Warszawa, 31-03-2025 r.

RZECZNIK PRAW OBYWATELSKICH

Marcin Wiącek

II.510.512.2024.DC

Pan

Adam Bodnar

Minister Sprawiedliwości

Prokurator Generalny

ePUAP

Szanowny Panie Ministrze,

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, 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). 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.

Na podstawie informacji, jakie wpływają do Biura Rzecznika Praw Obywatelskich, zidentyfikowana została wadliwa praktyka polegająca na przeprowadzeniu czynności oględzin telefonu komórkowego (art. 207 k.p.k.) w sytuacji, kiedy celem działań funkcjonariuszy Policji było ustalenie pinezek lokalizacyjnych, czy zapoznanie się z treścią wiadomości na komunikatorach internetowych, a zatem konieczne było przeprowadzenie przeszukania urządzenia (art. 236a k.p.k.).

Dlatego też, zwracam się z uprzejmą prośbą o podjęcie działań zmierzających do dostosowania przepisów ustawowych oraz wewnętrznych regulacji prokuratury do standardu konstytucyjnego oraz wiążącego Polskę standardu europejskiego.

1. Zapoznanie się z zawartością elektronicznych nośników danych i prawo do prywatności – konwencyjny i unijny.

Prawo do prywatności jest również chronione na gruncie art. 8 Europejskiej Konwencji Praw Człowieka oraz art. 7 Karty Praw Podstawowych UE. W swoim orzecznictwie Europejski Trybunał Praw Człowieka wskazuje, że ingerencja w prawo do prywatności jest możliwa, ale pod warunkiem:

1) istnienia podstawy prawnej w prawie krajowym (test legalności)[1]. Trybunał zwraca uwagę na dostępność prawa krajowego (możliwość zapoznania się ze szczegółowymi regulacjami) oraz jego przewidywalność (co oznacza możliwość zrozumienia przez jednostkę konsekwencji swojego zachowania)[2];

2) konieczności ingerencji w państwie demokratycznym w świetle art. 8 ust. 2 EKPC (bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochrona porządku i zapobieganie przestępstwom, ochrona zdrowia i moralności lub ochrona praw i wolności innych osób);

[1] Wyrok ETPC z 2.08.1984 r., w sprawie Malone przeciwko Wielkiej Brytanii, skarga nr 8691/79 (dotyczący kontroli rozmów).
[2] Wyrok ETPC z 6.11.1978 r. w sprawie Sunday Times przeciwko Wielkiej Brytanii, skarga nr 6538/74, pkt 49; wyrok ETPC z 25.03.1983 r. w sprawie Silver i in. przeciwko Wielkiej Brytanii, skargi nr 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75, pkt 86–97.

3) spełnienia warunku proporcjonalności – czy w danej okoliczności ingerencja organów państwa w prawo do prywatności mieściła się w odpowiednich granicach, np. nie była nadmierna w odniesieniu do wagi czynu i jego społecznej szkodliwości[3].

Dotychczas ETPC nie rozstrzygał kwestii przeszukania telefonu i danych na nim zapisanych, ale obecnie w Trybunale znajduje się sprawa przeciwko Polsce odnosząca się do tego zagadnienia[4].

Problematyka dostępu do elektronicznych nośników danych – telefonów – mieści się również w zakresie Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW[5]. W wyroku z dnia 4 października 2024 r. Trybunał Sprawiedliwości Unii Europejskiej[6] stwierdził, że „próba uzyskania przez organy policyjne wglądu do danych zapisanych w telefonie komórkowym na potrzeby postępowania przygotowawczego w sprawach karnych wchodzi, jak stwierdził rzecznik generalny w pkt 53 opinii[7], w zakres stosowania dyrektywy 2016/680”[8]. W tym orzeczeniu Trybunał luksemburski uznał, że dostęp do danych zapisanych w telefonie komórkowym jest możliwy nie tylko w poważnych

---

[3] Zob. szerzej: Guide on Article 8 of the European Convention on Human Rights, s. 7-15.
[4] Sprawa Nabrdalik i Moskwa p. Polsce, zakomunikowana 15.02.2023 r., skargi nr 30614/22 30848/22; https://hudoc.echr.coe.int/eng?i=001-223550. Postępowanie przed ETPC dotyczy nie tylko dostępu do telefonu, ale także ochrony tajemnic prawnie chronionych, tj. tajemnicy dziennikarskiej. Zob. także: https://privacyinternational.org/legal-action/nabrdalik-v-poland.
[5] Dz.U. L 119 z 4.05.2016, p. 89–131.
[6] Wyrok TSUE z 4.10.2024 r., w sprawie C-548/21, CG przeciwko Bezirkshauptmannschaft Landeck.
[7] Opinia Rzecznika Generalnego Manuela Camposa Sancheza-Bordony przedstawiona w dniu 20 kwietnia 2023 r.; https://curia.europa.eu/juris/document/document.jsf;jsessionid=C3D242B614933809F61AE5DAF60F5CA7?text=&docid=272699&pageIndex=0&doclang=pl&mode=lst&dir=&occ=first&part=1&cid=3823071.
[8] Wyrok TSUE z 4.10.2024 r., w sprawie C-548/21, CG przeciwko Bezirkshauptmannschaft Landeck; pkt 77.

sprawach, ale także w celu zwalczania przestępstw w ogólności. Możliwość uzyskania wglądu do danych zapisanych w telefonie komórkowym w celu zapobiegania przestępstwom w ogólności, ich dochodzenia, wykrywania i ścigania, wymaga, by prawo krajowe:

- w wystarczająco precyzyjny sposób określało charakter lub kategorie przestępstw,

- gwarantowało poszanowanie zasady proporcjonalności oraz

- uzależniało skorzystanie z tej możliwości, z wyjątkiem należycie uzasadnionych pilnych przypadków, od uprzedniej kontroli sądu lub niezależnego organu administracyjnego[9].

Osoba, do której telefonu organy procesowe chciały uzyskać dostęp, powinna zostać poinformowana o powodach uzyskania dostępu do danych zapisanych na telefonie (nośniku danych).

2. Zapoznanie się z zawartością elektronicznych nośników danych – regulacje ustawowe.

Biorąc pod uwagę różny stopień ingerencji w prawo do prywatności, ponadustawowe warunki limitowania praw i wolności jednostki, ustawodawca odmiennie określa zakres i warunki dopuszczalności tych czynności. Im bardziej jest ona dolegliwa (np. w przypadku kontroli i utrwalania rozmów – art. 237 k.p.k. i nast.), tym przepisy wprowadzają wyższy standard dotyczący następujących kwestii:

- przesłanek warunkujących przeprowadzenie danej czynności;

- organu uprawnionego do zarządzenia wykonania danej czynności lub jej przeprowadzenia;

- granic przedmiotowych (rodzaj czynu, określenie katalogu przestępstw);

- granic podmiotowych (osoby, wobec których czynność może zostać przeprowadzona);

[9] Pkt 110.

- sposób przeprowadzenia czynności, w tym czas jej prowadzenia[10].

Istotne jest także to, czy osoba, której czynność ingerująca w prywatność dotyczy, ma możliwość jej zaskarżenia i do jakiego organu.

Jeśli chodzi o zapoznanie się z zawartością elektronicznych nośników danych – telefonu – to zgodnie z art. 236a k.p.k. „przepisy rozdziału niniejszego (rozdziału 25 k.p.k. „Zatrzymanie rzeczy. Przeszukanie. – przyp. aut.) stosuje się odpowiednio do dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego, w zakresie danych przechowywanych w tym urządzeniu lub systemie albo na nośniku znajdującym się w jego dyspozycji lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną".

Przepis art. 236a k.p.k. w zasadzie od początku jego wprowadzenia[11] poddawany był krytyce[12]. Zwracano uwagę, że nie przystaje on do zmieniającej się rzeczywistości, uregulowań międzynarodowych w zakresie tej problematyki, podkreślano niecelowość stosowania tradycyjnych regulacji procesowych do dowodów elektronicznych[13]. Dodatkowo, zakres art. 236a k.p.k. uniemożliwia przeprowadzenie zdalnych przeszukań i uzyskiwania dostępu do zawartości urządzenia na odległość, co z jednej strony ogranicza możliwość działania organów procesowych, a z drugiej – wymusza przeprowadzenie tych czynności w drodze

[10] Zob. szerzej: 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.

[11] Ustawa z dnia 10 stycznia 2003 r. o zmianie ustawy - Kodeks postępowania karnego, ustawy - Przepisy wprowadzające Kodeks postępowania karnego, ustawy o świadku koronnym oraz ustawy o ochronie informacji niejawnych (Dz.U. z 2003, nr 17, poz. 155).

[12] Zob. K. Jarząbek, 3. *Przeszukanie urządzenia zawierającego dane informatyczne a jego oględziny* [w:] *Przeszukanie w polskim procesie karnym*, Warszawa 2024; A. Lach, *Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego*, Prok. i Pr. 2003, nr 10, s. 20; 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.

[13] Zob. szerzej: K. Jarząbek, 3. *Przeszukanie urządzenia zawierającego dane informatyczne a jego oględziny* [w:] *Przeszukanie w polskim procesie karnym*, Warszawa 2024.

czynności pozaprocesowych (czynności operacyjno-rozpoznawczych)[14]. Niezwykle istotna przestrzeń – jaką jest „życie cyfrowe" każdej osoby, dane i informacje, jakie ma na swoim telefonie, komputerze, tablecie itp. – jest uregulowana za pomocą bardzo ogólnego odesłania, które nie zapewnia odpowiedniego poziomu gwarancyjności[15].

Przeszukanie telefonu (innego nośnika danych informatycznych) może nastąpić na polecenie sądu lub prokuratora, a wyjątkowo, w wypadkach niecierpiących zwłoki – na podstawie nakazu kierownika jednostki lub legitymacji służbowej[16]. Prowadzone badania akt pokazują[17], że wyjątkowa możliwość przeprowadzenia przeszukania na podstawie nakazu kierownika jednostki/legitymacji służbowej, jest w praktyce regułą, zaś przeszukania przeprowadzane w trybie art. 220 § 3 k.p.k. zwykle są zatwierdzane[18] (nawet jeśli przeszukanie nie było skuteczne, tj. nie dostarczyło dowodów niezbędnych dla prowadzonego postępowania). Ustawa nie wprowadza żadnego ograniczenia przedmiotowego w zakresie możliwości przeprowadzenia przeszukania (jest możliwe w każdej sprawie), a granice podmiotowe są w zasadzie otwarte (można przeszukać telefon osoby podejrzanej, ale także innej osoby (dysponenta lub użytkownika), jeżeli istnieją uzasadnione podstawy do przypuszczenia, że nośnik informacji zawiera dane mogące stanowić dowód w sprawie – art. 236a k.p.k. w zw. z art. 219 § 1 k.p.k.). Sposób przeprowadzenia przeszukania urządzenia teleinformatycznego jest uregulowany w drodze odesłania z art. 236a k.p.k. i „odpowiedniego" stosowania przepisów o przeszukaniu rzeczy. Warto jednak zauważyć, że częściowo procedura

---

[14] Tak: W. Jasiński, *O potrzebie zmian w regulacjach prawnych dotyczących pozyskiwania informacji pochodzących z nośników danych dla celów postępowania karnego*, Gdańskie Studia Prawnicze 2024, nr 2, s. 65-66.

[15] W. Jasiński, *O potrzebie zmian w regulacjach prawnych...,* s. 59 i wskazana tam literatura.

[16] Art. 220 § 3 k.p.k.

[17] Zob. M. Basa, K. Jarząbek, *Praktyka prowadzenia przeszukań w wypadkach niecierpiących zwłoki – przesłanki i podstawa dowodowa przeszukania,* Przegląd Sądowy 2023, nr 6, s. 50 i nast. Autorzy wskazali, że „rezultat przeprowadzonych badań aktowych dostarczył najwięcej informacji w zakresie praktyki dokonywania przeszukań na podstawie art. 220 § 3 k.p.k. ze względu na to, że z 1340 zbadanych przypadków przeszukań aż 1310 (97,7%) zostało dokonanych w wypadku niecierpiącym zwłoki, a zaledwie 30 (2,3%) na podstawie postanowienia".

[18] Spośród 1310 zbadanych przeszukań dokonanych w omawianym trybie 1158 (88,3%) zostało zatwierdzonych. W. Jasiński, *O potrzebie zmian w regulacjach prawnych...,* s. 62.

przeszukania urządzeń informatycznych, w tym telefonu, jest uregulowana w § 66–69 Wytycznych Komendanta Głównego Policji z dnia 30 sierpnia 2017 r. w sprawie wykonywania niektórych czynności dochodzeniowo-śledczych przez policjantów[19]. Nie jest to jednak akt powszechnie obowiązującego prawa. Pokazuje to natomiast potrzebę uregulowania procedury – trybu – przeprowadzenia przeszukania elektronicznych nośników danych w sposób bardziej szczegółowy w ustawie, tak, aby każda osoba, której dotyczy czynność z art. 236a k.p.k. była w stanie przewidzieć, jakie konsekwencje wiążą się z dostępem do jej danych (np. że urządzenie zostanie zatrzymane przez określony czas, dane zostaną skopiowane, jaki zakres danych może zostać skopiowanych itp.).

Uwagi krytyczne dotyczące nieprzystawania do dynamicznie zmieniającej się rzeczywistości formułowane w momencie wprowadzania przepisu i później (czyli prawie 20 lat temu), obecnie są jeszcze bardziej aktualne. Telefon – smartfon – nie jest wyłącznie środkiem komunikowania się, ale nośnikiem najbardziej prywatnych informacji o życiu danej osoby. Zawiera nie tylko wykaz połączeń czy wiadomości, ale także zdjęcia, filmy, informacje dotyczące lokalizacji, aplikacje bankowe i wiele więcej. Co więcej, **w praktyce przepis art. 236a k.p.k. bywa pomijany, a dostęp do danych informatycznych zapisanych na urządzeniu (telefonie) jest uzyskiwany za pomocą oględzin (art. 207 k.p.k.).**

Prokuratura Krajowa dopuszcza dwa sposoby uzyskiwania informacji zawartych w urządzeniach/systemach zawierających dane informatyczne dla potrzeb postępowania karnego – przeszukanie oraz oględziny[20]. Zasadniczo, uzyskanie dostępu do zawartości telefonu powinno nastąpić w drodze przeszukania – art. 236a k.p.k. „Dopuszczalne jest także uzyskanie danych informatycznych w toku czynności oględzin, o ile urządzenie zawierające dane znalazło się w dyspozycji organu ścigania,

[19] Dz.Urz.KGP. z 2017, poz. 59.

[20] 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.

a jego dysponentowi lub użytkownikowi zapewniono gwarancje procesowe przewidziane przepisami k.p.k."[21]. Także publikacje funkcjonariuszy Policji wskazują, że przeprowadzenie oględzin telefonu nie jest sprzeczne z prawem, o ile policjant znalazł się legalnie w posiadaniu urządzenia, „a dysponentowi urządzenia zapewniono gwarancje procesowe przewidziane art. 217 k.p.k."[22].

Nie wskazano 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 gwarantuje 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[23] 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.

3. Przeszukanie a oględziny – kryteria wyboru rodzaju czynności procesowej.

Podsumowując dotychczasowe uwagi dotyczące postawy prawnej zapoznania się z zawartością elektronicznych nośników danych – zwłaszcza z zawartością telefonu – kluczowe znaczenie mają kryteria, na jakich podstawie dokonuje się wyboru czynności przeszukania albo oględzin[24]. Z pisma Prokuratury Krajowej wynika, że oględziny są dopuszczalne, jeśli „urządzenie zawierające dane znalazło się w

[21] 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.
[22] R. Wojtuszek, *Jednak przeszukujemy, czasem tylko oglądamy,* Gazeta Policyjna 2018, nr 164; https://gazeta.policja.pl/997/archiwum-1/2018/numer-164-102018/166717,Jednak-przeszukujemy-czasami-tylko-ogladamy.html.
[23] Poza oględzinami zwłok. Zob. art. 209 k.p.k.
[24] 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.

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[25] 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 – 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

[25] Poza sytuacjami takimi jak znalezienie urządzenia.

(*fishing expeditions*[26]), 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 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

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

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 zawartością 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. Niemniej, każdorazowo organ procesowy – np. funkcjonariusz publiczny – ma możliwość zastosowania takiego przymusu, co sprawia, że jednostka przestaje być dysponentem naruszanych dóbr[27]. 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**[28]. Wydaje się zatem, że osoba, wobec której kierowane jest żądanie wydania telefonu, będzie bardziej skłonna je wydać

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

[28] 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.

dobrowolnie, licząc na możliwie szybki zwrot i obawiając się zatrzymania urządzenia w celu przeprowadzenia badań i analizy informatycznej.

Zgodnie z § 66 ust. 8 Wytycznych nr 3 Komendanta Głównego Policji[29], „przeprowadzający przeszukanie ma prawo zażądać od dysponenta lub użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego ujawnienia hasła lub haseł umożliwiających dostęp do urządzenia lub systemu, nawet wówczas, gdy dysponentem lub użytkownikiem jest osoba, o której mowa w art. 74, art. 182 lub art. 183 k.p.k.". Brak jest podobnych regulacji w przypadku oględzin, ale biorąc pod uwagę mniejszy stopień gwarancyjności czynności, wydaje się, że organ procesowy, który chce przeprowadzić oględziny wewnętrzne telefonu, również może zwrócić się o podanie hasła albo innych informacji, które umożliwią zapoznanie się z jego zawartością, informując jednocześnie, że w przypadku odmowy podania hasła, możliwe będzie skorzystanie z urządzeń lub programów komputerowych umożliwiających przełamanie zabezpieczeń[30], co będzie wiązało się z pozbawieniem możliwości korzystania z telefonu.

Z przepisów k.p.k. ani wytycznych Komendanta Głównego Policji nie wynika, czy funkcjonariusz Policji, 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 palców w celu odblokowania urządzenia (art. 74 § 1 pkt 1 k.p.k.[31]), czy odblokowując urządzenie przykładając telefon blisko twarzy, aktywując usługę Face ID, czy zbliżone usługi na innych modelach telefonów oparte na analizie tęczówki oka. We wszystkich tych przypadkach, nawet gdy nastąpiło dobrowolne wydanie urządzenia, to osoba nie

[29] Dz.Urz.KGP. z 2017, poz. 59.

[30] Zob. § 8 ust. 10 wytycznych nr 3 KGP; Dz.Urz.KGP. z 2017, poz. 59.

[31] 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".

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).

4. Wnioski w przedmiocie podjęcia dalszych działań.

Obecne uregulowanie przeszukania elektronicznych nośników danych (art. 236a k.p.k.) nie przystają do zdigitalizowanego, współczesnego świata. Oględziny telefonu (art. 207 k.p.k.) – dopuszczalne na gruncie wewnętrznych regulacji Policji i Prokuratury Krajowej – są jeszcze mniej gwarancyjne dla jednostki, a ustawodawca nie wprowadza odpowiednich zabezpieczeń przed arbitralnością działania organów władzy publicznej[32].

Uwzględniając standard ponadustawowy – wymagania konstytucyjne, konwencyjne oraz unijne – konieczne jest wprowadzenie szczegółowych regulacji dotyczących pozyskiwania informacji pochodzących z elektronicznych nośników danych. Jest to konieczny krok do zagwarantowania odpowiedniego poziomu ochrony prawnej – w wymiarze indywidualnym (wprowadzenie gwarancji i zabezpieczeń przed arbitralnością władzy) i powszechnym (umożliwienie prowadzenia czynności na odległość, które obecnie nie mogą być wykonywane na podstawie przepisów k.p.k.).

Rozważenia wymaga, czy nowe przepisy powinny być zawarte w osobnym rozdziale k.p.k. (np. w nowododanym rozdziale 25a k.p.k., czy 36a k.p.k.), czy jako grupa przepisów w ramach już istniejącego podziału Kodeksu postępowania karnego.

[32] 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. Wydaje się zatem, że sądy nie dostrzegają braku gwarancyjności czynności oględzin telefonu i nie rozważają kwestii legalności i dopuszczalności tak pozyskanych dowodów.

Ogólne odesłanie z art. 236a k.p.k. i odpowiednie stosowanie przepisów rozdziału o przeszukaniu nie spełnia wymogu określoności prawa i jego przewidywalności dla jednostki. Nie jest możliwe ustalenie, jak – krok po kroku – będzie prowadzone przeszukanie elektronicznego nośnika danych, co organ może samodzielnie wykonać w miejscu przeszukania itp.

Biorąc pod uwagę stopień ingerencji w prawo do prywatności, konieczne jest rozważenie, jaki stopień gwarancyjności powinny mieć nowe przepisy. **Obecnie zatarta jest różnica między statycznym a dynamicznym pozyskiwaniem danych**[33]. 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[34]. Rozważenia wymaga, jaki organ byłby uprawniony do zarządzenia przeszukania elektronicznych nośników danych, i czy nie powinien być to wyłącznie sąd, a w wypadkach niecierpiących zwłoki prokurator, pod warunkiem zatwierdzenia czynności przez sąd. Nowe regulacje powinny również uwzględniać kwestię tajemnic prawnie chronionych i wprowadzać procedurę eliminacji informacji wchodzących w zakres tych tajemnic z akt sprawy. Należy także rozważyć wprowadzenie granic podmiotowych i przedmiotowych, by ograniczyć arbitralność działania organów władzy publicznej i korzystanie z czynności dowodowych ingerujących w prywatność jednostki w sprawach błahych.

---

[33] 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.

[34] 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.

Celowe wydaje się także wydanie wytycznych przez Prokuratora Generalnego dotyczących sposobu postępowania z elektronicznymi nośnikami danych, w tym wprowadzenia (opisania) trybu przeszukania telefonu (innego nośnika danych) i wykluczenia możliwości dokonania oględzin wewnętrznych.

Mając na uwadze przedłożone racje, stosownie do art. 16 ust. 2 pkt 1 ustawy z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich[35], zwracam się do Pana Ministra z uprzejmą prośbą o dokonanie analizy wskazanych w niniejszym stanowisku problemów i rozważenie zainicjowania zmian legislacyjnych w Kodeksie postępowania karnego we wskazanych zakresach. Będę także wdzięczny za poinformowanie mnie o stanowisku zajętym w przedstawionej materii.

Z wyrazami szacunku

Marcin Wiącek

Rzecznik Praw Obywatelskich

/-wydano i podpisano elektronicznie/

Do wiadomości:
- Pan Poseł Marek Ast Przewodniczący Komisji Ustawodawczej Sejmu RP (ePUAP);
- Pan Senator Krzysztof Kwiatkowski Przewodniczący Komisji Ustawodawczej Senatu RP (ePUAP).

[35] Ustawa z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2024 r., poz. 1264).