



Warszawa, 27-08-2026 r.

RZECZNIK PRAW OBYWATELSKICH

Sylvia Gregorczyk-Abram

II.510.512.2024.DC

Pan

Waldemar Żurek

**Minister Sprawiedliwości – Prokurator
Generalny**

/ePUAP/

Szanowny Panie Ministrze,

w dniu 31 marca 2026 r. ówczesny Rzecznik Praw Obywatelskich sformułował wystąpienie generalne¹, w którym zwrócił uwagę na dwie kwestie. Po pierwsze, na wadliwą praktykę organów ścigania (w tym Policji i prokuratury) w zakresie przeprowadzania tzw. oględzin wewnętrznych telefonu (smartfona), tj. czynności w trybie art. 207 k.p.k.², a nie przeszukania elektronicznego nośnika danych w trybie z art. 236a k.p.k. Po drugie zaś, na niedostosowanie obecnych przepisów w zakresie przeszukania elektronicznego do warunków nowej, cyfrowej rzeczywistości. Jeśli celem czynności podejmowanej przez organy postępowania przygotowawczego nie jest zapoznanie z cechami i właściwościami rzeczy (np. modelem telefonu/smartfona), tylko dostęp do zawartości urządzenia, to stosowanie innego trybu niż przeszukiwanie, jest nieprawidłowe.

Obecnie telefon (smartfon) nie jest jedynie urządzeniem służącym do prowadzenia rozmów i komunikowania się na odległość. Urządzenie to stało się rozbudowanym

¹ Wystąpienie generalne dostępne na stronie: <https://bip.brpo.gov.pl/pl/content/rpo-nosniki-danych-ogledziny-wewnetrzne-ms-pk>.

² Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (t.j. Dz. U. z 2026 r. poz. 490 z późn. zm.).

archiwum informacji dotyczących niemal wszystkich sfer życia użytkownika. Może zawierać jego/jej wieloletnią korespondencję, fotografie i nagrania, historię przemieszczania się, dane dotyczące stanu zdrowia (np. wyniki badań lekarskich), informacje finansowe, dokumenty, kalendarz, listę kontaktów oraz dostęp do rachunków bankowych, poczty elektronicznej i innych usług cyfrowych. Informacje te mogą dotyczyć nie tylko właściciela lub użytkownika urządzenia, lecz również osób trzecich (np. rodziny). Dostęp do zawartości telefonu pozwala więc na odtworzenie szerokiego obrazu życia prywatnego jednostki, jej relacji osobistych, aktywności zawodowej, poglądów oraz sposobu spędzania czasu. **Tak daleko idąca ingerencja w prywatność jednostki powinna zostać obwarowana adekwatnymi gwarancjami proceduralnymi, w tym następczą kontrolą sądową.**

Wystąpienie generalne z dnia 31 marca 2025 r. ponownie przesyłam w załączeniu. **Chciałabym jednak po raz kolejny zwrócić uwagę na zasadnicze wątpliwości odnośnie do trybu zapoznawania się z zawartością telefonu komórkowego (smartfona) w trybie oględzin.**

Prokuratura Krajowa dopuszcza dwa sposoby uzyskiwania informacji zawartych w urządzeniach/systemach zawierających dane informatyczne dla potrzeb postępowania karnego – przeszukanie oraz oględziny³. 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, a jego dysponentowi lub użytkownikowi zapewniono gwarancje procesowe przewidziane przepisami k.p.k.”⁴. 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.”⁵.

³ 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.

⁴ 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.

⁵ 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>.

Urządzenie – nośnik informacji – może znaleźć się w dyspozycji organu procesowego⁶ 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 (*fishing expeditions*⁷), a po taki wstępnym ustaleniu przydatności informacji – „zmieniają 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

⁶ Poza sytuacjami takimi jak znalezienie urządzenia.

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

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.

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 odmawianie ich przyjęcia przez sąd i przekazywanie 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 nieprzekazywanie 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 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 dóbr⁸. 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

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

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 elektronicznej⁹. Wydaje się zatem, że osoba, wobec której kierowane jest żądanie wydania telefonu, będzie bardziej skłonna je wydać 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 Policji¹⁰, „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, które lub programów komputerowych umożliwiających przełamanie zabezpieczeń¹¹, co będzie wiązało się z pozbawieniem możliwości korzystania z telefonu.

Z przepisów k.p.k. ani wytycznych KGP 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” odcisku palców w celu odblokowania urządzenia

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.

¹⁰ Dz.Urz.KGP. z 2017, poz. 59.

¹¹ Zob. § 8 ust. 10 wytycznych nr 3 KGP; Dz.Urz.KGP. z 2017, poz. 59.

(art. 74 § 1 pkt 1 k.p.k.¹²), czy odblokowując urządzenie przykładając telefon blisko twarzy, aktywując usługę Face ID, czy zbliżone usługi na innych modelach telefonów oparte na analizie tęczy 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).

Jeśli zaś chodzi o ingerencję w prawo do prywatności jednostki w kontekście dostępu do elektronicznych nośników danych, to warto zwrócić uwagę na kontekst prawnomiędzynarodowy. **Chociaż Europejski Trybunał Praw Człowieka jest powściągliwy, gdy chodzi o wprowadzenie kontroli uprzedniej w przypadku czynności przeszukania, w tym przeszukania elektronicznych nośników danych¹³, to zwraca uwagę na konieczność sądowej kontroli tego rodzaju czynności w formie kontroli ex post¹⁴.** Brak uprzedniego sądowego nakazu w przypadku przeszukania może zostać zrównoważony dostępnością sądowej kontroli ex post factum¹⁵.

Gdy prawo krajowe nie przewiduje uprzedniej kontroli sądowej zgodności z prawem i konieczności zastosowania czynności dochodzeniowej ingerującej w prywatność jednostki, to muszą istnieć inne gwarancje, w szczególności dotyczące sposobu wykonania nakazu przeszukania, czy następczej kontroli sądowej, które równoważyłyby „braki” na wstępnym etapie wykonania czynności¹⁶. W wyroku w sprawie Modestou przeciwko Grecji, ETPC przypominał, że kontrola sądowa czynności przeszukania, w tym przeszukania urządzenia elektronicznego (cyfrowego nośnika danych) musi być skuteczna w okolicznościach konkretnej sprawy¹⁷. We wskazanym wyżej orzeczeniu, brak było zarówno kontroli uprzedniej (przeszukanie nastąpiło na podstawie bardzo ogólnie sformułowanego prokuratorskiego nakazu przeszukania), a kontrola następca

¹² 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”.

¹³ Zob. m.in. wyrok ETPC z 30 maja 2017 r. w sprawie Trabajo Rueda p. Hiszpanii, skarga nr 32600/12.

¹⁴ Zob. wyrok ETPC z dnia 16 marca 2016 r. w sprawie Modestou p. Grecji, skarga nr 51693/13, § 49.

¹⁵ Wyrok ETPC z dnia 15 lutego 2011 r. w sprawie Heino przeciwko Finlandii, skarga nr 56720/09, § 45.

¹⁶ Zob. wyrok ETPC z dnia 16 marca 2016 r. w sprawie Modestou p. Grecji, skarga nr 51693/13, § 49.

¹⁷ Zob. wyrok ETPC z dnia 16 marca 2016 r. w sprawie Modestou p. Grecji, skarga nr 51693/13, § 49-52.

miała miejsce po ok. 2 latach od przeszukania i zatrzymania rzeczy (w tym m.in. komputerów). Kontrola następca powinna uwzględniać kryteria legalności, konieczności ingerencji w prawo do prywatności w społeczeństwie demokratycznym i proporcjonalności. Musi ona gwarantować weryfikację podstawy faktycznej i prawnej czynności¹⁸. **Kontroli następcej czynności ingerującej w prywatność jednostki nie może zastąpić późniejsza ocena np. dopuszczalności materiału dowodowego pozyskanego w drodze przeszukania/zatrzymania elektronicznego nośnika danych na etapie postępowania sądowego.** Kluczowa jest możliwość zbadania prawidłowości samej czynności oraz – ewentualne – zapewnienie odpowiedniego środka naprawczego.

W sprawach, w których na elektronicznych nośnikach danych mogą znajdować się informacje objęte tajemnicą zawodową, np. tajemnicą, adwokacką¹⁹, czy notarialną²⁰, ocena ETPC jest bardziej rygorystyczna.

W wyroku w sprawie Sărgava przeciwko Estonii²¹, Trybunał strasburski analizował kwestię gwarancji proceduralnych w przypadku przeszukania i zatrzymania nośników danych zawierających tajemnicę adwokacką. ETPC zwrócił uwagę, że prawo estońskie przewidywało ogólne gwarancje dotyczące czynności przeszukania i zatrzymania rzeczy, w tym szczególne gwarancje dotyczące pomieszczeń adwokatów (osób świadczących pomoc prawną)²². Przeszukanie, zgodnie z regulacjami estońskimi, może bowiem zostać przeprowadzone, jeżeli istnieje uzasadnione podejrzenie, że w przeszukiwanym miejscu znajduje się poszukiwany przedmiot, a „nakaz przeszukania” powinien, co do zasady, określać przedmiot, miejsce i przyczyny przeszukania²³. Jeżeli przeszukanie ma zostać przeprowadzone w kancelarii adwokackiej, musi być ono zatwierdzone postanowieniem sędziego do spraw postępowania przygotowawczego albo orzeczeniem sądu i przeprowadzone w obecności adwokata, którego pomieszczenia są przeszukiwane, lub innego adwokata. Jednocześnie, prawo krajowe pozostawia margines swobody odnośnie do formy uzasadnienia decyzji o przeszukaniu (tj. czy

¹⁸ Wyrok ETPC z dnia 2 października 2014 r. w sprawie DELTA PEKÁRNY a.s. przeciwko Republice Czeskiej, skarga nr 97/11, § 83-87.

¹⁹ Zob. wyrok ETPC z dnia 5 listopada 2024 r. w sprawie Nezirić przeciwko Bośni i Hercegowinie, skarga nr 4088/21.

²⁰ Zob. wyrok ETPC z dnia 29 kwietnia 2025 r. w sprawie Kavečanský przeciwko Słowenii, skarga nr 49617/22.

²¹ Wyrok ETPC z dnia 16 listopada 2021 r. w sprawie Sărgava przeciwko Estonii skarga nr 698/19.

²² Wyrok ETPC z dnia 16 listopada 2021 r. w sprawie Sărgava przeciwko Estonii skarga nr 698/19, § 96.

²³ Wyrok ETPC z dnia 16 listopada 2021 r. w sprawie Sărgava przeciwko Estonii skarga nr 698/19, § 31.

będzie ono w pełni uzasadnioną decyzją procesową, czy jedynie w formie adnotacji²⁴). ETPC zwrócił jednak uwagę na brak praktycznych ram ochrony tajemnicy adwokackiej w sytuacji, w której zatrzymywane są elektroniczne nośniki danych. **O ile bowiem selekcja lub rozdzielenie dokumentów objętych i nieobjętych tajemnicą adwokacką jest istotna w odniesieniu do dokumentów papierowych, o tyle nabiera jeszcze większego znaczenia, gdy treści objęte tajemnicą stanowią część większych zbiorów danych zapisanych cyfrowo**²⁵. Jak słusznie zauważył ETPC, „w takiej sytuacji, nawet jeżeli zainteresowany adwokat lub jego przedstawiciel jest obecny w miejscu przeszukania, szybkie rozróżnienie w toku czynności, które dokładnie pliki elektroniczne są objęte tajemnicą adwokacką, a które nie, może okazać się trudne.”²⁶. Kolejnym problemem z perspektywy ochrony tajemnic zawodowych, w szczególności tajemnicy związanej z udzielaniem pomocy prawnej, jest wykonywanie kopii lustrzanych. Z jednej strony, wykonanie kopii umożliwia szybsze zwrócenie urządzeń, co ma istotne znaczenie w pracy m.in. adwokatów, oraz gwarantuje, że treści na nim zapisane nie zostaną zmanipulowane²⁷. Z drugiej strony samo wykonanie kopii lustrzanej nie rozwiązuje problemu ochrony danych objętych tajemnicą zawodową. Konieczne jest bowiem ustanowienie reguł określających sposób dalszego postępowania ze skopiowanymi danymi²⁸. **ETPC podkreślił, że prawo powinno zabezpieczać je przed nieuprawnionym lub nieudokumentowanym dostępem oraz przetwarzaniem od chwili zatrzymania nośnika aż do jego zwrotu albo zniszczenia**²⁹.

W sprawie Särgava przeciwko Estonii, mimo wskazania we wniosku prokuratora, że na urządzeniach mogą znajdować się dane i informacje związane z wykonywaniem zawodu adwokata, decyzja sędziego nie zawierała żadnych postanowień/adnotacji, które gwarantowałyby poszanowanie tajemnicy zawodowej³⁰. Skarżący został jedynie poinformowany o tym, że przeszukanie zawartości jego laptopa i telefonu będzie prowadzone przy użyciu słów kluczowych. Obowiązek zastosowania takiej metody nie wynikał ani z ustawy, ani z wydanego przez sąd nakazu przeszukania, i był decyzją

²⁴ Wyrok ETPC z dnia 16 listopada 2021 r. w sprawie Särgava przeciwko Estonii skarga nr 698/19; § 97.

²⁵ Wyrok ETPC z dnia 16 listopada 2021 r. w sprawie Särgava przeciwko Estonii skarga nr 698/19; § 99.

²⁶ Wyrok ETPC z dnia 16 listopada 2021 r. w sprawie Särgava przeciwko Estonii skarga nr 698/19; § 99.

²⁷ Wyrok ETPC z dnia 16 listopada 2021 r. w sprawie Särgava przeciwko Estonii skarga nr 698/19; § 100.

²⁸ W tym także, ewentualną kwestię usuwania danych, które zawierają informacje objęte tajemnicą zawodową.

²⁹ Wyrok ETPC z dnia 16 listopada 2021 r. w sprawie Särgava przeciwko Estonii skarga nr 698/19; § 102-103.

³⁰ Wyrok ETPC z dnia 16 listopada 2021 r. w sprawie Särgava przeciwko Estonii skarga nr 698/19; § 104.

organów prowadzący postępowanie przygotowawcze³¹. ETPC zwrócił również uwagę, że przepisy krajowe nie określały sposobu rozstrzygania sporów między organami postępowania a adwokatem dotyczących wyboru słów kluczowych, metody filtrowania danych czy zakresu materiałów objętych tajemnicą. Chociaż prawo estońskie przewidywało możliwość zaskarżenia czynności organów prowadzących postępowanie, nie gwarantowało, że dane, co do których istniał spór dotyczący ochrony tajemnicy adwokackiej, nie zostaną im udostępnione przed przeprowadzeniem przez sąd konkretnej i szczegółowej kontroli³². Jednocześnie, Trybunał wskazał, że nie ma podstaw do rozstrzygnięcia, czy doszło do naruszenia poufności kontaktów w relacji adwokat-klient. Niemniej, „sam brak gwarancji proceduralnych odnoszących się konkretnie do ochrony tajemnicy adwokackiej nie spełniał jednak wymagań wynikających z kryterium, zgodnie z którym ingerencja musi być zgodna z prawem w rozumieniu art. 8 ust. 2 Konwencji”³³.

Porównując wymagania, jakie wynikają z orzecznictwa ETPC w kwestii dostępu do informacji zawartych na elektronicznych nośnikach danych, warto zwrócić uwagę, że dostęp do elektronicznych nośników danych w formie „oględzin wewnętrznych” nie gwarantuje ani następcej kontroli sądowej ani ochrony tajemnic zawodowych. Brak jest także jasnych procedur dotyczących wykonywania kopii lustrzanych, dopuszczalnego zakresu kopiowania materiałów oraz procedur usuwania materiałów zbędnych dla postępowania karnego. Jednocześnie, nawet jeśli dostęp do zawartości elektronicznych nośników danych nastąpił w prawidłowej formie, tj. w formie przeszukania z art. 236a k.p.k., to obecne przepisy – nakazujące stosować „odpowiednio” regulacje stworzone dla potrzeb przeszukania „w świecie analogowym”, nie chronią przed arbitralną ingerencją w prawo do prywatności jednostki.

Jak to już zostało poprzednio wskazane w wystąpieniu generalnym z dnia 31 marca 2025 r.³⁴, obecne uregulowania 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

³¹ Wyrok ETPC z dnia 16 listopada 2021 r. w sprawie Särgava przeciwko Estonii skarga nr 698/19; § 105. Warto także podkreślić, że ETPC odniósł się do wyboru słów kluczowych, zwracając uwagę, że miały one bardzo szeroki zakres, a skarżący nie bał udziału w czynności przeszukania urządzeń elektronicznych z wykorzystaniem słów kluczowych.

³² Wyrok ETPC z dnia 16 listopada 2021 r. w sprawie Särgava przeciwko Estonii skarga nr 698/19; § 107 i cytowane tam orzecznictwo ETPC.

³³ Wyrok ETPC z dnia 16 listopada 2021 r. w sprawie Särgava przeciwko Estonii skarga nr 698/19; § 109.

³⁴ Wystąpienie generalne dostępne na stronie: <https://bip.brpo.gov.pl/pl/content/rpo-nosniki-danych-ogledziny-wewnetrzne-ms-pk>.

Krajowej – są jeszcze mniej gwarancyjne dla jednostki, a ustawodawca nie wprowadza odpowiednich zabezpieczeń przed arbitralnością działania organów władzy publicznej³⁵. **Celowe 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.³⁶).** Rozważenia wymaga to, czy nowe przepisy powinny być uregulowane w osobnym rozdziale k.p.k. (np. w nowo dodanym rozdziale 25a k.p.k., czy 36a k.p.k.), czy jako grupa przepisów w ramach już istniejącego podziału Kodeksu postępowania karnego. 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 zaciera się różnica między statycznym a dynamicznym pozyskiwaniem danych³⁷. Dostęp do danych zapisanych na elektronicznym nośniku danych, biorąc pod uwagę zakres historyczny tych danych, może w porównywalnym stopniu ingerować w sferę

³⁵ 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.

³⁶ Mogą być natomiast wykonywane w formie mniej gwarancyjnej dla jednostki, tj. w drodze czynności operacyjno-rozpoznawczych, m.in. na podstawie art. 19 ust. 6 pkt 4 ustawy o Policji (ustawa z dnia 6 kwietnia 1990 r. o Policji; t.j. Dz. U. z 2025 r. poz. 636 z późn. zm.).

³⁷ 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.

prywatności jednostki, co ich dynamiczne pozyskiwanie w czasie rzeczywistym³⁸. **Rozważenia wymaga, jaki organ byłby uprawniony do zarządzania 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.**

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 Obywatelskich³⁹, ponownie 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 wdzięczna za poinformowanie mnie o stanowisku zajęтым w przedstawionej materii w terminie 30 dni od daty otrzymania niniejszego wystąpienia.**

Z wyrazami szacunku

Sylwia Gregorczyk-Abram

Rzecznik Praw Obywatelskich

/-wydano i podpisano elektronicznie/

Załączniki:

³⁸ 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.

³⁹ Ustawa z dnia 15 lipca 1987 r. o Rzeczniku Praw Obywatelskich (Dz. U. z 2024 r., poz. 1264).

- wystąpienie generalne RPO do Prokuratora Generalnego – Ministra Sprawiedliwości z dnia 31 marca 2025 r.