

DOI: 10.4467/29567610PIB.26.011.23483

**dr hab. Dariusz Brakoniecki**

Szkoła Główna Mikołaja Kopernika

ORCID: 0000-0001-7967-9172

dariusz.brakoniecki@gmail.com

**Gabriela Derehajło**

Szkoła Główna Mikołaja Kopernika

ORCID: 0009-0002-8087-2329

gabriela.derehajlo@vp.pl

**Julia Niemyjska**

Okręgowa Izba Radców Prawnych w Białymstoku

ORCID: 0009-0004-2133-1033

j.niemyjska1234@gmail.com

## PRAWNE UWARUNKOWANIA WYKORZYSTANIA MEDIÓW CYFROWYCH W PROCESACH POSZUKIWAWCZYCH

### LEGAL CONDITIONS FOR THE USE OF DIGITAL MEDIA IN SEARCH OPERATIONS

#### **Streszczenie**

Artykuł podejmuje problematykę wykorzystania mediów cyfrowych i śladów cyfrowych w poszukiwaniach osób zaginionych w Polsce, analizując ją z perspektywy prawnej, technologicznej i etycznej. Autorzy wskazują, że dynamiczny rozwój technologii informacyjno-komunikacyjnych zasadniczo zmienił charakter działań poszukiwawczych, czyniąc dane generowane przez urządzenia mobilne, media społecznościowe, aplikacje lokalizacyjne czy systemy monitoringu jednym z kluczowych zasobów operacyjnych. Szczególną uwagę poświęcono znaczeniu śladów cyfrowych – zarówno aktywnych, jak i pasywnych – w rekonstrukcji ostatnich aktywności osoby zaginionej oraz w planowaniu działań terenowych. W artykule omówiono obowiązujące w Polsce podstawy prawne pozyskiwania i przetwarzania danych cyfrowych przez Policję, ze wskazaniem na konstytucyjne gwarancje ochrony prywatności oraz ograniczenia wynikające z prawa Unii Europejskiej i orzecznictwa Trybunału Sprawiedliwości UE. Zwrócono również uwagę na rosnącą rolę metod OSINT i SOCMINT, a także na udział podmiotów niepublicznych, w tym prywatnych detektywów i organizacji pozarządowych, w działaniach

poszukiwawczych. Studium przypadku zaginięcia Iwony Wieczorek posłużyło do zilustrowania konsekwencji opóźnień proceduralnych w zabezpieczeniu materiału cyfrowego. W konkluzji sformułowano postulaty *de lege ferenda* dotyczące potrzeby stworzenia kompleksowych regulacji prawnych oraz wzmocnienia standardów etycznych i kompetencji cyfrowych podmiotów zaangażowanych w poszukiwania osób zaginionych.

**Słowa kluczowe:** zaginięcia osób, media społecznościowe, OSINT, ochrona prywatności

## Abstract

The article addresses the issue of using digital media and digital traces in the search for missing persons in Poland, analysing it from legal, technological, and ethical perspectives. The authors argues that the dynamic development of information and communication technologies has fundamentally transformed the nature of search operations, making data generated by mobile devices, social media platforms, location-based applications, and surveillance systems one of the key operational resources. Particular attention is given to the significance of digital traces – both active and passive – in reconstructing the last activities of a missing person and in planning field operations.

The article discusses the legal framework in force in Poland governing the acquisition and processing of digital data by the Police, with reference to constitutional guarantees of privacy protection and limitations arising from European Union law and the case law of the Court of Justice of the European Union. Attention is also drawn to the growing role of OSINT and SOC-MINT methods, as well as to the involvement of non-public entities, including private detectives and non-governmental organisations, in search activities. A case study of the disappearance of Iwona Wieczorek is used to illustrate the consequences of procedural delays in securing digital evidence. In conclusion, *de lege ferenda* postulates are formulated concerning the need to establish comprehensive legal regulations and to strengthen ethical standards and digital competencies among entities involved in the search for missing persons.

**Keywords:** missing persons, social media, OSINT, privacy protection

## Wprowadzenie

Zaginięcia osób to wciąż istotny problem społeczny i operacyjny, z którym mierzą się zarówno służby państwowe, jak i organizacje pozarządowe czy sami obywatele. Każdego roku w Polsce zgłaszanych jest kilkanaście tysięcy przypadków, z czego część dotyczy osób szczególnie narażonych: dzieci, seniorów, osób chorych czy ofiar przemocy<sup>1</sup>. Skuteczność poszukiwań w dużej mierze zależy od szybkości reakcji oraz dostępu do informacji o ostatnich aktywnościach zaginionego, co w realiach współczesnych coraz częściej oznacza konieczność sięgania po dane pochodzące z mediów cyfrowych.

---

<sup>1</sup> P. Mieszkalska, *Ocena funkcjonowania systemu poszukiwania osób zaginionych w Polsce*, „Prokuratura i Prawo” 2023, nr 9, s. 136.

Celem badawczym pracy jest analiza obowiązujących w Polsce – z uwzględnieniem standardów konstytucyjnych i unijnych – podstaw prawnych oraz ograniczeń pozyskiwania, przetwarzania i wykorzystywania danych z mediów cyfrowych (w tym OSINT/SOCMINT, danych telekomunikacyjnych i chmurowych) w poszukiwaniach osób zaginionych, a następnie wskazanie luk regulacyjnych i sformułowanie rekomendacji zmian proceduralnych i legislacyjnych, które zwiększą skuteczność poszukiwań przy jednoczesnej ochronie praw jednostki. Przyjęta hipoteza zakłada, że obecny, rozproszony model regulacji prawnych dotyczących wykorzystywania danych z mediów cyfrowych w poszukiwaniach osób zaginionych w Polsce (oparty głównie na ustawie o Policji i aktach wewnętrznych) jest niewystarczający do sprawnego działania w pierwszych 24–48 godzinach zaginięcia, ponieważ nie zapewnia jednolitych procedur, zwłaszcza w zakresie SOCMINT oraz zabezpieczania materiału cyfrowego, co obniża skuteczność poszukiwań i zwiększa ryzyko naruszeń prywatności. W konsekwencji przyjmuje się, że wprowadzenie spójnych regulacji i standardów postępowania poprawi efektywność działań oraz poziom ochrony praw obywatelskich.

Teza pracy sprowadza się do stwierdzenia, że skuteczność poszukiwań osób zaginionych w realiach cyfrowych zależy od szybkiego i prawidłowego pozyskania oraz zabezpieczenia śladów cyfrowych, jednak w Polsce wykorzystanie mediów cyfrowych w tych procesach ograniczają luki i niejednoznaczności regulacyjne (szczególnie w obszarze SOCMINT i dostępu do danych). Z tego względu konieczne są kompleksowe uregulowania oraz ujednoczenie procedur i standardów etycznych.

W pracy postawiono następujące pytania badawcze: Jakie są podstawy prawne i granice pozyskiwania oraz wykorzystywania danych z mediów cyfrowych w poszukiwaniach osób zaginionych w Polsce (w szczególności przez Policję)? Jakie kategorie danych cyfrowych (metadane/retencja, dane lokalizacyjne, treść komunikacji, dane z chmury i urzędzeń) mogą być legalnie pozyskiwane w toku poszukiwań i w jakich trybach? W jakim zakresie dopuszczalne jest stosowanie OSINT/SOCMINT w poszukiwaniach oraz gdzie przebiega granica między legalną analizą informacji publicznych a ingerencją w prywatność i dane osobowe? Jakie luki i ryzyka (prawne, proceduralne, etyczne) ujawnia praktyka (w tym studium przypadku) oraz jakie zmiany *de lege lata* i *de lege ferenda* są potrzebne, by zwiększyć skuteczność poszukiwań przy ochronie praw jednostki?

Tak przyjęte wytyczne wpłynęły na ostateczny kształt opracowania.

## Media cyfrowe i ślady cyfrowe w poszukiwaniach: źródła danych i ich wartość operacyjna

Rozwój technologii cyfrowych w ostatnich latach wyraźnie zmienił sposób, w jaki funkcjonujemy jako społeczeństwo – także w sytuacjach trudnych, takich jak zaginięcia osób. Coraz częściej okazuje się, że klasyczne metody poszukiwawcze, choć wciąż bardzo potrzebne, wymagają wsparcia ze strony narzędzi cyfrowych. Media społecznościowe, aplikacje lokalizacyjne, komunikatory czy inne platformy online stają się nieocenioną pomocą w szybkim przekazywaniu informacji, docieraniu do świadków czy analizie ostatnich aktywności osoby zaginionej. Po tego typu rozwiązania sięgają dziś nie tylko wyspecjalizowane służby mundurowe, lecz także fundacje, bliscy zaginionych, a nawet całe społeczności internetowe angażujące się w nagłaśnianie spraw. Zjawisko to znajduje uzasadnienie – jak pokazują najnowsze dane, z mediów społecznościowych w Polsce korzysta już ponad 90% internautów. To około 27,5–28 milionów dorosłych użytkowników, co czyni z nich jedno z najpotężniejszych narzędzi komunikacji i organizacji działań, jakie mamy do dyspozycji<sup>2</sup>. W tym kontekście media społecznościowe nie są już tylko platformą do kontaktu z bliskimi czy zapewnienia rozrywki. Stały się przestrzenią, w której można budować zasięg, mobilizować innych i realnie wpływać na przebieg akcji poszukiwawczych. Ich rola w takich działaniach staje się z roku na rok coraz bardziej zauważalna i – co ważne – coraz lepiej wykorzystywana.

Współczesna obecność człowieka w przestrzeni cyfrowej generuje nieustannie ogromne ilości danych. Korzystanie z urządzeń mobilnych, mediów społecznościowych, komunikatorów czy usług lokalizacyjnych w naturalny sposób prowadzi do powstawania tzw. śladów cyfrowych czyli pozostałości po aktywności użytkownika, które mogą mieć wartość nie tylko informacyjną, ale i operacyjną. Ich znaczenie dostrzegalne jest szczególnie w sytuacjach nagłych, jak zaginięcie osoby, gdzie liczy się szybki dostęp do możliwie szerokiego obrazu ostatnich działań, kontaktów i przemieszczania się zaginionego. W literaturze przyjmuje się najczęściej podział śladów cyfrowych na dwie główne kategorie: aktywne – świadomie pozostawiane przez użytkownika, jak wpisy, zdjęcia, komentarze czy lokalizacje, oraz pasywne – rejestrowane automatycznie przez systemy i urządzenia, obejmujące m.in. adresy *IP*, *metadane*, dane lokalizacyjne *GPS*, historię logowań czy zapisy z czujników mobilnych<sup>3</sup>.

<sup>2</sup> *Social Media 2025, raport opracowany przez Polskie Badania Internetu i Gemiusa na podstawie badania Mediapanel; uzupełniony danymi z raportu Digital 2025: Poland (DataReportal, Meltwater); dane z końca 2024 i początku 2025 r.*

<sup>3</sup> J. Kozłowski, *Ochrona danych w cyberprzestrzeni. Aspekty prawne i organizacyjne*, Warszawa 2020, s. 42–44.

Dla skuteczności tego rodzaju analiz niezwykle ważne jest, by ślady cyfrowe posiadały określone cechy: trwałość, precyzję czasowo-przestrzenną oraz obiektywność. Ich przewaga nad tradycyjnymi formami informacji polega m.in. na tym, że rejestrowane są automatycznie, co ogranicza ryzyko błędu lub fałszu. Dzięki znacznikom czasowym i lokalizacyjnym można z dużą dokładnością odtworzyć chronologię zdarzeń, a także wzorce przemieszczania się zaginionej osoby. Również różnorodność tych danych – obejmująca zarówno informacje systemowe (logi, dane *GPS*, pliki tymczasowe), jak i społeczne (komentarze, relacje, udostępnienia) – stanowi wartość dodaną w procesie poszukiwawczym<sup>4</sup>. W działaniach tego typu szczególnie cenne okazują się narzędzia pozwalające na tzw. rekonstrukcję ostatnich aktywności, czyli stworzenie „mapy cyfrowej ścieżki” zaginionego. To właśnie połączenie wielu źródeł danych – od mediów społecznościowych po aplikacje zdrowotne – umożliwia uzyskanie szerszego kontekstu sytuacyjnego i wyciąganie bardziej trafnych wniosków operacyjnych. Warto jednak podkreślić, że skuteczność tego procesu jest ściśle zależna od poprawnego ujawnienia i zabezpieczenia danych, zgodnie z obowiązującymi procedurami i standardami pracy z materiałem cyfrowym<sup>5</sup>.

Aby dane cyfrowe mogły być skutecznie wykorzystywane w działaniach poszukiwawczych, konieczne jest uwzględnienie ich charakterystycznych właściwości – takich jak dokładność lokalizacyjna, różnorodność źródeł oraz możliwość szczegółowego odtworzenia przebiegu zdarzeń. Szczególnie cenne okazują się dane pozyskiwane z urządzeń mobilnych, aplikacji lokalizacyjnych, mediów społecznościowych oraz komunikatorów, które – poddane odpowiedniej analizie – umożliwiają stworzenie, wspomnianej wyżej tzw. „cyfrowej mapy aktywności” osoby zaginionej, odzwierciedlającej jej ostatnie działania, lokalizacje oraz potencjalne kontakty<sup>6</sup>. W toku poszukiwawczym okazuje się być to podstawą do ustalenia ostatniego miejsca pobytu osoby zaginionej. Szczególne znaczenie mają dane uzyskane z aplikacji takich jak *Google Maps* czy *Life360*, które pozwalają ustalić precyzyjny przebieg trasy osoby zaginionej, uwzględniając czas i miejsce poszczególnych zatrzymań. Na tej podstawie możliwe jest zawężenie obszaru przeszukiwań i lepsze zaplanowanie działań terenowych. Wartościowe bywają również metadane zdjęć (np. geolokalizacja

---

<sup>4</sup> A. Sołódow, *Zabezpieczanie śladów cyfrowych w praktyce kryminalistycznej*, [w:] A. Sołódow (red.), *Prawne i społeczne aspekty bezpieczeństwa w dobie transformacji cyfrowej*, Warszawa 2022, s. 104–106.

<sup>5</sup> R. Jabłoński, *Ujawnianie i zabezpieczanie śladów cyfrowych*, [w:] J. Widacki (red.), *Ślady cyfrowe*, Kraków 2022, s. 123–130.

<sup>6</sup> A. Tusnio, A. Wolny, *Nowoczesne narzędzia i sprzęt wykorzystywane do poszukiwań osób zaginionych*, „Zeszyty Naukowe SGSP” 2022, nr 61, t. 2, s. 27–29.

EXIF), informacje z czujników ruchu, a także dane pobierane z urządzeń rejestrujących funkcje życiowe – które mogą wskazywać na nagłą zmianę stanu fizycznego lub stres<sup>7</sup>. W świetle analiz kryminologicznych, współczesna problematyka zaginięć jest nierozdzielnie powiązana z postępowaniem naukowo-technicznym oraz rozwojem obowiązujących przepisów prawa<sup>8</sup>. Ekspertki wskazują<sup>9</sup>, że szybki rozwój cywilizacyjny niesie ze sobą niestety negatywne konsekwencje społeczne, takie jak osłabienie więzi międzyludzkich oraz problemy wynikające z braku dostatecznej wiedzy w społeczeństwie, co bezpośrednio intensyfikuje wykluczenie społeczne. W rezultacie, zjawisko zaginięcia często bywa uwarunkowane niekorzystnymi czynnikami sprzyjającymi przestępczości, co musi znaleźć odzwierciedlenie zarówno w procedurach poszukiwawczych opartych na mediach cyfrowych, jak i w kształcie obowiązującego systemu prawnego.

### **Znaczenie czasu i praktyka pozyskiwania danych: 24–48 godzin po zaginięciu**

W pierwszej fazie działań poszukiwawczych – najczęściej obejmującej 24–48 godzin od zaginięcia – dostęp do danych cyfrowych ma kluczowe znaczenie z punktu widzenia szybkości reakcji. Wczesne ustalenie ostatniej aktywności w sieci może nie tylko skrócić czas prowadzenia akcji, ale również znacząco zwiększyć jej skuteczność poprzez ukierunkowanie działań na określony obszar lub środowisko społeczne<sup>10</sup>. Zbieranie i wykorzystywanie śladów cyfrowych musi być jednak prowadzone z zachowaniem obowiązujących przepisów prawa. W przypadku danych gromadzonych przez operatorów telefonii komórkowej, dostawców usług internetowych czy administratorów serwisów społecznościowych, dostęp do tych informacji może nastąpić wyłącznie na podstawie odpowiednich decyzji procesowych – takich jak postanowienie sądu, zgoda prokuratora lub – w przypadkach zagrożenia życia i zdrowia – na podstawie przesłanki wynikającej z art. 20c ustawy o Policji<sup>11</sup>. Uprawnienia te są kluczowe w poszukiwaniach, ponieważ obejmują sięganie po dane reten-

<sup>7</sup> A. Wentkowska, *Poszukiwania osób zaginionych. System i metody działania w procedurach służb*, Warszawa 2016, s. 89–94.

<sup>8</sup> I. Malinowska, *Problematyka zaginięć ludzi w aspekcie prawnokryminologicznym*, „Problemy Współczesnej Kryminologii” 2023, t. XXII, s. 129.

<sup>9</sup> Zob. I. Malinowska, *Zaginięcia ludzi i aspekty bezpieczeństwa – podejście komparatystyczne*, Sofia 2025, s. 284–316.

<sup>10</sup> M. Konieczny, *Znaczenie serwisów społecznościowych w pracy służby prasowej Policji i ich wpływ na skuteczność działań informacyjnych*, „Przegląd Policyjny” 2021, nr 2, s. 91–93.

<sup>11</sup> Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 1990 r., nr 30, poz. 179, z późn. zm.).

cyjne (*metadane*) – takie jak lokalizacja urządzenia mobilnego (logowanie do stacji bazowej BTS) i historia połączeń, co jest niezbędne w sytuacjach bezpośredniego zagrożenia życia i zdrowia zaginionego.

## **Ramy prawne i ograniczenia dostępu do danych: konstytucja, prawo UE, chmura i retencja**

Największe prawne wyzwanie stanowi uzyskanie dostępu do treści komunikacji (np. wiadomości *SMS*, *e-maile*, zawartość kont w chmurze) oraz do systemów zabezpieczonych hasłem (np. *smartfon*). Informacje te stanowią tajemnicę komunikowania się chronioną na mocy Art. 49 Konstytucji RP<sup>12</sup>. Jej naruszenie jest dopuszczalne wyłącznie w trybie i na zasadach określonych przez prawo, co zwykle wymaga postanowienia sądu i jest ograniczone do postępowań karnych. Uzyskanie dostępu do danych na zabezpieczonym hasłowo urządzeniu wymaga zastosowania specjalistycznej wiedzy z zakresu informatyki kryminalistycznej i jest trudne technicznie, ponieważ wymaga zastosowania metod takich jak obrazowanie fizyczne (*physical imaging*)<sup>13</sup>. Te krajowe ograniczenia proceduralne nakładają się na bardziej fundamentalne wyzwania, wynikające bezpośrednio z prawa Unii Europejskiej. Polski system dostępu do danych telekomunikacyjnych jest stale krytykowany na tle orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej (TSUE)<sup>14</sup>. Trybunał stoi na stanowisku, że państwa członkowskie nie mogą zezwalać na generalną i nieodróżnicowaną retencję danych ani na niekontrolowany dostęp do nich, gdyż narusza to prawo do prywatności. Dostęp do tych wrażliwych informacji jest dopuszczalny tylko w celu zwalczania poważnej przestępczości (zagrożonej karą nie mniejszą niż 3 lata pozbawienia wolności) i musi podlegać uprzedniej kontroli sądu lub niezależnego organu<sup>15</sup>. Ta rozbieżność stawia polskie organy ścigania w trudnym położeniu, równoważącym konstytucyjną ochronę tajemnicy komunikowania się z koniecznością natychmiastowego ratowania życia. Wraz z rozwojem usług chmury obliczeniowej (*cloud computing*), dane są przechowywane zdalnie na serwerach, co utrudnia

<sup>12</sup> Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r., nr 78, poz. 483).

<sup>13</sup> M. Nowikowska, *Procesowa kontrola danych informatycznych w chmurze obliczeniowej*, „Zeszyty Naukowe Akademii Sztuki Wojennej” 2021, s. 165.

<sup>14</sup> Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 6 października 2020 r., La Quadrature du Net i in. przeciwko Premier ministre i in., sprawy połączone C-511/18, C-512/18 i C-520/18.

<sup>15</sup> Stanowisko Prezesa Urzędu Ochrony Danych Osobowych w sprawie dostępu policji do danych telekomunikacyjnych (lipiec 2024), na tle Wyroku TSUE C-178/22.

tradycyjne metody przeszukania i zatrzymania rzeczy. Stosowanie przepisów krajowych jest skomplikowane, gdyż serwery dostawców usług (np. *Meta*, *Google*) często znajdują się poza polską jurysdykcją. Mimo tych wyzwań, Policja jest uprawniona do przetwarzania informacji, w tym danych osobowych, na podstawie Art. 20 Ustawy o Policji. Dotyczy to również danych z mediów społecznościowych (*SOCMINT*), które są klasyfikowane i wykorzystywane na potrzeby pracy śledczej. Niemniej jednak, luki proceduralne w systemie (np. nierzetelne wprowadzanie danych do KSIP i opóźnienia w pobieraniu *DNA*) osłabiają realizację konstytucyjnych gwarancji bezpieczeństwa<sup>16</sup>.

Oprócz aspektu prawnego nie mniej istotne jest zabezpieczenie materiału cyfrowego w sposób umożliwiający jego późniejsze wykorzystanie dowodowe. Wymaga to zastosowania specjalistycznych procedur informatyki śledczej, m.in. tworzenia kopii bitowych, zabezpieczania oryginałów, dokumentowania każdej ingerencji oraz przechowywania danych w warunkach wykluczających ryzyko ich modyfikacji<sup>17</sup>.

### **Metody OSINT/SOCMINT oraz udział podmiotów niepublicznych: możliwości i granice legalności**

Istotnym elementem współczesnych technik analitycznych staje się również zastosowanie metod *SOCMINT* (*Social Media Intelligence*), umożliwiających przeszukiwanie, klasyfikowanie i analizowanie publicznej aktywności użytkownika w mediach społecznościowych. Pozwala to nie tylko na określenie lokalizacji zaginionego, ale również na rozpoznanie jego stanu emocjonalnego, motywacji oraz kontekstu relacyjnego – co może być szczególnie istotne w przypadkach zaginięć o podłożu psychicznym, konfliktowym lub przemocowym<sup>18</sup>. Narzędzia z zakresu *SOCMINT* to nie tylko śledzenie otwartych kont użytkowników, ale przede wszystkim analiza ich aktywności w sposób dynamiczny – z wykorzystaniem specjalistycznego oprogramowania do monitorowania treści w czasie rzeczywistym, przeszukiwania komentarzy, lokalizacji czy multimediów. Takie podejście nie tylko przyspiesza identyfikację osób, które mogą mieć związek ze sprawą, ale pozwala również „czytać między wierszami”, np. wyciągając wnioski na podstawie powtarzalnych wzorców

<sup>16</sup> P. Waszkiewicz (red.), *Media społecznościowe w pracy organów ścigania*, Warszawa 2021, s. 12.

<sup>17</sup> R. Jabłoński, *Ujawnianie i zabezpieczanie...*, op. cit., s. 122–141.

<sup>18</sup> K. Bayer, J. Bitner, *Wykorzystanie mediów społecznościowych przez funkcjonariuszy polskiej Policji – próba wstępnego opisu*, „Przegląd Wschodnioeuropejski” 2020, nr 2, s. 305–307.

zachowań, lokalizacji czy interakcji online<sup>19</sup>. Analiza wpisów i postaw pozwala zrozumieć motywy ucieczek lub świadomego zerwania kontaktu. są nieocenione w fazie analitycznej, stanowią uzupełnienie dla danych telekomunikacyjnych i geograficznych. Potencjał ten wzmacniany jest przez systemy takie, jak Geographic Information System (GIS), które służą do tworzenia precyzyjnych map cyfrowych i wizualizacji rejonów poszukiwań oraz Bezzałogowe Systemy Powietrzne (BSP), które w terenie umożliwiają zlokalizowanie osoby w strefie 1 km<sup>2</sup> w ok. 20 minut. Aktualnie jest to najprężniej rozwijająca się dziedzina analizy danych, która opiera się na przetwarzaniu informacji udostępnianych w mediach społecznościowych. Początkowo wykorzystywana w ramach operacji wywiadowczych, z biegiem lat zyskała szerokie zastosowanie w codziennej pracy służb – zwłaszcza Policji, Straży Granicznej czy innych podmiotów odpowiedzialnych za bezpieczeństwo wewnętrzne. Jej potencjał dostrzegany jest również w działaniach poszukiwawczych, gdzie szybki dostęp do danych cyfrowych bywa kluczowy dla określenia ostatnich kroków osoby zaginionej<sup>20</sup>.

Aktywność w mediach społecznościowych w tym kontekście jest istotna ze względu na ich popularność, każdy bowiem korzysta z jakiegoś komunikatora do wymiany informacji bądź kontaktu. Nie ogranicza się jedynie do danych technicznych lecz stało się istotnym elementem relacji społecznych. W akcjach poszukiwawczych pozwala na szybsze i szersze rozprzestrzenienie się informacji poprzez *repost*, udostępnianie i zasięg jaki generują platformy mediów społecznościowych. Należy jednak zaznaczyć, że metody SOCMINT, mimo ich rosnącej popularności, nadal funkcjonują na granicy dozwolonego zakresu operacyjnego. W polskim systemie prawnym brak jest jednoznacznych regulacji dotyczących zasad pozyskiwania i przetwarzania danych z mediów społecznościowych, w szczególności tych pochodzących z prywatnych kont użytkowników, co budzi kontrowersje na gruncie konstytucyjnych praw do prywatności i ochrony danych osobowych. Dane pozyskiwane z przestrzeni cyfrowej nie zawsze są kompletne, aktualne czy w pełni wiarygodne. Zdarza się, że są one fragmentaryczne lub trudne do jednoznacznej interpretacji, dlatego tak ważne jest ich odpowiednie sprawdzenie i potwierdzenie w toku dalszych działań. Selekcja i analiza tych informacji wymaga nie tylko wiedzy technicznej, ale też wyczucia i doświadczenia w pracy operacyjnej. Pomimo

---

<sup>19</sup> P. Mieszkalska, *Wykorzystanie analizy treści publikowanych w mediach społecznościowych w ramach pracy operacyjno-rozpoznawczej*, [w:] *Bezpieczeństwo i prawo. Współczesne wyzwania*, (red.) E. Gromek-Broc, Warszawa 2023, s. 125–126.

<sup>20</sup> A. Płatek, *Media społecznościowe w pracy organów ścigania i wymiaru sprawiedliwości*, [w:] *Regulacje prawne funkcjonowania społeczeństwa informacyjnego*, (red.) A. Płatek, Kraków 2022, s. 125–126.

ogromnego potencjału, wdrożenie *SOCMINT* na poziomie operacyjnym stwarza wyzwania proceduralne. Skuteczne posługiwanie się *SOCMINT* wymaga adekwatnej i aktualnej wiedzy informatyczno-technicznej. Staje się to szczególnie złożone, gdy dane są chronione hasłem lub dostęp jest ograniczony (np. prywatne profile), wykraczając poza ramy białego wywiadu<sup>21</sup>. W takim przypadku, pozyskanie informacji wymaga podjęcia dodatkowych czynności dochodzeniowo-śledczych.

Niezależnie od działań podejmowanych przez Policję, która jako jedyna w Polsce jest zobligowana prawnie do prowadzenia poszukiwań osób zaginionych, dynamicznie rośnie rola podmiotów prywatnych. W systemie tym kluczową pozycję zajmują prywatni detektywi, działający na zlecenie osób najbliższych zaginionego<sup>22</sup>. Ich działalność jest ściśle regulowana przez Ustawę z dnia 6 lipca 2001 r. o usługach detektywistycznych<sup>23</sup>, która określa ramy ich uprawnień i ograniczeń, wskazując, że detektyw ma prawo do przetwarzania danych osobowych oraz gromadzenia informacji o osobach i zdarzeniach na zlecenie klienta, z zachowaniem przepisów prawa. W kontekście zaginięć, detektywi nierzadko angażowani są przez rodziny zaginionych do prowadzenia działań równoległych wobec procedur policyjnych<sup>24</sup>. Z perspektywy rodziny, detektywi stanowią uzupełnienie lub – w wielu przypadkach – alternatywę dla działań służb państwowych, zwłaszcza gdy działania Policji są uznawane za zbyt powolne lub niewystarczające. Detektywi mogą zaangażować się w sprawę natychmiast, bez konieczności czekania na spełnienie wymogów formalnych, które ograniczają Policję (np. czas minimalny, który upłynął od zaginięcia, czy kwalifikacja zdarzenia. Mogą oni szybciej dotrzeć do świadków, przeprowadzić wywiad środowiskowy, zabezpieczyć materiały w mediach społecznościowych czy zlokalizować urządzenia mobilne, a także monitorować aktywność online zaginionego. Ich działania często koncentrują się na aspektach, które mogą zostać pominięte przez formalne struktury – jak relacje osobiste, konflikty rodzinne, czy alternatywne hipotezy zdarzenia<sup>25</sup>.

<sup>21</sup> K. Bayer, J. Bitner, *Wykorzystanie mediów społecznościowych przez funkcjonariuszy polskiej Policji. Próba wstępnego opisu zjawiska na podstawie wyników badań kwestionariuszowych*, [w:] *Media społecznościowe w pracy organów ścigania*, (red.) P. Waszkiewicz, Warszawa 2021, s. 2.

<sup>22</sup> D. Brakoniecki, *Detektywi*, [w:] *Pracownicy formacji bezpieczeństwa i porządku publicznego, służb ratownictwa i ochrony*, (red.) M. Czuryk, M. Karpiuk, Olsztyn 2017, s. 423.

<sup>23</sup> Ustawa z dnia 6 lipca 2001 r. o usługach detektywistycznych (t.j. Dz. U. z 2020 r., poz. 129).

<sup>24</sup> Zob. D. Brakoniecki, *Detektywistyka. Prawne i funkcjonalne aspekty działalności detektywistycznej w Polsce i na świecie*, Warszawa 2016, s. 158–176.

<sup>25</sup> P. Mieszkalska, *Zaginięcie osoby jako sytuacja kryzysowa z perspektywy psychologii i praktyki działań służb*, [w:] *Zaginięcia osób. Aspekty kryminalistyczne, psychologiczne i społeczne*, (red.) J. Widacki, P. Mieszkalska, Katowice 2023, s. 217–219.

Współcześnie, dzięki postępującej cyfryzacji, kompetencje detektywów muszą obejmować również podstawy informatyki śledczej i analizy cyfrowych śladów. W wielu przypadkach to właśnie prywatni specjaliści jako pierwsi weryfikują aktywność zaginionego w mediach społecznościowych, analizują jego ostatnie logowania, miejsca pobytu zapisane w aplikacjach lokalizacyjnych, czy pozyskują informacje z komunikatorów<sup>26</sup>.

Aktywność detektywów w obszarze cyfrowym koncentruje się przede wszystkim na legalnie dostępnych źródłach, wpisując się w szeroko rozumiane metody *OSINT (Open-Source Intelligence)*<sup>27</sup>. Jest to kluczowy aspekt, gdyż detektywi, w przeciwieństwie do Policji i Prokuratury, nie posiadają uprawnień do:

1. Wymuszania udostępnienia danych retencyjnych od operatorów telekomunikacyjnych (lokalizacja BTS, historia połączeń).
2. Uzyskiwania w drodze procesowej dostępu do prywatnych danych na serwerach zewnętrznych, np. wiadomości e-mail czy zawartości kont społecznościowych zabezpieczonych hasłem<sup>28</sup>.

W związku z tym, ich praca w zakresie cyfrowym polega na zaawansowanej analizie białego wywiadu, koncentrując się między innymi na wizualizacji i analizie publicznej aktywności poprzez systematyczne przeszukiwanie mediów społecznościowych, forów, blogów i innych otwartych źródeł w celu zrekonstruowania ostatnich interakcji, ustalenia planów zaginionego, jego stanu emocjonalnego oraz potencjalnej trasy przemieszczania się. Jak również przez wywiad środowiskowy cyfrowy poprzez szybkie identyfikowanie i kontaktowanie się z osobami z kręgu znajomych zaginionego (często zidentyfikowanymi poprzez media społecznościowe), w celu pozyskania informacji o jego aktywności w sieci bezpośrednio przed zaginięciem. Ich skuteczność wzrasta szczególnie w sytuacjach, gdy dostęp do informacji możliwy jest bez angażowania aparatu państwowego, np. przez współpracę z rodziną lub za zgodą samego zaginionego, jeśli wcześniej wyraził taką wolę. Odpowiednio przeprowadzona analiza cyfrowa może przynieść szybkie efekty w sytuacjach,

---

<sup>26</sup> B. Koper, *Praktyczne kompetencje detektywa w kontekście współczesnych zagrożeń bezpieczeństwa*, [w:] *Bezpieczeństwo a działalność detektywistyczna*, (red.) J. Widacki, T. Hanausek, Kraków 2020, s. 148–150.

<sup>27</sup> D. Brakoniecki, *Ustawa o usługach detektywistycznych jako forma prywatyzacji zadań administracji publicznej w obszarze bezpieczeństwa i porządku publicznego*, „Journal of Modern Science” 1/36/2018, s. 229.

<sup>28</sup> A. Wasik, W. Strynkowska, *Rola prywatnego detektywa w poszukiwaniach osób zaginionych*, „Prace Naukowe Uniwersytetu Jana Długosza w Częstochowie. Prawo” 2022, t. XVII, nr 1, s. 165–179.

gdy czas reakcji jest kluczowy – nie rzadko również skutecznie pomagają nagłośnić sprawę zaginięć.

### **Praktyczne konsekwencje i potrzeba zmian: studium przypadku, etyka i postulaty legislacyjne**

Sprawa zaginięcia Iwony Wieczorek w lipcu 2010 roku stanowi modelowy przykład na masowe i długotrwałe wykorzystanie mediów cyfrowych w procesie poszukiwawczym, a jednocześnie na systemowe wyzwania prawne i techniczne w zakresie pozyskiwania cyfrowego materiału dowodowego. Mimo, iż sprawa pozostaje nierozwiązana, ilustruje ona kluczowe aspekty wykorzystania technologii w służbie prawa, a także zaniechania na etapie proceduralnym, zwłaszcza w zabezpieczeniu dowodów cyfrowych. W obliczu braku fizycznych świadków i tradycyjnych śladów kryminalistycznych, ciężar dowodowy w tej sprawie przeniósł się niemal całkowicie na analizę danych cyfrowych, co potwierdza tezę o kluczowym znaczeniu nowoczesnych technologii w pracy organów ścigania. Fundamentem rekonstrukcji ostatnich godzin przed zaginięciem stały się nagrania z monitoringu miejskiego i prywatnego oraz dane telekomunikacyjne, które pozwoliły na precyzyjne odtworzenie trasy przemieszczania się zaginionej oraz weryfikację zeznań osób z jej otoczeniu. Niemniej jednak, analiza przeprowadzona przez Najwyższą Izbę Kontroli wykazała, że potencjał ten został drastycznie ograniczony przez błędy popełnione w pierwszej fazie działań. Kluczowym uchybieniem była błędna kwalifikacja zdarzenia przez funkcjonariuszy, którzy nadali sprawie drugą, zamiast obligatoryjnej w okolicznościach nagłego zaginięcia, pierwszą kategorię poszukiwań<sup>29</sup>. Decyzja ta pociągnęła za sobą łańcuch negatywnych konsekwencji, z których najbardziej dotkliwą była zwłoka w zabezpieczeniu cyfrowych nośników danych. Działania zmierzające do przejęcia nagrań z kamer przemysłowych i prywatnych zlokalizowanych na trasie przejścia zaginionej podjęto dopiero po upływie siedmiu dni od zgłoszenia. Ze względu na specyfikę systemów monitoringu, które w wielu placówkach komercyjnych nadpisują dane w cyklach kilkudziesięciogodzinnych, kluczowy materiał dowodowy uległ bezpowrotnemu zniszczeniu, uniemożliwiając pełną wizualizację zdarzenia. Równolegle do działań służb, sprawa ta stała się precedensem w zakresie wykorzystania wywiadu jawnoźródłowego (*OSINT*) i mobilizacji społecznej w sieci. Intensywna aktywność internautów na forach dyskusyjnych i w mediach społecznościowych doprowadziła do powstania

---

<sup>29</sup> Najwyższa Izba Kontroli, *Informacja o wynikach kontroli. Poszukiwanie osób zaginionych*, Warszawa 2015, s. 25.

ogromnego zbioru danych, co z jednej strony dostarczyło nowych tropów, lecz z drugiej wygenerowało potężny szum informacyjny, utrudniający pracę analityczną. Przypadek ten dobitnie unaoczniał, że w erze cyfrowej skuteczność poszukiwań jest wprost proporcjonalna do szybkości reakcji na ulotne ślady elektroniczne. Mimo to, rozwój nowoczesnych narzędzi techniki kryminalistycznej, takich jak zaawansowane bazy *DNA* czy systemy fotogrametrii wykorzystywane przez policyjne zespoły do spraw przestępstw niewykrytych, daje nadzieję, że nawet w sprawach obarczonych pierwotnym błędem, trwale zabezpieczony ślad cyfrowy lub biologiczny może po latach doprowadzić do przełomu<sup>30</sup>.

Warto również wspomnieć, iż wśród spraw poszukiwawczych, zaginięcia małoletnich mają szczególne znaczenie z uwagi na ich tło społeczno-prawne<sup>31</sup>. Często ucieczka dziecka jest bezpośrednim rezultatem zaniedbań opiekuńczych lub braku świadomości prawnej ze strony rodziców i opiekunów. Z uwagi na konieczność ochrony fundamentalnej wartości, jaką jest życie i zdrowie dziecka, na organach ścigania spoczywa obowiązek dysponowania uprawnieniami do szybkiego pozyskania niezbędnych informacji, w tym danych elektronicznych. Ta pilna potrzeba interwencji, wynikająca z nadrzędności dobra dziecka, stanowi kluczowe uzasadnienie dla odstępstw od rygorystycznej ochrony prywatności w początkowej fazie poszukiwań, co jest centralnym zagadnieniem etycznym

W kontekście demokratycznego państwa prawa, każda forma ingerencji w prywatność obywatela w tym wykorzystanie danych pochodzących z mediów cyfrowych musi znaleźć podstawę w obowiązującym ustawodawstwie. Oznacza to, że zarówno uprawnienia organów publicznych do stosowania narzędzi cyfrowych w działaniach poszukiwawczych, jak i aktywność podmiotów niepublicznych (np. fundacji, mediów czy użytkowników sieci) powinny być ściśle określone przez normy prawne co jednocześnie wybrzmiewa w dyspozycji art. 6 ust. 1 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE<sup>32</sup>.

<sup>30</sup> M. Zubańska, P. Knut, *Niewykryte przestępstwa sprzed lat, nowoczesne narzędzia techniki kryminalistycznej i policyjne Zespoły do spraw Przestępstw Niewykrytych, czyli crimen grave non potest esse impunibile – cz. II*, „Przegląd Policyjny” 2016, nr 3 (123), s. 31.

<sup>31</sup> I. Malinowska, M. Adamus, *Kiedy zaginęło dziecko – podstawowe informacje prawne*, [w:] *Wolni od patologii*, (red.) M. Krysiak, Maków Mazowiecki 2011.

<sup>32</sup> (Dz.U. UE L 119/1).

Współczesne organy ścigania, realizując swoje zadania związane z poszukiwaniem osób i informacji, coraz częściej sięgają po zasoby dostępne w sieci. W praktyce oznacza to zarówno korzystanie z publicznie dostępnych treści, np. w ramach działań opartych na otwartych źródłach tzw. *OSINT*, jak i możliwość kierowania formalnych wniosków do dostawców usług cyfrowych o udostępnienie określonych danych. Co ciekawe, badania przeprowadzone na Uniwersytecie Warszawskim pokazują, że funkcjonariusze Policji rzeczywiście wykorzystują media społecznościowe jako źródło informacji nie tylko w działaniach operacyjnych, ale również w trakcie prowadzenia śledztw czy czynności procesowych<sup>33</sup>.

W Polsce, w obliczu braku kompleksowej regulacji ustawowej dotyczącej poszukiwań osób zaginionych, prawne uwarunkowania wykorzystania mediów cyfrowych opierają się głównie na ustawowych uprawnieniach Policji oraz na aktach prawa wewnętrznego tej formacji, w szczególności na zarządzeniach Komendanta Głównego Policji (KGP)<sup>34</sup>.

Działania Policji mające na celu poszukiwanie osób zaginionych są prawnie umocowane w Ustawie z dnia 6 kwietnia 1990 r. o Policji. Artykuł 14 ust. 1 pkt 3 tej ustawy uprawnia Policję do prowadzenia czynności operacyjno-rozpoznawczych, dochodzeniowo-śledczych i administracyjno-porządkowych w celu odnalezienia osób, których zaginięcie uniemożliwia ustalenie ich miejsca pobytu, a które należy odnaleźć w celu zapewnienia ochrony ich życia, zdrowia lub wolności<sup>35</sup>.

Istotne dla działań poszukiwawczych wykorzystujących media cyfrowe są uprawnienia Policji w zakresie pozyskiwania i przetwarzania danych:

1. Dane Telekomunikacyjne i Pocztove: Ustawa o Policji przyznaje formacji uprawnienie do pozyskiwania i przetwarzania danych telekomunikacyjnych (o których mowa w art. 180d Prawa telekomunikacyjnego) oraz do ujawniania danych dotyczących osób korzystających z usług pocztowych oraz faktu i okoliczności korzystania z tych usług, w celu poszukiwania osób zaginionych. To uprawnienie jest niezwykle istotne, gdyż często pozwala Policji ustalić ostatnią znaną lokalizację smartfona (na podstawie logowania do stacji bazowej) lub adres IP.
2. Bazy Danych *DNA*: Ustawą wprowadzono możliwość tworzenia i przetwarzania baz danych zawierających kody *DNA* osób zaginionych. Umożliwia to

<sup>33</sup> H. Dębniak, S. Rabczuk, *Wybrane aspekty prawne pozyskiwania danych z mediów społecznościowych przez polskie organy ścigania. Obtaining Data from Social Media by Polish Law Enforcement Agencies – Selected Aspects*, b.m 2019.

<sup>34</sup> P. Mieszkalska, *Wykorzystanie mediów społecznościowych jako narzędzia poszukiwania osób zaginionych. Aspekty prawne i praktyczne*, Warszawa 2022, s. 132.

<sup>35</sup> P. Łabuz, *Ustawa o Policji. Komentarz*, Warszawa 2022, s. 174–175.

- porównywanie profili *DNA* osób zaginionych z profilami niezidentyfikowanych zwłok (NN zwłok) w policyjnej bazie *GENOM* (Zbiorów Danych *DNA*).
3. Dane Osobowe i Linii Papilarnych: Policja uzyskała uprawnienie do pobierania odcisków linii papilarnych lub wymazu ze śluzówki policzków (materiału biologicznego do badań *DNA*) w celu identyfikacji osób lub zwłok ludzkich o nieustalonej tożsamości<sup>36</sup>.

Pomimo znacznej skali zjawiska zaginięć w Polsce, gdzie co roku Policja odnotowuje około 17 do 20 tysięcy przypadków, jednym z podstawowych problemów systemu prawnego pozostaje brak jednolitej, powszechnie obowiązującej definicji osoby zaginionej<sup>37</sup>. Ta niekonsekwencja w nazewnictwie, przejawiająca się w odmiennym traktowaniu terminu w prawie cywilnym i w procedurach policyjnych, utrudnia klarowność przepisów oraz budowanie efektywnego systemu poszukiwań. Co więcej, kryminologiczny wymiar zjawiska wskazuje, że obok wypadków losowych, zaginięcia są często powiązane z działalnością przestępczą, np. z uprowadzeniami lub handlem ludźmi. Ten naglący kontekst wzmacnia konieczność podejmowania przez Policję szybkich i celowych działań w cyberprzestrzeni.

Zarządzenie nr 48 Komendanta Głównego Policji z 28 czerwca 2018 r. wprowadza podział poszukiwań na trzy poziomy – I, II i III – które określają, jak pilne i jak szeroko zakrojone mają być działania, w zależności od tego, czy istnieje realne zagrożenie dla życia, zdrowia lub wolności osoby zaginionej<sup>38</sup>. W przypadku I i II poziomu, czyli tych najbardziej krytycznych, zarządzenie nakłada obowiązek szybkiego zabezpieczenia materiałów wideo z kamer monitoringu z ostatnich miejsc, gdzie zaginiona osoba mogła przebywać. Dodatkowo, akt ten reguluje sposób publikowania wizerunku zaginionych zarówno w oficjalnej, internetowej bazie Policji, jak i jeśli sytuacja tego wymaga w środkach masowego przekazu, w tym także w mediach społecznościowych. Chodzi o to, by informacja jak najszybciej dotarła do możliwie szerokiego grona odbiorców i zwiększy szansę na szybkie odnalezienie danej osoby<sup>39</sup>.

W sytuacjach zaginięcia osób małoletnich szczególnego znaczenia nabiera funkcjonujący w strukturze Komendy Głównej Policji system Child Alert,

<sup>36</sup> A. Wentkowska, *Poszukiwania osób zaginionych. Aspekty prawne i praktyczne*, Katowice 2016, s. 28.

<sup>37</sup> I. Malinowska, A. Rybicka, *Zagrożenia społeczne wynikające z zaginięć ludzi we współczesnym świecie*, „Kwartalnik Policyjny” 2016, nr 1 (36), s. 49.

<sup>38</sup> P. Wojnicz, *Zaginięcia osób. Studium prawne, kryminalistyczne i kryminologiczne*, Olsztyn 2021, s. 59.

<sup>39</sup> P. Mieszkalska, *Wykorzystanie mediów społecznościowych...*, op. cit., s. 140.

którego obsługą zajmuje się Centrum Poszukiwań Osób Zaginionych. Jego uruchomienie polega na natychmiastowym upublicznianiu wizerunku i danych dziecka przy wykorzystaniu środków masowego przekazu, w tym mediów elektronicznych i internetowych. Działanie to ma na celu szybkie dotarcie z komunikatem do jak najszerszego grona odbiorców i zwiększenie szans na odnalezienie osoby zaginionej w możliwie najkrótszym czasie<sup>40</sup>.

Na mocy art. 19 ust. 6 ustawy o Policji, ustawodawca dopuszcza możliwość wykorzystywania w ramach kontroli operacyjnej wszelkich dostępnych i zgodnych z prawem środków technicznych, które umożliwiają niejawnie pozyskiwanie informacji, ich utrwalanie oraz gromadzenie w systemach informatycznych<sup>41</sup>. Przepis ten zwiększa skuteczność działań poszukiwawczych w środowisku cyfrowym, zapewniając jednocześnie ich legalność. Zgodnie z art. 14 ust. 5 ustawy o Policji, każdy administrator danych, a więc podmiot decydujący o celach i środkach przetwarzania, np. *Meta Platforms Inc.* zobowiązany jest do udostępnienia Policji informacji, dokumentów i przedmiotów w jakiegokolwiek formie, jeśli są one niezbędne do realizacji zadań ustawowych. Dane te mogą pochodzić m.in. z komunikatorów internetowych<sup>42</sup>. Wedle art. 14 ust. 4 ustawy o Policji, formacja ta jest uprawniona do przetwarzania informacji pozyskanych przez inne służby państwowe, takie jak Straż Graniczna czy Agencja Bezpieczeństwa Wewnętrznego, jeżeli są one niezbędne do realizacji ustawowych zadań Policji. Dotyczy to również danych uzyskanych z wykorzystaniem mediów cyfrowych, w szczególności w toku czynności operacyjno-rozpoznawczych. Rozwiązanie to usprawnia współdziałanie pomiędzy organami odpowiedzialnymi za bezpieczeństwo publiczne oraz pozwala na szybsze podejmowanie działań, zwłaszcza w sytuacjach nagłych.

Wraz z rozwojem nowoczesnych technologii i rosnącą rolą cyfrowych śladów w działaniach poszukiwawczych, pojawiają się też poważne wyzwania zarówno prawne, jak i etyczne. Choć system poszukiwania osób zaginionych w Polsce z pewnością przeszedł dużą ewolucję, to wciąż nie brakuje problemów. Część z nich wynika z tego, że obowiązujące przepisy nie nadążają za technologią, a część ze specyfiki samego procesu zabezpieczania i przetwarzania danych. Mówiąc wprost: nawet jeśli narzędzia są nowoczesne, to procedury i regulacje bywają dziurawe albo zbyt ogólne. A przy pracy z danymi wrażliwymi i sprawach, gdzie liczy się każda minuta, nie ma miejsca na niedopowiedzenia. Dlatego właśnie kwestia uregulowania tych procesów nabiera coraz większego znaczenia.

<sup>40</sup> A. Wentkowska, *Poszukiwania osób zaginionych...*, op. cit., s. 156.

<sup>41</sup> P. Łabuz, *Ustawa o Policji...*, op. cit., s. 244.

<sup>42</sup> Ibidem, s. 177.

Podczas działań poszukiwawczych z wykorzystaniem mediów cyfrowych ważne jest, żeby informacje były rzetelne i nie naruszały praw osoby zaginionej oraz działania prowadzone w sposób etyczny. Policja i inne służby powinny dążyć do tego, żeby przekaz był spójny i kontrolowany tak, by nie dochodziło do przecieków czy chaosu informacyjnego<sup>43</sup>. Zgodnie z zasadami etyki zawodowej, nawet jeśli jakaś sytuacja nie jest wprost opisana w przepisach albo nie została ujęta w kodeksie etycznym, policjant powinien kierować się zdrowym rozsądkiem, uczciwością i ogólnie przyjętymi normami społecznymi. Chodzi o to, żeby swoim zachowaniem dawać przykład, działać zgodnie z prawem i wzmacniać zaufanie ludzi do Policji<sup>44</sup>. Niestety, w praktyce bywa różnie. Często w akcje angażują się osoby z zewnątrz wolontariusze, fundacje czy zwykli internauci którzy chcą pomóc, ale nie zawsze wiedzą, co wolno, a czego nie. Zdarza się wtedy, że publikują wizerunki czy dane, do których nie mają prawa, albo powielają niepotwierdzone tropy. To z kolei może prowadzić do plotek, stygmatyzacji albo niepotrzebnego stresu dla rodziny.

Jednym z często wykorzystywanych narzędzi jest tzw. biały wywiad, czyli pozyskiwanie informacji z ogólnodostępnych źródeł, takich jak media społecznościowe. W polskim porządku prawnym termin biały wywiad nie posiada formalnej definicji ani nie jest objęty żadną regulacją ustawową. W związku z tym, przy jego interpretacji należy sięgać do ustaleń doktryny. Jedną z przyjętych definicji zaproponował Krzysztof Mroziewicz, który odnosi to pojęcie do procesu analizy informacji pochodzących z jawnych, ogólnodostępnych źródeł. W przypadku mediów społecznościowych oznacza to dostęp do danych, które użytkownicy publikują publicznie często możliwy nawet dla osób nieposiadających konta w danym serwisie<sup>45</sup>. Na pierwszy rzut oka nie wydaje się to naruszeniem prywatności, bo przecież dane są publiczne. Jednak kiedy zaczyna się je systematycznie zbierać, analizować i łączyć w większe zestawienia na potrzeby działań operacyjnych, pojawia się pytanie, gdzie przebiega granica między etycznym wykorzystaniem takich informacji, a już w głębszą ingerencję w sferę prywatną<sup>46</sup>. Nawet jeśli treści są jawne, ich masowe przetwarzanie musi odbywać się zgodnie z zasadami wynikającymi z RODO przede wszystkim z zasadą

<sup>43</sup> D. Sołodow, *Poszukiwania osób zaginionych*, [w:] *Kryminalistyka*, (red.) E. Gruza, I. Sołtyśzewski, Warszawa 2022, s. 248–249.

<sup>44</sup> Zarządzenie nr 805 Komendanta Głównego Policji z dnia 31 grudnia 2003 r. w sprawie „Zasad etyki zawodowej policjanta” (Dz. Urz. KGP z 2004 r., nr 1, poz. 3).

<sup>45</sup> K. Mroziewicz, *Czas pluskiew*, Warszawa 2007, s. 334.

<sup>46</sup> K. Bayer, J. Bitner, *Wykorzystanie mediów społecznościowych...*, op. cit., s. 12–13.

minimalizacji danych i wykorzystywania ich wyłącznie w konkretnym, jasno określonym celu<sup>47</sup>.

Należy przyjąć, iż służby powinny prowadzić działania poszukiwawcze przy wykorzystaniu mediów cyfrowych z taką świadomością, jakby osoba zaginiona była przy nich obecna. To znaczy z pełnym szacunkiem do jej prywatności, godności i uczuć. Chodzi o to, by po odnalezieniu nie musiała się zmagać z tym, że jej dane, zdjęcia czy prywatne informacje trafiły do przestrzeni publicznej bez potrzeby. Żeby uniknąć takiego dyskomfortu i poczucia naruszenia prywatności, działania powinny być nie tylko skuteczne, ale też etyczne. A to wymaga dobrze przygotowanej kadry policjantów, którzy wiedzą, gdzie postawić granicę i jak korzystać z cyfrowych narzędzi z odpowiedzialnością.

W świetle zdiagnozowanych ryzyk prawnych i etycznych, a także braku kompleksowej regulacji, konieczne jest sformułowanie postulatów legislacyjnych (*de lege ferenda*) oraz propozycji działań usprawniających istniejący stan prawny (*de lege lata*), aby zapewnić skuteczność poszukiwań i ochronę praw obywatelskich.

Jednym z głównych problemów całego systemu poszukiwań jest brak jednego, kompleksowego aktu prawnego, który w całości regulowałby tę tematykę. Obecnie wszystko opiera się głównie na przepisach ogólnych, takich jak ustawa o Policji, oraz na wewnętrznych regulacjach, np. zarządzeniach Komendanta Głównego Policji<sup>48</sup>. To sprawia, że w praktyce pojawiają się konkretne ryzyka. Przede wszystkim brakuje jednolitych procedur skoro nie ma centralnego aktu ustawowego, różne jednostki mogą działać w odmienny sposób, co prowadzi do chaosu i niedopowiedzeń. Na ten problem zwracało już uwagę m.in. Biuro Rzecznika Praw Obywatelskich. Dodatkowo, tak niejasne ramy prawne powodują też pytania o to, kto dokładnie ma jakie kompetencje i do jakiego stopnia może ingerować w prywatność osoby zaginionej czy jej bliskich zwłaszcza gdy w grę wchodzi zbieranie informacji z mediów cyfrowych czy innych źródeł. Trzeba również w końcu ujednoczyć sposób dokumentowania tego, co służby pozyskują z mediów cyfrowych. Teraz wygląda to różnie czasem są to tylko notatki urzędowe, które nie mają takiej mocy jak protokoły i nie mogą być później użyte jako dowód w sprawie karnej. Brakuje jasnych zasad, jak to robić poprawnie, a bez tego zebrane informacje mogą po prostu „wypaść” z postępowania.

<sup>47</sup> J. Marczak, *Biały wywiad – źródło informacji w dobie społeczeństwa informacyjnego*, Warszawa 2020, s. 2–4.

<sup>48</sup> K. Bayer, J. Bitner, *Wykorzystanie mediów społecznościowych...*, op. cit., s. 12–13.

Ważne jest, żeby jasno uregulować zasady współpracy Policji z organizacjami pozarządowymi, jak np. Fundacja ITAKA, czy grupami ratowniczymi. Chodzi o to, żeby było wiadomo, kto, kiedy i na jakich zasadach może przekazywać sobie informacje np. zdjęcie zaginionego, jego dane czy inne ważne szczegóły. Dzięki temu apel do społeczeństwa będzie bardziej spójny, a działania będą szybsze i skuteczniejsze.

Na gruncie obecnego prawa widać, że przy obecnych przepisach brakuje funkcjonariuszom wystarczającego wsparcia, jeśli chodzi o działania z wykorzystaniem *SOCMINT*. Problemem jest mała liczba szkoleń i ograniczony dostęp do specjalistycznego sprzętu przez co policjanci często muszą korzystać z prywatnych urządzeń, co rodzi ryzyko dla bezpieczeństwa danych i zgodności z procedurami<sup>49</sup>. Do tego dochodzą błędy systemowe np. opóźnienia w pobieraniu *DNA* czy niepełne dane o zaginionych w KSIP które potrafią zablokować skuteczne działanie, nawet jeśli analiza z mediów społecznościowych wskazuje na realne zagrożenie. To wszystko pokazuje, że skuteczność poszukiwań z użyciem nowych technologii zależy nie tylko od narzędzi, ale też od inwestycji w ludzi i zasoby<sup>50</sup>.

## Podsumowanie

Dlatego tak ważne jest inwestowanie nie tylko w sprzęt, ale przede wszystkim w ludzi czyli dobrze przygotowane kadry policyjne. Szkolenia z zakresu wykorzystania mediów cyfrowych powinny być dostępne i obowiązkowe nie tylko dla funkcjonariuszy, ale też dla innych podmiotów biorących udział w poszukiwaniach takich jak fundacje, wolontariusze czy prywatni detektywi. To właśnie oni często jako pierwsi reagują i działają w przestrzeni online, dlatego muszą znać podstawowe zasady legalności, etyki i ochrony danych<sup>51</sup>. Wprowadzenie takiego systemowego podejścia do edukacji w tym zakresie z pewnością usprawni cały mechanizm poszukiwań, a w dłuższej perspektywie może nawet wpłynąć na potrzebę doprecyzowania regulacji prawnych tak, by były one dostosowane do realiów i narzędzi, którymi faktycznie się dziś posługujemy.

<sup>49</sup> P. Mieszkalska, *Ocena funkcjonowania...*, op. cit., s. 136.

<sup>50</sup> K. Bayer, J. Bitner, *Wykorzystanie mediów społecznościowych...*, op. cit., s. 34.

<sup>51</sup> D. Sołodow, *Poszukiwania osób zaginionych...*, op. cit., s. 248–249.

## Bibliografia

- Bayer K., Bitner J., *Wykorzystanie mediów społecznościowych przez funkcjonariuszy polskiej Policji – próba wstępnego opisu*, „Przegląd Wschodnioeuropejski” 2020, nr 2.
- Bayer K., Bitner J., *Wykorzystanie mediów społecznościowych przez funkcjonariuszy polskiej Policji. Próba wstępnego opisu zjawiska na podstawie wyników badań kwestionariuszowych*, [w:] *Media społecznościowe w pracy organów ścigania*, (red.) P. Waszkiewicz, Warszawa 2021.
- Brakoniecki D., *Detektywi*, [w:] *Pracownicy formacji bezpieczeństwa i porządku publicznego, służb ratownictwa i ochrony*, (red.) M. Czuryk, M. Karpiuk, Olsztyn 2017.
- Brakoniecki D., *Detektywistyka. Prawne i funkcjonalne aspekty działalności detektywistycznej w Polsce i na świecie*, Warszawa 2016.
- Brakoniecki D., *Ustawa o usługach detektywistycznych jako forma prywatyzacji zadań administracji publicznej w obszarze bezpieczeństwa i porządku publicznego*, „Journal of Modern Science” 1/36/2018.
- Dębniak H., Rabczuk S., *Wybrane aspekty prawne pozyskiwania danych z mediów społecznościowych przez polskie organy ścigania*, [online] (dostęp: 6.12.2025).
- Jabłoński R., *Ujawnianie i zabezpieczanie śladów cyfrowych*, [w:] *Ślady cyfrowe*, (red.) J. Widacki, Kraków 2022.
- Konieczny M., *Znaczenie serwisów społecznościowych w pracy służby prasowej Policji i ich wpływ na skuteczność działań informacyjnych*, „Przegląd Policyjny” 2021, nr 2.
- Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997 nr 78 poz. 483 ze zm.).
- Koper B., *Praktyczne kompetencje detektywa w kontekście współczesnych zagrożeń bezpieczeństwa*, [w:] *Bezpieczeństwo a działalność detektywistyczna*, (red.) J. Widacki, T. Hanausek, Kraków 2020.
- Kozłowski J., *Ochrona danych w cyberprzestrzeni. Aspekty prawne i organizacyjne*, Warszawa 2020.
- Łabuz P., *Ustawa o Policji. Komentarz*, Warszawa 2022.
- Malinowska I., Adamus M., *Kiedy zaginęło dziecko – podstawowe informacje prawne*, [w:] *Wolni od patologii*, (red.) M. Krysiak, Maków Mazowiecki 2011.
- Malinowska I., *Problematyka zaginięć ludzi w aspekcie prawno-krymonologicznym*, „Problemy Współczesnej Kryminalistyki” 2023, t. XXII.
- Malinowska I., Rybicka A., *Zagrożenia społeczne wynikające z zaginięć ludzi we współczesnym świecie*, „Kwartalnik Policyjny” 2016, nr 1 (36).
- Malinowska I., *Zaginięcia ludzi i aspekty bezpieczeństwa – podejście komparatystyczne*, Sofia 2025.
- Marczak J., *Biały wywiad – źródło informacji w dobie społeczeństwa informacyjnego*, Warszawa 2020.
- Mieszalska P., *Ocena funkcjonowania systemu poszukiwania osób zaginionych w Polsce*, „Prokuratura i Prawo” 2023, nr 9.
- Mieszalska P., *Wykorzystanie analizy treści publikowanych w mediach społecznościowych w ramach pracy operacyjno-rozpoznawczej*, [w:] *Bezpieczeństwo i prawo. Współczesne wyzwania*, (red.) E. Gromek-Broc, Warszawa 2023.
- Mieszalska P., *Wykorzystanie mediów społecznościowych jako narzędzia poszukiwania osób zaginionych. Aspekty prawne i praktyczne*, Warszawa 2022.

- Mieszalska P., *Zaginięcie osoby jako sytuacja kryzysowa z perspektywy psychologii i praktyki działań służb*, [w:] *Zaginięcia osób. Aspekty kryminalistyczne, psychologiczne i społeczne*, (red.) J. Widacki, P. Mieszalska, Katowice 2023.
- Mroziewicz K., *Czas pluskiew*, Warszawa 2007.
- Najwyższa Izba Kontroli, *Informacja o wynikach kontroli. Poszukiwanie osób zaginionych*, Warszawa 2015.
- Nowikowska M., *Procesowa kontrola danych informatycznych w chmurze obliczeniowej*, „Zeszyty Naukowe Akademii Sztuki Wojennej” 2021, nr 2.
- Płatek A., *Media społecznościowe w pracy organów ścigania i wymiaru sprawiedliwości*, [w:] *Regulacje prawne funkcjonowania społeczeństwa informacyjnego*, (red.) A. Płatek, Kraków 2022.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. UE L 119/1).
- Social Media 2025*, raport opracowany przez Polskie Badania Internetu i Gemiusa na podstawie badania Mediapanel; uzupełniony danymi z raportu *Digital 2025: Poland* (DataReportal, Meltwater).
- Sołodow A., *Zabezpieczanie śladów cyfrowych w praktyce kryminalistycznej*, [w:] *Prawne i społeczne aspekty bezpieczeństwa w dobie transformacji cyfrowej*, (red.) A. Sołodow, Warszawa 2022.
- Sołodow D., *Poszukiwania osób zaginionych*, [w:] *Kryminalistyka*, (red.) E. Gruza, I. Sołtyszewski, Warszawa 2022.
- Stanowisko Prezesa Urzędu Ochrony Danych Osobowych w sprawie dostępu policji do danych telekomunikacyjnych (lipiec 2024).
- Tusnio A., Wolny A., *Nowoczesne narzędzia i sprzęt wykorzystywane do poszukiwań osób zaginionych*, „Zeszyty Naukowe SGSP” 2022, nr 61, t. 2.
- Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz. U. z 2023 r., poz. 171 ze zm.).
- Ustawa z dnia 6 lipca 2001 r. o usługach detektywistycznych (t.j. Dz. U. z 2020 r., poz. 129).
- Wasik A., Strynkowska W., *Rola prywatnego detektywa w poszukiwaniach osób zaginionych*, „Prace Naukowe Uniwersytetu Jana Długosza w Częstochowie. Prawo” 2022, t. XVII, nr 1.
- Waszkiewicz P. (red.), *Media społecznościowe w pracy organów ścigania*, Warszawa 2021.
- Wentkowska A., *Poszukiwania osób zaginionych. System i metody działania w procedurach służb*, Warszawa 2016.
- Wojnicz P., *Zaginięcia osób. Studium prawne, kryminalistyczne i kryminologiczne*, Olsztyn 2021.
- Wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 6 października 2020 r., La Quadrature du Net i in. przeciwko Premier ministre i in., sprawy połączone C-511/18, C-512/18 i C-520/18.
- Zarządzenie nr 805 Komendanta Głównego Policji z dnia 31 grudnia 2003 r. w sprawie „Zasad etyki zawodowej policjanta” (Dz. Urz. KGP z 2004 r., nr 1, poz. 3).
- Zubańska M., Knut P., *Niewykryte przestępstwa sprzed lat, nowoczesne narzędzia techniki kryminalistycznej i policyjne Zespoły do spraw Przestępstw Niewykrytych, czyli crimen grave non potest esse impunibile – cz. II*, „Przegląd Policyjny” 2016, nr 3 (123).