

Sygnatura akt II AKa 480/21

WYROK

W IMIENIU RZECZYPOSPOLITEJ POLSKIEJ

Dnia 11 maja 2023 r.

Sąd Apelacyjny we Wrocławiu II Wydział Karny w składzie:

Przewodniczący SSA Edyta Gajgał (spr.)

Sędziowie: SA Agata Regulska

SA Andrzej Szliwa

Protokolant: Katarzyna Szypuła

przy udziale Przemysława Nowaka prokuratora Prokuratury (...)w W.

po rozpoznaniu w dniach: 1 grudnia 2022 r., 23 lutego 2023r. , 12 kwietnia 2023r. oraz 11 maja 2023 r. sprawy :

R. J. (1) oskarżonego 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. oskarżonej 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.

na skutek apelacji wniesionych przez oskarżonych

od wyroku Sądu Okręgowego we Wrocławiu

z 10 września 2021 r. sygn. akt III K 63/21

zmienia zaskarżony wyrok w ten sposób, że:

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

w zakresie czynu przypisanego oskarżonej K. T. w pkt II części rozstrzygającej ustala, że w dniach 27 i 28 marca 2019 roku w K. i 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 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tekst jednolity Dz. U. z 2022 roku, 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 (pięćdziesięciu) stawek dziennych,

w pozostałej części zaskarżony wyrok utrzymuje w mocy,

zwalnia oskarżoną K. T. od zapłaty na rzecz Skarbu Państwa kosztów sądowych postępowania odwoławczego, obciążając nimi Skarb Państwa, w tym nie wymierza jej opłaty za obie instancje.

UZASADNIENIE

R. J. (1) 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, sygn. akt III K 63/21:

uznał oskarżonego R. J. (1) za winnego popełnienia zarzucanego mu czynu opisanego w pkt I części dyspozytywnej wyroku, to jest 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;

uznał oskarżoną K. T. za winną popełnienia zarzucanego jej czynu opisanego w pkt II części dyspozytywnej wyroku, to jest 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;

na podstawie art. 69 § 1 k.k. i art. 70 § 1 k.k. orzeczoną wobec oskarżonego R. J. (1) karę pozbawienia wolności warunkowo zawiesił na 3 lata okresu próby;

na podstawie art. 69 § 1 k.k. i art. 70 § 1 k.k. orzeczoną wobec oskarżonej K. T. karę pozbawienia wolności warunkowo zawiesił na 3 lata okresu próby;

na podstawie art. 71 § 1 k.k. orzekł wobec oskarżonego R. J. (1) karę grzywny w wymiarze 100 stawek dziennych przy przyjęciu wysokości jednej stawki na kwotę 100 złotych;

na podstawie art. 71 § 1 k.k. orzekł wobec oskarżonej K. T. karę grzywny w wymiarze 100 stawek dziennych przy przyjęciu wysokości jednej stawki na kwotę 50 złotych;

na podstawie art. 72 § 1 pkt 1 k.k. zobowiązał oskarżonego R. J. (1) – w okresie próby – do informowania Sądu o przebiegu okresu próby;

na podstawie art. 72 § 1 pkt 1 k.k. zobowiązał oskarżoną K. T. – w okresie próby – do informowania Sądu o przebiegu okresu próby;

na podstawie art. 230 § 2 k.p.k. zwrócił Agencji Bezpieczeństwa Wewnętrznego dowód rzeczowy opisany pod poz. 3 w wykazie dowodów rzeczowych znajdującym się na karcie 1365 akt;

zasądził od każdego z oskarżonych przypadające na nich koszty sądowe w kwocie po 8.565,69 złotych oraz wymierzył oskarżonemu R. J. (1) opłatę sądową w kwocie 1.180 zł., zaś oskarżonej K. T. opłatę sądową w kwocie 680 zł.

Wyrok ten zaskarżyli w całości obrońcy obojga oskarżonych.

Obrońcy oskarżonego R. J. (1) zarzucili:

obrazę przepisów postępowania mającą wpływ na treść orzeczenia, to jest art. 7 k.p.k.:

polegającą na dokonaniu przez Sąd nieprawidłowej oceny zgromadzonego w sprawie materiału dowodowego wynikającej z przekroczenia przez Sąd zasady swobodnej oceny dowodów poprzez przyjęcie, iż w rozmowach tekstowych pomiędzy R. J. (1) a K. T. oskarżony nakłaniał K. T. do przekroczenia przysługujących jej jako funkcjonariuszowi ABW uprawnień i ujawnienia informacji niejawnych, co w konsekwencji doprowadziło do uznania przez Sąd, iż zachowanie R. J. (1) zrealizowało znamiona podżegania z art. 18 § 2 k.k., w sytuacji gdy prawidłowa ocena zebranych w sprawie dowodów, w tym w szczególności analiza rozmów pomiędzy oskarżonymi utrwalonych w toku kontroli operacyjnej, wyraźnie wskazuje, iż R. J. (1) w kierowanych wiadomościach do K. T. w żaden sposób nie nakłaniał jej do popełnienia przestępstwa, to jest nie zmierzał do wywołania u K. T. zjawiska psychicznego w postaci decyzji popełnienia czynu zabronionego, a nadto charakter rozmów tekstowych wskazuje, iż oskarżona K. T. samodzielnie, bez jakiegokolwiek wpływu R. J. (1) wysyłała mu wiadomości tekstowe o określonej treści, co tym samym dowodzi braku realizacji przez oskarżonego znamion niesprawczej formy popełnienia przestępstwa w postaci podżegania;

poprzez uznanie wyjaśnień oskarżonego R. J. (1) oraz K. T. w zakresie, w jakim wskazują o samodzielnym ustaleniu przez oskarżonego, iż względem niego są prowadzone czynności operacyjno-rozpoznawcze za niewiarygodne i przyjęciu, że R. J. (1) miał jedynie domysły co do możliwej inwigilacji względem niego, ze względu na co miał nakłaniać K. T. do przekroczenia przysługujących jej jako funkcjonariuszowi uprawnień i ujawnienia informacji niejawnych, które miały potwierdzić prowadzoną względem oskarżonego kontrolę operacyjną, co w konsekwencji doprowadziło do uznania, że R. J. (1) zrealizował swoim zachowaniem znamiona zarzucanego mu czynu, w sytuacji gdy zgromadzony w sprawie materiał dowodowy, w tym między innymi utrwalone podczas czynności operacyjno-rozpoznawczych treści wiadomości oskarżonego, jednoznacznie potwierdzają wyjaśnienia R. J. (1) oraz K. T. co do wiedzy oskarżonego odnośnie do prowadzonych względem niego czynności operacyjnych, która wynikała z nieprofesjonalnego prowadzenia przez funkcjonariuszy służb czynności operacyjnych skutkujących ich dekonspiracją, a wiadomości wysłane przez oskarżonego były stwierdzeniem działań operacyjno-rozpoznawczych prowadzonych względem niego przez służby i w żaden sposób nie wiązały się z pozyskaniem od K. T. informacji niejawnych, które miały potwierdzić prowadzoną kontrolę, co dowodzi także tego, że R. J. (1) nie nakłaniał K. T. do przekroczenia przez nią przysługujących jej uprawnień, a tym samym, iż nie wypełnił on znamion zarzucanego mu przestępstwa w postaci podżegania funkcjonariusza do popełnienia czynu z art. 231 § 1 k.k.;

poprzez dokonanie przez Sąd dowolnej, a nie swobodnej oceny dowodów przejawiającej się w przyjęciu, że R. J. (1) nakłaniał K. T. do przekroczenia uprawnień w celu osiągnięcia przez nią korzyści majątkowej w postaci obietnicy

przyszłego zatrudnienia w prywatnej firmie, co w konsekwencji doprowadziło do uznania przez Sąd, iż doszło do zrealizowania przez oskarżonego znamion czynu zabronionego z art. 18 § 2 k.k. w zw. z art. 233 § 1 i 2 k.k., w sytuacji gdy zebrany w sprawie materiał dowodowy, w tym w szczególności dowody utrwalone w toku kontroli operacyjnej, wykazują, iż ze strony oskarżonego R. J. (1) nie padła żadna konkretna propozycja zatrudnienia K. T. polegająca na wskazaniu firmy, stanowiska czy też kwoty jaką miałyby uzyskiwać w związku z zatrudnieniem, a co więcej dowodzą, że R. J. (1) w swoich wiadomościach wysyłanych do K. T. nie tylko nie nakłaniał oskarżonej do przekroczenia przez nią uprawnień służbowych, a także nie nakłaniał jej do przekroczenia przysługujących jej uprawnień jako funkcjonariusza ABW w celu osiągnięcia przez nią korzyści majątkowej – która w żaden sposób nie została sformułowana w trakcie rozmów tekstowych pomiędzy oskarżonymi – a przyjęcie przez Sąd, iż oskarżona zaciekawiona przedsięwzięciem biznesowym oskarżonego działała z wizją przyszłej pracy w firmie R. J. (1), jest dowolną oceną Sądu nieodnajdującą żadnych podstaw w zgromadzonym w sprawie materiale dowodowym, a tym samym, brak jest realizacji przez oskarżonego znamion zarzucanego mu czynu;

polegającą na nieprawidłowej ocenie zgromadzonego w sprawie materiału dowodowego i przyjęciu przez Sąd, iż K. T. jako funkcjonariusz ABW miała dostęp do informacji tajnych związanych z prowadzeniem czynności operacyjno-rozpoznawczych w stosunku do R. J. (1), M. M. i M. S., w sytuacji gdy zeznania złożone przez funkcjonariuszy służb wyraźnie potwierdzają, że K. T. nie mogła posiadać wiedzy co do czynności operacyjno-rozpoznawczych prowadzonych względem powyższych osób, gdyż dostęp do danych operacyjnych posiadała jedynie wąska grupa osób i to w określonym czasie, przez co tym samym R. J. (1) nie mógł nakłaniać K. T. do ujawnienia informacji niejawnych, na temat których nie miała ona żadnej wiedzy,

obrazę przepisów postępowania, mającą wpływ na treść orzeczenia, tj. art. 170 § 1 pkt 1 k.p.k. w zw. z art. 168a k.p.k. w zw. z art. 17 ust. 1 pkt 1 ustawy z dnia 9 czerwca 2006 roku o Centralnym Biurze Antykorupcyjnym – polegającą na dopuszczeniu i przeprowadzeniu dowodów utrwalonych w trakcie prowadzonej na podstawie art. 17 ust 1 pkt 1 ustawy o CBA pozaprocessowej kontroli operacyjno-rozpoznawczej w zakresie dotyczącym popełnienia przez oskarżonego R. J. (1) przestępstwa z art. 265 § 1 k.k. i dokonaniu na podstawie tych dowodów ustaleń faktycznych stanowiących podstawę wyroku skazującego, w sytuacji gdy dowód ten został uzyskany z naruszeniem przepisów postępowania przez funkcjonariuszy publicznych w związku z pełnieniem przez nich obowiązków służbowych, a tym samym jest on dowodem nielegalnym i niedopuszczalnym, który winien być oddalony na podstawie art. 170 § 1 pkt 1 k.p.k., bowiem stosownie do treści art. 17 ust. 1 pkt 1 ustawy o CBA pozaprocessowe czynności operacyjno-rozpoznawcze mogą być prowadzone tylko względem przestępstw ujętych w katalogu przewidzianym w treści art. 17 ustawy o CBA, wśród których nie ma czynu zabronionego z art. 265 k.k., przez co tym samym niedopuszczalnym było utrwalanie i gromadzenie materiału dowodowego w zakresie dotyczącym przestępstwa z art. 265 § 1 k.k. przeciwko oskarżonemu R. J. (1), a ponadto, stosownie do utrwalonego w orzecznictwie poglądu, w tym także stanowiska Sądu Najwyższego, ujawnienie dowodu dotyczącego przestępstwa z art. 265 § 1 k.k. nie mogło zostać ujęte zgodą następczą w rozumieniu art. 168b k.p.k., gdyż zgodą taką mogą zostać objęte jedynie inne enumeratywnie wymienione w ustawie o CBA przestępstwa, przez co tym samym dowody dotyczące podejrzenia popełnienia przestępstw z art. 265 § 1 k.k. ujawnione i utrwalone w toku czynności operacyjno-rozpoznawczych nie mogły zostać dopuszczone do postępowania i nie mogły stanowić podstawy ustaleń faktycznych, ze względu na co nie powinny być również podstawą wyroku skazującego,

obrazę przepisów postępowania, mającą wpływ na treść orzeczenia, to jest art. 168b k.p.k. w zw. z art. 168a k.p.k. w zw. z art. 170 § 1 pkt 1 k.p.k., poprzez dopuszczenie i przeprowadzenie dowodów utrwalonych w toku czynności operacyjno-rozpoznawczych prowadzonych względem oskarżonego na podstawie art. 17 ust 1 pkt 1 ustawy o CBA, w sytuacji gdy nie zostało wydane przez prokuratora postanowienie legalizujące powyższe dowody, przez co tym samym dowody te jako zgromadzone z naruszeniem przepisów postępowania przez funkcjonariuszy publicznych w związku z pełnieniem przez nich obowiązków służbowych były nielegalne i niedopuszczalne, ze względu na co podlegały oddaleniu na podstawie art. 170 § 1 pkt 1 k.p.k. i nie mogły stanowić podstawy wyroku skazującego,

obrazę przepisów postępowania, mającą wpływ na treść orzeczenia, to jest art. 7 k.p.k., polegającą na nieprawidłowej ocenie zgromadzonego w sprawie materiału dowodowego, skutkującej przyjęciem przez Sąd, iż R. J. (1) przekazywał informacje niejawne M. M., a nadto że wykorzystywał te informacje do modyfikacji własnych działań, w sytuacji gdy

zgromadzony w sprawie materiał dowodowy wyraźnie wykazuje, że zarówno oskarżony jak i M. M. samodzielnie rozpoznali działania operacyjno-rozpoznawcze funkcjonariuszy służb, którzy w sposób nieprofesjonalny dokonywali czynności inwigilacyjnych prowadząc do swojej dekonspiracji, przez co tym samym dowody zebrane w niniejszym postępowaniu nie udowodniły, iż oskarżony przekazywał informacje niejawne M. M. skoro ten już posiadał wiedzę co do prowadzonej względem niego inwigilacji, a nawet treści wiadomości pomiędzy nimi, które nie powinny być dopuszczone w przedmiotowej sprawie z uwagi na powyższe zarzuty, wykazują, iż wymieniali się oni swoimi spostrzeżeniami co do działań funkcjonariuszy służb, a nadto materiał dowodowy w żaden sposób nie wykazał jakoby oskarżony R. J. (1) miał wykorzystać informacje przekazane mu przez K. T., o których to działaniach służb i tak już wiedział z własnych obserwacji, do modyfikacji swoich działań, a ustalenia dokonane przez Sąd I instancji w tym zakresie są wynikiem dowolnej oceny materiału dowodowego, nieznajdującej żadnych podstaw, co tym samym wyraźnie dowodzi o braku realizacji przez oskarżonego znamion z art. 265 § 1 k.k.

Stawiając te zarzuty obrońcy wniesli o zmianę zaskarżonego wyroku przez uniewinnienie oskarżonego od popełnienia zarzucanego mu czynu zabronionego.

W apelacji obrońcy oskarżonej K. T. podniesione zostały zarzuty:

obrazy przepisów postępowania, mającej wpływ na treść orzeczenia, a to art. 7 k.p.k. w zw. z art. 410 k.p.k. poprzez dowolną ocenę wyjaśnień współoskarżonych jako niewiarygodnych, podczas gdy pozostają one spójne i korespondują z treścią pozostałych dowodów w sprawie (wiadomości pisemne między oskarżonymi, zeznania świadków), a co w konsekwencji doprowadziło do dokonania przez Sąd I instancji wadliwych ustaleń faktycznych, iż:

oskarżony R. J. jedynie snuł domysły co do prowadzonych wobec niego działań operacyjno-rozpoznawczych i dlatego nakłonił K. T. do przekroczenia uprawnień i ujawnienia mu informacji niejawnych, podczas gdy całokształt dowodów potwierdza wyjaśnienia obojga oskarżonych, że oskarżony R. J. miał wiedzę i był dobrze zorientowany o trwającej wobec niego obserwacji towarzyszącej, a jego wiedza w tym zakresie wynikała z dekonspiracji nieprofesjonalnie prowadzonych działań, nie zaś jakichkolwiek informacji pochodzących od oskarżonej,

oskarżona posiadała informacje tajne związane z prowadzeniem czynności operacyjno-rozpoznawczych w stosunku do współoskarżonego i innych osób, podczas gdy zgodnie z treścią niekwestionowanych przez Sąd I instancji zeznań świadków, tj. funkcjonariuszy, wynika, że nie miała ona do nich dostępu, albowiem nie należała do grupy zajmującej się prowadzeniem tych czynności wobec w/w, a co koresponduje z faktem, że wiadomości wysyłane przez oskarżoną, w przeważającej części miały charakter ogólny, wtórny do uzyskanej przez niego wiedzy wskutek znajomości mechanizmów działania służb (jako że sam był wcześniej funkcjonariuszem) i jedynie potwierdzały spostrzeżenia oskarżonego R. J., nie prowadząc w żaden sposób do modyfikacji jego działań,

oskarżona działała w celu osiągnięcia korzyści majątkowej w postaci obietnic przyszłego zatrudnienia w prywatnej firmie, podczas gdy z całokształtu materiału dowodowego wynika, iż oskarżony R. J. (1) nie złożył oskarżonej żadnej obietnicy ani nawet propozycji zatrudnienia w jakiegokolwiek prywatnej firmie, albowiem oskarżeni wyłącznie rozmawiali o planach biznesowych oskarżonego, który zakończył służbę i analizował perspektywę samozatrudnienia, zaś oskarżona nie zamierzała odchodzić ze służby, nie planowała zmiany zawodu, nie była ukierunkowana na poszukiwanie innej pracy i w żaden sposób nie inicjowała poważnych rozmów na ten temat ze współoskarżonym; przy czym powyższe błędne ustalenia doprowadziły do wadliwego uznania, że oskarżona wyczerpała swoim zachowaniem znamiona przestępstwa z art. 231 § 1 i 2 k.k. w zbiegu z art. 265 k.k.,

obrazy przepisów postępowania, mającej wpływ na treść orzeczenia, a to art. 168a k.p.k. oraz 168b k.p.k. w zw. z art. 17 ust. 1 pkt 1 ustawy z dnia 9 czerwca 2006 roku o Centralnym Biurze Antykorupcyjnym w zw. z art. 170 § 1 pkt 1 k.p.k., przez przeprowadzenie dowodów z wiadomości tekstowych uzyskanych w trakcie kontroli operacyjno-rozpoznawczej prowadzonej na podstawie art. 17 ust. 1 pkt 1 ustawy o CBA wobec R. J. w zw. z art. 265 k.k., podczas gdy wskazane dowody są nielegalne, których przeprowadzenie było niedopuszczalne, ponieważ wskazany kierunek kontroli operacyjnej nie jest wymieniony w katalogu zawartym w art. 17 ust. 1 pkt 1 ustawy o CBA, w konsekwencji więc nie mogło zostać ujęte również zgodą następczą w rozumieniu art. 168b k.p.k. oraz nie mogły stanowić ustaleń

faktycznych, przy jednoczesnym zauważeniu, że w sprawie nie zostało wydane przez prokuratora postanowienie w przedmiocie wykorzystania tych dowodów w postępowaniu karnym, co łącznie spowodowało pozostawienie w podstawie faktycznej wyroku dowodów prawem niedopuszczalnych,

błędu w ustaleniach faktycznych przyjętych za podstawę wyroku i mającego wpływ na jego treść, polegającego na wadliwym określeniu stopnia społecznej szkodliwości i stopnia winy, ponad próg nieznaczności, wskutek nieuwzględnienia takich okoliczności jak:

- potwierdzenie przez oskarżoną ogólnych, nieprecyzyjnych uwag i spostrzeżeń oskarżonego R. J. odnośnie jego wiedzy w kwestii prowadzonej obserwacji towarzyszącej;
- prowokacyjna i kompromitująca dekonspiracja działań wywiadowczych wynikająca z nieprofesjonalnego prowadzenia obserwacji towarzyszącej;
- poniesienie przez oskarżoną najsurowszej kary dyscyplinarnej poprzez wydalenie ze służby,

co skutkowało chybnym niezastosowaniem środka probacyjnego w postaci warunkowego umorzenia postępowania.

Stawiając te zarzuty obrońca wniósł o zmianę zaskarżonego wyroku przez uniewinnienie oskarżonej od popełnienia zarzucanych jej czynów ewentualnie przez warunkowe umorzenie postępowania i orzeczenie okresu próby w wymiarze roku.

Sąd Apelacyjny zważył, co następuje.

Pierwsza uwaga, jaka nasuwa się w tej sprawie, dotyczy tego, że pisemne uzasadnienie zaskarżonego wyroku zostało sporządzone przez Sąd pierwszej instancji jako dokument w całości opatrzony klauzulą „ściśle tajne”. Pojawia się pytanie, czy determinuje to konieczność sporządzenia także uzasadnienia wyroku Sądu odwoławczego w takiej formule. W złożonych apelacjach zakwestionowane zostały bowiem ustalenia faktyczne przyjęte za podstawę zaskarżonego wyroku oraz ocena dowodów, w następstwie której zostały one poczynione. Negowana jest także prawidłowość procedowania przez Sąd pierwszej instancji. Odniesienie się do tych zarzutów wymaga zatem – w ściśle określonym zakresie – odwołania się do stanowiska, jakie zajął w tej mierze Sąd pierwszej instancji.

Rzecz jednak w tym, że uzasadnienie zaskarżonego wyroku zawiera takie elementy, które trudno uznać – na gruncie art. 5 ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (tekst jednolity Dz. U. z 2023 r. poz. 756, dalej jako ustawa o ochronie informacji niejawnych) – za podlegające ochronie w tym trybie. Dotyczy to przede wszystkim właśnie tych kwestii, które są przedmiotem zarzutów apelacyjnych – a więc przeprowadzonych przez Sąd Okręgowy rozważań prawnych, w tym co do przyjęcia za podstawę ustaleń faktycznych określonych dowodów, których legalność jest podważana w apelacjach, ale także zaprezentowanych wyników oceny tych dowodów i określonych elementów ustaleń faktycznych przyjętych za podstawę zaskarżonego wyroku. Zostały one zakwestionowane w sporządzonych apelacjach jako dokumentach jawnych, w których skarżący nie odnosili się do materiałów niejawnych, do treści zawartych w tych materiałach. Przemawia to przeciwko tezie o konieczności sporządzenia uzasadnienia wyroku Sądu odwoławczego jako dokumentu niejawnego. Trudno uznać, że niejawnym charakterem powinny mieć rozważania prawne odnoszące się do konkretnych przepisów prawa znajdujących zastosowanie w tej sprawie.

Znaczenie w tym zakresie ma także to, że jawny jest wydany przez Sąd pierwszej instancji wyrok (tak samo zresztą jak wyrok Sądu Apelacyjnego). Jak stanowi bowiem przepis art. 364 § 1 k.p.k., ogłoszenie wyroku odbywa się jawnie. Oznacza to między innymi, że jawne są te elementy stanu faktycznego, które swoje odzwierciedlenie znajdują w opisie czynów przypisanych oskarżonym w zaskarżonym wyroku.

Co do zasady jawne są także powody wyroku. Zgodnie z art. 364 § 2 k.p.k. możliwe jest ich przytoczenie z wyłączeniem jawności, jeżeli jawność rozprawy wyłączono w całości lub w części.

W realiach tej sprawy o takim wyłączeniu jawności nie zdecydował Sąd Apelacyjny na rozprawie w dniu 11 maja 2023 roku. W konsekwencji, także pisemne uzasadnienie wyroku sądu odwoławczego – w tym zakresie, w którym nie zachodzi potrzeba odwołania się wprost do materiałów opatrzonych odpowiednią klauzulą tajności – ma charakter dokumentu jawnego.

Druga uwaga ma związek z określoną konstrukcją wniesionych apelacji. Jako pierwsze w pisemnych środkach odwoławczych ujęte zostały te zarzuty, które dotyczą oceny dowodów (przede wszystkim materiałów uzyskanych w toku przeprowadzonej kontroli operacyjnej) i ustaleń faktycznych dokonanych na podstawie tych dowodów. W dalszej dopiero kolejności sformułowane zostały zarzuty dotyczące wprowadzenia tych dowodów do procesu i ich legalności. Jasne jest, że rozważania na temat prawidłowości dokonanej przez Sąd Okręgowy oceny dowodów poprzedzać musi odniesienie się do zarzutów dotyczących problemu legalności przeprowadzonej kontroli operacyjnej oraz tego, czy uzyskane w jej toku materiały zostały w sposób prawidłowy wprowadzone do procesu. Tylko odrzucenie zastrzeżeń wysuwanych w tej mierze przez obrońców otworzy drogę do oceny zasadności zarzutów sformułowanych jako pierwsze w apelacjach. Odniesienie się do nich będzie bezprzedmiotowe, gdy stwierdzone zostanie, że materiały uzyskane w ramach kontroli operacyjnej nie mogły zostać uwzględnione jako podstawa wyroku. Stąd też rozważania w sprawie rozpocząć należy od kwestii związanych z – ogólnie rzecz ujmując – legalnością dowodów uzyskanych w wyniku kontroli operacyjnej przeprowadzonej wobec oskarżonego R. J. (1).

Kwestia ta ma kluczowe znaczenie w sprawie z punktu widzenia standardów rzetelnego postępowania karnego w rozumieniu art. 6 ust. 1 Konwencji o ochronie praw człowieka i podstawowych wolności sporządzonej w R. dnia 4 listopada 1950 roku, zmienionej następnie Protokołami nr (...) oraz uzupełnionej Protokołem nr (...) (Dz. U. z 1993 roku, Nr 61, poz. 284 z późniejszymi zmianami, dalej jako Konwencja, Europejska Konwencja). Norma prawna wyrażona w tym przepisie prawa międzynarodowego znajduje zastosowanie w polskim porządku prawnym na mocy art. 9 Konstytucji, zgodnie z którym Rzeczpospolita Polska przestrzega wiążącego ją prawa międzynarodowego oraz art. 91 ust. 1 ustawy zasadniczej, który stanowi, że ratyfikowane umowy międzynarodowe stają się częścią krajowego systemu prawa i są stosowane bezpośrednio – a więc jako źródła prawa powszechnie obowiązującego.

W przepisie art. 6 ust. 1 Konwencji ustanowione zostało prawo do sprawiedliwego – rzetelnego – rozpoznania sprawy przez sąd. Z uwagi na to, że nie zostało ono sprecyzowane, Europejski Trybunał Praw Człowieka (dalej jako ETPC) w swoim orzecznictwie przez wykładnię art. 6 ust. 1 Konwencji kształtuje rozumienie tego pojęcia. W zakresie dotyczącym postępowania dowodowego ETPC wskazywał, że co do zasady kształtowanie reguł prawa dowodowego, w tym zagadnienie dopuszczalności poszczególnych dowodów czy metod dowodzenia, tak jak i ocena dowodów leżą poza zakresem jego kognicji. Nie oznacza to jednak, że nie wypowiedział się na ten temat. W swoim orzecznictwie odnosił się do zagadnień związanych z korzystaniem w toku procesu z dowodów przeprowadzonych z naruszeniem prawa lub pogwałceniem praw konwencyjnych, szczególnie prawa do obrony (zob. Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom I–II. Komentarz, prof. dr hab. Leszek Garlicki, prof. dr hab. Piotr Hofmański, prof. dr hab. Andrzej Wróbel, Rok 2010, teza 12, L.).

W wyroku z dnia 12 maja 2000 roku, Khan przeciwko Zjednoczonemu Królestwu, ETPC zwrócił uwagę na to, że z perspektywy art. 6 ust. 1 Konwencji nieodzowne jest rozstrzygnięcie, czy proces jako całość – łącznie ze sposobem uzyskania dowodów – był rzetelny. Obejmuje to ocenę naruszenia (ingerencji, bezprawia), do którego doszło oraz, w przypadkach stwierdzenia naruszenia innego prawa gwarantowanego Konwencją, istoty tego naruszenia. Znaczenie w tej mierze ma między innymi to, czy dowód uzyskany z naruszeniem prawa jest jedynym dowodem prowadzącym do uznania winy. Wymaga to oceny jego roli w procesie, tego, jak duży ma wpływ na rozstrzygnięcie, jaką ma moc (zob. wyrok ETPC z 12.05.2000 r., 35394/97, KHAN v. WIELKA BRYTANIA, LEX nr 76868; M. A. Nowicki, Khan przeciwko Wielkiej Brytanii - wyrok ETPC z dnia 12 maja 2000 r., skarga nr 35394/97, [w:] M.A. Nowicki, Nowy Europejski Trybunał Praw Człowieka. Wybór orzeczeń 1999-2004, Zakamycze, 2005, s. 509, Zakamycze 2005; Komentarz do Konwencji..., op. cit., teza 13).

W wyroku z 5 lutego 2008 roku, Ramanauskas przeciwko Litwie, przedmiotem rozważań ETPC była kwestia dopuszczalności dowodów uzyskanych w wyniku prowokacji policyjnej. I w tym orzeczeniu podkreślono konieczność

oceny całości procesu, łącznie ze sposobem przeprowadzenia postępowania dowodowego, jako rzetelnego. ETPC zauważył, że wzrost przestępczości, szczególnie korupcyjnej czy zorganizowanej, wymaga sięgania po odpowiednie środki, w tym między innymi praktyki niejawnie czy środki techniki operacyjnej. Jak stwierdził, korzystanie z tych specjalnych metod ścigania, samo w sobie nie może naruszać prawa do rzetelnego procesu. Podkreślił jednak, że z uwagi na ryzyko nadużycia, ich stosowanie musi mieścić się w wyraźnie określonych granicach. Wykorzystanie przez sąd w procesie takich źródeł jak anonimowi informatorzy jest do zaakceptowania jedynie wówczas, gdy wdrożone zostały odpowiednie i wystarczające zabezpieczenia, zwłaszcza jasna i przewidywalna procedura zezwalania, stosowania i nadzoru nad takimi czynnościami operacyjnymi. ETPC dobitnie stwierdził, że prawo do rzetelnego procesu zajmuje ważne miejsce w demokratycznym społeczeństwie. Z tego powodu nie można go poświęcić w imię względów praktycznych. Korzystanie z prowokacji policyjnej ETPC określił jako sytuację, która od samego początku naraża oskarżonego na ryzyko pozbawienia go prawa do rzetelnego procesu. Wyraźnie przy tym rozróżnił pasywne zachowania służb od działań aktywnych, takich, które wiążą się z wywieraniem wpływu (zob. wyrok ETPC(WI) z 5.02.2008 r., 74420/01, RAMANAUSKAS v. LITWA, LEX nr 3453651; M. A. Nowicki, Ramanauskas przeciwko Litwie - wyrok ETPC z dnia 5 lutego 2008 r., skarga nr 74420/01, [w:] M.A. Nowicki, Europejski Trybunał Praw Człowieka. Wybór orzeczeń 2008, Oficyna, 2009, s. 122, Oficyna 2009; Komentarz do Konwencji..., op. cit., teza 15).

Z orzecznictwa strasburskiego jasno wynika, że ocena dokonywana z perspektywy art. 6 ust. 1 Europejskiej Konwencji zawsze musi uwzględniać okoliczności konkretnej sprawy.

W tej sprawie materiały uzyskane w wyniku kontroli operacyjnej, prowadzonej z powołaniem się na przepis art. 17 ust. 5 ustawy z dnia 9 czerwca 2006 roku o Centralnym Biurze Antykorupcyjnym (tekst jednolity Dz. U. z 2022 roku, poz. 1900 z późniejszymi zmianami – dalej jako ustawa o CBA), stanowią kluczowy dowód w sprawie. To one – treść rozmów prowadzonych przez oskarżonego R. J. (1) za pośrednictwem komunikatorów internetowych – stały się podstawą podjęcia czynności o charakterze procesowym, to one doprowadziły do wszczęcia postępowania, bez nich nie byłoby to możliwe. W akcie oskarżenia prokurator wskazał na ten dowód oraz na wyjaśnienia oskarżonych jako dwa zasadnicze dowody w sprawie, uzasadniające tezy aktu oskarżenia. Nie ulega wątpliwości, że dowody te pełniły pierwszoplanową rolę w sprawie – to one były decydujące dla wydania wyroku skazującego oskarżonych. Z uzasadnienia zaskarżonego wyroku wynika, że za podstawę czynionych ustaleń faktycznych przyjęte zostały przede wszystkim materiały z kontroli operacyjnej. Wyjaśnienia oskarżonych były ściśle związane z tym, na co wskazywały te materiały, w określonym zakresie były ich pochodną. To powoduje, że dla stwierdzenia, czy proces oskarżonych był rzetelny, czy spełniał standardy konwencyjne, konieczne jest udzielenie odpowiedzi na pytanie, czy materiały uzyskane w toku przeprowadzonej wobec R. J. (1) kontroli operacyjnej mogły stanowić dowód, czy mogły być wprowadzone do postępowania oraz w jaki sposób.

Rozpoczynając szczegółowe rozważania w sprawie od tego ostatniego zagadnienia – będącego przedmiotem zarzutów postawionych przez obrońców oskarżonych – nie można zgodzić się ze skarżącymi, gdy zarzucają, że brak decyzji procesowej wydanej przez prokuratora na podstawie art. 168 b k.p.k. – postanowienia będącego formą zgody następczej – uniemożliwił wykorzystanie materiałów z kontroli operacyjnej w procesie przez Sąd pierwszej instancji. Stawiając taką tezę obrońcy odwołują się do stanowiska, jakie zajęły Sądy Apelacyjne w Warszawie i w Białymstoku, stwierdzając, że decyzja prokuratora w przedmiocie wykorzystania dowodu z kontroli operacyjnej, o jakiej mowa w art. 168 b k.p.k., wymaga materializacji w formie postanowienia określającego zakres materiałów legalnych i przydatnych w konkretnym postępowaniu (zob. wyrok SA w Warszawie z 14.08.2019 r., II AKa 202/18, LEX nr 2728224; wyrok SA w Białymstoku z 3.04.2017 r., II AKa 182/16, LEX nr 2307608; wyrok SA w Warszawie z 17.01.2018 r., II AKa 331/17, LEX nr 2447632).

Rzecz jednak w tym, że według innego stanowiska prezentowanego tak w doktrynie, jak i orzecznictwie, każdy sposób uzewnętrznienia przez prokuratora decyzji podjętej w trybie art. 168 b k.p.k. jest dopuszczalny. Może ona przybrać formę wniosku dowodowego w akcie oskarżenia, co do którego sąd rozstrzyga w toku postępowania. Może mieć także charakter konkludentny, czego wyrazem będzie włączenie dowodu do materiału dowodowego (zob. D. Szumiło-Kulczycka, Dalsze wykorzystywanie materiałów z kontroli operacyjnej. Uwagi na tle art. 168b k.p.k., PiP 2018, nr 10, s. 107-120; uchwała SN(7) z 28.06.2018 r., I KZP 4/18, OSNKW 2018, nr 8, poz. 53, niepublikowany

wyroku SN z 29 listopada 2021 roku, sygn. akt II K 402/21, k.1801-1816 akt sprawy). W tym ostatnim wyroku Sąd Najwyższy zwrócił uwagę, że czym innym jest gromadzenie dowodów z naruszeniem prawa, czym innym zaś niezachowanie właściwej formy decyzji otwierającej możliwość procesowego wykorzystania dowodów. Przypominał także, że w wypadku postawienia w środku odwoławczym zarzutu, w którym kwestionowany jest brak odpowiedniej formy decyzji procesowej prokuratora, dla jego skuteczności konieczne jest wykazanie wpływu takiego uchybienia na treść zaskarżonego wyroku. W tej sprawie, w złożonych apelacjach, skarżący tego nie uczynili.

Osobną sprawą pozostaje jednak to, że warunkiem wykorzystania w postępowaniu sądowym dowodu popełnienia przestępstwa przez inną osobę niż objęta postanowieniem o zgodzie na zastosowanie kontroli operacyjnej lub też dowodu przestępstwa innego niż objęte takim postanowieniem jest dopuszczenie go przez sąd. Tylko wówczas może on stanowić podstawę dowodową wyroku. Decyzja prokuratora podjęta w trybie art. 168 b k.p.k., niezależnie od tego, jaką formę przybrała, nie przesądza o tym, że takie dowody uzyskane podczas kontroli operacyjnej będą mogły być wprowadzone do postępowania sądowego i w konsekwencji stać się źródłem ustaleń faktycznych stanowiących podstawę orzekania. Nie jest ona dla sądu wiążąca, a złożony przez prokuratora wniosek podlega weryfikacji i kontroli sądu. Jak się wskazuje, przed podjęciem decyzji w trybie art. 168 b k.p.k., prokurator powinien ocenić procesową przydatność materiałów z kontroli operacyjnej. Następstwem tej oceny powinno być albo złożenie odpowiednich wniosków dowodowych albo uznanie tych materiałów za nieprzydatne procesowo czy to z uwagi na ich niską wartość dowodową czy to wadę uzyskania. Materiały nieprzydatne powinny zostać zniszczone. Kontrola dokonywana przez sąd w związku z odpowiednim wnioskiem dowodowym złożonym przez prokuratora obejmuje wszystkie ustawowe przesłanki stosowania kontroli operacyjnej. Tylko dowody uzyskane w wyniku legalnie prowadzonej kontroli operacyjnej – a więc w zgodzie z przepisami materialnymi określającymi warunki tej kontroli – mogą być wprowadzone do procesu, dopuszczone jako dowody przez sąd w toku postępowania sądowego, a w dalszej kolejności uwzględnione przy wyrokowaniu (zob. D. Szumiło-Kulczycka, op. cit.; uchwała SN z 28.06.2018 roku, op. cit.).

W rozpoznawanej sprawie, prokurator zawarł w akcie oskarżenia wnioski o przeprowadzenie dowodu z materiałów uzyskanych w wyniku kontroli operacyjnej prowadzonej wobec oskarżonego R. J. (1) (art. 333 § 1 pkt 2 k.p.k.). Sąd Okręgowy nie podjął odrębnej decyzji procesowej o dopuszczeniu tych dowodów. Jak należy przyjąć, zostały one włączone do materiału dowodowego w trybie art. 405 § 2 k.p.k. W uzasadnieniu zaskarżonego wyroku ocenę tych dowodów Sąd pierwszej instancji zawarł w krótkim stwierdzeniu, że są one wiarygodne, że nie budzą one wątpliwości jako dokumenty urzędowe.

Sąd Okręgowy nie badał i nie oceniał, czy kontrola operacyjna zarządzona wobec R. J. (1) była legalna, czy spełnione zostały warunki określone w art. 17 ust. 1 ustawy o CBA uzasadniające jej zarządzenie, a następnie przedłużenie. Pomijając ten etap weryfikacji przeszedł od razu do oceny wartości dowodowej materiałów uzyskanych w wyniku tej kontroli, uznając milcząco, że mogły one zostać wprowadzone do procesu jako dowód. Zakwestionowanie przez obrońców legalności tych dowodów między innymi z uwagi na to, że przedmiotem postawionych oskarżonych zarzutów było tzw. przestępstwo niekatalogowe – takie, które nie zostało wymienione w art. 17 ust. 1 ustawy o CBA – nie ograniczało Sądu Apelacyjnego do zbadania tylko tego jednego aspektu legalności kontroli operacyjnej. Zarzut, że kontrola nie była legalna, nakazywał zbadanie, czy odpowiadała ona wszystkim warunkom ustawowym sformułowanym w ustawie o CBA – a więc, czy była zgodna z przepisami mającymi charakter przepisów materialnych, a nie przepisów postępowania, jak błędnie ujęli to w apelacjach skarżący (zob. postanowienie SN z 26.06.2019 r., IV KK 328/18, OSNKW 2019, nr 8, poz. 46). Temu służyły podjęte w toku postępowania apelacyjnego czynności zmierzające do wyjaśnienia okoliczności związanych z zarządzeniem i przedłużeniem tej kontroli. Były one zatem uwarunkowane treścią postawionych przez skarżących zarzutów, choć nie wynikały z bezpośredniej inicjatywy dowodowej obrońców. Nie jest zatem tak, jak podniósł na rozprawie w dniu 11 maja 2023 roku prokurator, że kwestią legalności materiałów uzyskanych w wyniku kontroli operacyjnej Sąd Apelacyjny zajmował się z urzędu.

Zgodnie z art. 17 ust. 1 ustawy o CBA zarządzenie kontroli operacyjnej jest możliwe – w celu określonym w tym przepisie – tylko w związku z przestępstwami, które zostały w nim wymienione. Katalog ten ma charakter zamknięty. Wykorzystanie w trybie art. 168 b k.p.k. informacji tak pozyskanych także możliwe jest tylko w odniesieniu do

przestępstw katalogowych, a więc tych, co do których sąd może wyrazić zgodę na zarządzenie kontroli operacyjnej (zob. uchwała SN z 28.06.2018 roku; D. Szumiło-Kulczycka, op. cit.).

Nie ulega wątpliwości, że przestępstwo z art. 265 § 1 k.k., którego popełnienie zarzucono tak oskarżonemu R. J. (1), jak i oskarżonej K. T. nie zostało wymienione w art. 17 ust. 1 ustawy o CBA – nie jest to przestępstwo katalogowe. obrońcy pomijają jednak – konsekwentnie przemilczają tę okoliczność – że oskarżonym zarzucono popełnienie czynu kwalifikowanego kumulatywnie z art. 231 k.k. i art. 265 § 1 k.k. Przestępstwo nadużycia uprawnień przez funkcjonariusza publicznego (nadużycia władzy) z art. 231 k.k. stanowi przestępstwo katalogowe. W związku z tym przestępstwem możliwe jest zarządzenie kontroli operacyjnej (jej przedłużenie), a w konsekwencji także wykorzystanie uzyskanych w jej wyniku materiałów na podstawie art. 168 b k.p.k. w ramach rozszerzenia podmiotowego lub przedmiotowego. Zarzucane oskarżonej K. T. przekroczenie uprawnień funkcjonariusza Agencji Bezpieczeństwa Wewnętrznego wyrażać się miało ujawnieniem przez nią informacji niejawnych opatrzonej klauzulą „tajne”. Oskarżonemu R. J. (1) prokurator zarzucił natomiast podżeganie współoskarżonej jako funkcjonariusza publicznego do przekroczenia uprawnień przez ujawnienie tych informacji. Przy tak skonstruowanych zarzutach nie można podzielić zastrzeżeń wysuwanych w apelacjach przez obrońców i przyjąć, że w sytuacji, gdy materiały uzyskane w wyniku kontroli operacyjnej prowadzonej wobec R. J. (1) wskazywały na popełnienie przez niego i współoskarżoną K. T. przestępstwa o złożonej kwalifikacji prawnej, na którą składały się przepisy odnoszące się do przestępstwa tzw. katalogowego i niekatalogowego, przekreślać to powinno możliwość dopuszczenia ich jako legalnych dowodów w sprawie. Rzecz jasna jest tak przy założeniu, że kontrola operacyjna prowadzona była w związku z przestępstwem katalogowym. W tym jednak zakresie brak jest możliwości poczynienia pewnych i niebudzących wątpliwości ustaleń.

Szczegółowe odniesienie się do tej kwestii poprzedzić trzeba nakreśleniem pewnych okoliczności faktycznych i problemów, jakie z nimi się wiążą.

Kontrola operacyjna wobec R. J. (1) została zarządzona przez Sąd Okręgowy w Warszawie na wniosek Szefa Centralnego Biura Antykorupcyjnego z dnia 26 października 2018 roku, a następnie przedłużona kolejnym orzeczeniem Sądu Okręgowego w Warszawie na wniosek z dnia 16 stycznia 2019 roku. W obu wnioskach wskazane zostały – przez powołanie odpowiedniej kwalifikacji prawnej – przestępstwa katalogowe, jako te, które miały uzasadniać uruchomienie czynności operacyjno-rozpoznawczych oraz ich kontynuowanie – łącznie na okres sześciu miesięcy. Materiały niejawne przekazane wraz z aktem oskarżenia do sądu zawierają niepełne wersje każdego z wniosków – dołączone one zostały w formie wyciągów z oryginalnych dokumentów, zgodnie ze stosownym zarządzeniem – niezawierającym podstawy prawnej – odnotowanym na każdym z nich. W takiej formie zostały one przedłożone prokuratorowi, co potwierdził w piśmie z 4 listopada 2022 roku, a co przyznał także Szef Centralnego Biura Antykorupcyjnego w przesłanej Sądowi Apelacyjnemu korespondencji. Sporządzone wyciągi z wniosków o zarządzenie kontroli oraz o jej przedłużenie nie zawierają liczącego kilka stron uzasadnienia. Ta część dokumentów została usunięta. To, że kontrola operacyjna, o której zarządzenie wnioskowano, obejmować miała przestępstwo katalogowe wynika wyłącznie z powołanej w każdym z wniosków kwalifikacji prawnej z art. 231 k.k. We wnioskach udostępnionych w postępowaniu sądowym brak jest opisu przestępstwa, jak wymaga tego art. 17 ust. 7 pkt 2 ustawy o CBA. Nie pozwala to skonfrontować opisu czynu z powołaną kwalifikacją, a co za tym idzie stwierdzić, że przedmiotem kontroli rzeczywiście było przestępstwo katalogowe.

Jak należy założyć, ten niezbędny element każdego z wniosków – opis przestępstwa – zawarty został w uzasadnieniu. Tam też, jak należy przyjąć, zamieszczone zostały informacje o okolicznościach uzasadniających potrzebę zastosowania kontroli operacyjnej, w tym stwierdzonej bezskuteczności lub nieprzydatności innych środków (art. 17 ust. 7 pkt 3 ustawy o CBA). We wniosku o przedłużenie kontroli operacyjnej ujęta została dodatkowo kwalifikacja prawna przestępstwa innego niż z art. 231 k.k. – również katalogowego – jako tego, które uzasadniać miało kontynuowanie czynności operacyjno-rozpoznawczych.

Szef Centralnego Biura Antykorupcyjnego dwukrotnie nie wyraził zgody na udostępnienie Sądowi Apelacyjnemu pełnych wersji wniosków o zarządzenie i przedłużenie kontroli operacyjnej.

W jawnym piśmie z 23 listopada 2022 roku podniósł, że obowiązek przekazania Prokuratorowi Generalnemu wszystkich materiałów zgromadzonych w trakcie stosowania kontroli operacyjnej w sytuacji opisanej w art. 17 ust. 15 ustawy o CBA nie obejmuje materiałów wytworzonych przed zastosowaniem tej kontroli, w tym materiałów stanowiących podstawę jej zarządzenia, ocenionych uprzednio przez Sąd Okręgowy w Warszawie w trybie opisanym w art. 17 ustawy o CBA. Podkreślił ponadto, że Centralne Biuro Antykorupcyjne zobowiązane jest do ochrony środków, form i metod realizacji zadań a także zgromadzonych informacji czy danych identyfikujących funkcjonariuszy CBA. Wskazał na możliwość odstąpienia od tej ochrony jedynie w warunkach art. 28 ust. 3 i 4 ustawy o CBA.

W kolejnym piśmie, z dnia 22 grudnia 2022 roku, także jawnym, stanowiącym odpowiedź na wydane przez Sąd Apelacyjny na rozprawie postanowienie dowodowe, zastępca Szefa CBA powtórzył tę argumentację, dodając, że zakres żądanych przez Sąd informacji podlega podwyższonym rygorom ochrony i udostępniania. Podkreślił, że wnioski kierowane do Sądu Okręgowego w Warszawie zawierały wszystkie elementy wymagane dla tych dokumentów. Zwrócił uwagę, że Sąd Okręgowy w Warszawie ocenił je pozytywnie, opierając się na przedłożonych mu materiałach. Jak stwierdził, „poza sporem pozostaje, że kontrola operacyjna, której dotyczy zapytanie sądu zarządzona została z poszanowaniem zasady legalności, adekwatności i subsydiarności”. Z pisma wynika, że zgromadzone w wyniku kontroli materiały dwuetapowo zostały przekazane Prokuratorowi Generalnemu. W dniu 1 kwietnia 2019 roku przekazana została ta ich część, która stała się podstawą do wszczęcia śledztwa przeciwko oskarżonym. Natomiast 6 grudnia 2021 roku – a więc po upływie dwóch lat i ośmiu miesięcy od daty zakończenia kontroli operacyjnej wobec R. J. (1) – przekazano całość materiałów uzyskanych w ramach tej kontroli operacyjnej, a ponadto inne jeszcze materiały, które łącznie stały się podstawą do wszczęcia przez Prokuraturę Okręgową w Warszawie kolejnego śledztwa. W piśmie ponownie wskazano na możliwość zainicjowania procedury z art. 28 ust. 3 i 4 ustawy o CBA.

Prezes Sądu Okręgowego w Warszawie udostępnił pełne wersje wniosków o zarządzenie kontroli operacyjnej wobec R. J. (1) oraz o jej przedłużenie, jednak wyraźne i zdecydowanie zastrzegł, że dokumenty te przekazuje do wyłącznej wiadomości sędziów Sądu Apelacyjnego we Wrocławiu, a więc nie do wykorzystania procesowego. W konsekwencji tego bardzo wyraźnego ograniczenia dostępu do informacji, dokonanego przez dysponenta dokumentów niejawnych, uznać należało, że w istocie – faktycznie – żądane dokumenty nie zostały udostępnione. Zastrzeżenie nie dawało bowiem podstaw do zapoznania z nimi prokuratora oraz obrońców i oskarżonych, co tym samym uniemożliwiło wprowadzenie ich do procesu.

Brak pełnych wersji wniosków o zarządzenie kontroli operacyjnej oraz o jej przedłużenie powoduje określone konsekwencje procesowe. Uniemożliwia bowiem dokonanie oceny legalności tej kontroli. Nie jest tak, jak przedstawia to Szef CBA, że pozytywne rozstrzygnięcia co do każdego z wniosków podjęte przez Sąd Okręgowy w Warszawie zamykają sprawę i przesądzają kwestię legalności prowadzonej kontroli operacyjnej i jej zgodności z warunkami ustawowymi, określonymi w art. 17 ust. 1 ustawy o CBA. To sąd orzekający w przedmiocie odpowiedzialności oskarżonych w głównym nurcie procesu wypowiada się ostatecznie w tej mierze. Jeszcze raz wskazać trzeba, że w trybie art. 168 b k.p.k. do procesu mogą być wprowadzone materiały uzyskane podczas legalnie prowadzonej kontroli operacyjnej. Jasne jest zatem, że podejmując decyzję procesową w przedmiocie wniosku prokuratora w tym zakresie rzeczą sądu jest ocenić legalność tej kontroli. Tylko pozytywna ocena w tej mierze stwarza podstawy do dopuszczenia ich jako dowodów w sprawie. W ramach tej oceny sąd nie jest związany wcześniejszym orzeczeniem, mocą którego kontrola ta została zarządzona. Tak jak nie był związany zgodą następczą sądu na wykorzystanie materiałów pochodzących z kontroli operacyjnej uzyskanych poza zakresem podmiotowym lub przedmiotowym postanowienia wyrażającego zgodę na jej stosowanie w stanie prawnym obowiązującym przed dniem 15 kwietnia 2016 roku – a więc w czasie, gdy obowiązywały jeszcze przepisy art. 17 ust. 15 a-e ustawy o CBA. Może zatem inaczej ocenić to, czy zostały spełnione warunki ustawowe uzasadniające jej zarządzenie. Oczywiście jest przecież, że to sąd w postępowaniu sądowym weryfikuje zaofiarowane mu dowody i dokonuje oceny ich wartości i przydatności.

Nie ulega wątpliwości, że rozszerzenie podmiotowo-przedmiotowe z art. 168 b k.p.k. wchodzi w grę w odniesieniu do oskarżonej K. T., ponieważ nie była ona objęta zarządzoną kontrolą. Rzecz jednak nie przedstawia się w sposób tak oczywisty w odniesieniu do oskarżonego R. J. (1). W jego wypadku można by mówić wyłącznie o rozszerzeniu

przedmiotowym. Tyle tylko, że w sytuacji, gdy brak jest pełnych wersji wniosków o zarządzenie i przedłużenie kontroli operacyjnej wobec niego, a co za tym idzie brak jest opisu przestępstwa z art. 231 k.k., w związku z którym kontrola ta została zarządzona, można jedynie założyć, że postawiony mu w akcie oskarżenia zarzut był następstwem takiego właśnie rozszerzenia przedmiotowego. Zdaje się na to wskazywać akt oskarżenia. Już to pokazuje, jakie znaczenie w sprawie ma to, że wnioski w pełnych wersjach nie zostały udostępnione sądowi orzekającemu. Powoduje, to, że nie można z całą pewnością stwierdzić, czy materiały stanowiące podstawę aktu oskarżenia pochodziły z kontroli pierwotnej zarządzanej wobec oskarżonego czy też miały charakter wtórny, co nie pozostaje bez znaczenia dla wskazania właściwej podstawy ich wprowadzenia do procesu.

Brak ten powoduje jednak przede wszystkim to, że poza oceną pozostaje to, czy zarządzenie kontroli operacyjnej wobec oskarżonego było zasadne, czy istniała informacja o przestępstwie, czy dotyczyła ona przestępstwa katalogowego, jak też, czy konieczne było sięgnięcie do tej formy ograniczenia praw obywatelskich i w końcu, czy środki, jakie zostały zastosowane były proporcjonalne.

To, że istnienie informacji o przestępstwie stanowi jeden z warunków zarządzenia kontroli operacyjnej wynika z treści art. 17 ust. 1 ustawy o CBA. Kontrola operacyjna służyć ma bowiem wykrywaniu przestępstwa i uzyskaniu oraz utrwalaniu dowodów jego popełnienia (zob. wyrok SN z 7.05.2019 r., V KK 180/18, LEX nr 2671614).

Bez pełnych wersji wniosków nie jest możliwe ustalenie, że zarządzenie kontroli operacyjnej wobec R. J. (1) było konieczne, ponieważ inne środki okazały się bezskuteczne albo będą nieprzydatne. Jak należy przyjąć, argumenty mające za tym przemawiać zostały powołane w uzasadnieniu wniosków. Potwierdziła to w piśmie z dnia 30 grudnia 2022 roku przewodnicząca X Wydziału Karnego Odwoławczego Sądu Okręgowego w Warszawie.

Wszystko to łącznie prowadzi do konkluzji, że pełne wersje wniosków o zarządzenie kontroli operacyjnej oraz o jej przedłużenie stanowią immanentną część materiałów tej kontroli, kluczową z punktu widzenia ocen dokonywanych w postępowaniu sądowym, a co za tym idzie obowiązkiem służb realizujących czynności operacyjno-rozpoznawcze przy wykorzystaniu tego środka – w tej sprawie Szefa Centralnego Biura Antykorupcyjnego – jest przedstawić te dokumenty wraz z materiałami uzyskanymi w toku kontroli, w sytuacji gdy pozwalają one na wszczęcie postępowania karnego (art. 17 ust. 15 ustawy o CBA). Tylko wówczas możliwe będzie dokonanie oceny, czy kontrola zarządzona została zgodnie z prawem, a więc przy spełnieniu warunków ustawowych określonych w art. 17 ustawy o CBA. Powoływane przez Szefa CBA i jego zastępcę w pismach kierowanych do Sądu przepisy art. 28 ust. 3 i 4 ustawy o CBA w takiej sytuacji nie znajdują zastosowania.

Uchybienie, do jakiego doszło w tej sprawie w następstwie przekazania prokuratorowi wyciągów z wniosków, a w dalszej kolejności w następstwie odmowy przekazania Sądowi Apelacyjnemu ich pełnych wersji implikuje 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 służb jest w istocie iluzoryczna, ma fasadowy charakter, a funkcjonariusze właściwych służb prowadzą te czynności i jednocześnie sami decydują o tym, czy są one legalne, czy uzyskane w ich wyniku materiały mogą być wykorzystane w procesie.

Materiały z kontroli operacyjnej prowadzonej wobec R. J. (1) nie mogły być uznane za dowód w sprawie także z drugiego powodu.

Wdrożona wobec oskarżonego kontrola operacyjna polegała na uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych (art. 17 ust. 5 pkt 4 ustawy o CBA). W jej wyniku pozyskano treść rozmów prowadzonych przez oskarżonego R. J. (1) za pośrednictwem szyfrowanych komunikatorów internetowych (...)i (...) z oskarżoną K. T., z M. M. oraz innymi osobami. Kontrola została zarządzona na okres trzech miesięcy, a następnie została przedłużona o kolejne trzy miesiące. Jednak dane pozyskane w toku tej kontroli – przedstawione jako materiał dowodowy w sprawie

– wykraczały poza ramy czasowe wynikające z postanowień Sądu Okręgowego w Warszawie. Obejmowały bowiem także dane historyczne za okres poprzedzający zarządzenie kontroli – z kilku miesięcy sprzed października 2018 roku.

[część niejawna uzasadnienia wyroku SA pkt 1]

Powstaje pytanie o znaczenie tej okoliczności z punktu widzenia legalności czynności operacyjnych – ich zgodności z warunkami ustawowymi określonymi w art. 17 ustawy o CBA. Istotna w tym kontekście wydaje się odpowiedź na pytanie, w jaki sposób materiały te zostały pozyskane, czy znaczenie w tym zakresie miało posłużenie się określonym środkiem technicznym kontroli operacyjnej.

Przy poszukiwaniu odpowiedzi na to pytanie, zdaniem Sądu Apelacyjnego, rysują się dwie możliwości.

Pierwsza, 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, a następnie kontynuowane, już na mocy orzeczeń Sądu, przez kolejne niespełna 6 miesięcy.

Druga możliwość, to 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.

Wysoco wątpliwe wydaje się bowiem, by dane te zostały udostępnione polskim służbom przez zagranicznych operatorów każdego z tych szyfrowanych komunikatorów, których używał oskarżony, co ważne przy tym, poza zakresem zgody udzielonej przez Sąd. Operator szwajcarski ((...)), znany jest z ochrony prywatności. Z kolei amerykańska (...) ((...)) publicznie informuje o udostępnianiu organom ścigania danych, w których posiadaniu jest, wyłącznie przy spełnieniu szczególnych warunków wynikających z rygorystycznych regulacji obowiązujących w Stanach Zjednoczonych, a także regulacji międzynarodowych ((...)).

W pierwszym możliwym wariantcie pozyskania danych historycznych, nie może być mowy o legalności tak prowadzonych działań z uwagi na to, że pozostają one w rażącej sprzeczności z przepisami art. 17 ust. 8 i 9 ustawy o CBA. Zgodnie z nimi, kontrola operacyjna może trwać nie dłużej niż sześć miesięcy. Jej przedłużenie na kolejne okresy, łącznie nieprzekraczające 12 miesięcy, jest możliwe jedynie w uzasadnionych wypadkach, przy czym także na mocy decyzji sądu. W tej zaś sprawie pozyskane zostały materiały z okresu kilku miesięcy poprzedzających zarządzenie kontroli (ponad pół roku).

Jeśli chodzi o drugą z możliwości, to także ona nie może być uznana za legalny sposób pozyskania w wyniku kontroli operacyjnej materiałów mających stanowić dowód w procesie.

W przestrzeni publicznej pojawiły się informacje o wykorzystywaniu przez służby specjalne różnych państw, w tym europejskich, w tym w Polsce, oprogramowania do cybernetycznej inwigilacji izraelskiej firmy (...) o nazwie (...) (z danych, jakie dotąd udało się zdobyć wynika, że ponad połowę klientów (...) stanowiły agencje rządowe w krajach europejskich). Z uwagi na wyjątkowe możliwości, jakie to oprogramowanie oferuje użytkownikom jest ono określane jako broń cybernetyczna, jako ofensywne narzędzie klasy wojskowej. (...) to oprogramowanie szpiegujące (typu spyware), umożliwiające pełną zdalną inwigilację jednostki. Przeznaczony jest 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 – między innymi wgląd w treść wiadomości tekstowych, pozwala na przechwytywanie połączeń głosowych, zapewnia dostęp do lokalizacji urządzenia, do przechowywanych na nim filmów, zdjęć, notatek. Za pomocą oprogramowania możliwe jest włączenie w dowolnym momencie kamery i mikrofonu bez wiedzy użytkownika telefonu. W wypadku komunikatorów internetowych operator programu ma dostęp do wszystkich wiadomości zarchiwizowanych w pamięci telefonu oraz do każdej wiadomości wysłanej i odebranej od momentu infekcji, w tym także do tych, które zostały

skasowane przez użytkownika. Technologia ta pozwala przechwycić wiadomości przesyłane za pomocą szyfrowanych komunikatorów – mając dostęp do urządzenia danej osoby, ma się dostęp do całej prowadzonej przez nią komunikacji. Program umożliwia skuteczne monitorowanie, zbieranie i pobieranie danych z zainfekowanego nim urządzenia. Może też zostać użyty do modyfikowania zawartości urządzenia – określonych jego treści. Jak z tego wynika, jest oprogramowaniem wysoce inwazyjnym, wyrafinowanym i podstępym, o potężnym potencjale i praktycznie nieograniczonych możliwościach – po przejęciu kontroli nad telefonem operatorzy przeprowadzający atak uzyskują usprawnia administracyjne, co w praktyce oznacza, że mogą zrobić z zainfekowanym telefonem wszystko. Ich możliwości ingerencji w urządzenie są nawet większe niż użytkownika telefonu. Do zainfekowania telefonu złośliwym oprogramowaniem wykorzystywane są luki w systemie operacyjnym, a sam proces instalacji oprogramowania jest niewidoczny dla użytkownika. Przy wykorzystaniu określonego typu luk – za pomocą tzw. exploita zero-click – proces infekcji może się odbyć bez jakiegokolwiek aktywności użytkownika telefonu. Jak się wskazuje, do instalacji oprogramowania dochodzi w wyniku przełamania zabezpieczeń – włamania na telefon, które narusza strukturę urządzenia. (...) ma dostęp do informacji, kto jest obiektem inwigilacji – jest w stanie sprawdzić, kogo licencjobiorca programu inwigiluje. Jeśli zaś chodzi o transfer danych pozyskiwanych z zainfekowanego telefonu, to wykorzystywane są w tym procesie także serwery znajdujące się poza obszarem geograficznym licencjobiorcy oprogramowania (zob. L. Richard, S. Rigaud, (...). Jak szpieg, którego nosisz w kieszeni, zagraża prywatności, godności i demokracji, Insignis Media, Kraków 2023, str. 8, 145-148, 187, 229, 297, 317, 407-408; 431; A. Barczak-Oplustil, A. Behan, M. Małecki, S. Tarapata, W. Zontek, (...) w Polsce: niedopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych, Cz.PKiNP 2023, nr 1, s. 5-42; zapis stenograficzny z wysłuchania eksperta B. M. z (...) na Uniwersytecie w T. podczas posiedzenia senackiej Komisji Nadzwyczajnej do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych z dnia 17 stycznia 2022 roku; dane udostępnione przez (...): (...).

Poczynienie tych ogólnych uwag i przybliżenie tego, jak funkcjonuje oprogramowanie (...), jakie ma możliwości – na podstawie wyników badań prowadzonych w różnych obszarach, w tym przez specjalistów i ekspertów z (...) Uniwersytetu w T., ale także (...) – było konieczne, by móc odpowiedzieć na pytanie o dopuszczalność użycia takiego oprogramowania – tego konkretnego, ale też innego, działającego podobnie – na gruncie obowiązujących przepisów prawa w realiach tej konkretnej sprawy. Silne przesłanki zdają się bowiem wskazywać, że tego rodzaju system mógł zostać użyty w ramach kontroli operacyjnej prowadzonej wobec oskarżonego, na co zwrócił uwagę przede wszystkim on sam w postępowaniu apelacyjnym. Podniesione kilkakrotnie 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.

[część niejawna uzasadnienia wyroku SA pkt 2]

Problem dopuszczalności używania w ramach kontroli operacyjnej programu takiego jak (...) stał się już przedmiotem wypowiedzi doktryny. W cytowanej publikacji „(...) w Polsce: niedopuszczalność nabycia i używania w ramach kontroli operacyjnej określonego typu programów komputerowych” jej autorzy zwracają uwagę na to, że system ten nie mógł i nie może uzyskać świadectwa akredytacji informatycznej, wymaganego zgodnie z art. 48 ustawy o ochronie informacji niejawnych dla każdego z systemów, w którym przetwarzane są informacje niejawne o klauzuli „poufne” lub wyższej, a udzielanego przez Agencję Bezpieczeństwa Wewnętrznego lub Służbę Kontrwywiadu Wojskowego. Nie gwarantuje on bowiem bezpieczeństwa i poufności danych. Określony sposób transferu pozyskiwanych danych stwarza możliwość dostępu do nich innych podmiotów, jak choćby producenta oprogramowania, (...). Co nie mniej ważne, dane te są potencjalnie dostępne przed nadaniem im odpowiedniej klauzuli w trybie ustawy o ochronie informacji niejawnych, mającej zabezpieczać je przed nieuprawnionym dostępem. Kolejny problem, to brak gwarancji integralności pozyskiwanych danych, szczególnie wobec możliwości wysyłania na zainfekowane urządzenie danych przez operatora programu. Jak konkludują autorzy, „za niezgodne z przepisami polskiego prawa należy uznać wszelkie działania operacyjne z wykorzystaniem nieakredytowanych programów komputerowych, które nie zapewniają bezpieczeństwa informacji niejawnych bądź których użycie wiąże się z udostępnianiem tych danych

osobom trzecim nieuprawnionym do dostępu do informacji niejawnych” (tak A. Barczak-Oplustil i inni, Pegasus...op. cit. str. 11-14).

Na te aspekty zwraca się także uwagę w debacie publicznej (ważnej z punktu widzenia standardów demokratycznego państwa prawnego), jaka toczy się w związku z informacjami o stosowaniu (...) przez agencje rządowe, w tym polskie. Akcentowany jest w jej toku przede wszystkim aspekt wątpliwej wiarygodności pozyskiwanych danych z uwagi na możliwe manipulacje nimi, ale także konieczność używania przez służby sprzętu certyfikowanego. Kwestie te były podnoszone w toku prowadzonego postępowania apelacyjnego.

Rozważając zatem w tej sprawie drugi możliwy wariant pozyskania danych z telefonu oskarżonego w postaci wiadomości wymienianych ze współoskarżoną oraz innymi osobami za pomocą szyfrowanych komunikatorów internetowych (dane opatrzone klauzulą „poufne”), a więc ten, który zakłada użycie oprogramowania dającego nieograniczony dostęp do urządzenia, stwierdzić trzeba, że nie on być uznany za dopuszczalny, w sytuacji gdy poważne wątpliwości budzi to, czy zastosowanie takiego środka techniki operacyjnej gwarantuje bezpieczeństwo i poufność oraz integralność pozyskiwanych danych, co ma znaczenie z punktu widzenia uzyskania przez ten system wymaganej ustawą akredytacji bezpieczeństwa teleinformatycznego (art. 48 i art. 49 ustawy o ochronie informacji niejawnych). Wprawdzie w art. 51 ustawy o ochronie informacji niejawnych przewidziane zostało wyłączenie z obowiązku akredytacji, nie wydaje się ono jednak mieć zastosowania w omawianym wypadku. Jak się bowiem wskazuje, „wyjątek dotyczy systemów teleinformatycznych, które nie są zlokalizowane w budynkach należących do podmiotów realizujących czynności operacyjno-rozpoznawcze, i ograniczony jest jedynie do pozyskiwania i przekazywania informacji, co nie wyczerpuje ustawowej definicji przetwarzania” (zob. I. Stankowska [w:] Ustawa o ochronie informacji niejawnych. Komentarz, wyd. II, Warszawa 2014, art. 51). Tymczasem, zgodnie z zapisami § 8 rozporządzenia Rady Ministrów z dnia 29 maja 2012 roku w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. poz. 683 z późn. zm.) serwery i inne newralgiczne elementy systemów teleinformatycznych umieszcza się w odpowiednich strefach ochronnych (w wypadku przetwarzania informacji o klauzuli „poufne” i wyższej w strefie ochronnej I lub w strefie ochronnej II), a samo to oprogramowanie tego typu – umożliwiające zdalny dostęp do telefonu – nie służy wyłącznie do pozyskiwania i przekazywania informacji, ale do ich przetwarzania.

Kolejne wątpliwości, jakie w tej sprawie się rysują mają związek z tym, czy użycie w ramach kontroli operacyjnej prowadzonej wobec oskarżonego R. J. (1) takiego środka kontroli operacyjnej mogłoby być uznane za pozostające w zgodzie z warunkami ustawowymi. Zgodnie z art. 17 ust. 5 pkt 4 ustawy o CBA kontrola operacyjna polega na uzyskiwaniu i utrwalaniu danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych. Mogłoby się wydawać, że użycie oprogramowania takiego jak (...) odpowiada tej definicji ustawowej.

Treść przepisu 17 ust. 5 pkt 4 ustawy o CBA została zmieniona z dniem 7 lutego 2016 roku przez art. 11 pkt 2 lit. b ustawy z dnia 15 stycznia 2016 roku o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz.U. z 2016 roku, poz. 147), który uzupełnił katalog środków kontroli operacyjnej. W uzasadnieniu projektu ustawy zmieniającej wskazano, że jej celem było dostosowanie systemu prawa do wyroku Trybunału Konstytucyjnego z 30 lipca 2014 roku, sygn. akt K 23/11, że u jej podstaw leżała ścisła realizacja sentencji tego wyroku, między innymi przez sprecyzowanie niejawnego wkroczenia w sferę prywatności jednostki. Jak to ujęto, wychodząc naprzeciw sformułowanym w uzasadnieniu wyroku oczekiwaniom Trybunału odnośnie do sprecyzowania zamkniętego katalogu środków i metod działania, za pomocą których władze publiczne mogą w sposób niejawnym gromadzić informacje o osobach, zdecydowano się na wyczerpujące i jednolite dla wszystkich służb określenie sposobów prowadzenia kontroli operacyjnej (druk sejmowy nr 154 z 23 grudnia 2015 roku Sejmu Rzeczypospolitej Polskiej VIII kadencji).

W wyroku z 30 lipca 2014 roku, sygn. akt K 23/11, Trybunał Konstytucyjny (dalej też jako Trybunał) zajmował się między innymi kwestią zgodności z Konstytucją art. 17 ust. 5 pkt 3 ustawy o CBA na wniosek rzecznika Praw Obywatelskich, który zarzucił między innymi, że cechuje się on nadmierną nieprecyzyjnością z uwagi na otwarty katalog środków technicznych, które mogą być wykorzystywane przez służby w toku kontroli operacyjnej, a także

otwarty katalog informacji i dowodów, jakie mogą być pozyskane w tej procedurze (wniosek dotyczył także innych ustaw regulujących zasady prowadzenia kontroli operacyjnej przez służby policyjne i ochrony państwa). Trybunał stwierdził, że przepis ten, rozumiany w ten sposób, że właściwy organ zarządzający kontrolę operacyjną wskazuje określony w prawie rodzaj środka technicznego uzyskiwania informacji i dowodów oraz ich utrwalania stosowany w indywidualnej sprawie, jest zgodny z Konstytucją (wyrok opublikowany w OTK-A 2014/7/80, Dz. U z 2014 roku, poz. 1055, Lex nr 1491305). W uzasadnieniu tego wyroku Trybunał poruszył szereg istotnych kwestii związanych z ingerencją organów państwa w sferę konstytucyjnie chronionych praw i wolności jednostki przy realizacji czynności operacyjno-rozpoznawczych. Uwagi te aktualizują się w rozpoznawanej sprawie.

Nie negując tego, że przy realizacji obowiązku ochrony bezpieczeństwa obywateli przed poważnymi zagrożeniami zewnętrznymi i wewnętrznymi, w tym terroryzmem i przestępczością, państwo może ingerować w prywatność jednostki, w wolność komunikowania się, chronione na mocy art. 47 i art. 49 Konstytucji, że jest to nieodzowne, Trybunał zwrócił jednak uwagę, że ingerencja ta nie może być nadmierna. W tym kontekście kilkakrotnie podkreślił aspekt proporcjonalności działań podejmowanych w ramach czynności operacyjno-rozpoznawczych. Zauważył, że im bardziej czynności te ingerują w konstytucyjnie chroniony status człowieka i obywatela, tym większym, surowszym i bardziej rygorystycznym wymaganiom muszą odpowiadać. Za niedopuszczalne w demokratycznym państwie prawnym uznał rejestrowanie całokształtu życia prywatnego jednostek (art. 31 ust. 3 Konstytucji). Poruszył problem gwarancji bezpieczeństwa gromadzonych danych (art. 51 Konstytucji). Przypomniał, że w systemie Rady Europy ochronę prywatności, w tym korespondencji, gwarantuje art. 8 Konwencji o ochronie praw człowieka i podstawowych wolności, a na jego gruncie Europejski Trybunał Praw Człowieka wypracował minimalne standardy konwencyjne regulacji materii związanej z niejawnym przechwytywaniem informacji. Sprowadzają się one do określenia w prawie: rodzaju przestępstw, w odniesieniu do których jest to możliwe, rodzaju środka niejawnego pozyskiwania informacji, który musi być określony przez prawo w momencie jego zastosowania, kategorii podmiotów, w stosunku do których mogą być pozyskiwane w sposób niejawnie informacje, z uwzględnieniem ochrony osób postronnych, maksymalnego czasu stosowania niejawnego nadzoru, który musi mieć charakter oznaczony i definitywny, procedury wyrażania zgody na zastosowanie środka niejawnego, która musi mieć co do zasady charakter uprzedni i pisemny i nie może ograniczać się jedynie do kwestii formalnych, procedury badania wykorzystywania i przechowywania uzyskanych danych przez organ zewnętrzny i niezależny w stosunku do organów upoważnionych do niejawnego pozyskiwania informacji i okoliczności, w jakich zapisy mają być usunięte lub zniszczone, z uwzględnieniem zabezpieczenia ich integralności, obowiązku informowania osoby, której dane niejawnie pozyskano i warunków zaniechania takiej informacji (pkt 1.8; 1.12; 1.14; 2.1; 2.4; 2.4.2 uzasadnienia wyroku).

Uwzględniając między innymi te standardy konwencyjne, ale także swój dotychczasowy dorobek oraz ustalenia Trybunału Sprawiedliwości Unii Europejskiej, Trybunał Konstytucyjny przedstawił minimalne wymagania, jakie łącznie muszą spełniać przepisy ograniczające konstytucyjne wolności i prawa. Zwrócił uwagę na to, że: gromadzenie, przechowywanie oraz przetwarzanie danych dotyczących jednostek, a zwłaszcza sfery prywatności, dopuszczalne jest wyłącznie na podstawie wyraźnego i precyzyjnego przepisu ustawy, w ustawie muszą być sprecyzowane przesłanki niejawnego pozyskiwania informacji (wykrywanie i ściganie wyłącznie poważnych przestępstw oraz zapobieganie im, ustawa powinna wskazywać rodzaje takich przestępstw), ustawa musi określać kategorie podmiotów, wobec których mogą być podejmowane czynności operacyjno-rozpoznawcze, pożądane jest określenie w ustawie rodzajów środków niejawnego pozyskiwania informacji, a także rodzajów informacji pozyskiwanych za pomocą poszczególnych środków, czynności operacyjno-rozpoznawcze powinny być środkiem subsydiarnym (ultima ratio), procedura zarządzania ich wymaga precyzyjnego unormowania w ustawie, tak jak zasady postępowania z materiałami zgromadzonymi w ich toku, konieczne jest zagwarantowanie bezpieczeństwa zgromadzonych danych przed nieuprawnionym dostępem ze strony innych podmiotów, unormowanie procedury informowania jednostek o niejawnym pozyskaniu informacji na ich temat, zagwarantowanie transparentności stosowania czynności operacyjno-rozpoznawczych. Trybunał nie wykluczył potrzeby zróżnicowania intensywności ochrony prywatności oraz tajemnicy komunikowania się z uwagi na to, czy określone dane pozyskują służby policyjne, czy też służby wywiadowcze i zajmujące się ochroną państwa, a ponadto w zależności od tego, czy dotyczy to obywateli, czy osób niemających polskiego obywatelstwa (pkt 5.3).

Formułując postulat sprecyzowania sposobu niejawnego wkroczenia w sferę prywatności Trybunał zauważył, że nie jest konieczne wskazanie w przepisach konkretnych środków techniki operacyjnej ani tym bardziej zdefiniowanie ich parametrów. Dopuścił w tym zakresie pewien stopień ogólności. Podkreślił jednak, że katalog tych środków i metod działania musi mieć charakter zamknięty, co ograniczy arbitralność państwa i umożliwi sprawowanie efektywnej kontroli nad niejawną działalnością operacyjno-rozpoznawczą w zakresie wykorzystywanych metod pozyskiwania informacji o osobach. Zwrócił uwagę na sądową kontrolę legalności stosowanych w ramach kontroli operacyjnej środków i ich adekwatności w konkretnej sprawie (pkt 9.2.5).

Postawić należy pytanie, czy zmiana art. 17 ust. 5 ustawy o CBA dokonana w 2016 roku rzeczywiście odpowiada głównym tezom wyroku Trybunału, czy też paradoksalnie nie poszła dużo dalej, otwierając drogę do nieograniczonej inwigilacji. Odpowiedź na to pytanie nie jest możliwa bez odczytania treści tego przepisu, jego punktu 4, w kontekście standardów konwencyjnych i konstytucyjnych wypracowanych na gruncie art. 8 Europejskiej Konwencji oraz art. 47 i 49 Konstytucji. Te zaś, zdaniem Sądu Apelacyjnego, 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 zarządzanej kontroli operacyjnej.

Przepis art. 17 ust. 5 pkt 4 ustawy o CBA ogólnie mówi o uzyskiwaniu i utrwalaniu danych. Oprogramowanie typu spyware daje pełen dostęp do urządzenia mobilnego, pozwala tym samym na uzyskiwanie i utrwalanie danych z niego. Tyle tylko, że do jego instalacji dochodzi w drodze ominięcia i przełamania zabezpieczeń – włamania na telefon – i to w sposób naruszający jego strukturę. Tymczasem obowiązujące przepisy dotyczące kontroli operacyjnej, w tym omawiany art. 17 ustawy o CBA, nie zezwalają na tego rodzaju działania, nie przewidują takiej możliwości. Uzyskanie dostępu do informacji w wyniku ominięcia lub przełamania zabezpieczeń możliwe jest w trybie art. 32 a ust. 8 ustawy z dnia 4 maja 2002 roku o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tekst jednolity Dz. U. z 2023 roku poz. 1136, dalej jako ustawa o ABW). Może to jednak nastąpić wyłącznie w celu określenia przez ABW podatności systemu teleinformatycznego poddawanego ocenie bezpieczeństwa na możliwość popełnienia przestępstw, wymienionych w ust. 7 tego przepisu (zob. A. Barczak-Oplustil i inni, (...) cit. str. 14-15). Cele kontroli operacyjnej są natomiast inne.

Oznacza to, że posłużenie się oprogramowaniem szpiegowskim nie może być uznane za zgodny z ustawą, legalny sposób ich pozyskania. Trudno także przyjąć, że oprogramowanie pozwalające na przejęcie pełnej kontroli nad urządzeniem mobilnym odpowiada wymaganiom stawianym przez Trybunał Konstytucyjny co do właściwego sprecyzowania stosowanego środka techniki operacyjno-rozpoznawczej, takiego przy tym, który ma ograniczyć arbitralność państwa i umożliwić sprawowanie efektywnej kontroli nad niejawną działalnością operacyjno-rozpoznawczą.

Tak dalece inwazyjny środek, tak mocno ingerujący w prywatność jednostki, nie może także być uznany za adekwatny w konkretnych okolicznościach rozpoznawanej sprawy. Ocena ta odnosi się do przestępstw zarzuconych oskarżonym, które nie należą do kategorii najpoważniejszych, godzących w bezpieczeństwo państwa, jak terroryzm, nie są związane z zorganizowaną przestępczością. W debacie publicznej, jeśli już dopuszcza się użycie takiego środka kontroli operacyjnej jak oprogramowanie szpiegujące, to w odniesieniu do takich właśnie wyjątkowo poważnych i groźnych przestępstw albo w ramach działań wywiadowczych. Rzecz jasna przy określeniu odpowiednich warunków ustawowych, których aktualnie obowiązujące przepisy nie przewidują. Oceny tej nie można odnieść do przestępstw, które stały się podstawą zarządzenia kontroli operacyjnej wobec oskarżonego, ponieważ, jak już była o tym mowa, brak jest wystarczających informacji na ten temat. Jeśli zaś chodzi o przestępstwa zarzucone – do wykrycia których środek taki jak omawiany mógł być wykorzystany – to trudno je zakwalifikować do tych najpoważniejszych i wyjątkowo groźnych, przeciwdziałanie którym mogłoby uzasadniać sięgnięcie po broń cybernetyczną, jak określa się system pozwalający na przejęcie kontroli nad telefonem.

O spełnieniu standardów konwencyjnych i konstytucyjnych w razie posłużenia się takim środkiem nie może być mowy także, jeśli uwzględnić kwestie związane z bezpieczeństwem oraz integralnością danych pozyskanych przez tego rodzaju oprogramowanie, o czym była mowa w akapitach poprzedzających. Zasadnicze wątpliwości budzi także ten

aspekt korzystania z takiego oprogramowania, który wiąże się z możliwym jego aktywnym wykorzystaniem – w tym wpływaniem na treści znajdujące się na urządzeniu.

Trybunał Konstytucyjny zwracał uwagę na zasady postępowania z materiałami zgromadzonymi w toku kontroli operacyjnej. W tej sprawie tylko część z nich przekazana została po zakończeniu czynności Prokuratorowi Generalnemu. Pozostałe, jak wynika z informacji Zastępcy Szefa CBA, pozostawały w gestii służb przez okres prawie trzech kolejnych lat, choć zgodnie z art. 17 ust. 15 ustawy o CBA, w przypadku uzyskania dowodów pozwalających na wszczęcie postępowania karnego lub mających znaczenie dla toczącego się postępowania karnego przekazane powinny zostać wszystkie materiały. Nie można uznać, by tak długi okres przechowywania danych pozyskanych w następstwie tak daleko idącej ingerencji w prywatność i wolność komunikowana się był niezbędny w demokratycznym państwie prawnym.

W ocenie Sądu Apelacyjnego poważne wątpliwości z perspektywy standardów konwencyjnych i konstytucyjnych budzi także możliwość pozyskiwania danych historycznych. Kontrola operacyjna może zostać zarządzona na maksymalny okres 18 miesięcy. W czasie, w jakim jest prowadzona, uzyskiwane i utrwalane są dane zawarte w urządzeniu mobilnym, jak w tej sprawie (art. 17 ust. 5 pkt 4 ustawy o CBA). Oprogramowanie firmy (...) – daje możliwość pozyskania i utrwalenia danych z okresu poprzedzającego decyzję o zarządzeniu kontroli – a więc danych historycznych – jak się przy tym wydaje, bez ograniczeń czasowych, jeśli są tylko dostępne. Jak wynika z materiałów udostępnionych przez producenta oprogramowania, (...), możliwe jest wyłączenie opcji początkowej ekstrakcji danych, a tym samym pozyskania danych historycznych, w takiej sytuacji, gdy licencjodawca nie może uzyskać do nich dostępu zgodnie z obowiązującym prawem (dane udostępnione przez (...): (...): zob. A Barczak-Oplustil i inni, (...)...op. cit., str. 10).

Zdaniem Sądu Apelacyjnego trudno przyjąć, że przepis art. 17 ust. 5 pkt 4 ustawy o CBA zawiera upoważnienie do pozyskania danych historycznych. W czasie, gdy przepis ten był nowelizowany, gdy ten dodatkowy środek czy metoda kontroli operacyjnej wprowadzane były do ustawy o CBA, 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. Trudno w tej sytuacji uznać, że wprowadzając te regulacje ustawodawca mógł tym samym zezwolić, czy wprost zezwolił na dostęp służb do danych z okresu poprzedzającego moment zarządzenia kontroli operacyjnej, co ważne, bez ograniczeń czasowych, w sposób limitowany wyłącznie dostępnością tych danych. Zdaniem Sądu Apelacyjnego, poważna ingerencja, jaka się z tym wiąże, w prywatność i wolność komunikowania się, będące pod ochroną art. 47 i art. 49 Konstytucji, wymaga wyraźnej zgody ustawodawcy – wyraźnego zapisu ustawowego w tej mierze. Bez takiego wyraźnego upoważnienia ustawowego możliwość pozyskiwania tych danych należy wykluczyć. Odmienne stanowisko oznaczałoby, że określone w ustawie ramy czasowe prowadzenia kontroli operacyjnej tracą na znaczeniu. Zarządzenie kontroli operacyjnej jest przecież możliwe tylko przy spełnieniu warunku istnienia informacji o przestępstwie. Dane historyczne obejmują okres wcześniejszy, kiedy informacji o przestępstwie mogło jeszcze w ogóle nie być. Z kolei określony w ustawie maksymalny czas trwania kontroli operacyjnej służyć ma osiągnięciu określonego celu. Dane historyczne nie pozostają w związku z tym celem. Trybunał Konstytucyjny wykluczył możliwość bezterminowego prowadzenia czynności operacyjno-rozpoznawczych.

Pozyskanie w toku kontroli operacyjnej prowadzonej w określonych ramach czasowych danych o treści rozmów osoby objętej tą kontrolą z okresu poprzedzającego jej zarządzenie – co ważne, bez limitu czasowego – przy braku wyraźnego upoważnienia ustawowego – nie może być uznane za adekwatne i proporcjonalne wkroczenie w sferę prywatności jednostki. Dla oceny w tym zakresie nie może mieć decydującego znaczenia to, czy dane historyczne zostały uwzględnione przy wyrokowaniu, czy stały się podstawą ustaleń faktycznych.

W tej sprawie Sąd pierwszej instancji dopuścił jako dowód całość przekazanych wraz z aktem oskarżenia materiałów. Co do części z nich w toku postępowania odwoławczego (na tej części rozprawy, która była prowadzona z wyłączeniem jawności) zostały podniesione wątpliwości – których rozstrzygnięcie nie jest możliwe – co do integralności danych pozyskanych w toku kontroli operacyjnej. Danych historycznych dotyczyły pytania stawiane oskarżonym podczas ich przesłuchania w śledztwie, kiedy to ujawniono im materiały uzyskane w wyniku kontroli operacyjnej, a oskarżeni

odnosili się do poszczególnych komunikatów z rozmów. Z materiału dowodowego o charakterze jawnym jasno wynika, że na telefonie zabezpieczonym od oskarżonego nie zostały ujawnione te dane, które pozyskano w toku kontroli operacyjnej – na urządzeniu tym nie było żadnych przydatnych procesowo danych i informacji. Tak jak danych takich nie ujawniono na telefonach zabezpieczonych od oskarżonej K. T. oraz M. M.. To wyłącznie czynności o charakterze przedprocesowym doprowadziły do pozyskania materiału mającego stanowić dowód w sprawie przeciwko oskarżonym. By tak się stało, nie może być żadnych wątpliwości i zastrzeżeń co do legalności czynności, które doprowadziły do jego pozyskania. Tak jednak w tej sprawie nie jest.

Z jednej bowiem strony nie jest możliwe stwierdzenie, że kontrola operacyjna wobec oskarżonego zarządzona i prowadzona była przy spełnieniu warunków ustawowych (materialnych) – uniemożliwia to brak pełnych wniosków o zarządzenie i przedłużenie tej kontroli.

Z drugiej zaś, za niedopuszczalne uznać trzeba użycie w toku tej kontroli oprogramowania typu spyware – a na możliwość jego użycia w tej sprawie wskazują określone przesłanki – budzącego w wielu aspektach i na wielu płaszczyznach poważne i zasadnicze wątpliwości co do legalności jego wykorzystania.

Dopuszczenie w toku procesu tak pozyskanych dowodów pozostawałoby w sprzeczności ze standardami konwencyjnymi, czyniąc proces nierzetelnym (art. 6 ust. 1 i art. 8 Konwencji). Naruszałoby także standardy konstytucyjne (art. 47, art. 49 w zw. z art. 31 § 3 Konstytucji).

Zasadą i czymś jak najbardziej naturalnym jest komunikacja bezpośrednia między ludźmi – rozmowa twarzą w twarz – z założenia niepodlegająca kontroli i nadzorowi. Postęp techniczny sprawił, że we współczesnym świecie rozmowy prowadzone są w sposób umożliwiający przechwytywanie ich treści. Jest to jednak tak daleko idąca ingerencja w prywatność, że niepodobna uznać, by mogła odbywać się w sposób praktycznie nieograniczony, bez jasnych zasad i reguł, bez właściwej kontroli sądowej, a do tego prowadziłyby bezkrytyczne zaakceptowanie okoliczności, w jakich prowadzona była kontrola operacyjna w tej sprawie.

W konsekwencji uznać należało, że materiały uzyskane w toku kontroli operacyjnej prowadzonej wobec oskarżonego R. J. (1) nie mogły stanowić dowodu w sprawie. Ich wyeliminowanie z podstawy dowodowej powoduje określone konsekwencje jeśli chodzi o możliwość uznania za dowód wyjaśnień, jakie oskarżeni składali w toku postępowania.

O ile co do pierwszych składnych przez oskarżonych wyjaśnień brak jest podstaw, by negować możliwość ich uwzględnienia jako pełnowartościowych dowodów w sprawie, o tyle te wyjaśnienia, które złożone zostały podczas przesłuchań o charakterze niejawnym, zdaniem Sądu Apelacyjnego, nie mogły być uznane za dowód w sprawie jako pośrednio nielegalne. W trakcie niejawnych przesłuchań oskarżonych odczytywane były bowiem komunikaty z rozmów prowadzonych przez oskarżonego R. J. (1) za pośrednictwem komunikatorów internetowych z innymi osobami, w tym także z czasu poprzedzającego zarządzenie kontroli operacyjnej oraz te, co do których na etapie postępowania odwoławczego pojawiły się wątpliwości co do ich integralności.

[część niejawna uzasadnienia wyroku SA pkt 3]

Jak się wskazuje w piśmiennictwie, „dowód pośrednio nielegalny, to dowód uzyskany w wyniku przeprowadzenia innego dowodu posiadającego przymiot dowodu nielegalnego (a zatem uzyskanego na skutek przeprowadzenia czynności dowodowej w sposób nielegalny), [...] bez którego ten pierwszy nie zostałby prawdopodobnie odnaleziony”. Sam ten dowód jest dowodem przeprowadzonym zgodnie z prawem, jednak jego uzyskanie nie byłoby możliwe bez powzięcia informacji wynikających z innego środka dowodowego, który uzyskany został nielegalnie. W wypadku dowodu pośrednio nielegalnego, nie sposób jego uzyskania rodzi wątpliwości, ale źródło wiedzy o jego istnieniu (zob. H. Kuczyńska, Dopuszczalność dowodów uzyskanych w trakcie kontroli operacyjnej dotyczących innego czynu niż będący podstawą jej zastosowania. Glosa do wyroku Sądu Najwyższego – Izba Karna z dnia 9 grudnia 2021 r., II KK 170/21, OSP 2022, nr 10, s. 86, teza 10).

Podczas pierwszych przesłuchań oskarżeni składali wyjaśnienia nie mając informacji, że prowadzone przez nich rozmowy zostały pozyskane w ramach kontroli operacyjnej. Mogli się tego domyślać na podstawie przedstawionych im zarzutów, mogli snuć takie przypuszczenia, jednak to, co wyjaśniali było wynikiem ich swobodnej decyzji. Na treść ich wypowiedzi procesowych nie miały wpływu inne okoliczności. Inaczej rzecz się przedstawia, jeśli chodzi o przesłuchania o charakterze niejawnym. Ujawnienie materiałów pozyskanych w trakcie kontroli operacyjnej w sposób oczywisty rzutowało na treść składanych przez oskarżonych wyjaśnień. W tym czasie oskarżeni mieli już pełną świadomość tego, jakim materiałem organy postępowania przygotowawczego dysponują. Nie może ulegać wątpliwości, że mogło to wpłynąć na treść ich wypowiedzi procesowych. Zadawane oskarżonym pytania odnosiły się do konkretnych komunikatów. Treść ich wypowiedzi była determinowana tym, co im ujawniono. W tym zakresie, w jakim zdecydowali się odpowiadać na zadawane im pytania w związku z konkretnymi rozmowami tłumaczyli swoje postępowanie, okoliczności z tym związane oraz motywy, jakimi się kierowali. W składanych wówczas wyjaśnieniach oskarżeni odnosili się w szczególności do tych rozmów, które uznane zostały przez organy ścigania za zawierające elementy podżegania K. T. do ujawnienia R. J. (1) informacji niejawnych oraz związane z wątkiem dotyczącym przyszłego zatrudnienia oskarżonej przez R. J. (1), co potraktowane zostało jako obietnica korzyści majątkowej. We wcześniejszych wyjaśnieniach, jakie oskarżeni składali po zatrzymaniu (11 i 12 kwietnia 2019 roku), zaprzeczyli, by działania ich determinowane były korzyścią majątkową (jej obietnicą). Nie podawali także żadnych okoliczności, które mogłyby stać się podstawą ustaleń dotyczących podżegania K. T. do ujawnienia informacji niejawnych. Daje to podstawy do przyjęcia, że wyjaśnienia złożone przez oskarżonych podczas niejawnych czynności ich przesłuchania – w tej części, w jakiej zawierają one informacje, których oskarżeni nie podawali wcześniej – uzyskane zostały dzięki dowodom nielegalnym, a to nie pozwala na włączenie ich do podstawy dowodowej wyroku.

Z pierwszych wyjaśnień oskarżonych wynika, że oskarżona K. T. w dniach 27 i 28 marca 2019 roku podczas rozmów prowadzonych za pośrednictwem komunikatora internetowego przekazała R. J. (1) informacje o tym, że funkcjonariusze jednej z delegatur ABW, a wśród nich ona, prowadzą na terenie L. czynności operacyjno-rozpoznawcze wobec M. M., polegające na jego obserwacji (art. 23 ust. 1 pkt 6 ustawy o ABW). Oskarżona udzieliła R. J. (1) instrukcji, by M. M. nie podejmował w tym czasie aktywności. Uzyskawszy tę informację R. J. (1) przekazał ją M. M.. Ten zrezygnował ze spotkania, które miał zaplanowane na ten dzień. W trakcie czynności operacyjnych oskarżona kontaktowała się z R. J. (1) i komentowała zachowanie M. M. (k. 51-59; k. 65-76).

Z materiałów niejawnych wynika, że informacje o operacji towarzyszącej przekazywane agentom przed jej rozpoczęciem były opatrzone klauzulą „tajne”.

[część niejawną uzasadnienia wyroku SA pkt 4]

Oboje oskarżeni przyznali w swoich pierwszych wyjaśnieniach, że w rozmowach między nimi padła nazwa operacji, której część stanowiły działania operacyjno-rozpoznawcze prowadzone wobec M. M..

Ich wyjaśnienia nie dają jednak podstaw do przyjęcia, że R. J. (1) nakłaniał K. T. do ujawnienia mu informacji o klauzuli „tajne”, że obiecywał jej w zamian za to korzyść majątkową. Nie pozwalają także na odtworzenie – z precyzją wymaganą dla ustaleń faktycznych stanowiących podstawę wyroku skazującego – innych zdarzeń, podczas których miałyby dojść do ujawnienia informacji niejawnych o klauzuli „tajne”, jak zarzucił w akcie oskarżenia prokurator.

W świetle wyjaśnień oskarżonych nie może budzić wątpliwości, że K. T. ujawniła R. J. (1) informacje niejawne o klauzuli „tajne”, przekraczając tym samym swoje uprawnienia i działając na szkodę interesu publicznego. Jako funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego była zobowiązana do dochowania obowiązków wynikających z rotacji złożonego przez nią przed podjęciem służby ślubowania (art. 79 ust. 1 ustawy o ABW). Ślubując, oskarżona zobowiązała się do strzeżenia tajemnicy prawnie chronionej (art. 47 ust. 2 ustawy o ABW). Taką informacją prawnie chronioną o klauzuli „tajne” stanowi informacja o prowadzonej w trybie art. 23 ust. 1 pkt 6 ustawy o ABW operacji towarzyszącej. Nie ulega wątpliwości, że informacja ta spełniała cechy informacji niejawnej w rozumieniu art. 1 ust. 1 ustawy o ochronie informacji niejawnych i formalnie była opatrzona właściwą klauzulą (art. 5 ust. 2 ustawy o ochronie informacji niejawnych). Przekazana przez K. T. informacja nie była znana R. J. (1), skoro po jej uzyskaniu

udzielił rady M. M., by nie wychodził z domu, a ten zmodyfikował swoje zamierzenia, rezygnując w tym dniu z zaplanowanego spotkania. Wprawdzie w składanych przez oskarżonych wyjaśnieniach mowa jest o wcześniejszej dekonspiracji funkcjonariuszy ABW prowadzących działania wobec R. J. (1), co w części potwierdziły materiały niejawne z tych działań, to jednak ta konkretna informacja o konkretnych czynnościach realizowanych w dniach 27 i 28 marca 2019 roku wobec M. M. nie była znana oskarżonemu, na co jednoznacznie wskazuje jego zachowanie. W złożonych wyjaśnieniach K. T. tłumaczyła, że nie kierowała się tym, by szkodzić interesowi publicznemu. Jej obrońca akcentował, że prowadziła niefrasobliwe rozmowy z kolegą. Jednak nie ulega wątpliwości, że jej zachowanie szkodziło interesowi publicznemu – wprost dekonspirowało bowiem działania funkcjonariuszy ABW. Dawalo to podstawy do przyjęcia odpowiedzialności oskarżonej za przestępstwo z art. 231 § 1 k.k. i art. 265 § 1 k.k. w zw. z art. 11 § 2 k.k.

Oskarżona przekazała R. J. (1) kryptonim operacji prowadzonej wobec niego oraz jego znajomego – cudzoziemca, pozostającego w zainteresowaniu służb. Brak jest jednak podstaw, by przyjąć, że nazwa operacji, jej kryptonim stanowią informację prawnie chronioną w rozumieniu art. 1 ust. 1 oraz art. 5 ust. 2 ustawy o ochronie informacji niejawnych. Dość odwołać się do tego, czym jest kryptonim, w jakim celu jest nadawany. Kryptonim w znaczeniu językowym to nazwa używana zamiast prawdziwej nazwy jakiejś rzeczy, miejsca, akcji lub osoby, mająca zataić rzeczywiste znaczenie tego, o czym się mówi, a w wypadku ludzi ukrywająca czyjąś tożsamość (zob. Wielki Słownik Języka Polskiego, domena publiczna). Nadanie kryptonimu operacji prowadzonej niejawnie pozwala zatem ukryć jej rzeczywiste znaczenie, a posłużenie się nim umożliwia swobodną wypowiedź o tej operacji bez ujawnienia jej przedmiotu – w takim celu nadawane są kryptonimy. Przekazanie przez oskarżoną R. J. (1) nazwy nadanej czynnościom operacyjno-rozpoznawczym nie wyczerpuje zatem znamion z art. 265 § 1 k.k. Z akt sprawy nie wynika przy tym, by ujawniony przez oskarżoną kryptonim operacji opatrzony był klauzulą „tajne” lub wyższą.

Jak już była o tym mowa, z braku wystarczających podstaw dowodowych nie wchodzi w grę przyjęcie odpowiedzialności oskarżonego R. J. (1) za zarzucane mu przestępstwo podżegania K. T. do przekroczenia, w celu osiągnięcia korzyści majątkowej, przysługujących jej uprawnień przez ujawnienie mu informacji o klauzuli „tajne”. Materiał dowodowy – ten, który może stanowić podstawę wyrokowania – nie pozwala bowiem na poczynienie takich ustaleń.

Brak jest także podstaw do przyjęcia odpowiedzialności oskarżonego za ten sposób realizacji przestępstwa z art. 265 § 1 k.k., który polega na wykorzystaniu informacji niejawnych. Prokurator zarzucił, że oskarżony wykorzystywał przekazywane mu przez K. T. informacje niejawne przekazując je dalej, M. M. oraz modyfikując własne działania. Sąd Okręgowy uznał ten zarzut za udowodniony i przypisał oskarżonemu odpowiedzialność za wykorzystanie informacji o klauzuli „tajne”. Stanowisko to nie może jednak zostać zaakceptowane.

Po pierwsze, brak jest wystarczających dowodów – spośród tych, które mogą stanowić podstawę wyrokowania – pozwalających na ustalenie, że oskarżony, uzyskawszy określone informacje od K. T., zmieniał swoje plany i zamierzenia. Nie wynika to tak z jego wyjaśnień, jak i wyjaśnień współoskarżonej.

Po drugie, warunkiem karalności za wykorzystanie informacji niejawnych jest naruszenie zakazu takiego wykorzystania ustanowionego poza Kodeksem karnym. Jak się wskazuje w literaturze przedmiotu, zakazu tego nie można domniemywać, ani wyprowadzać go wyłącznie z treści art. 265 § 1 k.k. Zachowanie polegające na wykorzystaniu informacji niejawnych oznacza złamanie pozakodeksowego zakazu uczynienia jej wiadomym, musi zatem naruszać przepis ustawy (zob. W. Wróbel, D. Zajac [w:] Kodeks karny. Część szczególna. Tom II. Część II. Komentarz do art. art. 212-277d, red. A. Zoll, Warszawa 2017, art. 265, tezy 26-27; T. Razowski [w:] Kodeks karny. Część szczególna. Komentarz, red. J. Giezek, Warszawa 2021, art. 265, teza 6; P. Kozłowska-Kalisz [w:] Kodeks karny. Komentarz aktualizowany, red. M. Mozgawa, LEX/el. 2023, art. 265, teza 11).

W przepisach ustawy o ochronie informacji niejawnych brak jest tego rodzaju regulacji. Zakazu wykorzystania informacji niejawnych nie można wyprowadzić z treści art. 4 tej ustawy. Reguluje on bowiem wyłącznie kwestię udostępniania informacji niejawnych, a więc ich ujawnienia. Odrębna typizacja „wykorzystania” obok „ujawnienia” informacji niejawnych świadczy jednak o woli ustawodawcy objęcia karalnością także takich zachowań, które polegają

na wykorzystywaniu tajemnicy państwowej bez jej ujawnienia. Brak innych przepisów ustawowych reglamentujących wykorzystywanie informacji niejawnych, oznacza, że odpowiednia część typu czynu karalnego z art. 265 § 1 k.k. ma zakres pusty (tak wprost W. Wróbel, D. Zając, op. cit.).

To zaś oznacza, że zarzucane oskarżonemu R. J. (1) wykorzystanie informacji niejawnych nie miało charakteru bezprawnego.

W tej sytuacji pozostaje rozważyć, czy przekazując M. M. uzyskane od K. T. informacje, oskarżony R. J. (1) nie ujawnił tym samym tych informacji objętych tajemnicą.

I ten wariant jego odpowiedzialności należy jednak wykluczyć.

Dostrzegając, że tak w doktrynie, jak i orzecznictwie zagadnienie to nie jest ujmowane jednolicie, Sąd Apelacyjny opowiada się za stanowiskiem, że przestępstwo z art. 265 § 1 k.k. nie jest przestępstwem powszechnym, ale indywidualnym właściwym (zob. W. Wróbel, D. Zając, op. cit. teza 11; A. Sakowicz [w:] M. Królikowski, R. Zawłocki, (red.) Kodeks karny. Część szczególna. Tom II. Komentarz. Art. 222–316, Wyd. 4, W. 2017, L.; R. Hałas [w:] A. Grześkowiak, K. Wiak (red.), Kodeks karny. Komentarz. Wyd. 7, W. 2021, L.; S. Steinborn, Zwolnienie świadka w procesie karnym z tajemnicy państwowej, PiP 2008, nr 2, s. 61-74, teza 1; odmiennie jednak L. Gardocki (red.), Przepięstwa przeciwko państwu i dobrom zbiorowym. System Prawa Karnego. Tom 8, W. 2013; uchwała SN z 26.03.2009 r., I KZP 35/08, OSNKW 2009, nr 5, poz. 33).

Choć literalne brzmienie przepisu – użyty w nim został zaimek „kto” – zdawałoby się wskazywać na powszechny charakter tego przestępstwa, to jednak dokonując wykładni art. 265 § 1 k.k. nie można czynić tego w oderwaniu od przepisów ustawy o ochronie informacji niejawnych, w której uregulowane zostały zagadnienia związane z ochroną tych informacji. Ustawa nie ma zastosowania powszechnego. Nie jest ona adresowana do wszystkich. Podmiotowy zakres ustawy o ochronie informacji niejawnych został wyraźnie określony w jej art. 1 ust. 2 przez wskazanie kategorii podmiotów, do których ma ona zastosowanie. Nie może to pozostawać bez znaczenia dla ustalenia zakresu podmiotowego penalizacji zachowań na płaszczyźnie art. 265 § 1 k.k., szczególnie że z dniem 2 stycznia 2011 roku, w następstwie nowelizacji Kodeksu karnego, pojęcie tajemnicy państwowej, którym operował przepis, zastąpione zostało terminem zaczerpniętym wprost z ustawy o ochronie informacji niejawnych (informacje niejawne o klauzuli „tajne” lub „ściśle tajne”). Ustawa o ochronie informacji niejawnych – w odróżnieniu od nieobowiązującej ustawy z 14 grudnia 1982 roku o ochronie tajemnicy państwowej i służbowej (Dz. U. Nr 40, poz. 271 z późn. zm.) – nie zawiera przepisu, będącego odpowiednikiem art. 5 pkt 1, który stanowił, że zachowanie tajemnicy państwowej jest obowiązkiem każdego, do czyjej wiadomości dotarła. Nie został w niej sformułowany szczególnie obowiązek zachowania tajemnicy w odniesieniu do informacji niejawnych. Zakaz ujawniania informacji objętych tajemnicą wynika nie z samej tej ustawy, ale z innych ustaw. Jak się przyjmuje, źródłem obowiązku zachowania w tajemnicy informacji niejawnych, obok ustawy, może być także jednostronne zobowiązanie się do tego przez akt publicznoprawny (np. ślubowanie) lub czynność prawną (np. umowa o pracę). Przemawia to przeciwko wyprowadzaniu powszechnego obowiązku zachowania w tajemnicy informacji niejawnych z samej treści art. 265 § 1 k.k. Negowałoby to bowiem sens istnienia tych szczególnych regulacji. Oznacza to w konsekwencji, że w wypadku, gdy nie istnieje norma o charakterze ustawowym, zakazująca ujawnienia informacji prawnie chronionych, to ujawnienie takie nie może być uznane za bezprawne i nie może prowadzić do pociągnięcia do odpowiedzialności karnej. Warunkiem odpowiedzialności karnej z art. 265 k.k. jest bowiem naruszenie konkretnego zakazu ujawnienia tajemnicy zawartego w ustawach innych niż Kodeks karny. W literaturze przedmiotu przywoływany jest w tej mierze dodatkowy argument wypływający z konstytucyjnej zasady subsydiarności. Ten mianowicie, że ograniczanie wolności słowa i komunikowania nie może prowadzić do nakładania obowiązku strzeżenia informacji objętych tajemnicą na inne osoby niż pełniące służbę publiczną (tak S. Steinborn, op. cit.; W. Wróbel, D. Zając, op. cit.; W. Wróbel, Prawnokarna ochrona tajemnicy państwowej, Cz.PKiNP 2000, nr 1, s. 121; R. Hałas, op. cit.).

Za przyjęciem poglądu przeciwnego, zgodnie z którym przestępstwo z art. 265 § 1 k.k. ma charakter powszechny, nie może przemawiać ranga dóbr, które chroni ten przepis, ich znaczenie dla społeczeństwa oraz to, że są to wartości,

których zabezpieczenie warunkuje również bezpieczeństwo innych prawnie chronionych dóbr obywateli (tak SN w uchwale z 26 marca 2009 roku, I KZP 35/08, OSNKW 2009, nr 5, poz. 33). Zgodzić się należy z krytykami tego poglądu, wskazującymi, że interpretacja taka stanowiłaby wyraz wykładni rozszerzającej obowiązki ograniczające prawa i wolności obywatela, a więc trudnej do zaakceptowania w świetle norm konstytucyjnych (tak A. Sakowicz, op. cit.).

Oskarżony R. J. (1) w marcu 2019 roku nie pełnił już żadnej funkcji publicznej. Nie ciążył na nim obowiązek ochrony informacji niejawnych. Przekazując M. M. określone informacje uzyskane od K. T., nie działał zatem bezprawnie, bo nie naruszył żadnego, wiążącego go, zakazu ustawowego w tej mierze. Podzielając zapatrywanie o indywidualnym charakterze przestępstwa z art. 265 § 1 k.k. odrzucić należy zdecydowanie możliwość przyjęcia, że zakaz taki – ujawnienia informacji objętych tajemnicą – wyprowadzić należy z samej treści tego przepisu. Z tych powodów oskarżony nie może odpowiadać przestępstwo ujawnienia informacji niejawnych o klauzuli „tajne”.

Jako osoba, której ujawniono informacje niejawne był on koniecznym współuczestnikiem przestępstwa z art. 265 § 1 k.k., który jednak za swoje zachowanie nie odpowiada karnie (zob. W. Wróbel, *Prawnokarna...op.cit.*).

Sąd Apelacyjny rozważał, czy oskarżony nie powinien odpowiadać jako współdziałający w ujawnieniu informacji prawnie chronionych o klauzuli „tajne” przy przyjęciu jego roli jako posłańca, który realizuje uzgodniony wcześniej plan, zakładający, że ma on przekazać ujawnioną mu informację dalej, innej osobie. W literaturze przedmiotu wskazuje się, że osoba taka, choć sama nie posiada kwalifikacji na sprawcę przestępstwa ujawnienia informacji prawnie chronionej, może zostać pociągnięta do odpowiedzialności karnej wówczas, gdy właśnie zgodnie z planem wykonuje rolę posłańca (zob. W. Wróbel, *Prawnokarna..., op. cit.* teza 10).

Możliwość taką w tej sprawie należało jednak odrzucić z dwóch powodów.

Po pierwsze, wyjaśnienia oskarżonych nie dają wystarczających podstaw ku temu, by przyjąć, że współdziałali oni ze sobą w dokonaniu przestępstwa ujawnienia informacji prawnie chronionych – a więc, że doszło między nimi do określonych uzgodnień, że zaplanowali taki podział ról, w ramach którego R. J. (1) miał przekazać M. M. informację uzyskaną od K. T. o podjętej wobec niego obserwacji towarzyszącej. Nie wskazują na to przede wszystkim wyjaśnienia K. T., ale także i R. J. (1). Z jego wyjaśnień wynika wyłącznie to, że ograniczył się do przekazania koledze informacji o charakterze ogólnym – bez podawania ich źródła oraz szczegółów – i udzielił mu rady, by nie wychodził z domu. Żadnych informacji na temat tego zdarzenia nie dostarczają zeznania M. M..

Po drugie, poczynienie takich ustaleń – których nie poczynił Sąd Okręgowy, a które bez wątpienia są niekorzystne z punktu widzenia odpowiedzialności oskarżonego, stojącego pod zarzutem wykorzystania informacji niejawnych – było wykluczone z uwagi na to, że apelacja w sprawie wniesiona została tylko na jego korzyść (art. 434 § 1 k.p.k.).

Mając na uwadze te wszystkie okoliczności Sąd Apelacyjny zmienił zaskarżony wyrok i uniewinnił R. J. (1) od popełnienia zarzucanego mu czynu.

Ograniczając odpowiedzialność oskarżonej K. T. do zdarzenia, które miało miejsce w dniach 27 i 28 marca 2019 roku, Sąd Apelacyjny uznał, że prowadzić to powinno do obniżenia o połowę liczby stawek dziennych wymierzonej jej kary grzywny. Nie stwarza to jednak podstaw do korekty rozstrzygnięcia o karze pozbawienia wolności, orzeczonej z warunkowym zawieszeniem jej wykonania. Wykluczyć także należało możliwość zastosowania wobec oskarżonej instytucji warunkowego umorzenia postępowania, zgodnie z postulatem jej obrońcy sformułowanym w apelacji.

Prokurator określił zachowanie oskarżonej, która ujawniła informacje niejawne swojemu koledze, byłemu funkcjonariuszowi Agencji Bezpieczeństwa Wewnętrznego, jako zdradę. Nie wydaje się, by ocena taka była nieuzasadniona czy przesadzona. To właśnie od funkcjonariuszy takich służb jak ABW, którzy w ramach swoich obowiązków mogą między innymi podejmować pozaprocesowe działania bardzo mocno ingerujące w życie osobiste, prywatność, wolność komunikowania się innych osób, wymagać należy najwyższych standardów postępowania. Okoliczności tej sprawy pokazały jak ważne jest dochowanie przez służby procedur, postępowanie zgodne z prawem,

realizacja czynności operacyjnych wyłącznie przy spełnieniu materialnych warunków określających możliwości ich wdrożenia i prowadzenia – bez marginesu dowolności. Zapobiec nadużyciom w tej sferze może między innymi jasne i zdecydowane oczekiwanie od funkcjonariuszy służb przestrzegania prawa. Nie można z jednej strony zarzucać służbom, że nie dochowują procedur, a z drugiej jako mniej szkodliwe oceniać zachowanie funkcjonariusza tych służb ujawniającego informacje prawnie chronione, dekonspirującego w efekcie swoich kolegów i ich działania. Wątpliwości czy dylematy moralne, na które powoływała się oskarżona w związku z przydzieleniem jej zadań wobec osób, które znała, można i trzeba było wyrazić inaczej aniżeli przez naruszenie prawa. W okolicznościach zdarzenia nie można uznać, że czyn oskarżonej cechował się społeczną szkodliwością, o jakiej mowa w art. 66 § 1 k.k. Brak jest również podstaw do oceny na tej płaszczyźnie zawinienia oskarżonej. Wymierzona jej kara roku pozbawienia wolności z warunkowym zawieszeniem jej wykonania nie może być uznana za rażąco surową.

W części nieobjętej korektą zaskarżony wyrok został utrzymany w mocy.

O kosztach postępowania w części dotyczącej oskarżonego R. J. (1) Sąd Apelacyjny orzekł na podstawie art. 632 pkt 2 k.p.k. Na podstawie art. 624 § 1 k.p.k. zwolnił oskarżoną K. T. od kosztów postępowania odwoławczego uznając, że obciążenie jej tymi kosztami – w sytuacji gdy jest ona zobowiązana do poniesienia kosztów postępowania przed Sądem pierwszej instancji w niemalej wysokości – stanowiłoby dla niej nadmierną dolegliwość.

Andrzej Szliwa Edyta Gajgał Agata Regulska