możliwość zapoznawania się z informacjami przekazywanymi za pośrednictwem komunikatorów korzystających z szyfrowania *end-to-end* bez potrzeby ich deszyfracji<sup>20</sup>. Podobnie jak większość takich narzędzi wymagało jednak interakcji z fizycznym urządzeniem. W porównaniu z nim system Pegasus okazał się narzędziem o wiele dojrzalszym, gdyż wykorzystując lukę *0-day*, nie wymagał żadnej aktywności ze strony użytkownika<sup>21</sup>. Świadek opisał, że trzymał w ręku aparat telefoniczny korzystający z systemu

<sup>18</sup> M. Matusiak-Frączczak, *Kontwencyjne...*, s. 29.

<sup>19</sup> Pełny zapis przebiegu posiedzenia Komisji Śledczej do zbadania legalności, prawidłowości oraz celowości czynności operacyjno-rozpoznawczych podejmowanych m.in. z wykorzystaniem oprogramowania Pegasus przez członków Rady Ministrów, służby specjalne, Policję, organy kontroli skarbowej oraz celnoskarbowej, organy powołane do ścigania przestępstw i prokuraturę w okresie od 16.11.2015 r. do 20.11.2023 r., nr 4, z 15.03.2024 r., s. 7, <https://orka.sejm.gov.pl/zapisy10.nsf/0/F2D9E8013C0D37E5C1258AEE002C1F7F/%24File/0002610.pdf> (dostęp: 26.04.2024 r.) – dalej zapis przebiegu posiedzenia.

<sup>20</sup> Zapis przebiegu posiedzenia, s. 14.

<sup>21</sup> Zapis przebiegu posiedzenia, s. 33.

Android, kiedy przejęto nad nim kontrolę. Nie było żadnego komunikatu, telefon nie zadrżał ani nie zasygnalizował, że cokolwiek się z nim dzieje, podczas gdy na konsoli operatorskiej pojawiła się informacja, że jest już pod kontrolą. W przypadku telefonu z systemem firmy Apple przyszedł natomiast typowy *phishingowy* komunikat z przekierowaniem na stronę internetową. Zaraz po wejściu na nią pojawiła się na konsoli informacja, że telefon został przejęty<sup>22</sup>. Podczas prezentacji uczestnicy uzyskali możliwość nawiązywania połączeń za pośrednictwem przejętych urządzeń, rozmawiania przez nie. Wykonali także próby dotyczące włączania mikrofonu i nasłuchiwanie otoczenia, jak również mieli bezpośredni dostęp do kamer, które w każdym momencie mogli uruchomić i za których pomocą mogli zdalnie robić zdjęcia. Ponieważ telefon przejmowany był praktycznie kompletnie, więc można było korzystać ze wszystkich jego funkcjonalności i narzędzi, które zostały zainstalowane na telefonie, czyli podszywać się pod jego właściciela, np. w jego imieniu funkcjonować na portalach społecznościowych, na komunikatorach, w systemach bankowości<sup>23</sup>. W przypadku gdy telefon komórkowy był zsynchronizowany z innymi urządzeniami mobilnymi typu tablet, laptop czy smartwatch, Pegasus dawał możliwość uzyskania danych również z tych urządzeń, a więc wglądu we wszystkie zapisane na nich pliki tekstowe, zdjęcia, filmy itd. Jak wynika ze słów J. Kosińskiego, operator przejętego systemu miał w takiej sytuacji więcej możliwości niż właściwy użytkownik urządzenia. W szczególności mógł skopiować całą bazę danych, a następnie odczytać informacje skasowane przez użytkownika, które dla tamtego nie były już dostępne<sup>24</sup>. Mógł także modyfikować treści zapisane w pamięci urządzenia, np. zmieniając treść znajdujących się tam wiadomości tekstowych<sup>25</sup>. Charakterystyczną cechą Pegasusu stanowiła przy tym jego trudna wykrywalność, gdyż w odróżnieniu od innych tego typu programów ten nie zapisywał się trwale na nośniku, lecz instalował się tylko w pamięci operacyjnej, gdzie funkcjonował tylko przez okres inwigilacji lub do chwili wyłączenia aparatu<sup>26</sup>. Jego użycie pozostawiało bardzo mało śladów zainfekowania<sup>27</sup>, tak że nawet ekspert miałby trudności z rozróżnieniem, które znajdujące się w nim dane zostały wprowadzone przez operatora systemu, a które z nich pochodziły od właściwego użytkownika tego urządzenia<sup>28</sup>.

#### 4. Wykorzystanie w postępowaniu karnym materiałów uzyskanych za pomocą Pegasusu

Powyższa okoliczność nabiera szczególnego znaczenia dla oceny, czy materiały pochodzące z urządzeń mobilnych, podatnych na działanie oprogramowania szpiegującego

<sup>22</sup> Zapis przebiegu posiedzenia, s. 8–9.

<sup>23</sup> Zapis przebiegu posiedzenia, s. 50.

<sup>24</sup> Zapis przebiegu posiedzenia, s. 9–10, 40.

<sup>25</sup> Zapis przebiegu posiedzenia, s. 13.

<sup>26</sup> Zapis przebiegu posiedzenia, s. 12.

<sup>27</sup> Zapis przebiegu posiedzenia, s. 49–50.

<sup>28</sup> Zapis przebiegu posiedzenia, s. 35.

typu Pegasus, mogą być traktowane jako pełnowartościowy dowód w procesie karnym, zwłaszcza w kontekście zasady rzetelnego procesu. Rozstrzygnięcie tej kwestii należy poprzedzić przypomnieniem, że mimo różnic doktrynalnych<sup>29</sup> rzetelny proces karny daje się zdefiniować poprzez odwołanie się do cech i warunków granicznych, które muszą zostać spełnione. Za rzetelny można więc uznać tylko taki proces, w którym uczestnicy mieli zapewnioną możliwość ochrony swoich interesów procesowych przy pomocy metod prawnie dopuszczalnych, z poszanowaniem praw innych uczestników. Implikuje to nałożenie na organy procesowe obowiązku stworzenia warunków pozwalających na realizację praw tych osób, których dobra prawne są zaangażowane<sup>30</sup>. Chodzi zatem o dążenie do osiągnięcia takiej sytuacji, w jakiej osoba, przeciwko której lub na rzecz której toczy się proces, ma przeświadczenie, że organy procesowe zrobiły wszystko, by prawu stało się zadość, postępując wobec niej sumiennie, zgodnie z prawem i w najlepszej woli<sup>31</sup>. Procedowanie winno więc przebiegać w taki sposób, aby żadna ze stron nie miała powodów do obaw, że padła ofiarą nieuczciwej gry<sup>32</sup>.

Tak sformułowany warunek od lat budzi dyskusje, gdy chodzi o wykorzystanie materiałów uzyskanych w toku czynności operacyjno-rozpoznawczych. W okresie gdy w polskim ustawodawstwie nie było w tym zakresie jednoznacznej regulacji prawnej, przeciwko bezpośredniemu wykorzystaniu dowodów zdobytych za pomocą – jak wówczas określano – niekonwencjonalnych metod<sup>33</sup> opowiadali się m.in. Maksymilian Lityński<sup>34</sup>, Stanisław Owczarski<sup>35</sup> i Tadeusz Hanausek<sup>36</sup>. Możliwość taka została krytycznie oceniona również przez Sąd Najwyższy (dalej SN), który odmówił mocy dowodowej milicyjnym notatkom powstałym w wyniku pracy operacyjnej<sup>37</sup>. Inne stanowisko zajmowali Zbigniew Sobolewski<sup>38</sup>, Stanisław Hoc<sup>39</sup>, Jan Żak<sup>40</sup>, Stanisław Pikulski<sup>41</sup>, Romuald

<sup>29</sup> Zob. A. Skowron, *Rzetelny proces karny w ujęciu Karty Praw Podstawowych Unii Europejskiej oraz Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*, Prokuratura i Prawo 2017, nr 11, s. 10–11.

<sup>30</sup> P. Wiliński, *O koncepcji rzetelnego procesu*, [w:] *Rzetelny proces karny. Materiały konferencji naukowej. Trzebiezówice 17–19 września 2009 r.*, red. J. Skorupka, W. Jasiński, s. 174–175, Warszawa 2010.

<sup>31</sup> J. Skorupka, *Paradygmat współczesnego polskiego procesu karnego – próba ujęcia*, [w:] *Współczesne tendencje w rozwoju procesu karnego z perspektywy dogmatyki oraz teorii i filozofii prawa*, red. J. Skorupka, I. Hańdzyk-Hawrylak, Warszawa 2011, s. 25.

<sup>32</sup> A. Jakubiak-Mirończuk, *Alternatywne a sądowe rozstrzyganie sporów sądowych*, Warszawa 2008, s. 66.

<sup>33</sup> J. Skorupka, *Dogmatyczne uzasadnienie wyróżnienia dowodów niekonwencjonalnych*, [w:] *System Prawa Karnego Procesowego*, t. 8, Dowody, cz. 1, red. J. Skorupka, Warszawa 2019, s. 451.

<sup>34</sup> M. Lityński, *Czynności operacyjne M.O. w procesie karnym. Z problematyki dochodzenia*, „Państwo i Prawo” 1961/6, s. 1002.

<sup>35</sup> S. Owczarski, *Problematyka postępowania operacyjnego w świetle prawa i praktyki*, „Przegląd Sądowy” 1994/4, s. 77.

<sup>36</sup> T. Hanausek, *Ustawa o Policji. Komentarz*, Kraków 1996, s. 55.

<sup>37</sup> Zob. wyrok SN z 5.12.1957 r., II KRn 888/57, OSNCK 1959/2, poz. 24.

<sup>38</sup> Z. Sobolewski, *Zasada „Nemo se ipsum accusare tenetur” w polskim procesie karnym*, Lublin 1979, s. 209.

<sup>39</sup> S. Hoc, *Refleksje na marginesie art. 10 Ustawy o urzędzie ochrony państwa*, „Wojskowy Przegląd Prawniczy” 1992/3–4, s. 34.

<sup>40</sup> J. Żak, *Dowody rzeczowe w sprawach o szpiegostwo*, „Wojskowy Przegląd Prawniczy” 1991/1, s. 103–104.

<sup>41</sup> S. Pikulski, *Działania operacyjne Policji*, „Wojskowy Przegląd Prawniczy” 1996/2, s. 61.

Kmiecik<sup>42</sup>, Adam Taracha<sup>43</sup>, Kazimierz Marszał<sup>44</sup>, Monika Klejnowska<sup>45</sup>, Tomasz Grzegorzczak<sup>46</sup> i Aleksander Herzog<sup>47</sup>. Szerokie możliwości, jakie dawało zastosowanie tego instrumentu oraz jego wysoka skuteczność, wynikająca z uzyskiwania informacji od samego sprawcy, których zdobycie w inny sposób nie byłoby możliwe<sup>48</sup>, wobec konieczności skutecznej walki ze zjawiskiem przestępczości zorganizowanej<sup>49</sup>, spowodowały, że ustawodawca zdecydował się przeciąć spór, dokonując nowelizacji tzw. ustaw policyjnych, co nastąpiło w latach 2001–2002. Wówczas to możliwość prowadzenia kontroli operacyjnej jako pierwsza uzyskała Straż Graniczna<sup>50</sup>, a w art. 9e ust. 16 ustawy o Straży Granicznej<sup>51</sup> znalazł się jednoznaczny zapis, że do materiałów uzyskanych, w wyniku kontroli operacyjnej, stosuje się odpowiednio przepisy art. 393 § 1 zd. 1 Kodeksu postępowania karnego<sup>52</sup>, regulujące przeprowadzanie dowodów z dokumentów urzędowych. Od momentu przyjęcia tak uzyskanych materiałów przez prokuratora lub sąd i dopuszczenia ich jako dowodu w sprawie karnej zostawały one objęte reżimem postępowania dowodowego<sup>53</sup> i mogły zostać wprowadzone do procesu karnego po przeprowadzeniu czynności dowodowej odczytania dokumentów. Na podstawie wymienionych materiałów sąd orzekający w danej sprawie mógł więc ustalać fakty mające istotne znaczenie dla rozstrzygnięcia o winie oskarżonego<sup>54</sup>. Analogiczne regulacje zostały wprowadzone następnie w ustawie z 6.04.1990 r. o Policji<sup>55</sup>, ustawie z 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu<sup>56</sup>, ustawie z 9.06.2006 r. o Centralnym Biurze

<sup>42</sup> R. Kmiecik, *Prawnodowodowe aspekty ochrony programów komputerowych w postępowaniu karnym (problematyka wszczęcia postępowania)*, „Prokuratura i Prawo” 1997/6, s. 17.

<sup>43</sup> A. Taracha, *Wykorzystanie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych w procesie karnym*, [w:] *Nowy kodeks postępowania karnego. Zagadnienia węzłowe*, red. E. Skrętowicz, Kraków 1998, s. 181.

<sup>44</sup> K. Marszał, *Proces karny*, Katowice 1998, s. 181.

<sup>45</sup> M. Klejnowska, *Podstuch pozaprocesowy (operacyjny) na gruncie znowelizowanej ustawy z dnia 6 kwietnia 1990 r. o Policji*, „Przegląd Sądowy” 2004/4, s. 95–96.

<sup>46</sup> T. Grzegorzczak, *Wykorzystywanie i przekształcanie materiałów operacyjnych w materiał dowodowy w postępowaniu karnym*, [w:] *Przestępczość zorganizowana. Świadek koronny. Terroryzm*, red. E. Pływaczewski, Kraków 2005, s. 229–231.

<sup>47</sup> A. Herzog, *Wykorzystanie materiałów operacyjnych w postępowaniu dyscyplinarnym prokuratorów*, „Prokuratura i Prawo” 2007/2, s. 92.

<sup>48</sup> M. Klejnowska, *Podstuch operacyjny i prowokacja policyjna*, „Prokuratura i Prawo” 2004/3, s. 94; zob. także M. Klejnowska, *Podstępne uzyskanie przyznania się oskarżonego do winy*, „Rzeszowskie Zeszyty Naukowe” 2001/30, s. 258–260.

<sup>49</sup> J. Kudła, Z. Bielecki, *Wybrane aspekty zakupu kontrolowanego w pracy Policji*, „Przegląd Policyjny” 2005/77, s. 86.

<sup>50</sup> Ustawa z 11.04.2001 r. o zmianie ustawy o Straży Granicznej oraz o zmianie niektórych innych ustaw (Dz.U. z 2001 r. Nr 45, poz. 498).

<sup>51</sup> Ustawa z 12.10.1990 r. o Straży Granicznej (tekst jedn.: Dz.U. z 2025 r. poz. 914).

<sup>52</sup> Ustawa z 6.06.1997 r. – Kodeks postępowania karnego (tekst jedn.: Dz.U. z 2025 r. poz. 46 ze zm.) – dalej k.p.k.

<sup>53</sup> M. Chrabkowski, *Wykorzystanie materiałów kontroli operacyjnej w postępowaniu przygotowawczym*, Szczytno 2009, s. 127.

<sup>54</sup> J. Skorupka, *Dogmatyczne...*, [w:] *System...*, t. 8, *Dowody*, cz. 1, s. 454.

<sup>55</sup> Tekst jedn.: Dz.U. z 2025 r. poz. 636. Wspomniana zmiana została wprowadzona ustawą z 27.07.2001 r. o zmianie ustawy o Policji, ustawy o działalności ubezpieczeniowej, ustawy – Prawo bankowe, ustawy o samorządzie powiatowym oraz ustawy – Przepisy wprowadzające ustawy reformujące administrację publiczną (Dz.U. z 2001 r. Nr 100, poz. 1084).

<sup>56</sup> Tekst jedn.: Dz.U. z 2025 r. poz. 902.

Antykorupcyjnym<sup>57</sup>, ustawie z 9.06.2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego<sup>58</sup>, ustawie z 24.08.2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych<sup>59</sup>. W ten sposób czynności operacyjne, wcześniej uważane za „ubogie krewne” procesu i z założenia służące profilaktyce walki z przestępczością<sup>60</sup>, ewentualnie sprawdzeniu prawdziwości pozyskanych informacji o popełnieniu przestępstwa<sup>61</sup>, stały się uznaną metodą zdobywania dowodów na potrzeby procesu karnego. W czasach gdy telefonia komórkowa dopiero kielkowała, a społeczeństwo stawiało w internecie pierwsze kroki, nie można było nawet przypuszczać, że w ciągu niespełna dwóch dekad narzędzia służące inwigilacji elektronicznej ewoluują w kierunku, który otworzy przed służbami specjalnymi możliwość nie tylko zapoznawania się z informacjami wymienianymi przez osoby poddane kontroli, ale również ingerencji w ich treść.

W takim kontekście szczególnego znaczenia nabiera wynikająca z art. 7 Konstytucji RP ustrojowa zasada prawna legalizmu nakładająca określone obowiązki zarówno na organy władzy publicznej stosujące prawo, jak i na organy tworzące prawo, w myśl odpowiednich przepisów kompetencyjnych, proceduralnych i materialnych. Rzecz jednak w tym, że art. 7 Konstytucji RP stanowi jednocześnie podstawę domniemania prawnego, że działania pochodzące od organów państwa cieszą się domniemaniem ich zgodności z prawem<sup>62</sup>. I chociaż presumpcję tę uznaje się za podważalną, to jej konsekwencją jest również to, że to na podmiocie przedstawiającym tezę o naruszeniu prawa przez organy władzy publicznej ciąży, co do zasady, obowiązek wykazania przekroczenia kompetencji przez dany organ państwa bądź że dana czynność wykroczyła poza ramy przewidziane prawem<sup>63</sup>. Tymczasem w obecnych realiach nałożenie na jednostkę ciężaru wykazania, że doszło do nieprawidłowości w przebiegu inwigilacji, staje się zadaniem praktycznie niemożliwym do wykonania. Na przeszkodzie stają bowiem regulacje ustawowe, gdyż wymóg ochrony form, środków i metod realizacji zadań wyłącza możliwość szczegółowego poznania mechanizmów oprogramowania użytego do kontroli operacyjnej<sup>64</sup>. W przypadku Centralnego Biura Antykorupcyjnego obowiązek „utajnienia” narzędzi stosowanych przez tę służbę do realizacji kontroli operacyjnej wynika wprost z art. 24 ust. 1 ustawy o Centralnym Biurze Antykorupcyjnym. Podobne regulacje zawierają pozostałe

<sup>57</sup> Tekst jedn.: Dz.U. z 2025 r. poz. 712.

<sup>58</sup> Tekst jedn.: Dz.U. z 2024 r. poz. 1405 ze zm.

<sup>59</sup> Tekst jedn.: Dz.U. z 2025 r. poz. 12 ze zm.

<sup>60</sup> L. Schaff, *Zakres i formy postępowania przygotowawczego*, Warszawa 1961, s. 77.

<sup>61</sup> R. Ponikowski, *Aspekty procesowe i kryminalistyczne pierwszej informacji o przestępstwie*, „Nowe Prawo” 1973/5, s. 685; M. Siewierski, *Nowe rozwiązania kodyfikacyjne w części szczególnej kodeksu postępowania karnego*, „Państwo i Prawo” 1970/1, s. 29.

<sup>62</sup> Zob. uchwała SN 7 sędziów z 9.10.2007 r., III CZP 46/07, OSNC 2008/3, poz. 30; wyrok SN z 20.05.2011 r., IV CSK 563/10, LEX nr 864020; postanowienie SN z 11.04.2014 r., I CSK 324/13, LEX nr 1523351; wyrok NSA z 10.10.2013 r., I OSK 1573/13, LEX nr 1381658; wyrok SN z 8.01.2014 r., IV KK 183/13, LEX nr 1409532; wyrok NSA z 13.09.2013 r., II FSK 2644/11, LEX nr 1369043.

<sup>63</sup> M. Zubik, W. Sokolewicz, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. 1, red. L. Garlicki, Warszawa 2016, komentarz do art. 7.

<sup>64</sup> Zob. wyrok NSA z 2.02.2018 r., I OSK 668/16, LEX nr 2475548.

ustawy kompetencyjne służb przewidujące procedurę realizacji kontroli operacyjnej, a więc art. 20a ust. 1 ustawy o Policji, art. 35 ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, art. 9c ust. 1 ustawy o Straży Granicznej, art. 131 ust. 1 ustawy o Krajowej Administracji Skarbowej<sup>65</sup>, art. 40 ust. 1 ustawy o Żandarmerii Wojskowej i wojskowych organach porządkowych. W świetle orzecznictwa NSA wszystkie informacje, których ujawnienie utrudniłoby wykonywanie służbom ich zadań, w tym wykonywanie czynności operacyjno-rozpoznawczych bez względu na to, czy dotyczą one konkretnych postępowań, podlegają ochronie zasadom ochrony informacji niejawnych<sup>66</sup>. Poznanie charakterystyki narzędzi pracy operacyjnej groziłoby bowiem ujawnieniem techniki stosowanej do realizacji czynności i w konsekwencji brakiem faktycznych możliwości realizacji przez nie ustawowych zadań, a co za tym idzie – demontażem tej służby<sup>67</sup>. Wspomniane ograniczenia normatywne powodują, że możliwość udowodnienia przez zainteresowanego ewentualnych naruszeń, jakich dopuściły się organy ścigania podczas czynności operacyjno-rozpoznawczych, a w efekcie podważenie domniemania legalności tych działań, są jedynie pozorne, czego nie sposób pogodzić z zawartą w art. 2 Konstytucji RP zasadą demokratycznego państwa prawnego (która zakłada m.in., że organy władzy publicznej powinny działać w sposób lojalny i uczciwy względem jednostki, budzący w niej poczucie stabilności i bezpieczeństwa prawnego)<sup>68</sup>, tak samo jak z ujętym w art. 42 Konstytucji RP prawem do obrony oraz wynikającą z art. 6 Europejskiej Konwencji Praw Człowieka<sup>69</sup> zasadą rzetelnego procesu.

## 5. Uboczne skutki rozwoju technologii szpiegowskich – problem wiarygodności materiałów z urządzeń końcowych

Wobec możliwości Pegasus można oczywiście głosić przekonanie, że skoro organy ścigania mają obowiązek działać na podstawie i w granicach prawa, to z góry wykluczone jest, aby kiedykolwiek podjęto, przy zastosowaniu tego oprogramowania, totalną inwigilację, lub że jego operator mógłby próbować tą drogą manipulować danymi, aktywnie oddziałując na system informatyczny urządzenia i wprowadzając w nim zmiany<sup>70</sup>. Wspomniane funkcjonalności są jednak efektem postępu technologicznego, którego nie da się powstrzymać poprzez wprowadzanie regulacji normatywnych o charakterze powinnościowym, o ile te nie są uzupełnione mechanizmami gwarantującymi skuteczną kontrolę i przeciwdziałanie potencjalnym nadużyciom, jakie

<sup>65</sup> Ustawa z 16.11.2016 r. o Krajowej Administracji Skarbowej (tekst jedn.: Dz.U. z 2025 r. poz. 1131).

<sup>66</sup> Wyrok NSA z 2.02.2018 r., I OSK 668/16, LEX nr 2475548; zob. S. Hoc, P. Szustakiewicz, *Ustawa o Centralnym Biurze Antykorupcyjnym. Komentarz*, wyd. 2, LEX/el. 2023, komentarz do art. 24.

<sup>67</sup> P. Opitek, *Kontrola...*, s. 60–61.

<sup>68</sup> M. Florczak-Wątor, [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Tuleja, Warszawa 2023, s. 31.

<sup>69</sup> Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie 4.11.1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz.U. z 1993 r. Nr 61, poz. 284 ze zm.) – dalej EKPC.

<sup>70</sup> Zob. P. Opitek, *Kontrola...*, s. 46.

mogą się zdarzyć. W świetle obecnych polskich unormowań, skoro użycie Pegasusa pozwala operatorowi na zarządzanie mikrofonem oraz kamerą telefonu i rejestrację zapisu audio-video z otoczenia aparatu, a więc właśnie na totalną inwigilację, to z uwagi na to, że przebieg kontroli operacyjnej pozostaje utajniony, a prawidłowość jego realizacji podlega ocenie organów zewnętrznych tylko w bardzo nieznacznym zakresie, naiwne albo celowo uspokajające opinię publiczną wydaje się *a priori* odrzucenie hipotezy, że funkcjonalność ta zostanie wykorzystana.

Zachodząca w takim wypadku kolizja pomiędzy zasadami prawa do obrony i rzetelnego procesu a potrzebą ograniczenia dostępu do informacji o środkach, formach i metodach realizacji zadań przez służby specjalne może być rozstrzygnięta na dwa sposoby. Skoro podstawowym warunkiem wprowadzenia do procesu karnego dowodów niekonwencjonalnych jest zgodność z przepisami prawa, i to zarówno samego dowodu, jak i jego uzyskania, to obowiązkiem sądu rozpoznającego daną sprawę jest wnikliwe i gruntowne ustalenie wymienionej okoliczności. W każdym wypadku niezgodności tych dowodów z przepisami prawa albo choćby wątpliwości co do ich zgodności z prawem obowiązkiem sądu jest niedopuszczenie tych dowodów do procesu karnego, a jeżeli zostały wcześniej dopuszczone, to wyeliminowanie ich z podstawy dowodowej rozstrzygnięcia, gdyż także wątpliwości prawne powinny być rozstrzygane na korzyść oskarżonego, stosownie do normy wyrażonej w art. 5 § 2 k.p.k.<sup>71</sup> Powoduje to, że sąd rozstrzygający w procesie karnym, w którym jako źródło ustaleń faktycznych zostały wskazane dowody uzyskane w wyniku kontroli operacyjnej, powinien uzyskać wyczerpujące materiały z tej kontroli, nie wyłączając pełnych wersji wniosków o zarządzenie kontroli operacyjnej oraz o jej przedłużenie, gdyż tylko wówczas możliwe staje się dokonanie oceny, czy kontrola została przeprowadzona w całości zgodnie z prawem. W przeciwnym razie zachodzi konieczność przyjęcia, że materiały uzyskane w toku kontroli operacyjnej, co do której nie można w sposób pewny i niewątpliwy ustalić, że była prowadzona legalnie, nie mogą stanowić dowodu w sprawie. Zaakceptowanie innego stanowiska oznaczałoby, że kontrola sądowa nad czynnościami operacyjno-rozpoznawczymi jest w istocie iluzoryczna i ma fasadowy charakter, a funkcjonariusze właściwych służb prowadzą te czynności i jednocześnie sami decydują o tym, czy są one legalne oraz czy uzyskane w ich wyniku materiały mogą być wykorzystane w procesie<sup>72</sup>.

Podkreślić należy, że zgodnie z art. 49 Konstytucji RP ograniczenie tajemnicy komunikowania się „może nastąpić jedynie w przypadkach określonych w ustawie i w sposób w niej określony”. Ustawowe ograniczenia wolności traktowane być muszą w kategoriach wyjątków, które zgodnie z zasadą *exceptiones non sunt extendendae*<sup>73</sup> nie mogą być interpretowane rozszerzająco, nawet jeśli prowadzi to do sytuacji, w której organy ścigania, dysponując materiałami wskazującymi na popełnienie przestępstwa ściganego z oskarżenia publicznego, nie mogą go wykorzystać na potrzeby

<sup>71</sup> J. Skorupka, *Dogmatyczne...*, [w:] *System...*, t. 8, *Dowody*, cz. 1, s. 452.

<sup>72</sup> Wyrok Sądu Apelacyjnego we Wrocławiu z 11.05.2023 r., II AKa 480/21, LEX nr 3652572.

<sup>73</sup> D. Drązewicz, *Dowodowe wykorzystanie wyników kontroli operacyjnej w postępowaniu karnym*, „Prokuratura i Prawo” 2010/7–8, s. 171.

postępowania karnego. Przepisy ingerujące w życie prywatne, w tym tajemnicę komunikowania się, muszą być bowiem oparte na ustawie, która jest precyzyjna<sup>74</sup> i która zawiera gwarancje pozwalające uniknąć nadużyć władzy, a brak spełnienia tych wymagań może prowadzić do naruszenia art. 8 ust. 2 EKPC<sup>75</sup>.

Wyinterpretowany w ten sposób zakaz dowodowy osłabia jednak kontrowersyjny art. 168a k.p.k., zgodnie z którym „Dowodu nie można uznać za niedopuszczalny wyłącznie na tej podstawie, że został uzyskany z naruszeniem przepisów postępowania lub za pomocą czynu zabronionego, o którym mowa w art. 1 § 1 Kodeksu karnego, chyba że dowód został uzyskany w związku z pełnieniem przez funkcjonariusza publicznego obowiązków służbowych, w wyniku: zabójstwa, umyślnego spowodowania uszczerbku na zdrowiu lub pozbawienia wolności”. W efekcie dopiero pokonstytucyjna wykładnia tego przepisu<sup>76</sup> otwiera, na gruncie polskiej regulacji, możliwość odrzucenia wadliwie zdobytych dowodów. Koncepcję tę wspiera jednak system źródeł prawa, gdyż hierarchia aktów, z jakich wywodzą się zasady prawa do obrony i rzetelnego procesu oraz norma ograniczająca dostęp do informacji o środkach, formach i metodach realizacji zadań przez służby specjalne, wyraźnie świadczy o prymacie tych pierwszych. Prowadzi to do konkluzji, że dopóki czynności operacyjne pozostają poza sferą pełnej kontroli sądu orzekającego w sprawie karnej, dopóty zdobyte w ich wyniku informacje, jako niepoddające się weryfikacji pod względem legalności uzyskania, nie mogą zostać wykorzystane procesowo i stanowić dowodu w sprawie karnej.

Inna koncepcja przyjmuje natomiast, że jeśli chodzi o wykorzystanie informacji zdobytych za pomocą oprogramowania typu Pegasus, to sąd powinien zbudować swoje przekonanie o wartości dowodowej materiału zgromadzonego przez oskarżyciela publicznego na podstawie wszystkich zebranych dowodów, ocenianych swobodnie z uwzględnieniem zasad prawidłowego rozumowania oraz wskazań wiedzy i doświadczenia życiowego<sup>77</sup>. Takie rozwiązanie nie prowadzi więc do odrzucenia jako dowodów w sprawie nawet danych o nie w pełni transparentnym pochodzeniu, a jedynie nakazuje organom procesowym rozważenie wpływu tej okoliczności na ich wartość procesową w kontekście pozostałego materiału i dopiero wątpliwości – których nie dało się w ten sposób usunąć – rozstrzygnąć na korzyść oskarżonego.

<sup>74</sup> Wyrok ETPC z 27.04.2004 r., skarga nr 50210/99, Doerga przeciwko Holandii, LEX nr 125861.

<sup>75</sup> Wyrok ETPC z 30.07.1998 r., skarga nr 27671/95, Valenzuela Contreras przeciwko Hiszpanii, LEX nr 78163.

<sup>76</sup> Zob. Ł. Cora, *Aksjologia procesowa a dopuszczalność dowodu z art. 168a k.p.k.*, „Państwo i Prawo” 2018/10, s. 121–132; Ł. Cora, *Wykładnia dowodu z art. 168a k.p.k. w zgodzie z Konstytucją RP. Glosa do wyroku s.apel. z dnia 27 kwietnia 2017 r., II AKA 213/16*, „Gdańskie Studia Prawnicze – Przegląd Orzecznictwa” 2018/3, s. 105–108; D. Gruszecka, *W kwestii interpretacji znowelizowanego przepisu art. 168a k.p.k.*, „Palestra” 2017/1–2, <https://palestra.pl/pl/czasopismo/wydanie/1-2-2017/artukul/w-kwestii-interpretacji-znowelizowanego-przepisu-art.-168a-k.p.k> (dostęp: 12.06.2024 r.); D. Gruszecka, [w:] *Kodeks postępowania karnego. Komentarz*, red. J. Skorupka, Warszawa 2018, s. 340–341; K. Lipiński, *Klauzula uadekwatniająca przestanki niedopuszczalności dowodu w postępowaniu karnym (art. 168a k.p.k.)*, „Państwo i Prawo” 2016/11, s. 44–59; W. Jasiński, [w:] *System Prawa Karnego Procesowego*, t. 7, cz. 2, red. J. Skorupka, Warszawa 2019, s. 2559; J. Skorupka, *Prokonstytucyjna wykładnia przepisów prawa dowodowego w procesie karnym*, [w:] *Verba volant, scripta manent: proces karny, prawo karne skarbowe i prawo wykroczeń po zmianach z lat 2015–2016. Księga pamiątkowa poświęcona Profesor Monice Zbrojewskiej*, red. T. Grzegorzczak, R. Olszewski, Warszawa 2016, s. 362.

<sup>77</sup> P. Opitek, *Kontrola...*, s. 47–48.

Byłaby to więc znacznie słabsza gwarancja procesowa, zwłaszcza że poznanie przez uczestników postępowania metod, jakimi doszło do uzyskania tych materiałów, może mieć istotne znaczenie dla realizowanej linii obrony. Skoro zaś sąd miałby w procesie oceniać, czy ekstrakcja danych nie naruszyła porządku prawnego, czy dane w czasie transmisji nie były modyfikowane, w jaki sposób kontrola wpłynęła na administrowanie telefonem przez prawowitego posiadacza aparatu, czy podjęte przez służbę działania mieściły się w ramach przyznanych jej kompetencji itd., to również stronom, a zwłaszcza oskarżonemu, powinna zostać zapewniona realna, a nie tylko pozorna, możliwość podjęcia kroków zmierzających do weryfikacji tych okoliczności, a tym samym wytworzenia warunków do obalenia domniemania, że działania organów państwa przeprowadzone zostały zgodnie z prawem. W realiach kontradiktoryjnego postępowania karnego oskarżeni muszą mieć zapewnioną pełną możliwość weryfikacji przedstawionych przeciwko nim dowodów, nie wyłączając uzyskania informacji o metodach, jakimi je uzyskano. Stosownie do art. 2 § 2 k.p.k. podstawę wszelkich rozstrzygnięć powinny stanowić prawdziwe ustalenia faktyczne. Dyrektywa ta urealnia prawa stron do uczestnictwa w postępowaniu dowodowym i oznacza, że sąd może czynić ustalenia tylko na podstawie dowodów przeprowadzonych na etapie, do którego mają dostęp strony mogące realizować swe uprawnienia procesowe<sup>78</sup>.

## 6. Wnioski

Niezależnie od oceny dopuszczalności użycia systemu Pegasusa jako metody zdobywania informacji na potrzeby procesu karnego i skutków ewentualnych naruszeń w tym zakresie trzeba podkreślić, że oprogramowanie pozwalające na przejęcie pełnej kontroli nad urządzeniem mobilnym nie odpowiada wymaganiom co do właściwego sprecyzowania stosowanego środka techniki operacyjno-rozpoznawczej, a więc takiego, który ma ograniczyć arbitralność państwa i umożliwić sprawowanie efektywnej kontroli nad niejawną działalnością operacyjno-rozpoznawczą<sup>79</sup>. W przypadku zabezpieczania nośnika danych, co do zasady, najpierw jest wykonywana – po wcześniejszym podłączeniu stosownego bloкера zapisu (w celu uniemożliwienia nadpisania i modyfikacji zabezpieczonych danych) – kopia binarna, z której obliczana jest suma kontrolna mająca zagwarantować, że dane poddane analizie przez biegłego będą tożsame z danymi znajdującymi się na zabezpieczonym nośniku i nie dojdzie do jakiegokolwiek zmiany danych na skutek wdrożonej analizy. Przypadek, w którym na określonym urządzeniu instalowany jest program (agent Pegasusa) dający swojemu użytkownikowi uprawnienia administracyjne, pozwalające na swobodne manipulowanie zgromadzonymi tam danymi, pozbawia takie materiały waloru procesowej wiarygodności<sup>80</sup>. Funkcjonalność systemu Pegasus polegająca na nieskrępowanej edycji danych zapisanych w urządzeniu, w sytuacji gdy nie da się ustalić,

<sup>78</sup> K. Marszał, *Proces...*, s. 64.

<sup>79</sup> Wyrok Sądu Apelacyjnego we Wrocławiu z 11.05.2023 r., II AKa 480/21, LEX nr 3652572.

<sup>80</sup> A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zontek, *Dopuszczalność...*, s. 46.

czy dane te nie były w jakikolwiek sposób modyfikowane, czy operator Pegasusa nie inicjował połączeń lub wysyłki wiadomości bez wiedzy ofiary, czy wręcz nie przesłał na urządzenie dodatkowych plików o charakterze przestępnym, powoduje, że materiały muszą zostać uznane za nieprzydatne do wykorzystywania dowodowego na gruncie procedury karnej. Nie ma przy tym znaczenia, czy inwigilacja była prowadzona nielegalnie, czy też odbyła się na podstawie decyzji sądu. Sam fakt, że nie ma możliwości ustalenia, kto (podmiot inwigilowany czy operator Pegasusa) umieścił, zmodyfikował lub usunął dane treści z urządzenia, musi skutkować konkluzją, że wykorzystanie takich materiałów do czynienia niekorzystnych dla oskarżonego ustaleń spowoduje, iż proces karny, oceniany jako całość, nie będzie mógł być uznany za sprawiedliwy w świetle art. 45 Konstytucji RP oraz art. 6 ust. 1 EKPC<sup>81</sup>. Nie świadczy to negatywnie o samym oprogramowaniu szpiegowskim, ale o jego wykorzystaniu niezgodnie z zakładanym przez twórców przeznaczeniem. System ten został bowiem opracowany jako narzędzie aktywnej pracy wywiadowczej i miał służyć do zbierania informacji, bez względu na możliwość ich procesowego wykorzystania<sup>82</sup>.

Przedstawione funkcje Pegasusa przenoszą dyskusję daleko poza problem użycia tego systemu w celu zdobywania dowodów na potrzeby procesu karnego. Możliwość ingerowania przez operatora systemu w treść danych znajdujących się w urządzeniu końcowym, dokonywanie w nim ich zmian lub nawet implementacji rodzi bowiem konieczność diametralnej zmiany podejścia do wszelkich materiałów pochodzących z urządzeń końcowych. Ewentualność zmodyfikowania takich danych, która w praktyce okazała się nie być jedynie teoretyczna w świetle faktu, że na telefon senatora K. Brejzy polskie służby specjalne wprowadziły przy użyciu Pegasusa pliki o rozmiarach ok. 1 GB<sup>83</sup>, nawet jeśliby uznać, że *a limine* nie dyskwalifikuje jeszcze takich materiałów, to podważa założenie, które dotąd w praktyce procesowej było traktowane niemal jako pewnik, mianowicie że zabezpieczone z urządzenia końcowego informacje zostały wytworzone przez jego użytkownika albo osoby, z którymi je wymieniał. Obecnie w każdym przypadku zakwestionowania ich autentyczności przez domniemanego autora musi pojawić się uzasadniona wątpliwość co do tego, przez kogo został wprowadzony do urządzenia końcowego zabezpieczony materiał<sup>84</sup>. Trudno sobie wyobrazić, aby nie wpłynęło to na praktykę procesową, w której informacje z pamięci smartfonów i podobnych urządzeń dotąd traktowane były jako pierwszoplanowe źródło ustaleń o okolicznościach przestępstwa. W zaistniałej sytuacji takie materiały mogą pozostawać jedynie podstawą wniosku, że określona treść znalazła się w urządzeniu końcowym, ale już teza, że została ona wprowadzona przez użytkownika tego urządzenia, wymaga przeprowadzenia przez organy odrębnych ustaleń procesowych, a bez potwierdzenia tej okoliczności uzyskane z takiego źródła informacje nie będą mogły stać się podstawą ustaleń obciążających oskarżonego.

<sup>81</sup> M. Matusiak-Frącczak, *Kontrola...*, s. 19–20.

<sup>82</sup> Zapis przebiegu posiedzenia, s. 46.

<sup>83</sup> M. Matusiak-Frącczak, *Konwencyjne...*, s. 29.

<sup>84</sup> Por. D. Drajewicz, *Dowodowe...*, s. 177 i podane tam przypisy.

Wobec dyrektywy zawartej w art. 5 § 2 k.p.k. uczynienie materiałów z urządzeń końcowych podstawą niekorzystnych dla oskarżonego ustaleń wymaga zatem zbadania, czy nie doszło do zewnętrznej ingerencji w znajdujące się w nim dane. Oznacza to, że aby nie uchybić kryteriom rzetelnego procesu, w przypadku pojawienia się jakichkolwiek wątpliwości co do autorstwa zabezpieczonych danych, organy procesowe stoją co najmniej przed koniecznością dopuszczenia dowodu z opinii biegłego informatyka w każdym postępowaniu, w którym skazanie miałoby się opierać na materiale pochodzącym z urządzenia końcowego. Niezależnie jednak od wyników ekspertyz trzeba mieć na uwadze, że oprogramowanie typu Pegasus już w wersji z 2019 r. pozostawiało bardzo mało śladów zainfekowania. Z prawdopodobieństwem graniczącym z pewnością można przyjąć, że od tego czasu nastąpił rozwój systemu, a instrumenty służące do weryfikacji urządzenia końcowego mogą nie wykrywać jego najnowszych wersji<sup>85</sup>. Powyższa okoliczność stanowi ważny argument za koniecznością bardzo ostrożnego podchodzenia przez organy procesowe do danych uzyskanych z urządzeń końcowych, a nawet za ich deprecjacją jako źródła ustaleń procesowych włącznie, z uwagi na ryzyko arbitralności i nadużyć. Ponadto trzeba mieć na względzie, że chociaż dotąd najgłośniej było o przypadkach, kiedy za nielegalnym wykorzystaniem systemów szpiegujących stały służby specjalne, gdyż to właśnie państwa były nabywcami takiego oprogramowania, nie sposób wykluczyć, że wcześniej czy później podobne systemy trafią do innych podmiotów, o ile taka sytuacja już nie miała miejsca. Dotyczy to zwłaszcza grup przestępczych, które posiadają realne możliwości finansowe nabycia takiego oprogramowania i mogą być zainteresowane wykorzystaniem ich funkcjonalności, zarówno dla zdobywania informacji, jak i w celu preparowania materiałów obciążających konkurentów lub przeciwników, aby skierować na nich uwagę organów ścigania.

Resumując, ubocznym skutkiem postępu w dziedzinie metod niejawnego zdobywania informacji, który przyniósł rozwój oprogramowania typu Pegasus, stało się obniżenie wiarygodności dowodów pozyskanych z urządzeń podatnych na ataki przeprowadzane za pomocą takich systemów. Organy państwa zyskały zatem bardzo efektywne narzędzie do inwigilacji, które pozwala na skuteczne rozpoznanie środowisk kryminalnych oraz ukierunkowanie działań prewencyjnych i ewentualnych czynności procesowych, ale konsekwencją rozwoju technologii są ograniczenia w zakresie skutecznego procesowego wykorzystania danych pochodzących z urządzeń końcowych. Wobec funkcjonalności omawianego oprogramowania oraz słabości systemu kontroli nad jego wykorzystaniem użycie materiałów zabezpieczonych z pamięci smartfonów, tabletów czy komputerów w procesie karnym jako podstawy niekorzystnych dla oskarżonego ustaleń w sytuacji braku realnej możliwości weryfikacji, kto umieścił, zmodyfikował lub usunął te dane, prowadzić musi bowiem do wniosku, że proces karny – jako całość – nie jest sprawiedliwy i narusza art. 45 Konstytucji RP oraz art. 6 ust. 1 EKPC.

<sup>85</sup> A. Barczak-Oplustil, M. Małecki, S. Tarapata, A. Behan, W. Zontek, *Dopuszczalność...*, s. 45.

## Bibliografia

1. Barczak-Oplustil A., Małecki M., Tarapata S., Behan A., Zontek W., *Dopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych (casus Pegasus)*, Kraków 2022, <https://kipk.pl/wp-content/uploads/2022/02/ekspertyzapegasus.pdf>.
2. Chrabkowski M., *Wykorzystanie materiałów kontroli operacyjnej w postępowaniu przygotowawczym*, Szczepiński 2009.
3. Cora Ł., *Aksjologia procesowa a dopuszczalność dowodu z art. 168a k.p.k.*, Państwo i Prawo 2018, nr 10.
4. Cora Ł., *Wykładnia dowodu z art. 168a k.p.k. w zgodzie z Konstytucją RP. Glosa do wyroku s.apel. z dnia 27 kwietnia 2017 r., II AKa 213/16*, Gdańskie Studia Prawnicze – Przegląd Orzecznictwa 2018, nr 3.
5. Drajewicz D., *Dowodowe wykorzystanie wyników kontroli operacyjnej w postępowaniu karnym*, Prokuratura i Prawo 2010, nr 7–8.
6. Florczak-Wątor M., [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Tuleja, Warszawa 2023.
7. Gruszecka D., [w:] *Kodeks postępowania karnego. Komentarz*, red. J. Skorupka, Warszawa 2018.
8. Gruszecka D., *W kwestii interpretacji znowelizowanego przepisu art. 168a k.p.k.*, Palestra 2017, nr 1–2, <https://palestra.pl/pl/czasopismo/wydanie/1-2-2017/artukul/w-kwestii-interpretacji-znowelizowanego-przepisu-art.-168a-k.p.k.>
9. Grzegorzczak T., *Wykorzystywanie i przekształcanie materiałów operacyjnych w materiał dowodowy w postępowaniu karnym*, [w:] *Przestępczość zorganizowana. Świadek koronny. Terroryzm*, red. E. Pływaczewski, Kraków 2005.
10. Hanausek T., *Ustawa o Policji. Komentarz*, Kraków 1996.
11. Herzog A., *Wykorzystanie materiałów operacyjnych w postępowaniu dyscyplinarnym prokuratorów*, Prokuratura i Prawo 2007, nr 2.
12. Hoc S., *Refleksje na marginesie art. 10 Ustawy o urzędzie ochrony państwa*, Wojskowy Przegląd Prawniczy 1992, nr 3–4.
13. Hoc S., Szustakiewicz P., *Ustawa o Centralnym Biurze Antykorupcyjnym. Komentarz*, wyd. 2, LEX/el. 2023.
14. Jakubiak-Mirończuk A., *Alternatywne a sądowe rozstrzyganie sporów sądowych*, Warszawa 2008.
15. Jasiński W., [w:] *System Prawa Karnego Procesowego*, t. 7, cz. 2, red. J. Skorupka, Warszawa 2019.
16. Klejnowska M., *Podstuch operacyjny i prowokacja policyjna*, Prokuratura i Prawo 2004, nr 3.
17. Klejnowska M., *Podstuch pozaprocesowy (operacyjny) na gruncie znowelizowanej ustawy z dnia 6 kwietnia 1990 r. o Policji*, Przegląd Sądowy 2004, nr 4.
18. Klejnowska M., *Podstępne uzyskanie przyznania się oskarżonego do winy*, Rzeszowskie Zeszyty Naukowe 2001, nr 30.

19. Kmiecik R., *Prawnodowodowe aspekty ochrony programów komputerowych w postępowaniu karnym (problematyka wszczęcia postępowania)*, Prokuratura i Prawo 1997, nr 6.
20. Kowalewski M., *Sąd Najwyższy zgadzał się na stosowanie Pegasus*, <https://www.salon24.pl/newsroom/1374074,sad-najwyzszy-zgadzal-sie-na-stosowanie-pegasusa>.
21. Kudła J., Bielecki Z., *Wybrane aspekty zakupu kontrolowanego w pracy Policji*, Przegląd Policyjny 2005, nr 77.
22. Lipiński K., *Klauzula uadekwatniająca przesłanki niedopuszczalności dowodu w postępowaniu karnym (art. 168a k.p.k.)*, Państwo i Prawo 2016, nr 11.
23. Lityński M., *Czynności operacyjne M.O. w procesie karnym. Z problematyki dochodzenia*, Państwo i Prawo 1961, nr 6.
24. Łodziana T., *Kontrola operacyjna oraz użycie systemu Pegasus w Polsce – polemika*, Palestra 2022, nr 9, <https://palestra.pl/pl/czasopismo/wydanie/9-2022/arttykul/kontrola-operacyjna-oraz-uzycie-systemu-pegasus-w-polsce-polemika>.
25. Marszał K., *Proces karny*, Katowice 1998.
26. Matusiak-Frącczak M., *Kontrola operacyjna oraz użycie systemu Pegasus w Polsce*, Palestra 2022, nr 7–8.
27. Matusiak-Frącczak M., *Konwencyjne standardy legalnej inwigilacji a zastosowanie systemu Pegasus w Polsce*, Europejski Przegląd Sądowy 2023, nr 12.
28. Ojczyk J., *Służby podsłuchują nas bez kontroli, bo pozwala na to prawo. Potwierdził to europejski trybunał*, Business Insider z 28.05.2024 r., <https://businessinsider.com.pl/prawo/europejski-trybunal-praw-czlowieka-wyda-wyrok-w-sprawie-inwigilacji-w-polsce/3b3e4kh>.
29. Opitek P., *Kontrola operacyjna urzędnika końcowego*, Prokuratura i Prawo 2023, nr 4.
30. Opitek P., *Poważnie kontrolować można nie tylko terrorystów*, Rzeczpospolita z 20.01.2022 r., <https://www.rp.pl/opinie-prawne/art19306701-pawel-opitek-powaznie-kontrolowac-mozna-nie-tylko-terrorystow>.
31. Owczarski S., *Problematyka postępowania operacyjnego w świetle prawa i praktyki*, Przegląd Sądowy 1994, nr 4.
32. Pikulski S., *Działania operacyjne Policji*, Wojskowy Przegląd Prawniczy 1996, nr 2.
33. Ponikowski R., *Aspekty procesowe i kryminalistyczne pierwszej informacji o przestępstwie*, Nowe Prawo 1973, nr 5.
34. Schaff L., *Zakres i formy postępowania przygotowawczego*, Warszawa 1961.
35. Siewierski M., *Nowe rozwiązania kodyfikacyjne w części szczególnej kodeksu postępowania karnego*, Państwo i Prawo 1970, nr 1.
36. Skorupka J., *Dogmatyczne uzasadnienie wyróżnienia dowodów niekonwencjonalnych*, [w:] *System Prawa Karnego Procesowego*, t. 8, Dowody, cz. 1, red. J. Skorupka, Warszawa 2019.
37. Skorupka J., *Paradygmat współczesnego polskiego procesu karnego – próba ujęcia*, [w:] *Współczesne tendencje w rozwoju procesu karnego z perspektywy dogmatyki oraz teorii i filozofii prawa*, red. J. Skorupka, I. Haýduk-Hawrylak, Warszawa 2011.

38. Skorupka J., *Prokonstytucyjna wykładnia przepisów prawa dowodowego w procesie karnym*, [w:] *Verba volant, scripta manent: proces karny, prawo karne skarbowe i prawo wykroczeń po zmianach z lat 2015–2016. Księga pamiątkowa poświęcona Profesor Monice Zbrojewskiej*, red. T. Grzegorzcyk, R. Olszewski, Warszawa 2016.
39. Skowron A., *Rzetelny proces karny w ujęciu Karty Praw Podstawowych Unii Europejskiej oraz Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*, Prokuratura i Prawo 2017, nr 11.
40. Sobolewski Z., *Zasada „Nemo se ipsum accusare tenetur” w polskim procesie karnym*, Lublin 1979.
41. Taracha A., *Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawno-dowodowe*, Lublin 2006.
42. Taracha A., *Wykorzystanie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych w procesie karnym*, [w:] *Nowy kodeks postępowania karnego. Zagadnienia węzłowe*, red. E. Skrętowicz, Kraków 1998.
43. Wiliński P., *O koncepcji rzetelnego procesu*, [w:] *Rzetelny proces karny. Materiały konferencji naukowej. Trzebiezowice 17–19 września 2009 r.*, red. J. Skorupka, W. Jasiński, Warszawa 2010.
44. Zubik M., Sokolewicz W., [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. 1, red. L. Garlicki, Warszawa 2016.
45. Żak J., *Dowody rzeczowe w sprawach o szpiegostwo*, Wojskowy Przegląd Prawniczy 1991, nr 1.