Wojciech Jasiński
Uniwersytet Wrocławski, Polska
wojciech.jasinski@uwr.edu.pl
ORCID: 0000-0002-7427-1474

https://doi.org/10.26881/gsp.2024.2.04

O potrzebie zmian w regulacjach prawnych dotyczących pozyskiwania informacji pochodzących z nośników danych dla celów postępowania karnego[1]

Wprowadzenie

Jednym z istotnych wyznaczników współczesnego rozwoju społecznego jest możliwość gromadzenia na nośnikach coraz większej ilości różnorakich danych, które mogą być łatwo przenoszone albo z których można swobodnie korzystać w różnych lokalizacjach. Nie wdając się w szczegółowe i techniczne w swojej istocie rozważania dotyczące sposobu rozumienia pojęć „dane" i „nośnik", przyjmuję na potrzeby niniejszego opracowania, że dane powinny być rozumiane jako reprezentacja faktów lub pojęć przekazanych w sposób sformalizowany[2]. Natomiast nośnik rozumiany jest jako wszelkie środki przenoszenia danych niosących jakiekolwiek informacje[3]. Największe znaczenie mają współcześnie dane cyfrowe i to na nich zostanie skupiona uwaga w artykule. Co oczywiste, takie dane w wielu sytuacjach mogą się okazać istotne nie tylko z perspektywy codziennej aktywności ludzi, ale także dla toczących się postępowań karnych. Przykłady można byłoby mnożyć. Najbardziej klasyczne wydaje się sięgnięcie po dane cyfrowe wytworzone przez określone osoby intencjonalnie, takie jak różnorakie dokumenty tekstowe, zdjęcia czy filmy. Bardzo duże znaczenie ma jednak także szereg danych, które powstają po prostu w związku z codzienną aktywnością jednostki (dane dotyczące wykonywanych połączeń telefonicznych, odwiedzanych stron internetowych, aktywności w ramach różnorakich programów i systemów wymiany danych etc.). Kwestią zasadniczą jest zatem to, jak uregulować dostęp do takich danych, aby z jednej strony umożliwić efektywne gromadzenie informacji, które pozwolą

[1] Artykuł powstał w ramach projektu naukowego finansowanego przez Narodowe Centrum Nauki nr 2018/30/E/HS5/00338 pt. „Uzasadnione przeszukanie. Między efektywnością ścigania a prawami jednostki". Projekt zrealizowano w Inkubatorze Doskonałości Naukowej – Centrum Digital Justice funkcjonującym w ramach Inicjatywy Doskonałości Naukowej – Uczelni Badawczej Uniwersytetu Wrocławskiego.

[2] A. Lach, *Dowody elektroniczne w procesie karnym*, Toruń 2004, s. 20.

[3] P. Lewulis, *Dowody cyfrowe – teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*, Warszawa 2021, s. 46.

skutecznie zwalczać przestępczość, a z drugiej strony zapewnić niezbędne gwarancje poszanowania praw jednostki, w tym zwłaszcza prawa do prywatności, i uniemożliwić nadużywanie środków inwigilacji przez organy państwa.

Zarysowana powyżej kwestia ma bardzo istotne znaczenie przede wszystkim z jednego zasadniczego powodu. Należy bowiem zauważyć, że łatwość w gromadzeniu danych cyfrowych na nośnikach sprawia, iż uzyskując dostęp w szczególności do telefonu komórkowego i komputera danej osoby, organy postępowania karnego są w stanie zebrać nieporównywalnie więcej danych niż w czasach, gdy takie możliwości nie istniały. Z tej zatem perspektywy rośnie znaczenie metod inwigilacji pozwalających uzyskać dostęp do wskazanych danych. W tym kontekście w zasadzie automatycznie, już na samym wstępie rozstrzygania kwestii legislacyjnych, pojawia się pytanie, czy konstruowanie optymalnego modelu pozyskiwania danych cyfrowych na potrzeby postępowania karnego powinno odbywać się przez poszukiwanie analogii między zbieraniem informacji w czasach, kiedy ich głównym źródłem były przedmioty materialne z miejsca zamieszkania, pracy oraz depozycje osób mających kontakt z daną osobą, a ich pozyskiwaniem dzisiaj, gdy wgląd choćby w telefon komórkowy czy komputer osobisty i przechowywane w nim dane pozwala szybciej i dużo dogłębniej zebrać informacje na temat określonej osoby. Odpowiedź na to pytanie powinna być negatywna. Z powodów wskazanych powyżej nie można postawić znaku równości między pozyskiwaniem informacji w erze cyfrowej i przedcyfrowej. Zarówno dostępność, jak i wolumen danych, jakie są możliwe do zdobycia obecnie, a także zakres informacji o życiu jednostki, jaki da się z nich pozyskać, są nieporównywalne z analogicznymi wskaźnikami, odnoszącymi się do klasycznych metod wykrywczych z ery przedcyfrowej (np. przeszukanie pomieszczeń, kontrola i utrwalanie rozmów telefonicznych). To sprawia, że ingerencja w prywatność jednostki, a w konsekwencji także możliwość nadużyć i ich negatywne skutki są również nieporównywalnie większe niż wcześniej. Trafnie wskazana różnica została dostrzeżona przez amerykański Sąd Najwyższy w wyroku w sprawie Riley *v.* California[4]. Abstrahując od meritum tej sprawy, dotyczącego dopuszczalności przeszukania osoby bez nakazu sądowego w trakcie zatrzymania, należy odnotować, że skład orzekający podkreślił istotną różnicę między przeszukaniem znajdującego się w kieszeni jednostki telefonu komórkowego, który zawiera dużą ilość prywatnych informacji, a przeszukaniem np. portfela, co byłoby swoistym odpowiednikiem tej czynności w erze przedcyfrowej[5].

Zobrazowana przez amerykański Sąd Najwyższy różnica w pozyskiwaniu informacji na potrzeby postępowania karnego sprawia, że konieczne jest wypracowanie podejścia do analizowanej kwestii, które uwzględni tę ważną specyfikę. Oczywiście nie oznacza to całkowitego zerwania z kształtowanymi przez lata sposobami definiowania

4 Riley *v.* California, 573 U.S. 373 (2014).

5 Szerzej o tej kwestii, a także podejściu do przeszukania telefonu komórkowego w orzecznictwie kanadyjskiego Sądu Najwyższego por. K. Kremens, *O znaczeniu prawa porównawczego dla nauki polskiego procesu karnego na przykładzie przeszukań telefonów komórkowych* [w:] *W pogoni za rzetelnym procesem karnym. Księga dedykowana Profesorowi Stanisławowi Waltosiowi*, red. D. Szumiło-Kulczycka, Warszawa 2022, s. 556–559.

i regulowania dowodowych czynności wykrywczych. Nadal więc, co oczywiste, będą musiały pojawiać się odniesienia do aktualnie dostępnych sposobów konceptualizacji procesu pozyskiwania informacji dla celów procesowych. Tym niemniej, jak zostało to już wskazane powyżej, musi odbywać się to w sposób uwzględniający charakter ingerencji w prywatność i nową jakość, jaką era cyfrowa wniosła w omawianym zakresie, a nie przez proste analogie do czasów przedcyfrowych.

Ramy niniejszego opracowania nie pozwalają na kompleksowe omówienie problematyki ustawowej regulacji pozyskiwania danych pochodzących z nośników na potrzeby procesu karnego. Uwaga zostanie zatem skupiona na wykazaniu wadliwości obowiązujących obecnie regulacji prawnych w tym zakresie, które uzasadniają konieczność wypracowania nowych unormowań. Jest to istotna kwestia, gdyż już sam sposób regulacji problematyki pozyskiwania danych cyfrowych w procesie karnym, a nie tylko jej zakres, ma niebagatelne znaczenie dla efektywności przyjętych rozwiązań. Należy także zastrzec, że przedmiotem rozważań są ustawowe regulacje o charakterze karnoprocesowym. Choć więc w dalszej części pojawią się nawiązania do czynności operacyjno-rozpoznawczych oraz standardów ponadustawowych, które niewątpliwie mają znaczenie dla tytułowej problematyki, to jednak kwestie te nie będą szczegółowo rozwijane. Podobnie, uwaga w niniejszym artykule została skupiona na pozyskiwaniu danych, które potencjalnie mogą stać się dowodem w postępowaniu karnym. Ze względu na ramy opracowania poza jego zakresem znalazła się kwestia możliwości wykorzystania takich danych w procesie.

1. Obowiązująca regulacja pozyskiwania informacji pochodzących z nośników danych dla celów postępowania karnego i jej mankamenty

Już pobieżna analiza przepisów Kodeksu postępowania karnego[6] wskazuje, że ustawodawca odnosi się wprost do kwestii pozyskiwania danych znajdujących się na nośnikach bardzo lakonicznie. Jedyne w zasadzie unormowania, które dotyczą, obrazowo rzecz ujmując, sfery wirtualnej, to art. 236a k.p.k., który stanowi, że przepisy rozdziału 25 k.p.k. dotyczącego przeszukania i zatrzymania rzeczy 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, oraz przepisy art. 218–218b k.p.k., które dotyczą danych telekomunikacyjnych. Znaczenie z omawianej perspektywy ma także art. 241 k.p.k., który przewiduje, że przepisy rozdziału 26 k.p.k. odnoszące się do kontroli i utrwalania rozmów telefonicznych stosuje się odpowiednio do kontroli oraz do utrwalania przy użyciu środków technicznych treści innych rozmów lub

[6] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (tekst jedn.: Dz. U. z 2024 r., poz. 37 ze zm.) (dalej: k.p.k.).

przekazów informacji, w tym korespondencji przesyłanej pocztą elektroniczną. W kontekście danych znajdujących się na nośnikach kluczową rolę odgrywa niewątpliwie art. 236a k.p.k.

Analizując przepisy regulujące problematykę prawnodowodową, trudno oprzeć się wrażeniu, że polski ustawodawca na trwałe pozostał w świecie analogowym, nie dostrzegając, jakie zmiany digitalizacja przyniosła w codziennym (także przestępczym) życiu. Już na pierwszy rzut oka widoczny jest bowiem paradoks, że niezwykle istotna przestrzeń, z której można pozyskiwać cenne dla procesu karnego informacje, nie jest przez ustawodawcę regulowana wprost, ale za pomocą bardzo ogólnego odesłania. Oczywiście przynajmniej teoretycznie sama przyjęta technika legislacyjna nie musi świadczyć o wadliwości omawianej regulacji. W tym wypadku należy jednak odnieść się krytycznie do dokonanego przez ustawodawcę wyboru. O ile obowiązujące unormowania prawne można byłoby ocenić, ze względu na kontekst społeczny, jako chociaż częściowo satysfakcjonujące w 2003 i 2004 r., gdy przepisom tym nadano obecny kształt, o tyle bez wątpienia nie można tego samego stwierdzić w trzeciej dekadzie XXI w. Za takim wnioskiem przemawia szereg argumentów odnoszących się do obserwacji praktyki ich stosowania, a także ich funkcjonalności. Nie można więc zgodzić się z wyrażanym w doktrynie w kontekście art. 236a k.p.k. stanowiskiem przeciwnym, opartym na założeniu, że wprowadzenie unormowań, które doprecyzowałyby obowiązujące regulacje, okazałoby się dysfunkcjonalne. Zakłada ono, że „zbyt kazuistyczna regulacja omawianej czynności procesowej mogłaby przynieść skutek odmienny od założonego i przyczynić się do powstania jeszcze większej liczby problemów i wątpliwości, kiedy można, a kiedy nie można realizować zdalne przeszukanie, lub zbytnio zawęzić sytuacje, w których jest ono dozwolone. Lepiej wyznaczać i wytyczać pewne uniwersalne przepisy pasujące do szybko zmieniającej się taktyki i techniki działań w cyberprzestrzeni, aniżeli bardzo szczegółowo określać hipotetyczne stany faktyczne, kiedy czynność jest dopuszczalna”[7]. Wniosek ten jest nietrafny z kilku zasadniczych powodów. Po pierwsze, wskazana bardzo ogólna regulacja nie sprzyja jednolitości stosowania prawa. Po drugie, obowiązujące unormowania wymagają zmian, gdyż nie zapewniają odpowiedniego poziomu gwarancyjności. Poglądy wskazujące na ich antygwarancyjność były już zresztą prezentowane w doktrynie[8]. Po trzecie, obowiązujące przepisy, dość zresztą paradoksalnie, nie gwarantują również efektywności ścigania, co – biorąc pod uwagę rozwój przestępczości w wymiarze wirtualnym – jest równie istotnym problemem jak nieproporcjonalna inwazyjność stosowanych metod

[7] P. Opitek, *Przeszukanie na odległość jako czynność procesowa (art. 236a k.p.k.)*, Prok. i Pr. 2020, nr 9, s. 126.

[8] Za precyzyjnym uregulowaniem przeszukania zdalnego opowiadał się już przed ponad dekadą A. Lach – zob. *idem*, *Przeszukanie na odległość systemu informatycznego*, Prok. i Pr. 2011, nr 9, s. 78. Tak też w: *idem*, *Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego*, Prok. i Pr. 2003, nr 10, s. 25. Podobnie krytycznie: K. Kremens, *Granice ingerencji w prawo do prywatności i prawo własności w postępowaniu karnym* [w:] *Model dopuszczalnej ingerencji w prawa wolności jednostki w procesie karnym/The Model of Acceptable Interference with the Rights and Freedoms of an Individual in the Criminal Process*, red. J. Skorupka, Warszawa 2019, s. 289–292.

wykrywczych. Po czwarte, analiza porządków prawnych innych państw wskazuje, że wprowadzenie szczegółowych regulacji dotyczących pozyskiwania informacji pochodzących z nośników danych nie jest postrzegane jako dysfunkcjonalne, a wręcz przeciwnie, jako konieczny krok do zagwarantowania właściwego poziomu ochrony prawnej. Wskazane kwestie zostaną omówione kolejno w dalszej części opracowania.

2. Niejednolitość w stosowaniu unormowań dotyczących pozyskiwania informacji pochodzących z nośników danych dla celów postępowania karnego

Analiza praktyki stosowania obecnie obowiązujących przepisów dotyczących pozyskiwania informacji pochodzących z nośników danych dla celów postępowania karnego prowadzi do wniosku, że budzą one wątpliwości. Przeprowadzone badania empiryczne wskazują, że występują rozbieżności w zakresie samego powoływania przez organy ścigania podstaw prawnych w przypadku żądania wydania danych (art. 217, art. 218 i art. 236a k.p.k.)[9]. Trzeba zgodzić się, że kwestia ta z praktycznego punktu widzenia ma drugorzędne znaczenie[10], tym niemniej nie należy zapominać, że adresatami przepisów procesowych są także funkcjonariusze organów ścigania i nie mogą one być konstruowane w sposób, który jest dla tych podmiotów niezrozumiały. Oczywiście problem ten ma szerszy wymiar i jest przejawem ogólnie niskiej świadomości prawnej i technologicznej organów ścigania. Nie zmienia to jednak faktu, że obrazuje również słabość obecnego unormowania problematyki pozyskiwania danych cyfrowych.

W przypadku pozyskiwania danych z nośników pozostających w dyspozycji organów procesowych (w szczególności telefonów komórkowych) zwraca również uwagę rozbieżność w charakterze czynności prawnodowodowej, która jest wykorzystywana do tego celu. Można bowiem dostrzec, że w praktyce sięga się zarówno po oględziny, jak i przeszukanie[11]. W doktrynie trafnie zwraca się uwagę, że pozyskiwaniu danych cyfrowych powinna służyć czynność przeszukania, o czym świadczy treść art. 236a k.p.k.[12] Jak pokazują jednak badania w praktyce, albo z niewiedzy, albo z innych pozamerytorycznych powodów istnieje pokusa sięgania po czynność oględzin, która generuje mniej „problemów" dla funkcjonariuszy organów ścigania. Powyższe wyraźnie więc wskazuje, iż uregulowanie kwestii uzyskiwania danych cyfrowych za pomocą jednego ogólnego odesłania rodzi w praktyce wątpliwości, a dodatkowo, w odniesieniu do kontrowersji dotyczących charakteru czynności dowodowej pozwalającej pozyskać dane (przeszukanie albo oględziny) zidentyfikowana niejednolitość w stosowaniu prawa wpływa także na oferowany jednostce poziom gwarancyjności. Ten ostatni budzi

[9] P. Lewulis, *Dowody cyfrowe*…, s. 143.
[10] *Ibidem*, s. 144.
[11] M. Chrabkowski, *Dostęp do treści korespondencji SMS-owej w telefonie zabezpieczonym na potrzeby sprawy karnej*, „Studia Iuridica Toruniensa" 2018, t. 22, s. 59.
[12] Por. np. *ibidem*; P. Lewulis, *Dowody cyfrowe*…, s. 127.

zresztą wątpliwości również z innych powodów, które zostaną omówione w punkcie czwartym opracowania.

3. Gwarancyjność unormowań dotyczących pozyskiwania informacji pochodzących z nośników danych dla celów postępowania karnego

W kontekście waloru gwarancyjnego unormowań dotyczących pozyskiwania informacji pochodzących z nośników danych dla celów postępowania karnego warto na wstępie zauważyć, że nawet w przypadku uznania, iż dane cyfrowe są pozyskiwane za pomocą przeszukania, a więc na lepszym poziomie gwarancyjności niż oferowanym przez oględziny, poszanowanie zabezpieczonych konstytucyjnie i w wymiarze prawnomiędzynarodowym praw jednostki (w szczególności prawa do prywatności) pozostawia wiele do życzenia. Wiąże się to z faktem, iż przepisy normujące „klasyczne" przeszukanie, do których odsyła art. 236a k.p.k., a więc swoiste unormowania „bazowe", słabo tę gwarancyjność realizują w praktyce. Co prawda unormowania kodeksowe przewidują zabezpieczenia przed nadużywaniem tego środka ingerencji w prawo do prywatności, ale problemem jest zarówno ich niewystarczająca precyzja, jak i realna egzekwowalność. W odniesieniu do tej pierwszej kwestii można wspomnieć przede wszystkim o samych przesłankach i podstawie dowodowej przeszukania, które są bardzo ogólne, a tym samym niespecjalnie zmuszają organy procesowe do wstrzemięźliwości w sięganiu po tę czynność[13]. Osobnym problemem jest też bardzo ogólna klauzula proporcjonalności (art. 227 k.p.k.). Jeżeli miałaby ona być środkiem zmierzającym do podwyższenia ustawowego standardu ochrony praw jednostki, a tak by się wydawało, patrząc na to, że jej wprowadzenie w obecnym kształcie było wynikiem negatywnej oceny tego poziomu przez Trybunał Konstytucyjny[14], to trudno ocenić powyższe działanie jako efektywne. To, że modyfikowanie brzmienia bardzo ogólnych klauzul generalnych przyniesie jakościową zmianę w pracy organów ścigania, można obecnie postrzegać raczej jako płonną nadzieję. W kwestii zaś praktycznej nieskuteczności ustawowych regulacji trzeba zwrócić uwagę zwłaszcza na problematykę przeprowadzania przeszukań w trybie ekstraordynaryjnym przewidzianym w art. 220 § 3 k.p.k. Zastrzeżenia należy sformułować zarówno w odniesieniu do nadużywania takiej możliwości, jak i wadliwie funkcjonującego systemu zatwierdzania wskazanego typu przeszukań. Nie ulega wątpliwości, że w założeniu ustawodawcy tryb z art. 220 § 3 k.p.k. ma charakter wyjątkowy. Doświadczenia praktyczne pokazują jednak, że przeprowadzanie przeszukania bez uprzedniej autoryzacji sądu albo prokuratora jest

[13] Por. K. Kremens, *Przesłanka i podstawa dowodowa przeszukania* [w:] *System prawa karnego procesowego*, t. 8, *Dowody*, cz. 3, red. J. Skorupka, Warszawa 2019, s. 3830–3833.

[14] W uzasadnieniu do projektu ustawy z dnia 14 grudnia 2018 r. o zmianie ustawy o Policji oraz niektórych innych ustaw (Dz. U. poz. 2399), która nadała art. 227 k.p.k. obecne brzmienie, wskazano, że ten akt prawny stanowi wykonanie wyroku Trybunału Konstytucyjnego z dnia 14 grudnia 2017 r. (K 17/14).

w praktyce regułą. W badaniach[15] przeprowadzonych w latach 2020–2021, które objęły 853 sprawy o czyny z art. 278 i art. 279 Kodeksu karnego[16] oraz art. 62 ustawy o przeciwdziałaniu narkomanii[17] z 12 sądów rejonowych (po trzy sądy z apelacji wrocławskiej, gdańskiej, łódzkiej i lubelskiej) zakończone w 2018 r., zidentyfikowano 1340 przypadków przeszukań. W tej liczbie aż 1310 (97,7%) przeszukań zostało dokonanych w trybie art. 220 § 3 k.p.k. Oczywiście nie można zaprzeczyć, że kwalifikacje prawne czynów będących przedmiotem analizowanych postępowań uzasadniają, być może nawet istotnie wyższą niż w innych sprawach, liczbę przeszukań dokonywanych w sytuacji niecierpiącej zwłoki. Symptomatyczne jest jednak to, że w badanych sprawach wielokrotnie i to niekoniecznie w tym samym dniu następowało przeszukanie mieszkania osoby, która była zatrzymywana w związku z podejrzeniem popełniania jednego ze wskazanych powyżej czynów zabronionych. Przeszukanie to odbywało się także z zasady w trybie art. 220 § 3 k.p.k. Wskazuje to zatem na utartą praktykę, w której to przeszukanie bez uprzedniej autoryzacji sądu albo prokuratora stało się wbrew ustawowej logice regułą[18].

Istotne wątpliwości budzi także efektywność kontroli przeszukań dokonywanych w trybie art. 220 § 3 k.p.k. W toku postępowania przygotowawczego czynność taka podlega zatwierdzeniu przez prokuratora. Spośród 1310 zbadanych przeszukań dokonanych w omawianym trybie 1158 (88,3%) zostało zatwierdzonych. W pozostałych przypadkach w zdecydowanej większości spraw w aktach po prostu nie było postanowienia o zatwierdzeniu przeszukania. Jedynie w 13 sprawach wydano postanowienie o odmowie zatwierdzenia przeszukania ze względu na przekroczenie terminu na dokonanie tej czynności[19]. W żadnej ze zbadanych spraw powodem niezatwierdzenia przeszukania nie była niezasadność czy nieproporcjonalność przeprowadzonej

---

[15] Badania aktowe zostały przeprowadzone przez dra K. Jarząbka i dra M. Basę w ramach projektu badawczego „Uzasadnione przeszukanie – między efektywnością ścigania a prawami jednostki" (nr 2018/30/E/HS5/00338) finansowanego przez Narodowe Centrum Nauki i kierowanego przez dr hab. K. Kremens. Szerzej o wynikach badań zob. M. Basa, K. Jarząbek, *Praktyka prowadzenia przeszukań w wypadkach niecierpiących zwłoki – przesłanki i podstawa dowodowa przeszukania*, „Przegląd Sądowy" 2023, nr 6, s. 50–67.

[16] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (tekst jedn.: Dz. U. z 2024 r., poz. 17 ze zm.) (dalej: k.k.).

[17] Ustawa z dnia 29 lipca 2005 r. o przeciwdziałaniu narkomanii (tekst jedn.: Dz. U. z 2023 r., poz. 1939 ze zm.) (dalej: u.p.n.).

[18] Na marginesie warto zwrócić uwagę na skuteczność dokonywanych w omawianych sprawach przeszukań. W sprawach o czyny z art. 62 u.p.n. na 774 przeszukania skutecznych było 370 (48%). Spośród przeszukań w sprawach o czyny z art. 278 i art. 279 k.k. na 566 skutecznych okazało się 179 przeszukań (32%). Co jeszcze bardziej interesujące, w przypadku przeszukań następczych mieszkań w sprawach o czyny z art. 278 i art. 279 k.k. skutecznych było tylko 17,5% przeszukań, a w sprawach o czyny kwalifikowane z art. 62 u.p.n. przeszukania okazały się skuteczne w 24,4%. Trudno jest uzasadnić, jak taka masowa i słabo skuteczna ingerencja w prywatność, w jej wymiarze chronionym notabene konstytucyjnie (art. 50 ustawy zasadniczej gwarantujący nienaruszalność mieszkania), ma się do proporcjonalności ingerencji w prawa jednostki i celowości podejmowania takich działań wykrywczych.

[19] Co interesujące, w 97 przypadkach przeszukań zostały one zatwierdzone mimo przekroczenia terminu określonego w art. 220 § 3 zdanie drugie k.p.k.

czynności. Inną ważną kwestią jest także lakoniczność rozstrzygnięć o zatwierdzeniu przeszukania. W wielu przypadkach (50,1%) uzasadnienie nie odnosiło się ani do faktów, ani do przesłanek przeszukania. Ogólnie dane te wskazują więc na automatyzm i w zasadzie iluzoryczność kontroli prokuratorskiej. Dodatkowym problemem zidentyfikowanym w trakcie badań była również częsta niedookreśloność samego żądania wydania rzeczy. Aż w 56% spraw nie sprecyzowano bowiem poszukiwanego przedmiotu, posługując się sformułowaniami „rzeczy pochodzące z przestępstwa" czy „rzeczy mogące stanowić dowód w sprawie".

Biorąc powyższe pod uwagę, należy skonstatować, że w odniesieniu do pozyskiwania danych cyfrowych i tak nie najlepsza gwarancyjność przepisów o przeszukaniu jest dodatkowo osłabiana dość ogólnym odesłaniem, które pozwala jeszcze bardziej rozmywać znaczenie unormowań limitujących ingerencję w prawa i wolności jednostki.

W kontekście ustawowych unormowań dotyczących zatrzymania rzeczy i przeszukania problemem jest także to, że czynność ta oparta jest częściowo na dobrowolnej współpracy jednostki z organami procesowymi. W praktyce jednak w przypadku osób, które nie posiadają niezbędnej wiedzy fachowej, może dochodzić do sytuacji, w których będą się one czuły zmuszone do współpracy, pomimo tego, że nie będą miały takiego prawnego obowiązku, albo atmosfera kontaktu z funkcjonariuszami organów ścigania sprawi, iż nie będą w stanie dokonać swobodnego i świadomego wyboru w zakresie potencjalnej współpracy. Osobnym problemem może być także wyzyskiwanie przymusowej sytuacji przez funkcjonariuszy zmierzających do zatrzymania rzeczy (danych), np. w postaci groźby zatrzymania urządzeń elektronicznych zawierających dane i faktycznego pozbawienia możliwości codziennego funkcjonowania (zawodowego lub prywatnego). Istniejące w Kodeksie postępowania karnego odesłanie z art. 236a k.p.k. w żaden sposób nie chroni jednostki przed potencjalnymi nadużyciami uprawnień w zakresie możliwości gromadzenia należących do niej lub pozostających w jej dyspozycji danych.

Kolejnym aspektem odnoszącym się do gwarancyjności, na który należy zwrócić uwagę, jest przyjęte przez ustawodawcę ogólne założenie przyświecające regulacjom art. 236 i art. 241 k.p.k. Obecnie obowiązujące unormowania przewidują bowiem, iż pozyskiwanie danych „statycznych", a więc zgromadzonych na określonych nośnikach, powinno być regulowane w sposób analogiczny do czynności przeszukania, a w przypadku komunikacji „w ruchu" według standardu właściwego dla kontroli i utrwalania rozmów (*vide* art. 236a i art. 241 k.p.k. w odniesieniu do poczty elektronicznej). Z pozoru mogłoby się wydawać, że ta analogia ze świata przedcyfrowego jest właściwa również dla rzeczywistości cyfrowej. Trafnie jednak w literaturze kwestionuje się to rozróżnienie, wskazując, że współcześnie dzięki nowym technologiom zaciera się różnica między tym, co statyczne, a tym, co dynamiczne[20]. Ta uwaga potwierdza sygnalizowaną już na wstępie artykułu wadliwość poszukiwania prostej analogii między czynnościami wykrywczymi ery przedcyfrowej i cyfrowej. W przypadku rozmów telefonicznych ich kontrola i utrwalanie są konieczne do tego, aby poznać ich treść. Dodatkowo skala

[20] K. Kremens, *Granice ingerencji*…, s. 290–291.

ingerencji w prywatność jednostki jest na tyle daleko idąca, że ustawodawca wymaga autoryzacji tej metody inwigilacji co do zasady przez sąd i to niezależnie od fazy trwającego postępowania. Przekładając założenia powyższego systemu na komunikację odbywającą się za pomocą poczty elektronicznej czy komunikatorów, należy zauważyć, że w przypadku, gdy udostępnione mają być jej zapisy, to pomimo tego, iż organy ścigania uzyskują dostęp do treści komunikacji (podobnie jak w przypadku rozmów telefonicznych) i skala ingerencji w prywatność jest (a przynajmniej może być) zbliżona, ustawodawca decyduje się na wprowadzenie standardu analogicznego do przeszukania, w którym dostęp do tych wiadomości może zostać uzyskany przez prokuratora w postępowaniu przygotowawczym, a nawet przez funkcjonariuszy organów ścigania (art. 220 § 3 k.p.k.). Powyższe dobrze obrazuje, że analogia oparta na odwołaniu do klasycznych czynności, takich jak przeszukanie oraz kontrola i utrwalanie rozmów, jest w świecie wirtualnym fałszywa. Oczywiście przedstawione uwagi nie oznaczają, 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. Kwestionowanie różnicy między przechwytywaniem w czasie rzeczywistym a uzyskiwaniem dostępu do zapisów komunikacji nie ma zatem na celu zrównania charakteru obu tych czynności, ale odrzucenie argumentu, że dostęp do zapisów nie wymaga takich gwarancji, jak przechwytywanie konwersacji w czasie rzeczywistym.

Na zakończenie warto także krótko nawiązać do standardów ponadustawowych. Nie należy bowiem zapominać, że ingerencja w prawo do prywatności musi spełniać określone wymagania. Zgodnie z art. 8 ust. 2 Europejskiej Konwencji Praw Człowieka[21] jest to możliwe tylko w przypadkach przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób. Wymóg legalności ingerencji w prawo do prywatności zakłada, że „podstawa prawna musi być zatem dostępna dla jednostki, kreować przewidywalne dla niej konsekwencje i być sformułowana dostatecznie precyzyjnie"[22]. Warto zauważyć, że problematyka niedostatecznej jakości prawa krajowego skłaniała już Europejski Trybunał Praw Człowieka (dalej: ETPC) do stwierdzenia naruszenia art. 8 EKPC w kontekście sfery wirtualnej ludzkiego życia. W sprawie Benedik przeciwko Słowenii[23] słoweńskie unormowania dotyczące pozyskiwania adresu IP zostały przez ETPC uznane za niewystarczające

[21] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz. U. z 1993 r. Nr 61, poz. 284) (dalej: EKPC).

[22] W. Jasiński, *Granice ingerencji w prawo do wolności, prawo do własności oraz prawo do nieobciążania się w postępowaniu karnym – standardy europejskie* [w:] *Model dopuszczalnej ingerencji*…, s. 108–109.

[23] Wyrok ETPC z dnia 24 kwietnia 2018 r. w sprawie Benedik *v.* Słowenia, skarga nr 62357/14.

z perspektywy standardu konwencyjnego. Analiza przepisu art. 236a k.p.k. pozwala uznać, że tylko pierwszy z warunków – warunek dostępności – jest spełniony. Trudno bowiem mówić o kreowaniu przewidywalnych konsekwencji i precyzji, gdy odesłanie zawarte we wskazanej jednostce redakcyjnej jest bardzo ogólne i odwołuje się do standardów odnoszących się do zbioru, którego cechy są dość odległe od specyfiki danych cyfrowych.

4. Funkcjonalność unormowań dotyczących pozyskiwania informacji pochodzących z nośników danych dla celów postępowania karnego

Obecnie funkcjonujące regulacje pozwalające na pozyskiwanie danych z nośników nie tylko są wadliwe z perspektywy gwarancyjnej, ale także jedynie w ograniczonym zakresie pozwalają na skuteczne zwalczanie przestępczości. Rzecz bowiem w tym, że odesłanie z art. 236a k.p.k. sprawia, iż możliwość pozyskiwania danych cyfrowych może odbyć się wyłącznie w sposób jawny. Przeszukanie na odległość jest zatem w takich warunkach dopuszczalne, ale tylko z zapewnieniem udziału w czynności osoby, która jest dysponentem określonych danych[24]. Problem jednak w tym, że celowe byłoby także, oczywiście po zabezpieczeniu należytymi gwarancjami, w tym ograniczonym zakresem przedmiotowym, umożliwienie dokonywania przeszukań, które odbywałyby się w sposób tajny. Obecnie obowiązujące przepisy takiego rozwiązania nie przewidują. Wątpliwości rodzą się również w odniesieniu do dopuszczalności tzw. przeszukania rozszerzonego. W tym bowiem przypadku osoba, która jest dysponentem pierwotnego urządzenia albo systemu, nie musi być też dysponentem urządzenia albo systemu wtórnego. To zaś powoduje, że tego ostatniego nie można przeszukać z poszanowaniem odpowiednio stosowanych przepisów o „klasycznym" przeszukaniu[25]. Nie tylko więc wzgląd na gwarancyjność, ale również na efektywność ścigania przestępstw przemawia za nowelizacją obecnych unormowań dotyczących pozyskiwania danych cyfrowych.

Oczywiście należy być świadomym, że *de lege lata* przedstawiony problem można rozwiązać w ten sposób, iż podstawą do przeprowadzenia wskazanych powyżej działań będą nie normy ustawy karnoprocesowej, ale ustaw policyjnych regulujących czynności operacyjno-rozpoznawcze. Te bowiem pozwalają na niejawne pozyskiwanie i utrwalanie danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych (np. art. 19 ust. 6 pkt 4 ustawy o Policji[26]). Rzecz jednak w tym, że różnica między czynnościami procesowymi nakierowanymi na pozyskiwanie dowodów a czynnościami operacyjno-rozpoznawczymi, które także mają taki cel (*vide* art. 19 ust. 1 u.p.), została w polskim porządku prawnym prawie całkowicie zamazana. W konsekwencji przepisy

[24] P. Opitek, *Przeszukanie*…, s. 108 i nn.
[25] A. Lach, *Przeszukanie*…, s. 74; P. Lewulis, *Dowody cyfrowe*…, s. 93–94.
[26] Ustawa z dnia 6 kwietnia 1990 r. o Policji (tekst jedn.: Dz. U. z 2024 r., poz. 145 ze zm.) (dalej: u.p.).

ustaw policyjnych na szeroką skalę służą *de facto* gromadzeniu dowodów na potrzeby postępowania karnego, co stanowi nic innego jak aberrację systemową. Czynności operacyjno-rozpoznawcze powinny być odseparowane od czynności procesowych i to te ostatnie powinny służyć pozyskiwaniu dowodów na potrzeby toczącego się postępowania karnego. W pewnym uproszczeniu należy stwierdzić, że czynności operacyjno-rozpoznawcze powinny mieć zasadniczo cel prewencyjny i wykrywczy, natomiast tylko w bardzo ograniczonym zakresie dowodowy. Jeśli więc zebrany materiał pozwala wnioskować, że zachodzi uzasadnione podejrzenie popełnienia przestępstwa, to w tym momencie reżim dokonywania dalszych czynności powinien być reżimem procesowym, z należytymi gwarancjami dla uczestników postępowania karnego. Tylko w ten sposób da się zapewnić rozsądne rozróżnienie obu reżimów i uniknąć sytuacji, gdy to organy ścigania *de facto* wybierają sposób gromadzenia i utrwalania dowodów. Należy zaakcentować, że poza czystością formy zaproponowany model sprawia, iż przynajmniej teoretycznie działalność organów ścigania podlega kontroli prokuratora będącego gospodarzem toczącego się postępowania przygotowawczego. Umożliwia to efektywniejszy nadzór nad prawidłowością i jakością przeprowadzanych czynności, a zarazem alokuje odpowiedzialność za ich podejmowanie nie tylko na organach ścigania. Oczywiście *de lege lata* pewna doza kontroli prokuratorskiej nad czynnościami operacyjno-rozpoznawczymi funkcjonuje (*vide* zgoda prokuratora na wystąpienie o kontrolę operacyjną). Tym niemniej nie ma ona efektywnego charakteru. Reasumując, wadliwości regulacji karnoprocesowej nie powinny być sanowane za pomocą sięgania po czynności operacyjno-rozpoznawcze. Zabieg ten bowiem pogłębia istniejące obecnie i szkodliwe zamazywanie różnicy między tymi czynnościami a czynnościami procesowymi.

5. Pozyskiwanie informacji pochodzących z nośników danych dla celów postępowania karnego – perspektywa prawnoporównawcza

Jak było to już sygnalizowane na wstępie niniejszego opracowania, nie sposób zgodzić się z argumentem, że obecnie obowiązujących w Polsce regulacji dotyczących pozyskiwania informacji pochodzących z nośników danych nie dałoby się skonstruować w sposób bardziej precyzyjny. Analiza prawnoporównawcza wskazuje, że inne niż Polska kraje europejskie znowelizowały unormowania procesowe, wprowadzając przepisy dotyczące wykorzystania nowych technologii w czynnościach wykrywczych. Przykładem kraju, który dodał takie specjalne regulacje w 2015 r., jest Hiszpania. Nowelizacja dotyczyła m.in. przeszukań nośników danych oraz przeszukań na odległość. Wprowadzone unormowania kodyfikują wcześniejsze orzecznictwo hiszpańskich sądów, które rozstrzygały w kwestii dopuszczalności czynności wprost

nieuregulowanych w ustawie procesowej[27]. Nowe unormowania zawierają nie tylko regulacje dotyczące poszczególnych czynności wykrywczych, ale także zasady ogólne (m.in. konieczności, proporcjonalności) oraz, co szczególnie istotne, wymóg sądowej autoryzacji ich przeprowadzenia (wyjątkowo następczej w przypadkach niecierpiących zwłoki). Warto zauważyć, że szczegółowość regulacji ustawowej w Hiszpanii przejawia się również w wyrażeniu wprost zasady, iż należy unikać zajęcia fizycznych nośników zawierających dane lub pliki komputerowe, jeżeli mogłoby to spowodować poważny uszczerbek dla ich posiadacza lub właściciela, a możliwe jest uzyskanie ich kopii na warunkach gwarantujących autentyczność i integralność danych (art. 588 sexies Ley de Enjuiciamiento Criminal[28]).

Podobne zmiany, choć o znacznie mniejszym zakresie szczegółowości, zostały wprowadzone w 2008 r. we Włoszech. Także w tym przypadku sięgnięcie po czynności wykrywcze z użyciem nowych technologii wymaga co do zasady autoryzacji urzędnika sądowego (sędzia, prokurator). Należy jednak zauważyć, że włoski ustawodawca, regulując zagadnienia dotyczące dowodów elektronicznych, zdecydował się na doprecyzowanie przepisów o przeszukaniu, uznając, że taki zabieg będzie wystarczający. Szybko jednak okazało się, że prosta analogia do przeszukania przedcyfrowego jest zawodna. Dowodem na powyższe było to, że w praktyce do 2017 r. odmawiano podmiotom uprawnionym sądowej kontroli zatrzymania danych cyfrowych, jeżeli uprzednio nastąpił zwrot nośnika, na którym dane te pierwotnie się znajdowały. Uznawano bowiem, że jeśli nośnik został zwrócony, to brakuje podstaw do weryfikacji sądowej samego zatrzymania pochodzących z niego danych. Dopiero orzecznictwo Sądu Kasacyjnego doprowadziło do zmiany powyższego sposobu rozumowania[29]. Ten przykład dobrze obrazuje wyzwania, jakie stawia przed wymiarem sprawiedliwości świat wirtualny.

Na marginesie powyższych uwag warto też odnotować, że w polskiej literaturze formułowane są stanowiska wskazujące, jak zmienić obowiązujące przepisy. Piotr Lewulis stwierdza, że „naczelnym elementem zmian może być wprowadzenie odrębnej czynności procesowej zaprojektowanej ściśle z myślą o zabezpieczaniu treści cyfrowych w różnych okolicznościach (w tym z uwzględnieniem problemu zdalnego dostępu do treści i dostępu do treści ze źródeł otwartych) lub chociażby wyraźne rozszerzenie katalogu przedmiotowego w art. 207 k.p.k. o treści cyfrowe rozumiane w oderwaniu od ich nośników. Warto rozważyć możliwości w zakresie ujednolicenia sposobu stosowania przepisów art. 217 i art. 218 k.p.k. (w zw. z art. 236a k.p.k.) w odniesieniu do

---

[27] Szerzej por. J. Ortiz-Pradillo, *The new regulation of technology-related investigative measures in Spain*, „ERA Forum" 2017, vol. 18, no. 1, s. 425–435; L. Bachmaier Winter, *The handling of digital evidence in Spain* [w:] *Digital Forensic Evidence. Towards common European standards in antifraud administrative and criminal investigation*, eds. M. Caianello, A. Camon, Milano 2021, s. 165–205. W polskiej literaturze zob. M. Kłopocka-Jasińska, *Prawo dowodowe w hiszpańskim procesie karnym* [w:] *System prawa karnego procesowego*, t. 8, *Dowody*, cz. 1, red. J. Skorupka, Warszawa 2019, s. 1475–1488.

[28] Real Decreto de 14 de septiembre de 1882 por el que se aprueba la Ley de Enjuiciamiento Criminal.

[29] Por. L. Bartoli, G. Lasagni, *The handling of digital evidence in Spain* [w:] *Digital Forensic Evidence*…, s. 87–121.

usługodawców internetowych i przedsiębiorców telekomunikacyjnych. Nawet jeżeli błędy w stosowaniu tych przepisów mają nikły wpływ na przebieg postępowania, należy dążyć do ujednolicenia praktyki i uzgodnienia jej z wytycznymi teoretycznymi, chociażby dla zachowania wewnętrznej spójności polskich postępowań karnych. Pomijając korektę w drodze odpowiedniego szkolenia przedstawicieli praktyki, rozważyć można uzupełnienie kręgu zobowiązanych do przekazania danych na gruncie art. 218 k.p.k. o podmioty świadczące usługi drogą elektroniczną w zakresie przetwarzanych przez nie danych"[30]. Autor ten wskazuje także konkretne brzmienie przepisów, które miałyby doprowadzić do korekty wadliwości obecnego stanu prawnego[31].

Podsumowanie

Przytoczone powyżej argumenty potwierdzają, że nie tylko możliwe, ale także pożądane jest znowelizowanie obowiązujących przepisów dotyczących pozyskiwania danych cyfrowych znajdujących się na różnorakich nośnikach. Obowiązujące regulacje są bowiem dalece niewystarczające. Oczywiście zasadnicze pytanie dotyczy kierunku pożądanej reformy. Przytoczone przykłady Hiszpanii i Włoch wskazują, że brak jest jednolitego podejścia do omawianej kwestii w krajach europejskich. Należałoby jednak optować, przez wzgląd na fundamentalne racje związane z koniecznością ochrony prawa do prywatności, aby przyjmowane w Polsce rozwiązania były bliższe hiszpańskim niż włoskim i propozycji przedstawionej w rodzimej literaturze przez P. Lewulisa opierającej dostęp do danych informatycznych na czynności oględzin[32]. Nie chodzi w tym wypadku tylko o optymalny poziom szczegółowości nowych przepisów, ale przede wszystkim o gwarancje dotyczące trybu podejmowania decyzji o zastosowaniu środków wykrywczych. Konieczne jest bowiem zapewnienie, aby w kwestii dostępu do danych cyfrowych rozstrzygał organ niezależny od organów ścigania, który osobiście nie jest zainteresowany wynikiem przeprowadzanych czynności. Tylko taki system ma w praktyce szansę zminimalizować pole do nadużyć. Pytaniem otwartym jest to, jaki to powinien być organ. W polskich realiach naturalną odpowiedzią jest wskazanie na sąd. Warto jednak zauważyć, że wprowadzony system musi zapewniać, iż wyznaczony sędzia będzie kompetentny do kontroli wniosków, będzie dysponował realną możliwością ich weryfikacji, a dodatkowo zostaną zapewnione sprawne kanały komunikacji między sędzią a organami ścigania i prokuratorem oraz dostępność tego pierwszego dla organów ścigania. Na pewno stanowić to będzie wyzwanie organizacyjne oraz instytucjonalne. W tym ostatnim wymiarze istotne będzie rozstrzygnięcie,

---

30 P. Lewulis, *Gromadzenie i ocena dowodów cyfrowych w polskim postępowaniu karnym. Kluczowe wnioski z badań aktowych*, Prok. i Pr. 2022, nr 3, s. 144.

31 P. Lewulis, *Dowody cyfrowe*…, s. 136–138.

32 Uwaga ta dotyczy danych, których pozyskanie stanowi ingerencję w prawo do prywatności jednostki. Osobną kwestią jest pozyskiwanie danych cyfrowych, które takiej ingerencji nie stanowią. W tym wypadku, co oczywiste, standardy gwarancyjne nie muszą być takie same.

czy omawianymi kwestiami powinien zajmować się wyodrębniony korpus sędziowski. Regulacje hiszpańskie (sędzia śledczy podejmujący decyzję co do zasady w ciągu 24 godzin od otrzymania stosownego wniosku, a wyjątkowo w przypadkach niecierpiących zwłoki zatwierdzający czynności policji sądowej *post factum*[33]) wskazują, że wprowadzenie kontroli sądowej jest możliwe. Oczywiście tak sprofilowany system nie gwarantuje, że jak za dotknięciem magicznej różdżki znikną nadużycia. Formalizacja drogi uzyskania zgody, oddanie decyzji w ręce organu bezstronnego (niezainteresowanego osobiście wynikiem podejmowanych czynności) oraz wymaganie uzasadniania wniosków pozwalają jednak przynajmniej ograniczyć możliwość dowolnego uzyskiwania dostępu do danych cyfrowych. Nie wydaje się też, że należałoby obawiać się, iż taki system zniweczy efektywność podejmowanych czynności śledczych. W przypadku jego sprawnego funkcjonowania, a także uwzględniając to, że w wielu sytuacjach gwarancję dostępu do danych stanowi zabezpieczenie samych fizycznych nośników, nie jawi się on z perspektywy potrzeb praktycznych jako z gruntu dysfunkcjonalny.

Bardzo istotne znaczenie w pakiecie potencjalnych zmian ma wprowadzenie przepisów gwarancyjnych dla podmiotów, których dane są pozyskiwane na potrzeby toczącego się postępowania karnego. Powinny one obejmować regulacje zapewniające ochronę przed niepotrzebnym zajmowaniem fizycznych nośników danych, co może być szczególnie dolegliwe dla jednostek, a także stanowić nieformalną metodę wymuszania „współpracy" z organami ścigania, jak również regulacje zapewniające przejrzystość procesu zabezpieczania zatrzymanych danych oraz ich analizy, w tym dostępu podmiotów zainteresowanych i ich przedstawicieli procesowych do czynności podejmowanych w tym celu przez informatyków. Ze względu na specyfikę omawianej materii refleksji wymaga również to, w jakim zakresie można byłoby dopuścić do przeprowadzanych czynności eksperta z zakresu informatyki reprezentującego interesy podmiotu będącego dysponentem danych. Rozwiązania takie są przewidziane we Włoszech (choć np. w postępowaniach karnych prowadzonych przez Guardia di Finanza wynikają one z wewnętrznych dokumentów przyjętych przez ten organ)[34], a także w Hiszpanii[35]. Co ciekawe, w obu tych krajach ważną rolę odgrywają wewnętrzne dokumenty organów ścigania określające standardy dokonywania czynności z urządzeniami elektronicznymi i danymi. Rozważenia wymaga zatem to, w jakim zakresie sposób prowadzenia postępowań, w których pozyskiwane są dane cyfrowe, powinien być regulowany przepisami ustawowymi, a w jakim materia ta mogłaby być regulowana podustawowo czy wręcz wewnętrznymi dokumentami określającymi pewne standardy w tym obszarze.

Do stworzenia wskazanej powyżej regulacji niezbędna jest nie tylko wiedza prawnicza, ale przede wszystkim wiedza z zakresu informatyki. Wypracowanie jej kształtu będzie zatem wymagało powołania zespołów roboczych złożonych z prawników

---

33 Artykuł 588 sexies c Ley de Enjuiciamiento Criminal.

34 Szerzej zob. L. Bartoli, G. Lasagni, *The handling*…, s. 104 i nn.

35 L. Bachmaier Winter, *The handling*…, s. 191 i nn.

(teoretyków i praktyków) oraz specjalistów z zakresu IT. Bez harmonijnej współpracy między tymi grupami trudno bowiem będzie przyjąć regulację, która w odpowiedni sposób odpowie na współczesne wyzwania, jakie stawia przed organami państwa i obywatelami cyfrowa rzeczywistość.

Literatura

Bachmaier Winter L., *The handling of digital evidence in Spain* [w:] *Digital Forensic Evidence. Towards common European standards in antifraud administrative and criminal investigation*, eds. M. Caianello, A. Camon, Milano 2021.

Bartoli L., Lasagni G., *The handling of digital evidence in Spain* [w:] *Digital Forensic Evidence. Towards common European standards in antifraud administrative and criminal investigation*, eds. M. Caianello, A. Camon, Milano 2021.

Basa M., Jarząbek K., *Praktyka prowadzenia przeszukań w wypadkach niecierpiących zwłoki – przesłanki i podstawa dowodowa przeszukania*, „Przegląd Sądowy" 2023, nr 6.

Chrabkowski M., *Dostęp do treści korespondencji SMS-owej w telefonie zabezpieczonym na potrzeby sprawy karnej*, „Studia Iuridica Toruniensa" 2018, t. 22.

Jasiński W., *Granice ingerencji w prawo do wolności, prawo do własności oraz prawo do nieobciążania się w postępowaniu karnym – standardy europejskie* [w:] *Model dopuszczalnej ingerencji w prawa wolności jednostki w procesie karnym/The Model of Acceptable Interference with the Rights and Freedoms of an Individual in the Criminal Process*, red. J. Skorupka, Warszawa 2019.

Kłopocka-Jasińska M., *Prawo dowodowe w hiszpańskim procesie karnym* [w:] *System prawa karnego procesowego*, t. 8, *Dowody*, cz. 1, red. J. Skorupka, Warszawa 2019.

Kremens K., *Granice ingerencji w prawo do prywatności i prawo własności w postępowaniu karnym* [w:] *Model dopuszczalnej ingerencji w prawa wolności jednostki w procesie karnym/The Model of Acceptable Interference with the Rights and Freedoms of an Individual in the Criminal Process*, red. J. Skorupka, Warszawa 2019.

Kremens K., *O znaczeniu prawa porównawczego dla nauki polskiego procesu karnego na przykładzie przeszukań telefonów komórkowych* [w:] *W pogoni za rzetelnym procesem karnym. Księga dedykowana Profesorowi Stanisławowi Waltosiowi*, red. D. Szumiło-Kulczycka, Warszawa 2022.

Kremens K., *Przesłanka i podstawa dowodowa przeszukania* [w:] *System prawa karnego procesowego*, t. 8, *Dowody*, cz. 3, red. J. Skorupka, Warszawa 2019.

Lach A., *Dowody elektroniczne w procesie karnym*, Toruń 2004.

Lach A., *Gromadzenie dowodów elektronicznych po nowelizacji kodeksu postępowania karnego*, „Prokuratura i Prawo" 2003, nr 10.

Lach A., *Przeszukanie na odległość systemu informatycznego*, „Prokuratura i Prawo" 2011, nr 9.

Lewulis P., *Dowody cyfrowe – teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*, Warszawa 2021.

Lewulis P., *Gromadzenie i ocena dowodów cyfrowych w polskim postępowaniu karnym. Kluczowe wnioski z badań aktowych*, „Prokuratura i Prawo" 2022, nr 3.

Opitek P., *Przeszukanie na odległość jako czynność procesowa (art. 236a k.p.k.)*, „Prokuratura i Prawo" 2020, nr 9.

Ortiz-Pradillo J., *The new regulation of technology-related investigative measures in Spain*, „ERA Forum" 2017, vol. 18, no. 1.

Streszczenie

Wojciech Jasiński

O potrzebie zmian w regulacjach prawnych dotyczących pozyskiwania informacji pochodzących z nośników danych dla celów postępowania karnego

W artykule omówiono problematykę regulacji ustawowej dotyczącej karnoprocesowego pozyskiwania informacji pochodzących z nośników danych. W pierwszej kolejności analizie zostały poddane obowiązujące unormowania karnoprocesowe, które oceniono jako niewystarczające i oparte na błędnym założeniu, że ogólne odesłanie do odpowiedniego stosowania przepisów regulujących standardowe czynności wykrywcze jest wystarczające. W opracowaniu zaprezentowano szereg argumentów natury praktycznej, aksjologicznej i gwarancyjnej, które przemawiają za wprowadzeniem bardziej szczegółowych unormowań regulujących omawianą materię. Za takim krokiem przemawia zresztą także analiza efektywności obowiązujących norm karnoprocesowych. Przyjęcie optymalnych regulacji dotyczących pozyskiwania informacji pochodzących z nośników danych wymaga ścisłej współpracy prawników (praktyków i teoretyków) oraz specjalistów z zakresu informatyki. Regulacje te powinny ukształtować autonomiczny reżim pozyskiwania danych, który opierałby się na powierzeniu decyzji o dostępie do nich niezależnemu od organów ścigania podmiotowi, a osobom zainteresowanym zapewniłby możliwość realnej weryfikacji dokonywanych w toku postępowania czynności.

Słowa kluczowe: pozyskiwanie dowodów, dowód cyfrowy, nośnik danych, dane cyfrowe, prawo do prywatności.

Summary

Wojciech Jasiński

On the Need for Changes in the Legal Regulation of Obtaining Information from Data Carriers for the Purposes of Criminal Proceedings

The article discusses the problem of statutory regulation of obtaining information from data carriers for the purposes of criminal proceedings. First, the analysis concerns the existing criminal procedural provisions which have been assessed as insufficient and based on the erroneous assumption that a general reference to the relevant provisions related to search and wire-tapping is sufficient. The article presents a number of practical and axiological arguments in favor of introducing more detailed norms regulating the matter in question. Moreover, an analysis of the effectiveness of the existing criminal procedural norms also argues in favour of such a step. Adopting optimal regulations for gathering information from data carriers requires close cooperation between lawyers (practitioners and theoreticians) and IT specialists. These regulations should shape an autonomous regime for data acquisition, which would be based on entrusting the decision on access to data to an organ independent of law enforcement agencies and would provide the persons concerned with the possibility of a real verification of the activities carried out in the course of the proceedings.

Keywords: evidence gathering, digital evidence, data carrier, digital data, right to privacy.