Warszawa, 31-03-2025 r.

RZECZNIK PRAW OBYWATELSKICH

Marcin Wiącek

II.510.512.2024.DC

Pan

Dariusz Korneluk

Prokurator Krajowy

ePUAP

Szanowny Panie Prokuratorze,

dostęp do elektronicznych nośników danych i zapisanych na nich informacji – korespondencji, zdjęć, nagrań, historii połączeń, historii wyszukiwań w przeglądarce internetowej, historii lokalizacji – jest jedną z czynności dowodowych w procesie karnym, której przydatności nie sposób przecenić. Organy procesowe, zwłaszcza Policja, mogą w stosunkowo łatwy sposób uzyskać dostęp do informacji, które mają istotne znaczenie w postępowaniu karnym. Jednocześnie, trudno jest zaprzeczyć, że dostęp do elektronicznych nośników danych, przede wszystkim telefonu, wiąże się z ingerencją w prawo do prywatności (art. 47 Konstytucji), może prowadzić do ingerencji w tajemnicę komunikowania się (art. 49 Konstytucji) oraz w prawo własności (art. 64 ust. 1 Konstytucji).

Choć obecne przepisy Kodeksu postępowania karnego nie gwarantują jednostce należytej ochrony przed dostępem do jej nośników danych (a przede wszystkim telefonu) w sprawach, w których działanie takie nie jest konieczne w demokratycznym społeczeństwie, tak **wprowadzenie zmian w stanowisku Prokuratury Krajowej z**

25 lipca 2018 r., PK II P 073.81.2016, w kwestii dopuszczalności przeprowadzenia oględzin telefonu, gdy celem działania jest zapoznanie się z zawartością – treściami intelektualnymi – znajdującymi się na urządzeniu, z pewnością przyczyni się do lepszej ochrony obywateli przez nadużywaniem przez organy ścigania czynności procesowej oględzin wewnętrznych (art. 207 k.p.k.), które w istocie swojej odpowiadają czynności przeszukania nośnika informatycznego (art. 236a k.p.k.).

Z informacji, jakie wpływają do Biura Rzecznika Praw Obywatelskich, wynika, że Policja oraz prokuratura przeprowadzają albo oględziny (art. 207 k.p.k.) albo przeszukanie (art. 236a k.p.k.) elektronicznego nośnika danych. Oględziny w praktyce organów ścigania są jednak oględzinami tylko z nazwy, bowiem organ procesowy zapoznaje się z treściami intelektualnymi zawartymi na urządzeniu i „oględziny" urządzenia są wykorzystywane do np. ustalenia pinezek lokalizacyjnych. Z analizy orzecznictwa wynika, m.in. że sądy sankcjonują sytuacje, w której w drodze oględzin telefonu porównano numery telefonów z billingów z książką adresową podejrzanego[1].

Obecnie Prokuratura Krajowa dopuszcza dwa sposoby uzyskiwania informacji zawartych w urządzeniach/systemach zawierających dane informatyczne dla potrzeb postępowania karnego – przeszukanie oraz oględziny[2]. Zasadniczo, uzyskanie dostępu do zawartości telefonu powinno nastąpić w drodze przeszukania – art. 236a k.p.k. Wskazuje się jednak, że „Dopuszczalne jest także uzyskanie danych informatycznych w toku czynności oględzin, o ile urządzenie zawierające dane znalazło się w dyspozycji organu ścigania, a jego dysponentowi lub użytkownikowi zapewniono gwarancje

[1] Zob. przykładowo wyrok SA w Warszawie z dnia 19 maja 2021 r., II AKa 145/20, z którego uzasadnienia wynika, że w drodze „oględzin" telefonu ustalono, jakie kontakty były zapisane w książce adresowej oskarżonego, czy wyrok SN z 30.01.2023 r., III KK 494/22, gdzie SN nie odniósł się do kwestii oględzin, a w sprawie w drodze oględzin telefonu zapoznano się z galerią zdjęć.

[2] Pismo PK II P 073.81.2016. Informacja uzyskana za: P. Olber, *Uzyskiwanie danych zlokalizowanych w urządzeniach lub systemach informatycznych — wybrane zagadnienia w świetle przepisów prawa karnego procesowego,* Przegląd Policyjny 2019, nr 4, s. 176.

procesowe przewidziane przepisami k.p.k."[3]. Nie wskazuje się jednak, jakie gwarancje procesowe powinny zostać zapewnione – czy chodzi o gwarancje zwrotu urządzenia, zatwierdzenia czynności zgodnie z art. 217 § 4 k.p.k., gdy nastąpiło dobrowolne wydanie, czy o możliwość wniesienia zażalenia i do jakiego organu. Na czynność przeszukania zażalenie przysługuje do sądu rejonowego, w okręgu którego prowadzone jest postępowanie – art. 236 k.p.k., na czynność oględzin – do prokuratora bezpośrednio przełożonego (art. 302 k.p.k.). Co więcej, czynność oględzin zapewnia jeszcze mniejszy stopień gwarancyjności niż przeszukanie z art. 236a k.p.k. Przepis art. 207 k.p.k. nie precyzuje ani zakresu przedmiotowego, ani podmiotowego, ani sposobu przeprowadzenia oględzin, a do ich przeprowadzenia jest co do zasady[4] uprawniony organ prowadzący postępowanie (zob. art. 312 k.p.k. w zw. z art. 325d k.p.k.), w tym Policja w ramach „własnych" uprawnień, tj. bez konieczności zatwierdzania tej czynności przez prokuratora lub sąd.

Kluczowe znaczenie mają kryteria, na podstawie jakich dokonuje się wyboru czynności przeszukania albo oględzin[5]. Ze stanowiska Prokuratury Krajowej z 25 lipca 2018 r., PK II P 073.81.2016, wynika, że oględziny są dopuszczalne, jeśli „urządzenie zawierające dane znalazło się w dyspozycji organu ścigania, a jego dysponentowi lub użytkownikowi zapewniono gwarancje procesowe przewidziane w k.p.k.".

Urządzenie – nośnik informacji – może znaleźć się w dyspozycji organu procesowego[6] w drodze dobrowolnego wydania albo przymusowego odebrania. W przypadku przymusowego odebrania rzeczy (art. 217 § 5 k.p.k. w zw. z art. 236a k.p.k.), czynność Policji musi zostać zatwierdzona przez sąd lub prokuratora w terminie 7 dni, jeśli została wykonana w wypadku niecierpiącym zwłoki. Oględziny zewnętrzne urządzenia

[3] P. Olber, *Uzyskiwanie danych zlokalizowanych w urządzeniach lub systemach informatycznych — wybrane zagadnienia w świetle przepisów prawa karnego procesowego,* Przegląd Policyjny 2019, nr 4, s. 185.
[4] Poza oględzinami zwłok. Zob. art. 209 k.p.k.
[5] Zob. szerzej: P. Lewulis, *Gromadzenie i ocena dowodów cyfrowych w polskim postępowaniu karnym. Kluczowe wnioski z badań aktowych*, Prok. i Pr. 2022, nr 3, s. 119-147 i wskazana tam literatura.
[6] Poza sytuacjami takimi jak znalezienie urządzenia.

– model, kolor, stan techniczny – są dopuszczalne w każdej z tych sytuacji, co nie budzi wątpliwości. **Zapoznanie się z zawartością telefonu w drodze oględzin (oględziny wewnętrzne) nie spełnia warunku określoności prawa i nie gwarantuje osobie, której telefon jest poddawany oględzinom odpowiedniej ochrony prawnej.** Może także prowadzić do naruszenia wymogu konieczności w państwie demokratycznym i niespełnienia warunku proporcjonalności (stopnia ingerencji w prawo do prywatności w kontekście wagi czynu).

Po pierwsze, nie jest wymagane podanie celu oględzin, a w przypadku przeszukania, organ procesowy jest zobowiązany do podania podstawy prawnej oraz celu przeszukania.

Po drugie, oględziny mogą nastąpić w każdej sprawie, niezależnie od istniejącej podstawy dowodowej. W przypadku przeszukania klauzula generalna, tj. istnienie uzasadnionej podstawy do przypuszczania, że na danym nośniku znajdują się potrzebne informacje, jest bardzo ogólna. Oględziny jednak mogą odbywać się w każdej sytuacji, co w żaden sposób nie chroni jednostki przed arbitralnością władzy. Zgodnie z art. 207 § 1 k.p.k. dokonuje się ich „w razie potrzeby". Można zatem wyobrazić sobie sytuację, kiedy oględziny są wykonywane w celu sprawdzenia, czy na telefonie znajdują się dowody/informacje mogące mieć znaczenie w postępowaniu (*fishing expeditions*[7]), a po taki wstępnym ustaleniu przydatności informacji – „zmienią się" w przeszukanie telefonu.

Po trzecie, brak jest jakiegokolwiek ograniczenia podmiotowego i przedmiotowego dokonania oględzin telefonu. Mogą nastąpić wobec każdej osoby, w każdej sprawie, jeśli organ procesowy – najczęściej Policja – widzą taką potrzebę.

Po czwarte, sposób przeprowadzenia oględzin „wewnętrznych" telefonu nie jest uregulowany – nie wiadomo, jaki zakres danych organ może powziąć dokonując tych

[7] Por. wyrok ETPC z 4.10.2022 r., w sprawie De Legé przeciwko Holandii, skarga nr 58342/15.

oględzin. Czy tylko zweryfikować numer IMEI, by ustalić, czy urządzenie nie jest kradzione lub numer seryjny, czy w wyniku oględzin ma on również uprawnienie do otworzenia galerii zdjęć, przeglądarki internetowej, czy aplikacji do wysyłania wiadomości.

Po piąte, w przypadku oględzin wewnętrznych telefonu brak jest jakiejkolwiek ochrony tajemnic prawnie chronionych. Przepisy art. 225 i 226 k.p.k. stosuje się w przypadku przeszukania i w odniesieniu do rzeczy znalezionych podczas przeszukania, a nie do informacji uzyskanych w wyniku oględzin.

Po szóste zaś, wadliwość przeprowadzenia oględzin i *de facto* przeprowadzenia przeszukania telefonu może być zaskarżona do prokuratora (art. 302 k.p.k.), a nie do sądu. Przepis art. 236 k.p.k. znajduje się w rozdziale 25 k.p.k. i dotyczy czynności zatrzymania rzeczy i przeszukania. Co prawda, czynność procesową należy oceniać według jej treści, a nie formy, zatem formalne przyporządkowanie (nazwanie) zapoznania się z zawartością telefonu jako oględziny nie wyłącza możliwości zaskarżenia jej do sądu, ale takie uprawnienie nie wynika wprost z przepisów. Dodatkowo, umożliwia czysto formalistyczne podejście do kwestii zażaleń poprzez odmawiania ich przyjęcia przez sąd i przekazywania do prokuratora (art. 118 § 3 k.p.k. w zw. z art. 429 § 1 k.p.k. w zw. z art. 465 k.p.k.) albo nieprzekazywania przez prokuratora zażaleń do sądu i przyjmowanie, że to prokurator bezpośrednio przełożony jest organem uprawnionym do rozpoznania środka zaskarżenia (art. 118 § 3 k.p.k. w zw. z art. 302 k.p.k.).

W kwestii wejścia w posiadanie urządzenia, należy podkreślić, że „dobrowolne wydanie" rzeczy nie powinno stanowić ewentualnego kryterium rozgraniczającego możliwość zapoznania się z zwartością telefonu w drodze oględzin albo przeszukania. W przypadku dobrowolnego wydania telefonu, organ procesowy nie zastosował żadnego „obiektywnego" przymusu związanego z wkroczeniem w sferę praw i wolności jednostki, tj. nie doszło do faktycznego zastosowania środków przymusu

bezpośredniego przez organy państwa. Jednak każdorazowo organ procesowy ma możliwość zastosowania takiego przymusu, co sprawia, że jednostka przestaje być dysponentem naruszanych dóbr[8]. Wybór, jaki ma osoba, wobec której zażądano wydania telefonu, jest w zasadzie pozorny – albo wyda go dobrowolnie albo zostanie jej, zgodnie z prawem, odebrany z użyciem siły. Niezależnie od „wyboru" nie będzie ona dysponentem urządzenia – przez określony czas, urządzenie będzie w dyspozycji organów procesowych i nie jest w stanie w żaden sposób zapobiec przeprowadzeniu czynności procesowej. Wydaje się także, że groźba pozbawienia możliwości korzystania z telefonu, może skłaniać do „dobrowolnego" wydania. **Obecnie bowiem na telefonach znajdują się aplikacje bankowe, kalendarze, aplikacje lotnicze (w tym także bilety lotnicze), aplikacje zdrowotne. Telefon wraz z kartą SIM jest niezbędny do logowania dwuskładnikowego, co może uniemożliwić zalogowanie się na np. komputerze służbowym, służbowej poczcie elektronicznej**[9]. Wydaje się zatem, że osoba, wobec której kierowane jest żądanie wydania telefonu, będzie bardziej skłonna go wydać dobrowolnie, licząc na możliwie szybki zwrot i obawiając się zatrzymania urządzenia w celu przeprowadzenia badań i analizy informatycznej.

Z przepisów k.p.k. ani wytycznych KGP ani z publicznie dostępnych dokumentów prokuratorskich, **nie wynika, czy funkcjonariusz Policji albo prokurator, który znalazł się w dyspozycji elektronicznego nośnika danych (telefonu) może podjąć próbę samodzielnego odblokowania urządzenia, gdy odmówiono podania hasła np. wpisując popularne kody (5555 albo 1111), popularne wzory do odblokowania telefonu, czy wykorzystując biometrię – „pobierając" odciski**

[8] Zob. szerzej: K. Jarząbek, *5. Przeszukanie jako środek przymusu* [w:] *Przeszukanie w polskim procesie karnym*, Warszawa 2024.

[9] Wydanie duplikatu karty SIM może być utrudnione, jeżeli na zatrzymanym telefonie użytkownik zastrzegł w aplikacji mObywatel numer PESEL, ponieważ do wydania duplikatu konieczne jest, by numer PESEL nie był zastrzeżony. Dla skorzystania z aplikacji mObywatel konieczne jest potwierdzenie tożsamości np. za pośrednictwem aplikacji bankowej, co – w przypadku zatrzymania urządzenia – będzie niemożliwe. Istnieje zatem niebezpieczeństwo „wpadnięcia" w błędne koło, którego przerwanie wymaga znacznego nakładu czasu.

palców w celu odblokowania urządzenia (art. 74 § 1 pkt 1 k.p.k.[10]), czy odblokowując urządzenie przykładając telefon blisko twarzy, aktywując usługę Face ID, czy zbliżone usługi na różnych modelach telefonów oparte na analizie tęczówki oka. We wszystkich tych przypadkach, nawet gdy nastąpiło dobrowolne wydanie urządzenia, to osoba nie udzieliła informacji, które pozwalałyby organowi procesowemu na zapoznanie się z jego zawartością. Dostęp do zawartości był możliwy przy wykorzystaniu okoliczności istniejących niezależnie od woli danej osoby (odciski palców, wizerunek) albo przy przełamaniu zabezpieczeń (niezależnie od tego, jak silne to były zabezpieczenia – wyrażały chęć ochrony zawartości urządzenia elektronicznego).

Niezależnie zatem od tego, że czynność przeszukania elektronicznych nośników danych powinna zostać skorygowana na poziomie ustawowym, a przepisy k.p.k. dostosowane do warunków aktualnej, zdigitalizowanej rzeczywistości, to zanim to nastąpi zasadne wydaje się wprowadzenie zmian w stanowisku Prokuratury Krajowej z 25 lipca 2018 r., PK II P 073.81.2016, aby podczas czynności procesowych nie dochodziło do naruszenia konstytucyjnych praw i wolności jednostki.

W załączeniu przedkładam uprzejmie wystąpienie generalne Rzecznika Praw Obywatelskich do Ministra Sprawiedliwości – Prokuratora Generalnego w kwestii dopuszczalności oględzin i przeszukań elektronicznych nośników danych.

Jednocześnie, w nawiązaniu do w/w wystąpienia generalnego na podstawie art. 16 ust. 2 pkt 1 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2024 r. poz. 1264 z późn. zm.) **zwracam się do Pana Prokuratora z uprzejmą prośbą o rozważenie wprowadzenia zmian w stanowisku Prokuratury Krajowej z 25 lipca 2018 r., PK II P 073.81.2016, w opisanym wyżej zakresie, z uwzględnieniem tego,**

[10] Przepis art. 74 § 2 pkt 1 k.p.k. nie precyzuje celu pobrania odcisków palców, a w związku z tym nie wyklucza pobrania ich w celu odblokowania urządzenia. Cel czynności z art. 74 § 2 pkt 1 k.p.k. został sprecyzowany wyłącznie w odniesieniu do okazania, które może być przeprowadzone „w celach rozpoznawczych".

że obecnie zatarta jest różnica między statycznym a dynamicznym pozyskiwaniem danych[11] i z tego względu dostęp do danych zapisanych na elektronicznym nośniku danych, biorąc pod uwagę zakres historyczny tych danych, może w porównywalnym stopniu ingerować w sferę prywatności jednostki, co ich dynamiczne pozyskiwanie w czasie rzeczywistym[12]. Będę także wdzięczny za poinformowanie mnie o stanowisku zajętym w przedstawionej materii.

Z wyrazami szacunku

Marcin Wiącek

Rzecznik Praw Obywatelskich

/-wydano i podpisano elektronicznie/

Załącznik:

- Wystąpienie Rzecznika Praw Obywatelskich do Ministra Sprawiedliwości w kwestii dopuszczalności przeszukań i oględzin telefonu

[11] K. Kremens, *Granice ingerencji w prawo do prywatności i prawo własności w postępowaniu karnym*, [w:] J. Skorupka (red.), *Model dopuszczalnej ingerencji w prawa wolności jednostki w procesie karnym,* Warszawa 2017, Legalis.

[12] Nie oznacza to zrównania obu czynności – pozyskiwania danych w czasie rzeczywistym i dostępu do danych zapisanych na urządzeniu. Słusznie wskazuje się jednak, że nie oznacza to, „że nie ma różnicy między inwigilacją w czasie rzeczywistym a pozyskiwaniem utrwalonych danych zawierających treść tej komunikacji. Biorąc jednak pod uwagę charakter ingerencji w prywatność, a także potencjalnie bardzo szeroki czasowo zakres danych, jaki można zebrać z nośników (np. z komunikatorów w telefonach komórkowych), nie można uznać, że w takim przypadku standard w porównaniu z kontrolą i utrwalaniem rozmów (które notabene też są utrwalane i odsłuchiwane post factum) powinien być niższy". Tak: W. Jasiński, W. Jasiński, *O potrzebie zmian w regulacjach prawnych…,* s. 64.