Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury
Quarterly of the National School of Judiciary and Public Prosecution
Zeszyt 1 (41)/2021

Wykorzystanie białego wywiadu w działalności Policji i prokuratury

ANDRZEJ LEBIEDOWICZ*

STRESZCZENIE
Artykuł wskazuje na szerokie możliwości, jakie daje wykorzystanie przez Policję w toku czynności operacyjno-rozpoznawczych oraz w ramach prowadzonych postępowań przygotowawczych przez Policję i prokuraturę tzw. informacji jawnoźródłowych. Stanowi syntezę definicji białego wywiadu i jego źródeł. Porusza kwestię inicjowania postępowań przygotowawczych dzięki informacjom pochodzącym z otwartych źródeł, odnosi się do zagadnienia korzystania z informacji jawnoźródłowych w pracy operacyjnej Policji. Ukazuje też zalety stosowania białego wywiadu w ramach działań poszukiwawczych oraz na tle narzędzia informatycznego ESOM (Elektroniczny System Odzyskiwania Mienia), przedstawiając go na tle analizy kryminalnej. Autor formułuje wnioski *de lege ferenda* w zakresie udoskonalenia narzędzia analitycznego w ramach Systemu Wsparcia Prokuratora. Przedmiotowa publikacja dostrzega znaczący potencjał śledczy, jaki daje właściwie ukierunkowany monitoring otwartych źródeł informacji.

Słowa kluczowe: czynności operacyjno-rozpoznawcze, biały wywiad, system wsparcia prokuratora

WSTĘP

Cechą charakterystyczną obecnych czasów jest systematyczny wzrost zapotrzebowania na informacje, które są kluczowe dla procesu podejmowania strategicznych

* Mgr Andrzej Lebiedowicz, Prokurator Prokuratury Rejonowej Lublin-Południe w Lublinie, delegowany do Prokuratury Okręgowej w Lublinie, Naczelnik Wydziału III ds. Przestępczości Gospodarczej Prokuratury Okręgowej w Lublinie.

decyzji z punktu widzenia danej instytucji[1]. Znaczący wpływ na wartość informacji mają jej jakość i użyteczność[2]. Wywiad oznacza działalność, w wyniku której uzyskuje się informacje, a informacja wywiadowcza to produkt, który powstaje w wyniku przetwarzania informacji dotyczących danej dziedziny lub obszaru zainteresowania[3]. Termin „biały wywiad" wraz z jego synonimami, takimi jak otwarte źródła informacji czy OSInt (ang. *Open Source Inteligence*), ugruntował swoją pozycję w fachowej literaturze przedmiotu (policyjnej, wojskowej, kryminalistycznej, dotyczącej bezpieczeństwa wewnętrznego)[4]. Zdaniem większości znawców omawianej tematyki zasadnym jest stawianie znaku równości pomiędzy szeroko rozumianym wywiadem ze źródeł otwartych (OSInt), a białym wywiadem[5]. Organy ścigania, realizując swoje ustawowe zadania, korzystają z otwartych źródeł informacji, a biały wywiad stanowi autonomiczną formę gromadzenia informacji. Według powszechnie panującej opinii na gruncie obecnego stanu wiedzy ustalenia faktyczne poczynione w oparciu o biały wywiad nie powinny mieć waloru dowodowego, gdyż jego funkcję należałoby odnosić przede wszystkim do funkcji rozpoznawczej[6]. Wyszukiwanie wartościowych informacji ze źródeł otwartych to tradycyjnie jedna z elementarnych metod pracy służb specjalnych powołanych do ochrony konstytucyjnych struktur państwowych narażonych na zagrożenia o charakterze zewnętrznym i wewnętrznym. Służby policyjne pomimo odmiennego od służb specjalnych celu działania, ukierunkowanego na zapewnienie porządku publicznego oraz bezpieczeństwa, na płaszczyźnie zwalczania przestępczości zorganizowanej, posługują się metodami zbliżonymi do tych praktykowanych przez służby specjalne, do których zalicza się także zdobywanie informacji pochodzących ze źródeł ogólnie dostępnych[7]. W. Mądrzejowski charakteryzuje biały wywiad policyjny w kategoriach systemu pomocniczego względem klasycznie już pojmowanej pracy operacyjno-śledczej, który winien być w sposób bezwzględny

---

1 Zob. J.W. Wójcik, *Wywiad i kontrwywiad gospodarczy*, Warszawa 2018, s. 11.

2 Zob. K. Liedel, T. Serafin, *Otwarte źródła informacji w działalności wywiadowczej. Zarys problematyki*, Warszawa 2011, s. 42.

3 Zob. M. Minkina, *Sztuka wywiadu w państwie współczesnym*, Warszawa 2014, s. 31.

4 Zob. K. Gradoń, *Możliwości taktycznego wykorzystania otwartych źródeł informacji w Internecie przez organa ścigania oraz sprawców przestępstw i zamachów terrorystycznych*, [w:] *Problemy współczesnej kryminalistyki*, t. XIX, E. Gruza, T. Tomaszewski, M. Goc (red.), Warszawa 2015, s. 44.

5 Zob. B. Saramak, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Warszawa 2015, s. 15.

6 Zob. P. Chlebowicz, *„Biały wywiad" z perspektywy kryminalistyki*, [w:] *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipkowski i W. Mądrzejowski (red. nauk.), Warszawa 2012, s. 70-71.

7 Zob. W. Mądrzejowski, *„Biały wywiad" w Policji*, [w:] *Biały wywiad. Otwarte źródła informacji…*, s. 118.

weryfikowany za pomocą innych metod uzyskiwania informacji[8]. Obecnie warunkiem skutecznego zwalczania przestępczości jest wielopłaszczyznowe gromadzenie i wykorzystanie wiedzy stymulowanej rozwojem technik informatycznych oraz nieustanną współpracą międzynarodową. Dzięki otwartym źródłom informacji udaje się zgromadzić mniej więcej 80% możliwych do pozyskania danych wywiadowczych[9]. Organy ścigania, pomimo istotności roli, jaką odgrywają dane uzyskiwane z otwartych źródeł informacji, nie dysponują zintegrowanym systemem korzystania z OSInt. Polskie ustawodawstwo nie zawiera regulacji odnoszących się do terminów: otwarte źródła informacji czy też biały wywiad, co należy ocenić w kategoriach luki ustawodawczej[10]. „Niewątpliwie główną zaletą białego wywiadu nad pozostałymi metodami wywiadowczymi jest szybkość, łatwość pozyskiwania informacji, ilość i różnorodność, przejrzystość i niskie koszty ich weryfikacji"[11]. Zdaniem zaś Ch. Westphala „skuteczne śledztwa są pochodną szybkiego i precyzyjnego łączenia danych z wielu źródeł"[12].

DEFINICJA BIAŁEGO WYWIADU

Informacja jest podstawowym elementem każdego systemu rozpoznania[13]. Zakresy ciężkości gatunkowej czynności wywiadowczych są wyznaczane stopniowalną nomenklaturą ciemności barw[14]. Na gruncie literatury przedmiotu klasyczny jest trójpodział wywiadu (z uwagi na trzy rodzaje informacji) na:

a) biały wywiad, tj. informacje pochodzące z otwartych źródeł, stanowiące 80% danych wygenerowanych w następstwie eksploracji źródeł jawnych: prawnych, prasowych, jak też prywatnych;
b) szary wywiad, określany jako źródła zamknięte, dostarczający ok. 15% danych uzyskanych w toku aktywności o charakterze śledczym i detektywistycznym,

---

8 Zob. ibidem, s. 129.

9 Zob. K. Jarczewska-Walendziak, *Wykorzystanie otwartych źródeł informacji przez służby śledcze*, „Toruńskie Studia Bibliologiczne" 2017, nr 1(18), s. 136.

10 K.B. Rapkowska, P.M. Zackiewicz, *Biały wywiad w zwalczaniu przestępczości kryminalnej i zorganizowanej*, http://www.knbm.amw.gdynia.pl/wp-content/uploads/2014/12/Rapkowska-Karolina-Zackiewicz-Paulina-Bia%C5%82y-wywiad-w-zwalczaniu-przest%C4%99pczo%C5%9Bci-kryminalnej-i-zorganizowanej.pdf. (dostęp: 20.07.2020 r.).

11 Ibidem, http://www.knbm.amw.gdynia.pl/wp-content/uploads/2014/12/Rapkowska-Karolina-Zackiewicz-Paulina-Bia%C5%82y-wywiad-w-zwalczaniu-przest%C4%99pczo%C5%9Bci-kryminalnej-i-zorganizowanej.pdf, (dostęp: 20.07.2020 r.).

12 Zob. K. Góral, Przewodnik po wybranych narzędziach białego wywiadu (OSINT), https://datawalk.com/wp-content/uploads/2018/06/DataWalk-Przewodnik-po-narzedziach-OSINT.pdf, (dostęp: 20.07.2020 r.).

13 Zob. A. Żebrowski, *Wywiad i kontrwywiad XXI wieku*, Lublin 2010, s. 223.

14 Zob. K. Turaliński, *Wywiad gospodarczy i polityczny. Metodyka, taktyka i źródła pozyskiwania informacji*, Radom 2011, s. 27.

w ramach infiltracji i inwigilacji, rozumianej jako monitoring oraz obserwacja, a także działań socjotechnicznych i analiz kryminalistycznych;

c) czarny wywiad, stanowiący synonim szpiegostwa, pozwalający uzyskać 5% najbardziej cennych informacji, pozyskiwanych ze źródeł niejawnych, korzystających z ochrony właściwych klauzul tajności, z uwagi na kluczową rolę w procesie obiegu informacji w danej instytucji[15].

Zgodnie z definicją wypracowaną przez NATO (*ang. North Atlantic Treaty Organization*) biały wywiad jest określany mianem „danych wywiadowczych ze źródeł otwartych". Są to dane pochodzące z publicznie dostępnych informacji, jak też z innych informacji o charakterze jawnym, cechujących się ograniczonym zakresem rozpowszechniania lub dostępem[16].

Korelującą z zaprezentowaną powyżej definicją sformułowaną przez Pakt Północnoatlantycki jest ta zakładająca, iż „OSInt to wynik przeprowadzenia pewnych czynności w stosunku do informacji. Są one specjalnie poszukiwane, porównywane ze sobą co do treści, wybierane są te najważniejsze dla odbiorcy procesu"[17].

Zdaniem B. Świączkowskiego „biały wywiad to jedna z metod działania służb specjalnych polegająca na uzyskiwaniu i monitoringu jawnych informacji przede wszystkim do celów analityczno-informacyjnych służb"[18].

J. Konieczny uważa natomiast, iż biały wywiad w najbardziej ogólnym ujęciu stanowi metodę pozyskiwania oraz analizy informacji wywodzących się ze źródeł otwartych o charakterze ogólnodostępnym[19].

Według innej definicji występującej na gruncie polskiej literatury przedmiotu biały wywiad, zwany także „wywiadem jawnoźródłowym", to jedna z dyscyplin wywiadowczych, której istota sprowadza się do zaplanowanego pozyskiwania informacji ze źródeł otwartych, celem poddania ich dalszemu selekcjonowaniu, zestawianiu, digitalizacji, transkrypcji, tłumaczeniu, analizie, wywiedzenia zestawień oraz wnioskowań na ich podstawie, przy czym produkt finalny po nadaniu odpowiedniej formy wizualnej podlega dystrybucji na rzecz uprzednio ustalonej grupy odbiorców[20].

---

15 Zob. J.W. Wójcik, *Wywiad i kontrwywiad…*, s. 140.

16 Zob. K. Gradoń, *Możliwości taktycznego wykorzystania…*, s. 43.

17 G. Dobrowolski, W. Filipkowski, M. Kisiel-Dorohnicki, W. Rakoczy, *Wsparcie informatyczne dla analizy otwartych źródeł informacji w Internecie w walce z terroryzmem. Zarys problemu*, [w:] L.K. Paprzycki, Z. Rau, *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu*, Warszawa 2009, s. 279.

18 B. Świączkowski, *Wykorzystanie tzw. białego wywiadu w działalności analityczno-informacyjnej Agencji Bezpieczeństwa Wewnętrznego*, [w:] *Biały wywiad. Otwarte źródła informacji…*, s. 165.

19 J. Konieczny, *Zagadnienia wprowadzające*, [w:] *Analiza informacji w służbach policyjnych i specjalnych*, J. Konieczny (red.), Warszawa 2012, s. 2.

20 Zob. K. Liedel, T. Serafin, *Otwarte źródła informacji…*, s. 54-55.

Z kolei zdaniem K. Mroziewicza biały wywiad stanowi analizę informacji uzyskanych z legalnie dostępnych źródeł, która z uwagi na swoją prostotę i poszanowanie legalizmu stanowi najbardziej przyjazną oraz najbezpieczniejszą „formę zdobywania tajemnic"[21].

Najbardziej zaawansowanym etapem analizowania otwartych danych – obok następujących po sobie kolejno: OSD – dane pochodzące z pierwotnego źródła (*ang. Open Source Data*), OSIF – dane poddane wstępnej analizie (*ang. Open Source Information*), OSInt – wybrane dane przekazane wyselekcjonowanej grupie odbiorców (*ang. Open Source Intelligence*) – stanowią dane uprzednio zweryfikowane, co do których można wywieść ocenę o wysokim poziomie ich pewności, zawierające potwierdzenie w innych źródłach, w tym tajnych, lub innych otwartych, określane mianem OSInt-V, tj. dane zweryfikowane (*ang. Validated OSInt*)[22].

Konieczne jest też wyraźne rozróżnienie jawnych danych otwartych od jawnych otwartych informacji, gdyż w drugim z przytoczonych terminów wyrażają się dane już wstępnie zebrane (wyrażone w formie drukowanej, w postaci przekazu telewizyjnego, radiowego, stron internetowych, wystąpień publicznych itp.) oraz przybierające postać jednego dokumentu poddanego zabiegom edytorskim[23].

Z kolei zweryfikowany, tj. potwierdzony biały wywiad (OSInt-V), jako efekt pracy wyszkolonego analityka posiadającego dostęp do różnorodnych baz danych (w tym objętych tajemnicą, niejawnych), stanowi produkt cechujący się wysokim stopniem pewności oraz prawdopodobieństwa[24].

ŹRÓDŁA BIAŁEGO WYWIADU

K. Liedel i T. Serafin wskazują, iż kanałami informacji o charakterze publicznym i otwartym, służącym do wysyłania komunikatów w eter, mogą być: środowiska naukowe i akademickie, administracja publiczna, organizacje międzynarodowe i pozarządowe, środki masowego przekazu, podmioty komercyjne, biblioteki, jak też osoby fizyczne, lub grupy osób[25].

Na gruncie literatury przedmiotu występują różne klasyfikacje źródeł informacji o charakterze otwartym.

---

[21] K. Mroziewicz, *Czas pluskiew*, Warszawa 2007, s. 334.

[22] Zob. B. Stromczyński, P. Waszkiewicz, Biały *wywiad w praktyce organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, „Prokuratura i Prawo" 2014, nr 5, 149.

[23] Zob. K.B. Rapkowska, P.M. Zackiewicz, *Biały wywiad w zwalczaniu przestępczości…*.

[24] Zob. K. Radwaniak, *Biały wywiad w Policji – narzędzie rozpoznawania zagrożeń terrorystycznych*, „Studia prawnicze. Rozprawy i Materiały" 2012, nr 2(11), s. 89.

[25] Zob. K. Liedel, T. Serafin, *Otwarte źródła informacji…*, s. 57.

Według jednej z nich z uwagi na lokalizację danych możemy wyróżnić:

1) media obejmujące media elektroniczne w postaci internetu, prasę codzienną, jak też tę ukazującą się periodycznie, audycje telewizyjne;
2) źródła akademickie oraz profesjonalne: artykuły naukowe, oświadczenia ekspertów, sympozja, konferencje, dane formułowane przez korporacje zawodowe;
3) dane o charakterze publicznym, tj. dane oficjalne (dane demograficzne), raporty rządowe, konferencje prasowe, debaty legislacyjne, oficjalne wystąpienia[26].

B. Saramak dzieli otwarte źródła informacji na:

a) prasę (codzienną, branżową, naukową, dziennikarstwo śledcze, monitoring branżowych periodyków);
b) szarą literaturę (publikacje książkowe, opracowania naukowe, zawierające fachową i przydatną wiedzę, teksty własne opublikowane w ramach self-publishingu, trudno dostępne książki nieobjęte rejestracją bibliograficzną, dokumenty rządowe, akademickie, biznesowe, przemysłowe znajdujące się poza komercyjnym obiegiem wydawniczo – księgarskim, raporty naukowe, techniczne);
c) radio telewizję (setki stacji nadawczych z tysiącami programów i audycji o charakterze tematycznym);
d) ogólnie dostępne rejestry i dokumenty (KRS,CEIDG, Rejestr Gospodarki Narodowej – REGON, MSiG – Monitor Sądowy i Gospodarczy, księgi wieczyste –KW, Orka, Orka 2, portal obywatelski mojePanstwo.pl);
e) geoinformację (System Informacji Geograficznej – GIS, Geoportal, Google Street View, wingle.net);
f) internet (Facebook, VK, Goldenline, LinkedIN, You Tube, Wikipedia, Wikileaks, NewspaperARCHIVE.com, Wayback Machine, osintinsight.com, CI CENTRE);
g) inne źródła (inżynieria odwrotna – ang. *reverse engineering*)[27].

Klasyfikacja otwartych źródeł informacji z punktu widzenia przydatności do wykorzystania w pracy organów ścigania, zaproponowana przez B. Stromczyńskiego i P. Waszkiewicza, obejmuje:

a) media określane na potrzeby klasyfikacji jako tradycyjne, tj. literaturę (książki, analizy, śledztwa dziennikarskie, użyteczną publicystykę), prasę drukowaną (dokumenty rządowe, czasopisma branżowe, dzienniki), telewizję o profilu informacyjnym, rozgłośnie radiowe;
b) usługi o charakterze komercyjnym świadczone przez wydawnictwa marketingowe, podmioty gospodarcze opracowujące w zamian za wynagrodzenie raporty o określonym profilu oraz analizy;

---

[26] Zob. K. Gradoń, *Możliwości taktycznego wykorzystania…*, s. 44.
[27] Zob. B. Saramak, *Wykorzystanie otwartych źródeł…*, s. 63-91.

c) internet dający dostęp do: portali społecznościowych, internetowych wydań gazet i czasopism, wikis (Wikileaks, Wikipedia), blogów, mikroblogów, stron internetowych przedsiębiorców, serwisów wideo, serwisów fotograficznych, map, zdjęć lotniczych lub satelitarnych, rejestrów domen WHOIS;
d) literaturę określaną jako niszową (ang. *grey literature*) obejmującą informacje, analizy, będące dostępnymi wyłącznie poprzez wyspecjalizowane kanały, tworzone przez ośrodki akademickie, organizacje o charakterze państwowym oraz pozarządowym;
e) katalogi oraz bazy danych[28].

Z kolei T. Aleksandrowicz wyróżnia cztery źródła otwartych danych, które podlegają analizie, tj.:

1) komercyjne bazy danych;
2) informacje ogólnodostępne;
3) opracowania wydawane przez indywidualnych ekspertów oraz
4) „szarą literaturę[29].

K. Wiciak do „białych" źródeł wywiadu państwowego oraz gospodarczego zalicza:

I. prasę (specjalistyczną, lokalną) oraz inne środki masowego przekazu;
II. internet,
III. ogólnie dostępne rejestry;
IV. dokumentację udostępnianą przez przedsiębiorców zgodnie z wymogami prawa;
V. wydawnictwa marketingowe (reklamy, informatory, biuletyny);
VI. sądowe ogłoszenia o upadłości, a także postanowienia o postępowaniu układowym;
VII. analizy produktów (ang. *reverse engineering*)[30].

P. Niemczyk jako jedno z podstawowych, a zarazem efektywnych źródeł informacji z zakresu białego wywiadu wskazuje na wywiadownie gospodarcze, korzystające z trzech standardowych źródeł informacji:

a) danych pochodzących z państwowych oraz samorządowych ewidencji, jak też rejestrów, przede wszystkim z Krajowego Rejestru Sądowego i Centralnej Ewidencji i Informacji o Działalności Gospodarczej;
b) danych pochodzących z kwerendy wycinków prasowych oraz publikacji internetowych;
c) ankiet wysyłanych do uzupełnienia przedsiębiorcom[31].

---

[28] Zob. B. Stromczyński, P. Waszkiewicz, *Biały wywiad w praktyce…*, s. 150.

[29] Zob. T. Aleksandrowicz, *Biały wywiad w walce z terroryzmem*, [w:] *Rola mediów w przeciwdziałaniu terroryzmowi*, K. Liedel, P. Piasecka (red.), Warszawa 2009, s. 81.

[30] Zob. K. Wiciak, *ESOM jako narzędzie „białego wywiadu"*, [w:] *Biały wywiad. Otwarte źródła informacji…*, s. 107.

[31] Zob. P. Niemczyk, *Wywiadownie gospodarcze jako źródło informacji białego wywiadu*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9 (5), s. 147, 149.

P. Maciołek w obrębie struktury internetu wyróżnia następujące źródła danych pozwalające czerpać informacje, tj.:

1) serwisy informacyjne, portale, wortale;
2) blogi (dzienniki internetowe);
3) fora internetowe, hosty dyskusyjne;
4) otwarte serwisy chat oraz IRC;
5) serwisy społecznościowe;
6) inne rodzaje źródeł internetowych (strony domowe, bazy danych, serwisy aukcyjne oraz z drobnymi ogłoszeniami, sieci wymiany plików, głęboka sieć)[32].

Z kolei A. Ziółkowska, analizując kwestię białego wywiadu jako narzędzia uzupełniającego czynności z zakresu techniki kryminalistycznej i odnosząc się do zagadnienia prognozowanego wykorzystania tego wywiadu w celach wykrywczych, wydzieliła trzy kategorie (które można ubocznie wykorzystać także do podziału otwartych źródeł informacji dostępnych w internecie), t.j.:

a) poszukiwanie motywów i świadków przestępstw (1 – źródło internetowe: fora internetowe zamieszczane pod artykułami zawierającymi opisy bulwersujących zbrodni);
b) poszukiwanie informacji o powiązaniach osobowych oraz kapitałowych pomiędzy osobami, tj. podejrzanymi, ofiarami przestępstw, sprawcą kierowniczym, a bezpośrednim wykonawcą (2 – źródło internetowe: Krajowy Rejestr Sądowy i Centralna Ewidencja i Informacja o Działalności Gospodarczej, serwisy społecznościowe, tj. Facebook, Nasza-klasa, LinkedIN, Golden Line, informacje marketingowe podmiotów gospodarczych;
c) analizy przesiewowe prowadzone na podstawie powszechnie dostępnych danych (3 – źródło internetowe: tematyczne grupy dyskusyjne na portalach społecznościowych dające możliwość prewencyjnego ustalania informacji o środowiskach niebezpiecznych)[33].

Według wiarygodnych szacunków największa wyszukiwarka Google indeksuje tylko 6% zawartości internetu, wobec czego korzystanie w procesie eksploracji przestrzeni z danymi z alternatywnych wyszukiwarek daje szanse na poszerzenie pola widzenia u poszukujących wartościowych informacji. Bardzo pomocne w wyszukiwaniu osób i biznesowych adresów e-mail okazują się takie wyszukiwarki i serwisy jak: pipl.com, spokeo.com, webmii.com, findthat.email, neadreach.com.

---

[32] Zob. P. Maciołek, *Internet, a OSINT – szanse i praktyczne zastosowania*, [w:] *Biały wywiad. Otwarte źródła informacji…*, s. 225-230.

[33] Zob. A. Ziółkowska, *Biały wywiad jako narzędzie uzupełniające czynności z zakresu techniki kryminalistycznej*, „Acta Universitatis Lodziensis Folia Iuridica" 2018 nr 82, https://doi.org/10.18778/0208-6069.82.06, (dostęp: 20.07.2020 r.).

Pośród zaś wyszukiwarek domen, e-maili i rejestru IP wskazuje się: hexillion.com, whois.net, website.informer, myip.ms (pozostałe narzędzia OSInt warte polecenia to: mxtoolbox.com, shodan.io, hamechk.com, similiarsites.com, debouncer.com, iplogger.org)[34].

W tym miejscu zasygnalizować tylko należy interesujące zagadnienie występujące w ramach omawianej tematyki pod nazwą Google hackingu, przez który to termin należy rozumieć takie formułowanie zapytań w przeglądarce Google, by udostępniała ona dane, do których użytkownik nie jest uprawniony w znaczeniu prawnym, etycznym, względnie w obu tych sensach, co zdaje się już wykraczać poza sferę wyznaczoną narzędziami białego wywiadu[35].

BIAŁY WYWIAD JAKO ŹRÓDŁO WIEDZY O PRZESTĘPSTWIE

Zgodnie z art. 303 kodeksu postępowania karnego z 1997 r.[36] podstawą do wydania postanowienia o wszczęciu postępowania przygotowawczego jest uzasadnione podejrzenie popełnienia przestępstwa, a dane, na których podstawie organy ścigania kształtują owo podejrzenie, mogą wynikać z różnorakich źródeł.

Asumptem do wszczęcia śledztwa może być klasyczne zawiadomienie o przestępstwie: ustne lub pisemne (art. 304 k.p.k.), informacja konfidencjonalna, własne spostrzeżenia poczynione przez organy ścigania, akt samodenuncjacji sprawcy, anonim, wynik własnych działań operacyjnych, ale także informacje płynące z radia, prasy czy telewizji[37].

„Coraz większy udział w ujawnieniu przestępstw mają publikatory, a zwłaszcza tzw. dziennikarstwo śledcze. Bardzo często w tropieniu tzw. afer, ujawnianiu nieprawidłowości w funkcjonowaniu sfery publicznej, korupcji, nadużyć prawa, niedopełnienia obowiązków czy przestępczości kryminalnej udział mają dziennikarze, wręcz prowadząc działania zbliżone do pracy operacyjnej służb państwowych, zbierając informacje i wyniki swoich prac publikują w środkach masowego przekazu. Informacja taka, bez względu na rodzaj publikacji (prasowa, radiowa, telewizyjna, internetowa), jeżeli zawiera dane uprawdopodabniające popełnienie przestępstwa, zgodnie ze wspomnianą zasadą legalizmu, powinna być potraktowana przez

---

[34] Zob. K. Góral, *Przewodnik po wybranych narzędziach białego wywiadu (OSINT)*, https://datawalk.com/wp-content/uploads/2018/06/DataWalk-Przewodnik-po-narzedziach-OSINT.pdf. (dostęp: 20.07.2020 r.).

[35] Zob. D. Mider, J. Garlicki, W. Mincewicz, *Poszukiwanie informacji z Internetu metodą Google Hacking – biały, szary, czy może czarny wywiad?*, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 20, s. 68.

[36] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2020 r. poz. 1086); dalej: k.p.k.

[37] Zob. T. Grzegorczyk, *Kodeks postępowania karnego. Komentarz*, Kraków 2004, s. 761.

uprawnione organy – Policję i prokuraturę – jako zawiadomienie o przestępstwie z pełnymi konsekwencjami wynikającymi z tego faktu”[38].

Wzmiankowane publikatory niewątpliwie zaliczyć należy do źródeł zewnętrznych pierwszych informacji o przestępstwie[39]. Nierzadko efekty śledztw dziennikarskich podane do wiadomości opinii publicznej przez różne kanały informacyjne stają się po ich dostrzeżeniu przez przedstawicieli organów ścigania impulsem do zainicjowania postępowań przygotowawczych. Nie mniej jednak każdy dziennikarz śledczy, realizując swoją aktywność zawodową musi mieć świadomość istnienia zasad procesowych, które obowiązują organy prowadzące śledztwo, dyrektywy zaś te winny, za sprawą określenia zakresu obowiązków, w sposób pośredni kształtować ich aktywność. „Dziennikarstwo śledcze ma na celu wykrywanie i publiczne ujawnianie zbrodni, korupcji wśród pełniących funkcje publiczne, nepotyzmu lub nadużyć władzy itp. Ujawnianie tych patologicznych zjawisk zawsze musi odbywać się w imię dobra publicznego oraz uwzględniać z jednej strony zasady wolnej prasy, z drugiej zaś chronić innych przed pochopnym osądem. Ma też zapewnić prawidłowe funkcjonowanie wymiaru sprawiedliwości”[40].

Pośród kryteriów, które współcześnie decydują o selekcji informacji dziennikarskich trafiających do mediów (z uwagi na stopień atrakcyjności dla odbiorców), wymienia się:

1) wartość progową zdarzenia;
2) przewidywalność;
3) uproszczenia;
4) indywidualizację;
5) ryzyko;
6) seksualność przestępstw;
7) osoby sławne lub o wysokim statusie;
8) bliskość;
9) przemoc;
10) spektakl i przedstawienie obrazowe;
11) dzieci;
12) ideologię konserwatywną i dywersję polityczną[41].

---

38 E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka, czyli rzecz o metodach śledczych*, Warszawa 2008, s. 32.

39 T. Hanausek, *Kryminalistyka. Zarys wykładu*, Zakamycze 2005, s. 79.

40 P. Kosmaty, *Dziennikarstwo śledcze musi być rzetelne*, https://archiwum.rp.pl/artykul/1384202-Dziennikarstwo-sledcze-musi-byc-rzetelne.html. (dostęp: 20.07.2020 r.).

41 W. Mądrzejowski, S. Śnieżko, P. Majewski, *Zwalczanie przestępczości. Wybrane metody i narzędzia*, Warszawa 2017, s. 189.

Głównym źródłem białego wywiadu w państwach demokratycznych deklarujących konstytucyjnie zagwarantowaną swobodę funkcjonowania prasy stanowią media. Za najbardziej cenne dla organów ścigania należy uznać te publikacje, które odnoszą się do różnego rodzaju afer (przejawy korupcji, defraudacji, koneksji politycznych, mobbingu). Nierzadko na łamach tych przekazów medialnych ukazywane są mniej lub bardziej czytelnie ujęte personalia osób, które były odpowiedzialne za będące przedmiotem opisu zdarzenia bulwersującego opinię publiczną. Często tego typu publikacje wskazują także dane na temat styczności konkretnych osób w pewnych kluczowych dla późniejszych śledztw lokalizacjach, co ma znaczenie podczas późniejszego weryfikowania alibi osób podejrzewanych[42].

Publikacje medialne będące efektem śledztw dziennikarskich z punktu widzenia prawa dowodowego nie są dowodem, lecz zawierają informacje o dowodzie lub dowodach. Dla odmiany waloru dowodowego nabierają już nawet treści zamieszczane w sieci teleinformatycznej przez osoby dopuszczające się zachowań wyczerpujących znamiona czynów zabronionych i jednocześnie, a które za sprawą chęci pochwalania się przed szerszą szerzą odbiorców dzięki możliwościom komunikacyjnym, jakie daje internet (np. nagrania sprawców z pobicia innej osoby zamieszczone na serwisie internetowym You Tube), utrwalają tę aktywność przestępczą. W tej samej grupie wymienić należy wszelkie wpisy, komentarze internetowe (na forach internetowych, w serwisach społecznościowych) wyczerpujące znamiona przestępstw, np.: gróźb, znieważenia, pomówienia, publikacje nawołujące do nienawiści na tle narodowościowym[43]. W obu omawianych przypadkach możemy zatem mówić o pełnowartościowym dowodzie o charakterze elektronicznym.

Każdy dowód ma bowiem swoje źródło, którym jest osoba lub rzecz dostarczająca ważnych informacji dla procesu karnego, przy czym z informacji tej czerpią swoją wiedzę uczestnicy procesu karnego, a ta wiedza przetworzona w odpowiedniej z punktu widzenia procesu karnego formie staje się środkiem dowodowym[44].

Poprzedzające ewentualne wszczęcie postępowania przygotowawczego, a uregulowane w art. 307 k.p.k. czynności sprawdzające, na etapie których organy ścigania mogą dokonać sprawdzenia danych zawartych w zawiadomieniu o podejrzeniu popełnieniu przestępstwa oraz sprawdzenia faktów w zakresie informacji podawanych w tym zawiadomieniu, są właściwym etapem dla stosowania narzędzi białego wywiadu. W ramach czynności sprawdzających – poza przyjęciem ustnego zawiadomienia o przestępstwie, przesłuchania w charakterze świadka osoby

---

42 Zob. K. Turaliński, *Wywiad gospodarczy i polityczny…*, s. 95-98.

43 Szerzej o tym aspekcie przestępczości zob. w pracy P. Niemczyka, *Pogarda. Dlaczego rośnie liczba przestępstw z nienawiści w Polsce*, Kraków 2019.

44 Zob. K.P. Pawelec, *Proces dowodzenia w postępowaniu karnym*, Warszawa 2010, s. 17.

zawiadamiającej dla uzupełnienia danych zawartych w jej zawiadomieniu, przyjęciu do protokołu wniosku o ściganie – pozostałe niezbędne czynności powinny mieć charakter nieprocesowy, operacyjny (rozpytanie, obserwacja itp.)[45].

J.D. Pogorzelski w toku weryfikacji wartości dowodowej informacji uzyskanej ze strony internetowej („dowód elektroniczny") dostrzega konieczność poczynienia ustaleń: kto prowadzi stronę, jaka jest zawartość strony, gdzie znajduje się jej serwer, w jaki sposób zdefiniowano cel funkcjonowania strony, zwrócenia uwagi na takie aspekty temporalne jak: kiedy stronę umieszczono w sieci, czy, a jeśli tak, to kiedy informacje były weryfikowane, jak świeże są informacje zawarte na tej stronie[46].

Autor ten dostrzega możliwość sporządzenia protokołu oględzin danej strony internetowej, przy czym załącznikiem do tego dokumentu byłby wydruk wygenerowany z takiej strony. Przedmiotowa praktyka zasługuje na afirmację, jednak nie znajduje zastosowania na etapie czynności sprawdzających wobec zakazu wykonywania czynności udokumentowanych protokołem (poza enumeratywnie wskazanymi przypadkami).

Na etapie prowadzenia czynności sprawdzających efekt podejmowania działań posługujących się technikami białego wywiadu przybiera postać notatki urzędowej, nie zaś protokołu oględzin.

Wersja śledcza rozumiana przez B. Hołysta jako „założenie hipotetyczne organów ścigania karnego co do charakteru zdarzenia, przebiegu oraz celu i motywów działania" jest budowana na podstawie informacji zdobytych w toku czynności pozaprocesowych, procesowych i pozostałych źródeł informacji. W związku z powyższym dane uzyskane z białego wywiadu mogą mieć pewien wpływ na budowanie wersji śledczych, a tym samym na kierunki prowadzonych śledztw już po ich wszczęciu[47].

WYKORZYSTANIE BIAŁEGO WYWIADU W PRACY OPERACYJNEJ POLICJI

Pojęciem szerszym zakresowo od białego wywiadu jest wywiad kryminalny rozumiany jako proces, który polega na ustawicznym gromadzeniu, pozyskiwaniu, analizowaniu informacji oraz dokonywaniu ocen w celu ukierunkowania działań policyjnych.

---

45 Zob. T. Grzegorczyk, *Kodeks postępowania karnego*, Kraków 2004, s. 777.

46 Zob. J.D. Pogorzelski, *Wykorzystanie otwartych źródeł informacji w pracy prokuratora*, [w:] *Biały wywiad. Otwarte źródła informacji…*, s. 190.

47 Zob. B. Hołyst, *Kryminalistyka*, Warszawa 2000, s. 1012.

Źródłem informacji dla wywiadu kryminalnego mogą być m.in.: czynności operacyjne i procesowe, przedsięwzięcia operacyjne Policji, współpraca z osobowymi źródłami informacji, informacje uzyskane przez Policję od osób niebędących jej współpracownikami, dane pochodzące z instytucji pozapolicyjnych, a także narzędzia białego wywiadu, poprzez wykorzystanie dostępnych informacyjnych baz danych, ogólnodostępne źródła informacji (mass media)[48].

Biały wywiad jako pozaagenturalna metoda pracy operacyjnej pozwala uzyskać dane o faktach, poglądach, zainteresowaniach, opiniach, systemie wartości, powiązaniach w sposób łatwy, tani oraz szybki, a zdobyte tą metodą informacje (co wymaga doświadczenia w zwalczaniu przestępczości, dużej wiedzy, jak też specyficznych umiejętności) mogą mieć znaczenie prewencyjne, rozpoznawcze, a nawet dowodowe[49].

Według T. Hanauska czynności operacyjno-rozpoznawcze to odrębny system tajnych lub poufnych działań organów ścigania, prowadzonych poza procesem karnym, nie mniej jednak zazwyczaj służących aktualnym, względnie przyszłym celom procesu karnego, których priorytetem jest zapobieganie oraz zwalczanie przestępczości, jak też innych określonych prawem negatywnych zjawisk występujących na płaszczyźnie społecznej[50].

J.D. Pogorzelski nie uznaje pozyskiwania informacji z otwartych źródeł informacji za przejaw działalności w ramach czynności operacyjno-rozpoznawczych[51].

Z kolei B. Świączkowski uważa, że z perspektywy Agencji Bezpieczeństwa Wewnętrznego prowadzenie działań w oparciu o informacje z otwartych źródeł informacji można potraktować jako działania analityczno-informacyjne, a nie czynności operacyjno-rozpoznawcze[52].

W regulaminie Komendy Głównej Policji z 2004 r., w załączniku nr 13 do zarządzenia nr 366 Komendanta Głównego Policji z dnia 20 kwietnia 2004 r. w sprawie regulaminu Komendy Głównej Policji, w ppkt. 2 wskazano, iż jednym z zadań Wydziału Wywiadu Kryminalnego jest „pozyskiwanie i gromadzenie informacji przydatnych do rozpoznania osobowego, obiektowego i zagadnieniowego w ogólnie dostępnych, otwartych źródeł informacji"[53].

---

[48] Zob. H. Tusiński, M. Bronicki, Wy*wiad kryminalny jako kierunek zwiększania efektywności policji w zdobywaniu, gromadzeniu i wykorzystaniu informacji*, [w:] *Przestępczość zorganizowana, świadek koronny, terroryzm w ujęciu praktycznym*, E.W. Pływaczewski (red.), Kraków 2005, s. 665-666.

[49] Zob. B. Sprengel, *Praca operacyjna policji*, Toruń 2018, s. 206.

[50] Zob. T. Hanausek, *Kryminalistyka. Zarys wykładu*, Kraków 2005, s. 133.

[51] Zob. J.D. Pogorzelski, *Wykorzystanie otwartych źródeł informacji…*, s. 186.

[52] Zob. B. Świączkowski, *Wykorzystanie tzw. białego wywiadu…*, s. 165-167.

[53] K. Radwaniak, *Biały wywiad w Policji…*, s. 90.

Funkcjonariusze Policji dzięki białemu wywiadowi, generując w ramach czynności operacyjno-rozpoznawczych profile przestępców i bazując m.in. także na cennych publikacjach dziennikarzy śledczych, nie legitymują się stosownym przeszkoleniem w tym zakresie (zaledwie 1-2% policjantów), gdy tymczasem mniej więcej 30% z nich korzysta z białego wywiadu[54].

Zdaniem K. Radwaniaka „odnosząc się do problematyki policyjnej i badań z tego zakresu, można przyjąć, że biały wywiad jest stosowany, ale w formie operacyjnej, niemalże intuicyjnie, bez wsparcia specjalistycznej wiedzy zawartej, np. w piśmiennictwie krajowym i zagranicznym. Korzystanie z doświadczeń wywiadowczych innych służb, przy uwzględnieniu specyfiki pracy Policji, z pewnością podniosłoby poziom tej pracy"[55].

Wykorzystanie białego wywiadu w zwalczaniu przestępczości, a w szczególności jej zorganizowanych form, odgrywa znacząca rolę, ponieważ dzięki temu następuje „uzyskiwanie, gromadzenie, weryfikacja i przetwarzanie informacji w oparciu o komunikaty funkcjonujące w oficjalnym obiegu publicznym, powszechnie dostępne, mające określone źródło"[56].

Kwestia korzystania z otwartych źródeł informacji w pracy Policji (jako jednej z metod jej pracy) nie została uregulowana przez ustawodawcę w sposób bezpośredni. Zgodnie z art. 20 ustawy z 1990 r. o Policji[57] może ona uzyskiwać informacje o siedmiu kategoriach osób w sposób niejawny, a także tym bardziej jawny, pobierać, gromadzić je, sprawdzać lub przetwarzać. Jedną z metod jawnego pozyskiwania tego typu danych jest posiłkowanie się wynikami monitoringu źródeł otwartych, ogólnie dostępnych. Mogą być one przydatne w prowadzonym postępowaniu do zrealizowania celów dowodowych, wykrywczych lub identyfikacyjnych[58].

Z punktu widzenia zwalczania przestępczości zorganizowanej szczególnie cenne dla organów ścigania mogą okazać się efekty pracy dziennikarzy śledczych zaprezentowane w formie audiowizualnej na łamach dokumentalnych programów interwencyjnych. Mogą one być przydatne dla Policji do „ustalenia przebiegu lub okoliczności zdarzeń, wskazania świadków, odnalezienia osób poszukiwanych i zaginionych, odzyskania utraconego mienia, identyfikacji przestępców i ich sprawców, identyfikacji zagrożeń, weryfikacji posiadanych informacji z innych źródeł, ustalania nowych źródeł informacji"[59].

---

54 Zob. B. Sprengel, *Praca operacyjna policji*, Toruń 2018, s. 207.
55 K. Radwaniak, *Biały wywiad w Policji…*, s. 90.
56 W. Mądrzejowski, S. Śnieżko, P. Majewski, *Zwalczanie przestępczości...*, s. 184.
57 Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2020 r. poz. 360), dalej: uPol.
58 Zob. W. Mądrzejowski, *Przestępczość zorganizowana. System zwalczania*, Warszawa 2015, s. 195.
59 Ibidem, s. 200.

Za niedopuszczalną należy uznać praktykę wprowadzania do materiałów spraw operacyjnych lub postępowania karnego informacji, które pochodzą ze źródeł otwartych, bez uprzedniego przeprowadzania ich weryfikacji[60]. Z kolei biały wywiad może być także narzędziem służącym do weryfikacji danych, które zostały pozyskane z innych źródeł operacyjnych[61].

Podczas podejmowania zabiegów organizacyjno-logistycznych w toku przygotowywania typowych czynności operacyjno-rozpoznawczych (zasadzka, obserwacja, zakup kontrolowany, przesyłka niejawnie nadzorowana) informacje pochodzące z białego wywiadu mogą być przydatne dla:

a) rozpoznania terenowego;
b) zapoznania się z rodzajem i natężeniem ruchu drogowego, modelem infrastruktury komunikacyjnej;
c) analizy danych o osobach zamieszkujących dany teren;
d) zapoznania się z funkcjonowaniem mediów (dostępność internetu, pozycje zainstalowania monitoringu);
e) ustalenia zlokalizowania oraz funkcjonowania w danej okolicy kluczowych obiektów typu: przedsiębiorstwa, sieci handlowe, obiekty sportowe[62].

Dane uzyskane z dostępnych baz danych tudzież ewidencji i rejestrów, jak też z internetu, mediów drukowanych i rozgłoszeniowych mogą w ramach czynności operacyjno-rozpoznawczych przyczynić się do realizacji funkcji rozpoznawczej ukierunkowanej na dane środowisko kryminogenne, co pozwoli na dookreślenie struktury i składu grupy przestępczej, występującej hierarchii i panujących w niej powiązań z określeniem specjalizacji poszczególnych ogniw, skonkretyzowania kontaktów zewnętrznych, określenia sposobu spędzania czasu w grupie[63].

Niezwykle cenne z punktu widzenia nie tylko pracy operacyjnej organów ścigania, lecz także kryminologii są celowo ukryte zasoby internetu – *dark web*. „W gęstwienie prywatnych sieci zapewniających poziom anonimowości nieosiągalnej w sieci zindeksowanej kwitnie handel narkotykami i bronią, reklamują się płatni zabójcy i hakerzy gotowi włamać się do komputera naszego wroga, a najbardziej zdeprawowani dewianci mogą zaspokoić apetyt, ściągając najdziwniejsze materiały pornograficzne”[64].

Wielu użytkowników internetu, chcąc uniknąć identyfikacji, stosuje rożne techniki anonimizacji, stanowiące kluczowy element taktyki działania

---

60 Zob. W. Mądrzejowski, S. Śnieżko, P. Majewski, *Zwalczanie przestępczości...*, s. 228.
61 Zob. ibidem, s. 237.
62 Zob. ibidem.
63 Zob. ibidem.
64 E. Ormsby, *Darknet*, Kraków 2019, s. 20.

cyberprzestępców. Używają wówczas takich technik maskowania jak: zastosowanie serwerów proxy (pośredniczących), VPN (*ang. Virtual Private Network*), czy sieci TOR (*ang. The Onion Routing*). Wykorzystanie sieci TOR uniemożliwia analizę ruchu sieciowego, co zapewnia użytkownikom praktycznie anonimowy dostęp do internetowych zasobów[65]. Funkcjonariusze Policji z wyspecjalizowanych komórek tej formacji regularnie monitorują *darknet* pod kątem analizy legalności transakcji zawartych pomiędzy poszczególnymi użytkownikami[66].

Historia kryminologii dowodzi, iż sprawcy wielu głośnych zbrodni, aktów przemocy o charakterze terrorystycznym radykalizowało się, szkoliło dzięki dostępnym w internecie źródłom, jak też ogłaszało swoje przestępcze plany[67]. Terroryści islamscy od dawna wykorzystują internet do werbunku, głoszenia swoich idei oraz poszukiwania źródeł finansowania zamachów terrorystycznych, toteż analiza tych danych również może dostarczyć organom ścigania cennych informacji[68].

WYKORZYSTANIE BIAŁEGO WYWIADU W DZIAŁANIACH POSZUKIWAWCZYCH ORAZ W TOKU CZYNIENIA USTALEŃ MAJĄTKOWYCH WOBEC WYTYPOWANYCH PODMIOTÓW

Każdy z nas, żyjąc w dobie społeczeństwa informacyjnego i informatycznego, pozostawia ślady w cyberprzestrzeni, które mogą zostać ujawnione także dzięki technikom białego wywiadu.

W tym miejscu warto przytoczyć przypadek słynnego meksykańskiego bossa narkotykowego Joaquina Guzmana, który po ucieczce z placówki penitencjarnej 11 lipca 2015 r. przez pewien czas ukrywał się na terenie Kostaryki. We wrześniu 2015 r. syn owego przestępcy opublikował w serwisie społecznościowym bardzo kontrowersyjne zdjęcie z wizerunkiem m.in. słynnego zbiega. Alfredo Guzman Salazar nie wyłączył geolokalizacji, co bardzo szybko zmobilizowało lokalną Policję do zintensyfikowania działań poszukiwawczych. Wprawdzie nie ujęto wówczas „El Chapo" (zatrzymano go dopiero w styczniu 2016 r.), ale ten błąd mógł wymiernie skrócić jego czas spędzony na wolności[69].

---

65 Zob. K. Wiciak, *Zapobieganie i zwalczanie cyberprzestępczości*, Lublin 2017, s. 17-20.

66 Zob. P. Zajdel, *Darknet, ciemniejsza moc Internetu (Technologie i innowacje)*, www.alebank.pl/darknet-ciemna-moc-internetu, (dostęp: 20.07.2020 r.).

67 Zob. K. Gradoń, *Możliwości taktycznego wykorzystania…*, s. 52.

68 Zob. J.W. Wójcik, *Cyberprzestrzeń – kryminologiczne i kryminalistyczne zagadnienie śladu transakcyjnego i elektronicznego*, [w:] *Co nowego w kryminalistyce – przegląd zagadnień z zakresu zwalczania przestępczości*, E. Gruz, M. Goc, T. Tomaszewski (red.), Warszawa 2010, s. 384.

69 Zob. www.fakt.pl/wydarzenia/swiat/el-chapo-wpadnie-przez-wybryk-syna/5rt9zrg. (dostęp: 20.07.2020 r.).

Monitoring otwartych źródeł informacji odegrał niebagatelną rolę w ustaleniu lokalizacji miejsca przebywania poszukiwanego listem gończym przestępcy o pseudonimie „Barbarzyńca", który latem 2012 r. został ujęty przez funkcjonariuszy z Zespołu Poszukiwań Celowych Komendy Wojewódzkiej Policji w Poznaniu. Ten znaczący członek kierownictwa jednej z grup przestępczych działających na terenie województwa zachodniopomorskiego, korzystając z portalu społecznościowego facebook.com, zamieszczał na swoim profilu dane o odwiedzanych miejscach oraz wskazywał dokumentację fotograficzną. Analiza metadanych pozwoliła na odtworzenie jego trasy przemieszczania się, a w momencie pojawienia się na terenie RP udało się przeprowadzić skuteczną realizację, której zwieńczeniem było ujęcie przestępcy[70].

Metadane stanowią dane opisujące inne dane, a w przypadku plików graficznych w postaci zdjęć są to m.in.: informacje o lokalizacji ich wykonania, dane o wielkości, autorze, rodzaju urządzenia, którym go wykonano. Przykładowym programem służącym do ustalenia lokalizacji wykonania zdjęcia jest IrfanView, co do zasady przeznaczony do przeglądania i podstawowej edycji plików wielu formatów w ramach programu operacyjnego Windows. Metadane mogą być analizowane także dzięki takim programom jak: Metadata Extractor v 3.0, RIOT (*ang. Rapid Information Technology*)[71].

Korzystanie z serwerów społecznościowych jest równoznaczne z domniemanym wyrażeniem zgody na prezentowanie naszego życia prywatnego na forum publicznym, co naraża naszą prywatność i bezpieczeństwo. Bardzo modne ostatnimi czasy serwisy społecznościowe nie zapewniają nam praktycznie żadnej anonimowości[72]. Jeśli dana treść już raz trafiła do internetu, to pozostaje w nim już na zawsze[73]. W dobie smartfonów, dronów, wszechobecnych kamer, jak też innych urządzeń fotograficznych i nagrywających, przestrzeń, co do której możemy być pewni, że nikt nie zrobi nam zdjęcia, które później ukaże się w sieci teleinformatycznej, jest coraz mniejsza i stale się zawęża[74]. Produkowane przez amerykańską firmę Apple iPhony zapisują geograficzną lokalizację użytkownika, przy czym poziom dokładności i częstotliwości jest duży. W 2011 r. dwaj młodzi programiści wykorzystali błędy tych urządzeń oraz oprogramowania Apple, a następnie napisali

---

70 Zob. B. Stromczyński, P. Waszkiewicz, *Biały wywiad…*, s. 146-147.

71 Zob. ibidem, s. 152-153.

72 Zob. K. Dziedzic, *Jak skutecznie zapewnić sobie anonimowość w Internecie. Kompletny poradnik krok po kroku*, Warszawa 2018, s. 4, 52.

73 Zob. ibidem, s. 38.

74 Zob. P. Niemczyk, J. Kapela, *Krótki kurs szpiegowania*, Warszawa 2019, s. 273.

nieskomplikowany program pozwalający ujawnić te dane, a nawet opublikować je w internecie[75].

Ślad cyfrowy rozumiany jako „zmiana w kodzie binarnym systemu teleinformatycznego, a także urządzenia cyfrowego zdolnego do przetwarzania, wysyłania, sprawdzania pakietów danych, będąca wynikiem ingerencji zewnętrznej (fizycznej) bądź wewnętrznej (zdalnej)", cechujący się trwałością na czynniki inne niż ingerencja użytkownika oraz osoby trzeciej, wydaje się być najbardziej narażonym na zatarcie i deformacje ze wszystkich śladów[76]. Dzieli się je na:

a) rezultat normalnej działalności w cyberprzestrzeni;
b) efekt celowego naruszenia ładu w cyberprzestrzeni;
c) wynik funkcjonowania urządzenia cyfrowego[77].

„Niezwykle istotnym śladem cyfrowym jest zapis zawierający obraz, a tutaj zaliczyć należy zapisy aparatów fotograficznych, smartfonów, kamer telewizyjnych itd. Ślady tego typu są ważne z dwóch powodów. Po pierwsze, ich analiza pozwala na opis zastanej na zdjęciu sytuacji, a przez to umożliwia identyfikację osoby, miejsca czy przedmiotu. Po drugie, niektóre z zapisów są otagowane, do pozwala na ustalenie, w którym miejscu zapis został wykonany"[78]. W sytuacji, gdy dane urządzenie rejestrujące korzysta z modułu GPS, wówczas dane lokalizacyjne mogą być zapisywane bezpośrednio na zdjęciach, w sposób automatyczny. Użycie „historii lokalizacji" zawartej na koncie Google pozwala ustalić lokalizację oszacowaną (informacja lokalizacyjna)[79].

B. Stromczyński i P. Waszkiewicz akcentują znaczącą rolę analizy przez organy ścigania danych zamieszczonych na serwisach społecznościowych rozumianych jako „platformy do budowania sieci społecznych lub relacji pomiędzy osobami, które łączą wspólne zainteresowania, aktywność, pochodzenie lub powiązania z realnego życia"[80]. Najbardziej popularnym serwisem społecznościowym jest facebook.com, a niewiele mniejszą popularnością cieszy się mikroblog – Twitter. ‚Cechą charakterystyczną portali społecznościowych jest zebranie w jednym miejscu niesłychanie dużej ilości informacji o ich użytkownikach. Informacje te pochodzą w głównej mierze z pierwszej ręki – od samych użytkowników[81]. Wymienieni autorzy, analizując możliwość wykorzystania przez organy ścigania informacji

---

75 Zob. T. Trejderowski, *Kradzież tożsamości. Terroryzm informacyjny. Cyberprzestępstwa. Internet. Telefon. Facebook*, Warszawa 2013, s. 94.
76 Zob. W.A. Kasprzak, *Ślady cyfrowe. Studium prawno-kryminalistyczne*, Warszawa 2015, s. 26, 121.
77 Zob. A. Hyła, *Analiza śladów cyfrowych*, „Prokuratura i Prawo" 2018, nr 5, s. 158.
78 Ibidem, s. 164.
79 Zob. ibidem, s. 165.
80 B. Stromczyński, P. Waszkiewicz, *Biały wywiad w praktyce…*, s. 155.
81 Zob. ibidem, s. 156.

jawnoźródłowych, pochodzących z serwisów społecznościowych wyodrębnili trzy grupy funkcji, tj.:

1) informacyjną (dzięki otwartym źródłom informacji z portali społecznościowych można pozyskać dane na temat aktualnego miejsca zamieszkania, wizerunku, informacje teleadresowe, dane odnoszące się do kręgu znajomych, zainteresowań, stylu życia);
2) dowodową;
3) poszlakową.

Dane zamieszczane na czy w serwisach społecznościowych stanowią zatem prawdziwą kopalnię wiedzy w sprawach poszukiwawczych dotyczących osób ukrywających się przed organami ścigania lub tych uznanych za zaginione.

Użyteczne nie tylko do badań genealogicznych, lecz także dla celów poszukiwawczych prowadzonych przez organy ścigania mogą okazać się dane zamieszczane na stronach internetowych nekropolii oraz wyszukiwarki grobów, np. www.findagrave.com czy www.interment.net (polski odpowiednik www.grobonet.com)[82].

Z punktu widzenia celów postępowania przygotowawczego równie ważnym jak ustalenie miejsca przebywania i ujęcie przestępcy jest pozbawienie go – po uprzednim dokładnym rozeznaniu sytuacji majątkowej – korzyści płynących z popełnionego przestępstwa (owoce przestępczej działalności). Podmioty prowadzące tzw. śledztwo finansowe, poszukując owoców nielegalnej działalności osób w nią zaangażowanych siłą rzeczy muszą posiłkować się różnymi bazami danych w ramach otwartych źródeł informacji.

Narzędziem informatycznym ułatwiającym im wielopłaszczyznowe i skonsolidowane wykorzystanie dostępnych baz danych, rejestrów, jest Elektroniczny System Odzyskiwania Mienia (ESOM), który pozwala na gromadzenie, sprawdzanie, kompletowanie, analizowanie, danych odnoszących się do składników majątkowych przestępców oraz osób z nimi powiązanych[83]. ESOM zawiera narzędzia, które ułatwiają korzystanie przez funkcjonariuszy Policji z otwartych baz danych oraz źródeł informacji, w następstwie czego dochodzi do zabrania pełnych danych o majątku osoby badanej, źródłach pochodzenia, jak też powiązaniach poszczególnych podmiotów gospodarczych uwikłanych w proces maskowania jego nielegalnego pochodzenia. Dzięki temu narzędziu informatycznemu powstaje realna możliwość wygenerowania profilu finansowego osoby, która pozostaje w zainteresowaniu podmiotów prowadzących śledztwo finansowe. „System ESOM zawiera różne warianty

---

[82] Zob. D. Szumilas, *Internetowy detektyw*, Warszawa 2008, s. 132-133.

[83] Zob. K. Wiciak, *ESOM jako narzędzie „białego wywiadu"*, [w:] *Biały wywiad. Otwarte źródła…*, s. 107-112.

ustalania, wyszukiwania i przetwarzania informacji, dzięki czemu jest może mało znanym, lecz niezwykle przydatnym narzędziem białego wywiadu"[84].

BIAŁY WYWIAD JAKO ELEMENT ANALIZY KRYMINALNEJ

Dane uzyskane w ramach białego wywiadu – po ich niezbędnej weryfikacji – mogą być z powodzeniem wykorzystane jako element analizy kryminalnej. Jej istota sprowadza się do prowadzonego w sposób metodyczny wykazywania i wyszukiwania związków pomiędzy samymi danymi dotyczącymi przestępstwa oraz pomiędzy nimi i innymi dającymi się wyróżnić informacjami w celu wygenerowania stosowanych konkluzji policyjnych i sądowych[85].

Analizę kryminalną określa się mianem „ekskluzywnej" policyjnej metody optymalizacji wykorzystania zgromadzonych danych[86]. Jako produkt jest ona dokumentem, który zawiera opis jej przebiegu oraz wyniki tej czynności, a jako rodzaj analizy informacji udziela odpowiedzi co najmniej na dwa pytania: co się stało oraz co jeszcze w danej kwestii należy zrobić[87].

Podstawowy podział analiz kryminalnych obejmuje: kryminalną analizę operacyjną (skupioną na informacjach uzyskanych w ramach czynności operacyjno-rozpoznawczych) oraz kryminalną analizę procesową (ukierunkowaną na uporządkowanie wiedzy pozyskanej w toku wykonywania czynności procesowych)[88].

Procesowa analiza kryminalna może przybrać postać analizy:

a) kompleksowej;
b) chronologii zdarzeń;
c) danych telekomunikacyjnych;
d) powiązań osobowych
e) przepływów finansowych;
f) powiązań kapitałowych[89].

„Procesowa analiza kryminalna nie jest więc dowodem *sensu stricte* w sprawie (w rozumieniu źródła dowodowego). Ale poprzez swoją istotę może posiadać fundamentalne znaczenie dzięki właściwemu umieszczeniu i zobrazowaniu w przebiegu zdarzenia określonych faktów i dowodów oraz powiązań pomiędzy nimi"[90].

---

84 W. Mądrzejowski, S. Śnieżko, P. Majewski, *Zwalczanie przestępczości…*, s. 220.
85 Zob. M. Kobylas, *Analiza kryminalna dla studentów bezpieczeństwa wewnętrznego*, Szczytno 2014, s. 12.
86 Zob. J. Widacki, J. Konieczny, *Wersja śledcza, modus operandi, analiza kryminalna – teoretyczne podstawy śledztwa*, [w:] *Kryminalistyka*, J. Widacki (red.), Warszawa 2016, s. 77, 82.
87 Zob. I. Gdak, *Analiza materiału dowodowego w procesie karnym*, Warszawa 2018, s. 85.
88 Zob. M. Gabriel-Węglowski, *Analiza kryminalna w pracy prokuratora*, „Prokuratura i Prawo" 2016, nr 10, s. 128.
89 Zob. ibidem, s. 128-129.
90 Ibidem, s. 134.

Według innego podziału analiz kryminalnych można wyróżnić ich odmiany w postaci:

1) analizy taktycznej (zwaną także operacyjną);
2) analizy strategicznej (jej przedmiotem są problemy i cele długoterminowe).

Biorąc zaś pod uwagę formy analizy kryminalnej można wyróżnić formy analizy koncentrujące się na:

I. przestępstwie (analiza przestępczości, analiza sprawy, analiza porównawcza spraw);
II. przestępcy (analiza profilu ogólnego, analiza grup przestępczych, analiza profilu szczególnego);
III. metodach stosowanych w sprawach (analiza metod stosowanych w sprawach, analiza prowadzenia sprawy)[91].

Analityk, sporządzając analizę kryminalną, korzysta nie tylko ze źródeł osobowych i rzeczowych, lecz także z baz danych i internetu, zapewniających dostęp do szerokiej gamy otwartych źródeł informacji[92].

„Analiza kryminalna nabiera szczególnego znaczenia w sprawach wielowątkowych, z udziałem dużej liczby osób, zdarzeń, miejsc, rzeczy, wymagających rzeczywistego wzajemnego powiązania ze sobą. Jest wykorzystywana zwłaszcza w przypadkach działań operacyjno-rozpoznawczych i prowadzenia śledztw w sprawach dotyczących zorganizowanej przestępczości"[93]. Nierzadko analiza kryminalna okazuje się przełomowym rozwiązaniem oraz jedynym sposobem, dzięki któremu możliwe jest uzyskanie spośród ogromu informacji odpowiedzi na pytania będące kluczowymi dla wyjaśnienia prowadzonej sprawy. „W ostatnich czasie coraz powszechniejsze staje się wykorzystanie analizy kryminalnej przez śledczych, jednak rezerwy niewykorzystanych możliwości tej metody wspomagania ich pracy pozostają nadal ogromne"[94].

Wybrane otwarte źródła informacji mogą służyć w ramach pracy analitycznej do:

a) analizy danych retencyjnych:
   1) wykazu pozwoleń radiowych dla stacji bazowych telefonii komórkowej wydawanych przez Prezesa UKE, a także stacji wykorzystujących technologię CDMA (np. http://uke.gov.pl/pozwolenia-radiowe-dla-stacji-gsm-umts-lte-oraz-cdma-4145);

---

[91] Zob. M. Kobylas, *Analiza kryminalna…*, s. 19.

[92] Zob. A. Kaucz, M. Kiedrowicz, M. Skinder-Pik, *Gromadzenie i przetwarzanie danych mających związek ze zwalczaniem przestępczości finansowej. Zasady dostępu, ograniczenia prawne*, Warszawa 2016, s. 74.

[93] J. Gołębiewski, *Praca operacyjna w zwalczaniu przestępczości zorganizowanej*, Warszawa 2008, s. 54.

[94] A. Saj, *Wykorzystanie analizy kryminalnej w procesie karnym*, [w:] *Przestępstwa rzadko podejmowane przez organy ścigania. Aspekty kryminalistyczne, materialno-prawne i procesowe*, M. Trybus, T. Wilk (red.), Rzeszów 2013, s. 271.

2) wyszukiwarka stacji bazowych telefonii komórkowej UMTS, LTE, GSM, wraz z mapą lokalizacji BTS (http://btssearch.pl/);
3) wyszukiwania modelu urządzenia dzięki numerowi IMEI (np. http://www.numberingplans.com/);
4) wyszukiwania po numerze urządzenia przynależności do danego operatora (np. http://www.wjakiejsieci.pl/);
5) ustalanie kodów pocztowych, jak też dodatkowo numerów kierunkowych (http://www.pl.all-biz.info/guide/phonecodes/index.php?ch=13&region=-11-strona);
6) ustalania danych sieci komórkowych na świecie (http://inviare.freetextuk.com/SMSByCountry.aspx);

b) analizy danych finansowych:
1) bazy danych firm na terenie RP: KRS, Monitor Sądowy i Gospodarczy, CEIDG (np. http://www.krs-online.com.pl/);
2) eksplorowania rejestrów działalności gospodarczej w UE – System Integracji Rejestrów Przedsiębiorców BRIS (http://e-justice.europa.eu/content_find_a_company-489-pl.do?clang=pl);
3) wyszukiwanie numerów identyfikacji podatkowej VAT-UE w ramach systemu VIES (http://uid-suche.at/);
4) wyszukiwarka dla ustalania powiązań pomiędzy osobami i organizacjami w oparciu na danych z KRS (https://mojePanstwo.pl/krs);
5) księgi wieczyste (http://ekw.ms.gov.pl/pdcbdkw.html);
6) weryfikowania poprawności numeru konta bankowego (np. http://numer-konta.com/);

c) analizy danych geograficznych:
1) poszukiwania danych przestrzennych działek lub adresów (np. http://mapy.geoportal.gov.pl/imap/);
2) mapy pozwalających umiejscowić dany punkt według adresu, współrzędnych geograficznych (np. http://mapa.targeo.pl/);

d) analizy danych sieciowych:
1) weryfikacji adresu IP (https://www.adres-ip.pl/sprawdz.html);
2) sprawdzenie właściciela domeny (https://www.adres-ip.pl/whois.html);
3) ustalania poprawności adresu e-mail (http://www.verifyemailaddress.org/);
4) poszukiwania w internecie danych o osobach w oparciu o takie parametry jak: numer telefonu, adres e-mail, imię i nazwisko (http://pipl.com)[95].

[95] Zob. C. Fiertek, K. Frąckowiak, T. Iwanowski, J. Motawski, P. Pawłowski, T. Piekarski, S. Stojak, W. Szelągowski, *Metodyki postępowań w sprawach o poszczególne rodzaje przestępstw*, Warszawa 2018, s. 430-434.

Instrumentem służącym do ustalenia, jak wyglądała archiwalna wersja danej strony internetowej (przed wprowadzonymi chronologicznie moderacjami), jest *WayBackMachine*, tj. narzędzie działające w ramach *Internet Archive* (funkcjonuje pod adresem: http:/www.archive.org). Wzmiankowany środek na własnych serwerach archiwizuje inne witryny internetowe, a następnie umożliwia zainteresowanym (bez jakichkolwiek ograniczeń) dostęp do tych zgromadzonych zasobów[96].

Europejski portal e-sprawiedliwość (www.e-justice.europa.eu), mając na uwadze okoliczność, iż stworzenie unijnego jednolitego rynku skutkowało tym, że wiele spółek rozszerzyło swoją działalność poza granice państwa pochodzenia, daje możliwość, począwszy od czerwca 2017 r., eksploracji połączonych rejestrów działalności gospodarczej wszystkich państw UE, w których można prowadzić owocne wyszukiwania (w związku z wystąpieniem Wielkiej Brytanii z Unii Europejskiej cennym źródłem o angielskich podmiotach gospodarczych pozostaje portal *CompaniesHouse* –www.gov.uk/government/organisations/companies-house)[97].

W tym miejscu warto także wspomnieć o wyszukiwarce o nazwie *Iconsquare*, która pozwala na efektywne wyszukiwanie hashtagów na *Instagramie*, dających z kolei możliwość uzyskania dostępu do informacji zawierających dane wrażliwe (np. zdjęcia dowodów tożsamości, praw jazdy, wyroków, umów itp.)[98].

Aktualnie w powszechnych jednostkach organizacyjnych prokuratury jest wdrażana bardzo użyteczna aplikacja w postaci Systemu Wsparcia Prokuratora – Moduł Analityczno-Śledczy, który po imporcie stosowanych danych (w tym plików JPK – Jednolity Plik Kontrolny) pozwala na wykonywania analiz danych bilingowych w drodze wygenerowania: statystyk – operacje analityczne (statystyki połączeń pomiędzy wybranymi MSISDN, statystyki dla MSISN, statystyki logowań w stacjach BTS, statystyki użycia numeru IMEI dla MSISDN), wyszukania – operacje analityczne (wspólne MSISDN dla MSISDN, wspólne IMEI dla MSISDN, wspólne BTS dla MSISDN, krąg abonenta, obszar abonenta), kalendarzy – operacje analityczne (kalendarz użytkowania MSISDN, kalendarz użytkowania IMEI, kalendarz logowań do BTS przez MSISDN, kalendarz współpracy MSISDN – IMEI).

Wskazane powyżej dane mogą być zwizualizowane na: diagramie powiązań, osi czasu, mapie. Dzięki opisanej aplikacji po importowaniu danych bankowych możliwe jest także uzyskanie statystyk dla danych bankowych (statystyki przelewów na rachunku, statystyki przelewów dla właściciela rachunku, statystyki przelewów pomiędzy wybranymi rachunkami, statystyki przelewów pomiędzy wybranymi

---

[96] Zob. B.A. Adamus, *Przygotowanie do popełnienia przestępstwa teleinformatycznego. Problematyka kryminalistyczna*, [w:] *Co nowego w kryminalistyce…*, s.12.

[97] Zob. e-justice.europa.eu/home.do?action=home&plang=pl. (dostęp: 20.07.2020 r.).

[98] Zob. www.http:/iconsquare.com. (dostęp: 20.07.2020 r.).

właścicielami, zestawienie transakcji typu input/output, kalendarz przelewów dla rachunku, kalendarz przelewów dla właściciela rachunku). W ramach analizy danych bankowych możliwe są: scalenie posiadaczy rachunków, wizualizacja danych na diagramie powiązań, wizualizacja danych na osi czasu. Z kolei analiza danych fakturowych pozwala na opracowanie statystyk dla danych fakturowych (komendy: generuj zestawienie faktur, wyszukaj powtarzających się sekwencji, sumuj wartość faktur, ustal powiązania pomiędzy podmiotami, porównaj zgodność plików JPK), które mogą zostać wizualizowane na diagramie powiązań lub na osi czasu.

Jako wniosek o charakterze *de lege ferenda* zasygnalizować należy potrzebę udoskonalenia tego jakże pożytecznego narzędzia analitycznego poprzez jego wzbogacenie o elementy zintegrowanego systemu dostępu do otwartych źródeł informacji – w formie dodatkowego obok Modułu Analityczno-Śledczego Modułu Informacyjnego – na wzór witryny mojePanstwo.pl.

Wzmiankowany portal stanowi otwarty zestaw aplikacji, który z uwagi na dużą liczbę funkcjonalności stanowi doskonały instrument do monitorowania sprawozdań, publicznych raportów, a dzięki współpracy z wyszukiwarką Google pozwala z jej poziomu na wyszukiwanie wielu użytecznych informacji (w tym te z Krajowego Rejestru Sądowego), co przy użyciu nieskomplikowanych narzędzi analitycznych daje możliwość wygenerowania automatycznej wizualizacji podlegających wyszukaniu powiązań kapitałowych oraz osobowych[99].

ZAKOŃCZENIE

Organy ścigania w toku prowadzenia czynności operacyjno-rozpoznawczych oraz postępowań przygotowawczych niejednokrotnie korzystają z otwartych źródeł informacji, które stanowią kopalnię cennych informacji. Pomimo istotności roli tych danych w procesie ustalania prawdy materialnej nie doszło do sformułowania przez ustawodawcę bezpośrednich, kompleksowych uregulowań w tym przedmiocie, jak też nie stworzono zintegrowanego systemu informacji jawnoźródłowych. Sam system szkoleń przedstawicieli organów ścigania w zakresie posługiwania się narzędziami białego wywiadu winien być dedykowany dla jak najszerszego kręgu adresatów z organów ścigania (prokuratorzy, policjanci, analitycy kryminalni, asystenci prokuratorów). Funkcjonowanie w społeczeństwie informatycznym, którego członkowie pozostawiają cyberprzestrzeni wiele śladów wymaga od przedstawicieli organów ścigania większej biegłości w poszukiwaniu danych jawnoźródłowych, co znalazłoby przełożenie na usprawnienie procesu ustalania

[99] Zob. B. Saramak, W*ykorzystanie otwartych źródeł…*, s. 79

odpowiedzialności karnej osób naruszających prawo. Pozytywnie zweryfikowane dane uzyskane z otwartych źródeł informacji mogą stać się istotnym filarem wielu analiz kryminalnych, których wnioski będą rzutowały na kierunki prowadzonych śledztw. Rzetelny śledczy, ustalając prawdę materialną, nie może ignorować tych danych, gdyż pełnią one co najmniej funkcję rozpoznawczą i pozwalają na kompleksową ocenę danej sytuacji procesowej, jak też pośrednio rzutują na jakość zgromadzonego materiału dowodowego.

BIBLIOGRAFIA

Literatura

Adamus B.A., *Przygotowanie do popełnienia przestępstwa teleinformatycznego. Problematyka kryminalistyczna*, [w:] *Co nowego w kryminalistyce – przegląd zagadnień z zakresu zwalczania przestępczości*, E. Gruz, M. Goc, T. Tomaszewski (red.), Warszawa 2010.
Aleksandrowicz T., *Biały wywiad w walce z terroryzmem*, [w:] *Rola mediów w przeciwdziałaniu terroryzmowi*, Liedel K., P. Piasecka (red.), Warszawa 2009.
Chlebowicz P., *„Biały wywiad" z perspektywy kryminalistyki*, [w:] *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipkowski i W. Mądrzejowski (red. nauk.), Warszawa 2012.
Dobrowolski G., Filipkowski W., Kisiel-Dorohnicki M., Rakoczy W., *Wsparcie informatyczne dla analizy otwartych źródeł informacji w Internecie w walce z terroryzmem. Zarys problemu*, [w:] *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu*, L.K. Paprzycki, Z. Rau (red.), Warszawa 2009.
Dziedzic K., *Jak skutecznie zapewnić sobie anonimowość w Internecie. Kompletny poradnik krok po kroku*, Warszawa 2018.
Fiertek C., Frąckowiak K., Iwanowski T., Motawski J., Pawłowski P., Piekarski T., Stojak S., Szelągowski W., *Metodyki postępowań w sprawach o poszczególne rodzaje przestępstw*, Warszawa 2018.
Gabriel-Węglowski M., *Analiza kryminalna w pracy prokuratora*, „Prokuratura i Prawo" 2016, nr 10.
Gdak I., *Analiza materiału dowodowego w procesie karnym*, Warszawa 2018.
Gołębiewski J., *Praca operacyjna w zwalczaniu przestępczości zorganizowanej*, Warszawa 2008.
Góral K., Przewodnik po wybranych narzędziach białego wywiadu (OSINT), https://datawalk.com/wp-content/uploads/2018/06/DataWalk-Przewodnik-po-narzedziach-OSINT.pdf.
Gradoń K., *Możliwości taktycznego wykorzystania otwartych źródeł informacji w Internecie przez organa ścigania oraz sprawców przestępstw i zamachów terrorystycznych*, [w:] *Problemy współczesnej kryminalistyki*, t. XIX, E. Gruza, T. Tomaszewski, M. Goc (red.), Warszawa 2015.
Gruza E., Goc M., Moszczyński J., *Kryminalistyka, czyli rzecz o metodach śledczych*, Warszawa 2008.
Grzegorczyk T., *Kodeks postępowania karnego. Komentarz*, Kraków 2004.
Hanausek T., *Kryminalistyka. Zarys wykładu*, Kraków 2005.
Hołyst B., *Kryminalistyka*, Warszawa 2000.
Hyła A., *Analiza śladów cyfrowych*, „Prokuratura i Prawo" 2018, nr 5.
Jarczewska-Walendziak K., *Wykorzystanie otwartych źródeł informacji przez służby śledcze*, „Toruńskie Studia Bibliologiczne" 2017, nr 1(18).
Kasprzak W.A., *Ślady cyfrowe. Studium prawno-kryminalistyczne*, Warszawa 2015.
Kaucz A., Kiedrowicz M., Skinder-Pik M., *Gromadzenie i przetwarzanie danych mających związek ze zwalczaniem przestępczości finansowej. Zasady dostępu, ograniczenia prawne*, Warszawa 2016.
Kobylas M., *Analiza kryminalna dla studentów bezpieczeństwa wewnętrznego*, Szczytno 2014.
Konieczny J., *Zagadnienia wprowadzające*, [w:] *Analiza informacji w służbach policyjnych i specjalnych*, J. Konieczny (red.), Warszawa 2012.

Kosmaty P., *Dziennikarstwo śledcze musi być rzetelne*, https://archiwum.rp.pl/artykul/1384202-Dziennikarstwo-sledcze-musi-byc-rzetelne.html.
Liedel K., Serafin T., *Otwarte źródła informacji w działalności wywiadowczej. Zarys problematyki*, Warszawa 2011.
Maciołek P., *Internet, a OSINT – szanse i praktyczne zastosowania*, [w:] *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipkowski i W. Mądrzejowski (red. nauk.), Warszawa 2012.
Mądrzejowski W., *„Biały wywiad" w Policji*, [w:] *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipkowski i W. Mądrzejowski (red. nauk.), Warszawa 2012.
Mądrzejowski W., *Przestępczość zorganizowana. System zwalczania*, Warszawa 2015.
Mądrzejowski W., Śnieżko S., Majewski P., *Zwalczanie przestępczości. Wybrane metody i narzędzia*, Warszawa 2017.
Mider D., Garlicki J., Mincewicz W., *Poszukiwanie informacji z Internetu metodą Google Hacking – biały, szary, czy może czarny wywiad?*, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 20.
Minkina M., *Sztuka wywiadu w państwie współczesnym*, Warszawa 2014.
Mroziewicz K., *Czas pluskiew*, Warszawa 2007.
Niemczyk P., Kapela J., *Krótki kurs szpiegowania*, Warszawa 2019.
Niemczyk P., *Pogarda. Dlaczego rośnie liczba przestępstw z nienawiści w Polsce*, Kraków 2019.
Niemczyk P., *Wywiadownie gospodarcze jako źródło informacji białego wywiadu*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9 (5).
Ormsby E., *Darknet*, Kraków 2019.
Pawelec K.P., *Proces dowodzenia w postępowaniu karnym*, Warszawa 2010.
Pogorzelski J.D., *Wykorzystanie otwartych źródeł informacji w pracy prokuratora*, [w:] *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipkowski i W. Mądrzejowski (red. nauk.), Warszawa 2012.
Radwaniak K., *Biały wywiad w Policji – narzędzie rozpoznawania zagrożeń terrorystycznych*, „Studia prawnicze. Rozprawy i Materiały" 2012, nr 2(11).
Rapkowska K.B., Zackiewicz P.M., *Biały wywiad w zwalczaniu przestępczości kryminalnej i zorganizowanej*, http://www.knbm.amw.gdynia.pl/wp-content/uploads/2014/12/Rapkowska-Karolina-Zackiewicz-Paulina-Bia%C5%82y-wywiad-w-zwalczaniu-przest%C4%99pczo%C5%9Bci-kryminalnej-i-zorganizowanej.pdf.
Saj A., *Wykorzystanie analizy kryminalnej w procesie karnym*, [w:] *Przestępstwa rzadko podejmowane przez organy ścigania. Aspekty kryminalistyczne, materialno-prawne i procesowe*, M. Trybus, T. Wilk (red.), Rzeszów 2013.
Saramak B., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Warszawa 2015.
Sprengel B., *Praca operacyjna policji*, Toruń 2018.
Stromczyński B., Waszkiewicz P., Biały *wywiad w praktyce organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, „Prokuratura i Prawo" 2014, nr 5.
Szumilas D., *Internetowy detektyw*, Warszawa 2008.
Świączkowski B., *Wykorzystanie tzw. białego wywiadu w działalności analityczno-informacyjnej Agencji Bezpieczeństwa Wewnętrznego*, [w:] *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipkowski i W. Mądrzejowski (red. nauk.), Warszawa 2012.
Trejderowski T., *Kradzież tożsamości. Terroryzm informacyjny. Cyberprzestępstwa. Internet. Telefon. Facebook*, Warszawa 2013.
Turaliński K., *Wywiad gospodarczy i polityczny. Metodyka, taktyka i źródła pozyskiwania informacji*, Radom 2011.
Tusiński H., Bronicki M., Wy*wiad kryminalny jako kierunek zwiększania efektywności policji w zdobywaniu, gromadzeniu i wykorzystaniu informacji*, [w:] *Przestępczość zorganizowana, świadek koronny, terroryzm w ujęciu praktycznym*, E.W. Pływaczewski (red.), Kraków 2005.
Wiciak K., *ESOM jako narzędzie „białego wywiadu"*, [w:] *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipkowski i W. Mądrzejowski (red. nauk.), Warszawa 2012.

Wiciak K., *Zapobieganie i zwalczanie cyberprzestępczości*, Lublin 2017.
Widacki J., Konieczny J., *Wersja śledcza, modus operandi, analiza kryminalna – teoretyczne podstawy śledztwa*, [w:] *Kryminalistyka*, J. Widacki (red.), Warszawa 2016.
Wójcik J.W., *Cyberprzestrzeń – kryminologiczne i kryminalistyczne zagadnienie śladu transakcyjnego i elektronicznego*, [w:] *Co nowego w kryminalistyce – przegląd zagadnień z zakresu zwalczania przestępczości*, E. Gruz, M. Goc, T. Tomaszewski (red.), Warszawa 2010.
Wójcik J.W., *Wywiad i kontrwywiad gospodarczy*, Warszawa 2018.
www.fakt.pl/wydarzenia/swiat/el-chapo-wpadnie-przez-wybryk-syna/5rt9zrg, dostęp: 20.07.2020 r.
Zajdel P., *Darknet, ciemniejsza moc Internetu (Technologie i innowacje)*, www.alebank.pl/darknet-ciemna-moc-internetu.
Ziółkowska A., *Biały wywiad jako narzędzie uzupełniające czynności z zakresu techniki kryminalistycznej*, „Acta Universitatis Lodziensis Folia Iuridica" 2018 nr 82, https://doi.org/10.18778/0208-6069.82.06.
Żebrowski A., *Wywiad i kontrwywiad XXI wieku*, Lublin 2010.

Akty normatywne

Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, Dz. U. z 2020 r. poz. 1086.
Ustawa z dnia 6 kwietnia 1990 r. o Policji, Dz. U. z 2020 r. poz. 360.
Zarządzenie nr 366 Komendanta Głównego Policji z dnia 20 kwietnia 2004 r. w sprawie regulaminu Komendy Głównej Policji w sprawie regulaminu Komendy Głównej Policji, Dz. Urz. Komendy Głównej Policji nr 7, poz. 31.

The use of "white intelligence" in the activities of the Police and the prosecutor's office

SUMMARY

The article indicates the wide possibilities offered by the use of operational and reconnaissance activities by the Police and preparatory proceedings conducted by the Police and the prosecutor's office, the so-called open source information.

It is a synthesis of the definition of white intelligence, its sources, raises the issue of initiating preparatory proceedings thanks to information from open sources, refers to the issue of using open source information in the operational work of the Police, shows the advantages of using white intelligence as part of search activities and against the background of the ESOM IT tool (Electronic Asset Recovery System), presents a white interview against the background of a criminal analysis, formulates de lege ferenda conclusions regarding the improvement of the analytical tool within the Prosecutor Support System.

The publication in question recognizes the significant investigative potential of properly targeted monitoring of open sources of information.

Keywords: operational and reconnaissance activities, white intelligence, Prosecutor Support System.