Kopiowanie przez kontrolujących informatycznych nośników danych kontrolowanego

Postanowienie SOKiK z 7 marca 2017 r., XVII Amz 15/17

Spis treści

Słowa kluczowe: kontrola; kontrolujący; kontrolowany; informatyczne nośniki danych; kopiowanie.

JEL: K21

I. Stan faktyczny

Na wniosek Prezesa Urzędu Ochrony Konkurencji i Konsumentów (dalej: UOKiK), dnia 17 stycznia 2017 r. Sąd Ochrony Konkurencji i Konsumentów (dalej: SOKiK) wyraził zgodę na przeprowadzenie przeszukania pomieszczeń i rzeczy w ramach toczącego się postępowania wyjaśniającego u przedsiębiorcy, ściśle określając jego zakres. W dniach 24–26 stycznia 2017 r. doszło do przeszukania, w ramach którego pracownicy UOKiK m.in. skopiowali na dyski zewnętrzne całą zawartość dysków twardych trzech komputerów oraz poczty elektronicznej (z jednego komputera), co do których przeszukiwany podniósł, że mogą zawierać chronione prawem tajemnice i informacje niezwiązane z przedmiotem przeszukania. Tak sporządzone kopie binarne zostały bez przeglądania włożone do koperty, oplombowane taśmą z hologramem UOKiK i przewiezione do siedziby UOKiK. Do czasu wydania glosowanego postanowienia nie zostały poddane analizie przez UOKiK (pozostawały zabezpieczone w kopertach). Postanowieniem z 7 marca 2017 r. (XVII Amz 15/17) SOKiK uznał, że sporządzenie kopii binarnych przez przeszukujących stanowiło zabezpieczenie dowodów, wskazując niemniej, że szereg argumentów przedstawionych przez przedsiębiorcę w zażaleniu, co do sposobu dokonywania przeszukania, było słusznych.

II. Komentarz

1. Zakres przeszukania

Przedsiębiorca w zażaleniu wskazał, że czynności przeszukania zostały przeprowadzone z naruszeniem przepisów ustawy o ochronie konkurencji i konsumentów (dalej: uokik)[1], ponieważ przekroczyły one zakres upoważnienia udzielonego przez SOKiK, co objawiało się m.in. żądaniem i skopiowaniem przez pracowników UOKiK dokumentów (w postaci dysków twardych) niezwiązanych z przedmiotem przeszukania. SOKiK w wydanym postanowieniu wyraźnie podkreślił konieczność selekcji i możliwość kopiowania gromadzonego materiału dowodowego jedynie w zakresie przedmiotu przeszukania określonego w postanowieniu SOKiK (wydanym na podstawie art. 105n ust. 2 uokik). W związku z podniesieniem przez Prezesa UOKiK trudności technicznych związanych z ograniczonym do przedmiotu przeszukania kopiowaniem dowodów zgromadzonych na informatycznych nośnikach danych z uwagi na konieczność posługiwania się specjalistycznymi narzędziami typu Forensic IT, SOKiK zauważył szereg kwestii, tj. fakt, że charakter nośnika informacji, z których mają być sporządzane kopie, nie może w żaden sposób ograniczać słusznych praw przedsiębiorcy; konieczność uwzględnienia przez przeszukujących zastrzeżeń przedsiębiorcy co do zakresu informacji zawartych na nośnikach informacji; fakt, że Prezes UOKiK posiada specjalistyczne oprogramowanie, które może być wykorzystywane do przeszukiwania informatycznych nośników czy konieczność poszanowania prawa do prywatności przedsiębiorcy.

Artykuł 105b ust. 1 pkt 2 uokik, który w myśl art. 105q pkt 1 uokik ma odpowiednie zastosowanie do przeszukania, dotyczy uprawnienia przeszukujących do żądania związanych z przedmiotem przeszukania różnego rodzaju przedmiotów i informacji, w tym korespondencji przesyłanej pocztą elektroniczną oraz informatycznych nośników danych. Tak sformułowane uprawnienie przeszukujących wynika z nowelizacji przepisów uokik z 2014 r.[2]. Wcześniej bowiem możliwość żądania informatycznych nośników danych wynikała z orzecznictwa Sądu Najwyższego[3]. Wskazać należy, że uprawnienie to ma bardzo szeroki zakres (Banasiński i Piontek, 2009, s. 868–869) i pozwala na uzyskanie dostępu i przeglądanie dokumentów oficjalnych i nieoficjalnych, tak papierowych, jak i elektronicznych etc. (Turno, 2016, s. 1273–1274). Taki sam zakres ma uprawnienie przeszukujących do dokonywania notatek (w tym kopii i wydruków), o którym mowa w art. 105o uokik (Kohutek, 2014, s. 998–999). Dyspozycją powoływanego przepisu jest objęte też sporządzanie kopii binarnych, co potwierdza uzasadnienie nowelizacji z 10 czerwca 2014 r.[4]. Przyznane uprawnienia przeszukujących, mimo że mają szeroki zakres, ograniczone są do takich przedmiotów i informacji, które „mogą stanowić dowód w sprawie". Przede wszystkim takie uregulowanie ma zapewnić niewykorzystywanie omawianych uprawnień do podejmowania przez przeszukujących działań, które byłyby sprzeczne z zakresem przeszukania określonym przez SOKiK (Materna, 2014, s. 1241). Jak wynika natomiast z orzecznictwa TSUE, Komisja na podstawie art. 20 ust. 4 rozporządzenia Rady (WE)

[1] Ustawa z 16.02.2017 r. o ochronie konkurencji i konsumentów (t.j. Dz.U. z 2017 r., poz. 229).

[2] Art. 1 pkt 46 ustawy z 10.06.2014 r. o zmianie ustawy o ochronie konkurencji i konsumentów oraz ustawy – Kodeks postępowania cywilnego (Dz.U. z 2014 r., poz. 945).

[3] Wyr. SN z 7.05.2004 r., III SK 34/04.

[4] Art. 105o dodany przez art. 1 pkt 52 ustawy z 10.06.2014 r. (Dz.U. z 2014 r., poz. 945) – jak wskazano w uzasadnieniu projektu ustawy, celem było wprowadzenie jasnej regulacji, iż możliwe jest kopiowanie informacji zawartych na informatycznych nośnikach danych (s. 18–19 uzasadnienia).

nr 1/2003[5] ma możliwość poszukiwania różnych elementów informacji, które nie są jeszcze znane lub w pełni zidentyfikowane[6], jednak które wydają się jej mieć związek z szeroko pojętym naruszeniem; nie musi to być związek ewidentny i ścisły, widoczny na pierwszy rzut oka (Vandenborre i Goetz, 2014, s. 653). Chodzi więc o takie informacje, które potencjalnie mogą stać się dowodem w sprawie (Jasiński, 2016, s. 175). Jak się wydaje, dyski twarde komputerów czy też informacje z poczty elektronicznej, z samej swej natury, mogą zawierać potencjalnie informacje, które „mogą stanowić dowód w sprawie", jak również takie, które nie będą związane z przedmiotem przeszukania (jak np. osobiste zdjęcia, wymianę korespondencji e-mail z rodziną w sprawach osobistych) czy informacje objęte tajemnicą zawodową, w tym tajemnicą adwokacką i radcowską (skopiowane informacje dotyczyły danych z komputerów należących do prezesa zarządu oraz dyrektora finansowego).

2. Tajemnice chronione prawem i niezwiązane z przedmiotem przeszukania a miejsce przeszukania

Kwestia, że informatyczne nośniki danych mogą zawierać tajemnice chronione prawem i niezwiązane z przedmiotem przeszukania została przez przedsiębiorcę podniesiona w trakcie przeszukania w jego siedzibie. Mimo tego doszło do ich skopiowania w całości i wyniesienia w zamkniętych kopertach do siedziby UOKiK; z związku jednak z tym, że przeszukiwany przedsiębiorca złożył zażalenie na czynności przeszukania, UOKiK wstrzymał działania na zabezpieczonym materiale dowodowym (UOKiK, 2017, pkt 6). Sąd w glosowanym postanowieniu wskazał na konieczność poszanowania prawa przedsiębiorcy do prywatności, co jest związane ograniczeniem miejsca dokonywania przeszukania do siedziby przedsiębiorcy, o czym stanowi art. 80a ust. 1 usdg w zw. z 105q pkt. 2 uokik. Podkreślił też, że w momencie przeglądania kopii binarnych dochodzi do zapoznania się przez UOKiK z materiałem dowodowym, co jest kluczowe z punktu widzenia sytuacji prawnej przedsiębiorcy (i w tym kontekście nie jest wyłącznie czynnością techniczną). Zwrócił też uwagę na konieczność poszanowania tajemnic, o których stanowi art. 225 kpk w zw. z 105q pkt. uokik. W tym sensie zakwestionował stanowisko Prezesa UOKiK, zgodnie z którym w razie zapoznania się z takimi informacjami wyłącznie przez informatyka pracującego na zlecenie urzędu, bez ich przekazania pracownikom merytorycznym UOKiK prowadzącym dane postępowanie, nie dochodzi do naruszenia tajemnic (w tym potencjalnie *legal professional privilege*). Z tego punktu widzenia istotne jest też uprawnienie do uczestniczenia przez przedstawiciela przeszukiwanego w celu bieżącego weryfikowania czy np. przeglądane e-maile lub dokumenty nie wykraczają poza zakres przedmiotowy przeszukania oraz czy nie zawierają informacji, z którymi przeszukujący nie ma prawa się zapoznać. Jeśli w toku kopiowania materiałów okazałoby się bowiem, że materiały te nie są jednak objęte zakresem przedmiotowym przeszukania, przeszukujący powinni odstąpić od dalszego dokonywania takiej czynności (Turno, 2016, s. 1276).

3. Selekcja dowodów a elektroniczne nośniki danych (twarde dyski)

Praktyka polegająca na kopiowaniu całej zawartości dysków twardych jest coraz częściej stosowana przez Komisję oraz krajowe organy ochrony konkurencji. O ile sama możliwość

[5] Rozporządzenie Rady (WE) nr 1/2003 z 16.12.2002 r. w sprawie wprowadzenia w życie reguł konkurencji ustanowionych w art. 81 i 82 Traktatu (Dz. Urz. L z 2003 r. Nr 1, s. 1).

[6] Wyr. Sądu z 14 listopada 2012 r., T-135/09, por. pkt 63.

„skopiowania" (a nie przeszukiwania informacji na oryginalnym dysku twardym) może się przyczynić do zminimalizowania zakłóceń w działalności przedsiębiorstwa spowodowanych prowadzeniem przeszukania (Michałek-Gervais, 2015, s. 33), o tyle zakres, w którym przeszukujący kopiują dyski twarde, jest kwestią zasadniczą. W doktrynie wskazuje się, że prawo przeszukujących do kopiowania z zasobów informatycznych przeszukiwanego zawartości dysków twardych komputerów, w tym pełnych kopii zawartości skrzynek poczty elektronicznej lub określonych folderów, nie będzie ograniczone, gdy uzasadniają to względy natury technicznej, tj. gdy „odseparowanie" tych informacji z pozostawieniem ich dotychczasowego kształtu nie jest możliwe (Materna, 2014, s. 1241–1242) lub jest zbyt utrudnione, co sprzeciwiałoby się celowi kontroli – szybkiemu i skutecznemu pozyskaniu materiału dowodowego w sprawie (Róziewicz-Ładoń, 2011, s. 247). Literalne brzmienie przepisów uokik wskazuje, że uprawnienie przeszukujących odnosi się do żądania czy kopiowania jedynie informacji, które mogą „stanowić dowód w sprawie". O ile dotychczas możliwość kopiowania całych informatycznych nośników danych nie została zakwestionowana przez TSUE[7], to ETPC uznał w jednym z orzeczeń[8], że poznanie i kopiowanie wszystkich dokumentów i plików dostępnych w kancelarii adwokackiej wykraczało poza zakres tego, co było konieczne dla osiągnięcia celu postępowania. W konsekwencji praktyka została uznana za sprzeczną z art. 8 Europejskiej Konwencji Praw Człowieka i z zasadą proporcjonalności.

Prezes UOKiK, uzasadniając kopiowanie całych informatycznych nośników danych wskazywał na trudności związane z ograniczeniem przedmiotu przeszukania. Jak jednak wskazał SOKiK, Prezes UOKiK dysponuje odpowiednim oprogramowaniem, które może być wykorzystywane do przeszukiwania informatycznych nośników, niezależnie od tego czy będzie to wpływać na długotrwałość procesu analizy danych. W tym ujęciu przykładowo można wskazać metodologię Triade, która jest procesem identyfikacji, sortowania oraz filtrowania danych w celu ustalenia priorytetów oraz kategorii gromadzonych danych w dużej mierze zautomatyzowanym (dzięki czemu przyśpiesza proces kopiowania danych) poprzez ustalenie kryteriów, według których dane zostaną zakwalifikowane jako istotne. Przykładami wskazywanymi przez autorów wykorzystania metodologii Triade jest sytuacja jednego z przedsiębiorstw, w którym podejrzewano pracownika o przechowywanie na komputerze dokumentów, co do których nie powinien mieć dostępu, gdzie udało się odnaleźć przeszukiwane dokumenty bez konieczności dokonywania kopii binarnej (Szczyrbowski, 2013, s. 4). Postulat wyodrębniania informacji wyrażony jest też np. w orzecznictwie francuskim, na co wskazał G. Materna (Materna, 2014, s. 1242).

4. Zabezpieczenie dowodów

SOKiK w glosowanym postanowieniu uznał, że skopiowanie informatycznych nośników danych było zgodne z prawem, gdyż stanowiło zabezpieczenie dowodów, o jakim mowa w art. 105f w zw. art. 105g ust. 4 uokik. SOKiK przyjął taką podstawę prawną, mimo że nie powoływał się na nią Prezes UOKiK. W myśl art. 105f ust. 1 uokik stan faktyczny jest ustalany przez przeszukujących (osoby upoważnione) na podstawie dowodów zebranych w toku kontroli. Ustawodawca w powołanym przepisie wskazał na przykładowe dowody, które mogą zostać objęte zabezpieczeniem,

[7] W jednej ze spraw, strona podniosła brak uzasadnienia skopiowania w całości twardych dysków i wyniesieniu ich z jej pomieszczeń w celu późniejszego przeszukiwania ich zawartości w siedzibie Komisji. TSUE stwierdził, że zarzut ten jest niedopuszczalny w tym postępowaniu – zob. wyr. TS (piąta izba) z 25.06.2014 r., C-37/13 P *Nexans SA i Nexans France SAS* przeciwko *Komisji.*

[8] Wyr. ETPC z 3.07.2012 r., nr skargi 30457/06, *Robathin* przeciwko *Austria*, pkt 64–71.

jednak używając sformułowania „w szczególności", co oznacza, że katalog ten ma charakter otwarty. W omawianym stanie faktycznym SOKiK uznał, że kopie dysków twardych mogą zostać objęte zabezpieczeniem, co uzasadnił tym, że w przypadku przyjęcia, iż zabezpieczenie może dotyczyć tylko oryginalnych dysków komputerów – w istocie w celu ich późniejszego lub sukcesywnego przeglądania – konieczne byłoby ich zajęcie, o jakim mowa w art. 105g uokik. Taki sam pogląd wyrażają również autorzy komentarza pod redakcją C. Banasińskiego oraz E. Piontka (Banasiński i Piontek, 2009, s. 894). Również B. Turno wyraźnie wskazuje, że kopie mogą być przedmiotem zabezpieczenia (Turno, 2016, s. 1319). Potwierdzenie, że kopie mogą stanowić przedmiot zabezpieczenia, znaleźć można też w orzecznictwie sądowym[9]. Zabezpieczenie ma na celu zapewnienie, że ryzyko zniknięcia materiałów już zgromadzonych w toku przeszukania zostanie znacznie zredukowane (Turno, 2016, s. 1320). W tym kontekście znaczenie mają też względy funkcjonalne i fakt, że zabezpieczenie oryginałów dysków twardych mogłoby się przyczynić do zakłócenia funkcjonowania przedsiębiorstwa.

Jak również wskazał SOKiK, zabezpieczenie dowodu nie wymaga wcześniejszej selekcji materiału dowodowego pod kątem przedmiotu przeszukania określonego w postanowieniu SOKiK. Kwestię, jakie dowody mogą zostać objęte zabezpieczeniem, reguluje art. 105f ust. 2 w zw. z ust. 1 powołanego przepisu uokik, wskazując, że mogą to być „dowody zebrane w toku kontroli (tu przeszukania)". Jak wskazuje się w doktrynie, chodzi o dowody mające służyć do ustalenia stanu faktycznego (Kohutek, 2014, s. 983), potwierdzające podejrzenia Prezesa UOKiK i pozwalające mu samodzielnie bądź w powiązaniu z innymi dowodami na stwierdzenie naruszenia przez przedsiębiorcę przepisów uokik (Turno, 2016, s. 1319). W tym sensie nie muszą być to wyłącznie dowody, które będą podstawą decyzji Prezesa UOKiK (Bernatt, 2014, s. 1255). Niemniej, muszą to być dowody, które mogą się okazać istotne z punktu widzenia przedmiotu przeszukania. Dodatkowo, wskazać należy, że dyspozycja przepisu art. 105f ust. 2 uokik przewiduje dwie metody zabezpieczenia dowodów zebranych w trakcie kontroli (tu przeszukania), w tym złożenie, za pokwitowaniem udzielonym kontrolowanemu, na przechowanie w pomieszczeniu UOKiK. Jak jednak wynika z przedstawionego stanu faktycznego oraz braku podniesienia przez Prezesa UOKiK takiego zdarzenia w odpowiedzi na zażalenie – pokwitowanie takie nie zostało przedstawione. Z przedstawionego stanu faktycznego nie wynika też, aby przeszukujący wskazali jako podstawę prawną podejmowanych przez siebie czynności art. 105f ust. 2 uokik. Jak natomiast wskazuje się w orzecznictwie, prowadzi to do powstania stanu niejednoznaczności co do stosowanego trybu postępowania, skutkującego brakiem możliwości jednoznacznej oceny przez przeszukiwanego, na jakiej podstawie i w jakim trybie działa Prezes UOKiK[10].

III. Podsumowanie

Glosowane orzeczenie porusza dwie zasadnicze kwestie w zakresie przeszukania na gruncie uokik, tj. kwestię kopiowania całych informatycznych nośników danych, bez ich selekcji pod kątem informacji służących celowi przeszukania oraz przeglądania tak skopiowanych informacji w siedzibie UOKiK. Wskazać bowiem należy, że praktyka kopiowania całych nośników danych i ich przeglądania poza siedzibą przedsiębiorcy w ramach przeszukania była zgodna z wieloletnim

[9] Zob. wyr. SOKiK z 28.04.2017 r., XVII AmA 11/16.

[10] Wyr. SOKiK z 28.04.2017 r., XVII AmA 11/16.

modelem postępowania przyjętym przez UOKiK (UOKiK, 2017, pkt 4). Należy jednak wskazać, iż oznaczała ona większą swobodę dla przeszukujących, zwiększając prawdopodobieństwo możliwości zapoznania się przez przeszukujących również z informacjami niemającymi związku z przedmiotem przeszukania oraz objętymi tajemnicą zawodową (Królak, 2017). Tym samym, sformułowane w treści postanowienia dyrektywy selekcji gromadzonego materiału dowodowego pod kątem celu przeszukania bez względu na rodzaj nośnika czy nakaz dokonywania takiej selekcji wyłącznie w siedzibie przedsiębiorcy oraz w obecności jej przedstawiciela mają charakter precedensowy i uniwersalny (Modzelewska de Raad, 2017). Zakwestionowanie bowiem przez SOKiK dotychczasowych praktyk UOKiK należy ocenić pozytywnie, jako mające się przyczynić do ochrony słusznych praw przedsiębiorcy i przestrzegania przepisów uokik, w szczególności w dobie coraz szerszych możliwości technologicznych selekcji informacji zgromadzonych na informatycznych nośnikach danych.

Niemniej, zastanawiająca jest przyjęta przez SOKiK wykładnia, iż w związku z tym, że sporządzone przez przeszukujących kopie binarne nie zostały przeanalizowane przez UOKiK, doszło do zabezpieczenia dowodów, która nie wymaga selekcji materiału dowodowego. Jest to również o tyle istotne, iż na taką kwalifikację prawną nie powoływał się Prezes UOKiK. W tym sensie, sąd stworzył i zaakceptował stan, w którym przeszukiwany nie miał wiedzy co do stosowanego trybu postępowania przeszukujących. SOKiK, czyniąc to, pominął fakt, iż aby możliwe było zabezpieczenie dowodu w siedzibie UOKiK, musi to nastąpić „za pokwitowaniem". Wątpliwa wydaje się też teza, zgodnie z którą w ramach zabezpieczenia nie ma konieczności selekcji dowodów. Podsumowując, przyjęta finalnie kwalifikacja czynności dokonanych w kontekście stanu faktycznego przez UOKiK jako „zabezpieczenie dowodów" wydaje się w świetle poczynionych rozważań niezgodna z przepisami uokik.

Końcowo, warto zauważyć, że UOKiK odniósł się do glosowanego postanowienia, wskazując, że dostosował swoją praktykę do wytycznych wynikających z orzeczenia (UOKiK, 2017, pkt 10), co też będzie mogło zostać poddane weryfikacji na podstawie kolejnych czynności przeszukań.

Bibliografia

Banasiński, C. i Piontek, E. (red.). (2009). *Ustawa o ochronie konkurencji i konsumentów. Komentarz*. Warszawa: LexisNexis.

Bernatt, M. (2011). *Sprawiedliwość proceduralna w postępowaniu przed organem ochrony konkurencji.* Warszawa: Wydawnictwo Naukowe Wydziału Zarządzania Uniwersytetu Warszawskiego.

Bernatt, M. (2014). W: T. Skoczny (red.), *Ustawa o ochronie konkurencji i konsumentów. Komentarz*. Warszawa: C.H. Beck.

Jasiński, W. (2016). Gwarancyjność przepisów regulujących przeszukania w sprawach ochrony konkurencji i konsumentów. W: W. Jasiński (red.), *Standardy rzetelności postępowania w sprawach z zakresu ochrony konkurencji i konsumentów. Między prawem administracyjnym a prawem karnym*. Warszawa: Wolters Kluwer.

Kohutek, K. (2014). W: K. Kohutek, M. Sieradzka, *Ustawa o ochronie konkurencji i konsumentów. Komentarz.* Warszawa: Wolters Kluwer.

Królak, J. (2017). UOKiK kontrolując, nadużywa władzy. *Puls Biznesu*, 6.08.2017. Pozyskano z: https://www.pb.pl/uokik-kontrolujac-naduzywa-wladzy-868254 (5.12.2017).

Materna, G. (2014). W: T. Skoczny (red.), *Ustawa o ochronie konkurencji i konsumentów. Komentarz*. Warszawa: C.H. Beck.

Michałek-Gervais, M. (2015). Granice zakresu uprawnień kontrolnych Komisji Europejskiej w świetle najnowszego orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej. *internetowy Kwartalnik Antymonopolowy i Regulacyjny, 8*(4).

Róziewicz-Ładoń, K. (2011). *Postępowanie przed Prezesem Urzędu Ochrony Konkurencji i Konsumentów*. Warszawa: LexisNexis.

Szczyrbowski, K. (2013). Triage i Live Forensic. Analizy w środowisku "big data" V Konferencja informatyki śledczej. *Magazyn Informatyki Śledczej i Bezpieczeństwa IT,* 19 (wrzesień).

Turno, B. (2016). W: A. Stawicki, E. Stawicki (red.), *Ustawa o ochronie konkurencji i konsumentów. Komentarz*. Warszawa: Wolters Kluwer Polska.

Urząd Ochrony Konkurencji i Konsumentów, Biuro Prezesa. (2017). *Wyjaśnienia do artykułu prasowego Jarosława Królaka, który ukazał się w Pulsie Biznesu 7 sierpnia 2017 r*. Pozyskano z: https://www.uokik.gov.pl/komentarze_wyjasnienia_i_stanowiska.php?news_id=13450 (5.12.2017).

Vandenborre, I. i Goetz, T. (2014). EU Competition Law Procedural Issues. *Journal of European Competition Law & Practice,* 9.

Julita Chomik
studentka V roku Prawa, Uniwersytet w Białymstoku
e-mail: julita.chomik1@gmail.com