Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury
Quarterly of the National School of Judiciary and Public Prosecution
Zeszyt 1 (49)/2023

ARTYKUŁY

Ustalanie tożsamości polskich użytkowników zagranicznych mediów społecznościowych – studium przypadków ścigania mowy nienawiści w cyberprzestrzeni

DOI:10.53024/5.1.49.2023

PIOTR LEWULIS*

STRESZCZENIE

Ściganie niektórych cyberprzestępstw jest w praktyce bardzo proste, innych wręcz niemożliwe – często w zależności od wzorca zachowania sprawcy. W przypadku czynów polegających na zamieszczaniu zabronionych treści w zagranicznych portalach społecznościowych, skuteczność działań śledczych opartych na analizie danych przekazywanych przez administratorów domen jest bardzo ograniczona. W artykule przedstawiono wyniki jakościowej analizy wybranych przypadków prawomocnie zakończonych postępowań dotyczących przekraczania granic swobody wypowiedzi w Internecie, w których ściganie było rzeczywiście skuteczne (tj. ustalono rzeczywistego sprawcę i pociągnięto go do odpowiedzialności sądowej). W analizowanych przypadkach wszyscy sprawcy działający w krajowej cyberprzestrzeni skutecznie ustalani byli w oparciu o współpracę organów ścigania z administratorami stron i podmiotami telekomunikacyjnymi. Natomiast sprawcy mowy nienawiści w zagranicznych portalach społecznościowych byli we wszystkich przypadkach ustalani w drodze prostej analizy białowywiadowczej, której podstawę stanowiły dane publicznie dostępne w profilach sprawców (imiona i nazwiska, miejsca pracy, dane o rodzinie lub znajomych). W artykule przedstawiono opisy stanów faktycznych i przebiegu postępowań w analizowanych przypadkach, co ukazuje różne warianty poznania tożsamości sprawcy w oparciu o analizę danych publicznie dostępnych.

Słowa kluczowe: media społecznościowe, mowa nienawiści, cyberprzestępczość, OSINT

* Doktor nauk prawnych, adiunkt w Katedrze Kryminalistyki WPiA Uniwersytetu Warszawskiego,| ORCID: 0000-0002-8303-0971.

WSTĘP

W pojęciu „cyberprzestępczości", niezupełnie do dziś zdefiniowanym[1], mieszczą się czyny o skomplikowanym technicznie charakterze, jak i prostsze w przebiegu przestępstwa. Wyniki dotychczasowych badań aktowych potwierdzają istnienie dwóch grup sprawców: dobrze zorganizowanych „profesjonalistów" oraz działających spontanicznie „amatorów"[2]. W odniesieniu do każdej z tych grup odmiennie kształtuje się faktyczna skuteczność działań śledczych. Skuteczne i ekonomiczne ściganie cyberprzestępstw może bardzo proste albo niemożliwe – w zależności wzorców zachowania się sprawcy. Pod pojęciem „skutecznego ścigania" rozumiane jest tu, w nawiązaniu do treści art. 2 §1 pkt. 1 k.p.k., takie przeprowadzenie postępowania, aby sprawca został wykryty i pociągnięty do odpowiedzialności karnej przed sądem. Szeroko dostępne taktyki i narzędzia anonimizujące mogą uniemożliwić ściganie osób, które chcą i potrafią z takich narzędzi skorzystać[3]. Natomiast wykrycie sprawcy nieprzestrzegającego zasad bezpieczeństwa operacyjnego (ang. *Operational Security,* OPSEC) bywa relatywnie proste. Łatwość ścigania nie oznacza jednak trywializacji nieskomplikowanych cyberprzestępstw – każdorazowo niezbędne jest poważne podjęcie adekwatnych działań na rzecz skutecznego ścigania.

Media społecznościowe są środowiskiem wyjątkowym pod względem kryminologicznym i kryminalistycznym. Mogą być równocześnie postrzegać jako „miejsce" popełnienia czynu, przestrzeń wiktymizacji i swoiste narzędzia sprawcze[4]. Wobec ogromnej popularności mediów społecznościowych[5] uderzająca jest łatwość ich wykorzystania do popełniania czynów zabronionych związanych z treścią zamieszczanych wpisów – w szczególności kwalifikowanych z art. 255, 256 czy 257 k.k. Choć nie są to zazwyczaj zachowania skomplikowane technicznie, są one wysoce szkodliwe społecznie, a rzeczywistą przeszkodą w ich ściganiu są często kwestie jurysdykcyjne[6]. W poszukiwaniu alternatywnych metod wykrywczych można odwołać się do empirycznej analizy skutecznych postępowań karnych. Analiza takich przypadków

---

[1] Niezależnie od licznych sporów terminologicznych prowadzonych na przestrzeni lat, w niniejszym opracowaniu pojęcie „cyberprzestępczości" będzie odnosiło się do ogółu przestępstw popełnianych w związku z wykorzystaniem sieci komputerowych, w szczególności Internetu. Por.: P. Lewulis, *O rozgraniczeniu definicyjnym pomiędzy przestępczością „cyber" i „komputerową" dla celów praktycznych i badawczych*, „Prokuratura i Prawo" 2021, nr 3.

[2] P. Waszkiewicz, *Media społecznościowe w postępowaniu karnym*, Warszawa 2022, s. 14.

[3] P. Szymański, P. Zalewski, *Aktywność zorganizowanych grup przestępczych w cyberprzestrzeni w czasach pandemii – analiza wybranych podatności i metod anonimizacji*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2022, nr 1 (45).

[4] P. Waszkiewicz, *op. cit*., s. 14.

[5] Oczywiste znaczenie dla skali przestępczości w Internecie ma fakt, że z mediów społecznościowych korzysta ponad połowa ludzkości, zob.: *Digital 2022: Global Overview Report*, [na:] „DataReportal – Global Digital Insights", https://datareportal.com/reports/digital-2022-global-overview-report (dostęp 25 lipca 2022 r.).

[6] P. Opitek, *Wybrane aspekty pozyskiwania dowodów cyfrowych w sprawach karnych*, „Prokuratura i Prawo" 2018, nr 7–8.

stanowi okazję do refleksji teoretycznej nad dalszymi kierunkami badań kryminologicznych. Ma też walor praktyczny – może pozwolić na harmonizację i podnoszenie podstawowych kompetencji śledczych u osób niezajmujących się w codziennej praktyce ściganiem cyberprzestępstw.

W pierwszej części niniejszego artykułu krótko scharakteryzowano znaczenie szeroko rozumianych mediów społecznościowych w kontekście kryminologicznym. Zarysowana została domyślna i prawidłowa w większości przypadków taktyka ustalania tożsamości sprawców działających w Internecie. Jako metodę komplementarną wskazano natomiast analizę danych ze źródeł otwartych, ukierunkowaną na poznanie tożsamości sprawcy. Omówione taktyki zostały zilustrowane jakościową analizą przypadków postępowań w sprawach przestępstw z nienawiści w Internecie, w których ściganie okazało się skuteczne (tj. ustalono rzeczywistego sprawcę i pociągnięto go do odpowiedzialności sądowej). Pociągnięte do odpowiedzialności karnej osoby działające na zagranicznym portalu społecznościowym ustalano w oparciu o dane widniejące w ich publicznie dostępnych profilach. Natomiast wszyscy sprawcy działający w polskiej cyberprzestrzeni byli skutecznie ustalani w rezultacie współpracy z administratorami stron i podmiotami telekomunikacyjnymi.

MEDIA SPOŁECZNOŚCIOWE JAKO ŚRODOWISKO I NARZĘDZIE CZYNÓW ZABRONIONYCH

Anglojęzyczny termin *social media* użyty został pierwszy raz użyty w 1994 r. – od tego czasu odbiór jego znaczenia i definicje zmieniały się wielokrotnie[7]. Choć pojęcie „mediów społecznościowych" jest dziś powszechnie zrozumiałe, jego zakres jest nieostry. Odbiór tego, co postrzegane jest jako „medium społecznościowe", pozostaje zmienny i wynika raczej ze zbiorowej intuicji użytkowników sieci niż definicji formalnych. Bez wątpienia konstytutywne elementy mediów społecznościowych można odnaleźć w najpopularniejszych platformach (takich jak Twitter czy należący do amerykańskiej spółki Meta[8] portal Facebook), jednak popularność mierzona liczbą aktywnych użytkowników czy skalą międzynarodowego sukcesu nie jest odpowiednim kryterium. W praktyce „media społecznościowe" są terminem parasolowym obejmującym różne usługi sieciowe ułatwiające bezpośrednie kontakty użytkowników w sieci i których funkcjonalności umożliwiają dzielenie się i komentowanie współtworzonych treści[9]. Dla celów niniejszego opracowania „media społecznościowe" klasyfikowane są przez swoje funkcjonalności: możliwość publikowania i ko-

[7] T. Aichner i in., *Twenty-Five Years of social media: A Review of Social Media Applications and Definitions from 1994 to 2019*, „Cyberpsychology, Behavior, and Social Networking" 2021, vol. 24, no. 4.

[8] Meta, *The Facebook Company Is Now Meta* [na:] „Meta", https://about.fb.com/news/2021/10/facebook-company-is-now-meta/, 28 października 2021 r., dostęp 28 grudnia 2021 r.; Meta, *Company Info*, https://about.facebook.com/company-info/ (dostęp 25 lipca 2022 r.).

[9] T. Aichner i in., *op. cit.*; L. Sloan, A. Quan-Haase, *The Sage handbook of social media research methods*, Los Angeles - London 2017, s. 17.

mentowania treści w Internecie. Ze względu na odmienności w funkcjonowaniu internetowych platform sprzedażowych i portali ogłoszeniowych, które wpływają na przebieg czynności wykrywczych, nie będą one zaliczane do mediów społecznościowych, choć czynią tak niektórzy inni badacze[10].

Pod względem karnomaterialnym nie istnieją „przestępstwa społecznościowe". Nieznana jest też, na tle ogółu cyberprzestępstw, liczba przestępstw popełnianych z wykorzystaniem mediów społecznościowych[11]. Wiadomo jednak, że kluczowe funkcje takich platform, mające na celu zwiększanie wzajemnej widoczności użytkowników sieci, ich poglądów, innych informacji na ich temat oraz amplifikację interakcji pomiędzy nimi, zwiększają jednocześnie podatność tych samych osób na wiktymizację[12]. Heterogeniczna charakterystyka tych funkcjonalności powoduje, że ich wykorzystanie może być elementem praktycznie czynu zabronionego[13]. Utrudnia to operacjonalizację badań kryminologicznych i prawnych. Zakres omówionej w niniejszym artykule analizy empirycznej został zatem zawężony do badania spraw związanych z przekraczaniem dozwolonych granic wolności wypowiedzi w mediach społecznościowych: związek pomiędzy popularnością mediów społecznościowych a liczbą przestępstw z nienawiści został wielokrotnie udowodniony[14], a ściganie takich zachowań nie jest proste nie tylko ze względu na wątpliwości interpretacyjne wokół typizacji art. 256 i 257 k.k.[15], lecz również z powodu trudności na etapie wykrywczym.

DOMYŚLNY MODEL ŚCIGANIA SPRAWCÓW

Podstawowy schemat postępowania w sprawach czynów popełnionych w mediach społecznościowych jest relatywnie nieskomplikowany, a przy tym typowy także dla

[10] A. Chabiera, M. Klotz, *Dowody z mediów społecznościowych w sprawach dotyczących przestępstw z nienawiści - praktyka polskich organów ścigania*, [w:] *Media społecznościowe w postępowaniu karnym*, red. P. Waszkiewicz Warszawa 2022, s. 109.

[11] H. Dębniak, S. Rabczuk, *Wybrane aspekty prawne pozyskiwania danych z mediów społecznościowych przez polskie organy ścigania*, „Problemy Współczesnej Kryminalistyki" 2019, t. 23, s. 50.

[12] M. Yar, *E-Crime 2.0: the criminological landscape of new social media*, „Information & Communications Technology Law" 2012, vol. 21, no. 3, s. 216.

[13] T. Hoffmeister, *The Challenges of Preventing and Prosecuting Social Media Crimes*, „Pace Law Review" 2015, vol. 35, no. 1.

[14] K. Müller, C. Schwarz, *Fanning the Flames of Hate: Social Media and Hate Crime*, „Journal of the European Economic Association" 2021, vol. 19 no. 4; G. Ocieczek, K. Samiczak, *Przestępstwa z nienawiści*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2022, nr 2 (46), s. 56; P. Patel i in., *A theoretical review of social media usage by cyber-criminals*, [w:] *2017 International Conference on Computer Communication and Informatics (ICCCI)*, Coimbatore 2017.

[15] M. Błaszczyk, *Odpowiedzialność za przestępstwa „mowy nienawiści" stypizowane w art. 256 § 1 i 257 k.k. – wybrane problemy normatywne i praktyczne*, „Studia Iuridica" 2021, nr 88, s. 22.

bardzo wielu innych cyberprzestępstw[16]. Oparty jest przede wszystkim na współpracy z administratorami domen internetowych i przedsiębiorcami telekomunikacyjnymi:

Po wszczęciu postępowania od administratora danego portalu uzyskiwany jest numer IP urządzenia, z którego łączył się użytkownik sieci w danym czasie[17]. Tu warto przypomnieć, że administratorzy domen internetowych nie należą do kręgu podmiotów wymienionych w art. 218 k.p.k. (nie są przedsiębiorcami telekomunikacyjnymi, a usługodawcami świadczącymi usługi drogą elektroniczną). Kierowane do nich postanowienia o zażądaniu wydania danych powinny być sformułowane przede wszystkim w oparciu o art. 217 k.p.k. (w zw. z art. 236a k.p.k. oraz w zw. z art. 18 ust. 6 Ustawy o świadczeniu usług drogą elektroniczną[18]). Ustalenie numeru IP i czasu połączenia ma umożliwić uzyskanie od przedsiębiorcy telekomunikacyjnego danych abonenta, dla którego realizowano określone połączenie. Podstawę prawną postanowienia w tym przedmiocie stanowi zaś przede wszystkim art. 218 k.p.k. (w zw. z art. 236a k.p.k. oraz odpowiednimi przepisami ustawy Prawo Telekomunikacyjne[19]). Dane abonenta mogą zaś umożliwić realizację kolejnych czynności procesowych – np. przesłuchania, w toku którego zostanie ustalony potencjalny związek abonenta usługi ze zdarzeniem (lub jego brak ‑ może się wszak okazać, że z Internetu w tym czasie korzystała inna osoba o tożsamości znanej lub nie).

Oczywiście, zarysowany schemat jest uproszczony i podlega licznym modyfikacjom w zależności od faktycznej sytuacji procesowej. W praktyce konieczne może się okazać chociażby rozszerzenie kręgu zaangażowanych podmiotów (np. o bank, zwłaszcza w sprawach oszustw internetowych – co wymaga uchylenia tajemnicy bankowej[20]). Nawet w razie efektywnej współpracy z administratorami domen, ustalenie sprawcy może okazać się utrudnione z innych przyczyn – np. w razie stosowania narzędzi anonimizujących, ale także gdy podejrzewany okaże się jedną z wielu osób korzystających z danego urządzenia lub sieci w miejscu publicznym.

Opisany schemat jest zdecydowanie najskuteczniejszy, gdy sprawca działał z terenu Polski i na stronach administrowanych przez polskie podmioty. Uzyskiwanie danych o użytkownikach portali zagranicznych, w szczególności amerykańskich, pozostaje natomiast wysoce problematyczne. Polskie ustawodawstwo nie przewiduje związania usługodawców nakazem udostępnienia danych wydanym bezpośrednio przez polskie organy ścigania (choć propozycje takich przepisów zostały

[16] A. Lebiedowicz, *Wybrane aspekty prawnokarne, kryminalistyczne i kryminologiczne cyberprzestępczości*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2022, nr 1 (45), s. 47; D. Taberski, *Postępowania w sprawach o oszustwa popełnione za pośrednictwem Internetu*, „Prokuratura i Prawo" 2018, nr 6, s. 65.

[17] Również w przypadku dynamicznych adresów IP wystarczające jest uzyskanie informacji o numerze IP wraz z czasem nawiązania połączenia. Numer portu nie jest wówczas niezbędny do dokonania identyfikacji abonenta przez przedsiębiorcę telekomunikacyjnego.

[18] tekst jednolity Dz. U. z 2020 r., poz. 344.

[19] tekst jednolity Dz. U. z 2022 r., poz. 1648. (ze zm.).

[20] D. Taberski, *op. cit*., s. 81.

przedstawione przez ministra sprawiedliwości w projekcie ustawy o wolności słowa w Internecie)[21]. Domyślnym z formalnego punktu widzenia sposobem uzyskiwania takich danych jest zatem wniosek wystosowany na podstawie umowy o międzynarodowej pomocy prawnej (ang. *Mutual Legal Assistance Treaty,* MLAT)[22], przy czym w kontekście ścigania cyberprzestępczości od wielu lat system MLAT uchodzi (zresztą nie tylko w Polsce)[23] za nieefektywny. Trafnie wskazuje się, że jest to powodowane konfliktami pomiędzy europejskimi i amerykańskim systemem prawnym oraz wielomiesięcznym czasem oczekiwania na rozpatrzenie wniosku[24]. W sprawach o niskim ciężarze gatunkowym (objętych klauzulą *de minimis),* a w szczególności we wszystkich sprawach związanych z przekroczeniem granic wolności słowa, silnie chronionej w prawodawstwie amerykańskim, realizacja wniosku będzie niemożliwa i często pozostanie on wręcz bez odpowiedzi[25]. Co prawda w odniesieniu do europejskich użytkowników administratorami danych osobowych są obecnie spółki z siedzibami w Irlandii, jednak kraj ten (podobnie Dania) nie jest związany przepisami o Europejskim Nakazie Dochodzeniowym[26] stanowiącym jak dotąd prawdopodobnie najprostsze narzędzie współpracy dochodzeniowej pomiędzy krajami w UE[27]. Procedura uzyskania pomocy prawnej ze strony Irlandii jest zatem także długotrwała i skomplikowana[28]. Możliwe, że sytuacja zmieni się, jeżeli Irlandia przystąpi do przepisów o transgranicznym dostępie do elektronicznego materiału dowodowego przewidzianych europejskim rozporządzeniem *e-evidence29* – wciąż jeszcze nieprzyjętym.

---

[21] Ministerstwo Sprawiedliwości, *Projekt ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych (projekt nr UD293)*; S. Rabczuk, *Pozyskiwanie danych pochodzących z mediów społecznościowych – perspektywy dla polskich organów ścigania w kontekście rozporządzenia e-evidence,* [w:] *Media społecznościowe w postępowaniu karnym*, red. P. Waszkiewicz, Warszawa 2022, s. 263.

[22] P. Opitek, *op. cit.*, s. 68–69.

[23] J. Hill, *Problematic Alternatives: MLAT Reform for the Digital Age*, „Harvard National Security Journal", https://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/, 28 stycznia 2015 r., (dostęp 16 sierpnia 2022 r.); G. Nojeim, *When Other Governments Want Your Stuff: Rules of the Road for Cross-Boarder Law Enforcement Demands*, „Georgetown Law Technology Review" 2016, vol. 1.

[24] P. Opitek, A. Choroszewska, *Uzyskiwanie dowodów cyfrowych z zagranicy w sprawach karnych – stan obecny i procedowane zmiany (cz. I)*, „Prokuratura i Prawo" 2020, nr 9, s. 129.

[25] P. Opitek, *op. cit.*, s. 65–66.

[26] Dyrektywa Parlamentu Europejskiego i Rady 2014/41/UE z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych.

[27] G. Krysztofiuk, *Europejski nakaz dochodzeniowy*, „Prokuratura i Prawo" 2015, t. 12; P. Olber, *Europejski nakaz dochodzeniowy jako mechanizm współpracy międzynarodowej w sprawach karnych na rzecz zwalczania cyberprzestępczości*, „Przegląd Policyjny" 2020, nr 1 (137).

[28] S. Rabczuk, *op. cit.*

[29] Komisja Europejska, *Wniosek ws. Rozporządzenia Parlamentu Europejskiego i Rady w sprawie europejskiego nakazu wydania dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych i europejskiego nakazu zabezpieczenia dowodów dotyczącego elektronicznego materiału dowodowego w sprawach karnych COM/2018/225 final - 2018/0108 (COD)*, https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52018PC0225, 2018 r. (dostęp 29 lipca 2022 r.).

W praktyce alternatywną metodą uzyskania informacji o użytkownikach mediów społecznościowych może być też bezpośrednie zwrócenie się do podmiotu zagranicznego z wnioskiem o dobrowolne przekazanie danych. Dedykowany w tym celu organom ścigania formularz kontaktowy *online* udostępnia m.in. Facebook[30]. Taka współpraca może być efektywniejsza od realizowanej oficjalnymi kanałami międzynarodowej pomocy prawnej, aczkolwiek opiera się na dobrowolnej kooperacji i jest zależna od przyjętej przez zagraniczne podmioty gospodarcze polityki wewnętrznej. Rozwiązania te są wykorzystywane w praktyce, choć mogą budzić zastrzeżenia co do tego, czy i w jakim zakresie właściwe jest zastępowanie nimi procedur pomocy prawnej[31].

USTALANIE TOŻSAMOŚCI SPRAWCY NA PODSTAWIE INFORMACJI OTWARTYCH

Wobec nieefektywności międzynarodowej pomocy prawnej w części spraw przydatna może okazać się prosta analiza informacji publicznie dostępnych zgodna z założeniami tzw. białego wywiadu (ang. *Open Source Intelligence,* OSINT[32]). Biały wywiad, będący elementem szeroko rozumianej analizy kryminalnej[33], jako zespół technik i narzędzi jest od dawna skutecznie wykorzystywany przez organy ścigania w postępowaniu karnym[34], jak i przez inne służby w celu zapewnienia bezpieczeństwa publicznego[35]. Z badań kwestionariuszowych wynika też, że policjanci w Polsce bardzo chętnie wykorzystują funkcjonalności mediów społecznościowych w pracy wykrywczej w celu identyfikacji uczestników postępowania (z tych samych badań wynika też, że procedury międzynarodowej pomocy prawnej, postrzegane jako skomplikowane i nieskuteczne, są wykorzystywane niechętnie, w dalszej kolejności albo wcale)[36].

---

[30] Facebook, *Internetowe zgłaszanie dla organów ścigania,* https://www.facebook.com/records/login/ (dostęp 6 marca 2023r.).

[31] P. Opitek, *Wybrane…, op.cit.,* s. 72-73.

[32] B. Saramak, Uniwersytet Warszawski, Wydzial Dziennikarstwa i Nauk Politycznych, *Wykorzystanie otwartych zródel informacji w dzialalnosci wywiadowczej: historia, praktyka, perspektywy*, Warszawa 2015, s. 15.

[33] P. Chlebowicz, W. Filipkowski, *Analiza kryminalna: aspekty kryminalistyczne i prawnodowodowe*, Warszawa 2011, s. 35.

[34] A. Lebiedowicz, *Wykorzystanie białego wywiadu w działalności Policji i prokuratury*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2021 nr 1 (41); B. Stromczyński, P. Waszkiewicz, *Biały wywiad w praktyce pracy organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, „Prokuratura i Prawo" 2014, nr 5; A. Ziółkowska, *Biały wywiad jako narzędzie uzupełniające czynności z zakresu techniki kryminalistycznej*, „Acta Universitatis Lodziensis. Folia Iuridica" 2018, t. 82.

[35] P. Karasek, *Social Media Intelligence as a tool for immigration and national security purposes,* „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 19 (10).

[36] M. Czekalska, K. Krawczyk, *Media społecznościowe jako narzędzie pracy polskiej policji. Wyniki badań kwestionariouszowych* [w:] *Media społecznościowe w pracy organów ścigania*, red. P. Waszkiewicz,Warszawa 2021, s. 19–40.

Podstawowe narzędzia białowywiadowcze są zresztą stosowane powszechnie w praktyce, nawet jeżeli osoby prowadzące postępowanie nie są tego w pełni świadome. Na przykład ustalenie podmiotu administrującego stroną internetową (do którego należy się zwrócić o dane jej użytkownika) a także ustalenie właściwego przedsiębiorcy telekomunikacyjnego (realizującego usługę dla danego numeru IP w określonym czasie) następuje często z użyciem wyszukiwarki opartej na protokole WHOIS[37] (łatwo dostępnych w Internecie bazach informacji o domenach internetowych)[38].

Wskazana metoda jest efektywna kosztowo i bardzo skuteczna pod warunkiem, że podejrzewany użytkownik sieci nie zadbał o możliwie maksymalną anonimowość swojego profilu. Dotychczasowe badania wskazują zaś, że wielu sprawców przestępstw z nienawiści posługuje się w mediach społecznościowych prawdziwymi danymi osobowymi lub nie potrafi ich skutecznie ukryć nawet posługując się pseudonimami[39]. Przy typowaniu tożsamości użytkownika należy wykorzystać informacje świadomie lub nieświadomie przez niego ujawnione, nie ograniczając się do brzmienia imienia i nazwiska (zwłaszcza że osób o podobnych personaliach może być wiele). Pomocne może być ujawnione w Internecie miejsce zamieszkania, miejsce pracy, czy nazwa ukończonej szkoły – do których można zwrócić się o stosowne informacje. Skuteczne może okazać się też przesłuchanie w charakterze świadków osób widniejących na jego „liście znajomych" (przy założeniu, że dane przynajmniej części takich osób okażą się prawdziwe i że podejrzewany użytkownik jest im faktycznie znany). Kluczowe jest połączenie pracy *stricte* białowywiadowczej z dostępem do baz danych i registratur pozwalających na doprecyzowanie i weryfikację ustaleń (w szczególności dzięki krzyżowym sprawdzeniom w bazie PESEL). Niezbędna jest ostrożność, gdyż zakres udostępnianych informacji może być niewielki, a ich wiarygodność – niepewna. Co oczywiste, poczynione ustalenia nie mogą zastąpić czynności dowodowych i muszą zostać nimi zweryfikowane[40]. Często następuje to w toku przesłuchania – przeprowadzona analiza przypadków wskazuje, że finał sądowy znajdują postępowania, w których osoba ustalona w powyższy sposób przyznaje się do sprawstwa.

Dalszą trudność stanowią niedociągnięcia prawno-organizacyjne dotyczące stosowania białego wywiadu w postępowaniu karnym. Pomimo dużej przydatności takich analiz, nie istnieją regulacje ukierunkowujące czy organizujące taką pracę

[37] P. Lewulis, *Dowody cyfrowe – teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*, Warszawa 2021, s. 240–241.

[38] V. Troia, *WHOIS* [w:] *Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques*, Wiley 2020.

[39] A. Chabiera, M. Klotz, *op. cit.* s. 115.

[40] W. Mądrzejowski, *„Biały wywiad" w Policji*, [w:] W. Filipkowski, *Biały wywiad: otwarte źródła informacji -- wokół teorii i praktyki*, red. W. Mądrzejowski, Warszawa 2012, s. 118.

organów ścigania[41]. Ponadto, o ile dostęp do danych upublicznionych w Internecie jest w dozwolony także dla służb, przepisy nie precyzują sposobu prowadzenia związanej z tym dokumentacji procesowej. Dane takie są często dokumentowane w notatkach służbowych albo toku oględzin (niezupełnie prawidłowo, mając na uwadze literalne brzmienie art. 207 k.p.k.)[42].

Kontrowersje mogą też budzić kwestie etyczne, związane z prywatnością użytkowników i wyodrębnieniem danych „publicznych". Wiele informacji widocznych jest tylko dla zalogowanych użytkowników danej platformy, a część może być dostępna jedynie dla „znajomych" danego użytkownika (w zależności od przyjętych ustawień prywatności). O ile samo założenie przez funkcjonariusza konta w mediach społecznościowych w celu biernego przeglądania zawartości publicznych profili nie wydaje się problematyczne, wchodzenie w interakcje z użytkownikami w celu uzyskania informacji o może stanowić pozbawione podstawy prawnej przekroczenie prawa do prywatności[43]. Problemy tego rodzaju są podnoszone w praktyce zagranicznej: brytyjscy policjanci biorący udział w badaniach kwestionariuszowych wskazywali, że granice etyki w wykorzystywaniu mediów społecznościowych są dla nich nieostre, a sytuację mogłyby ustabilizować klarowne instrukcje służbowe[44]. Dla porównania, w zbiorach zasad etyki kierowanych do amerykańskich adwokatów obowiązuje zakaz komunikacji z uczestnikami postępowania poprzez media społecznościowe oraz korzystania z fałszywych kont w celu gromadzenia informacji (dozwolone jest natomiast przeglądanie i analiza publicznie dostępnych treści profili)[45]. Oczywiście, takie ograniczenia niekoniecznie muszą być adekwatne w kontekście polskiego postępowania karnego – warto jednak podjąć wysiłek na rzecz czytelnego uregulowania metod pracy policji w mediach społecznościowych.

ANALIZA PRZYPADKÓW – UWAGI METODOLOGICZNE

W omawianym kontekście zasadne jest przedstawienie ogólnego pytania badawczego, sformułowanego w nurcie eksploracyjnych badań jakościowych[46]: jak przebiegają postępowania w sprawach przestępstw z nienawiści dokonywanych w mediach

[41] A. Lebiedowicz, op. cit., s. 72.

[42] P. Lewulis, *Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law*, „Criminal Law Forum" 2022, nr 33 (1), s. 39-62.

[43] Por. M. Tomaszewska-Michalak, *Prawne aspekty pozyskiwania informacji w Internecie*, „Studia Politologiczne" 2019, t. 54.

[44] J. Williams, *Legal and ethical issues surrounding open-source research for law enforcement purposes* [w:] *4th European Conference on Social Media (ECSM 2017): Vilnius, Lithuania, 3-4 July 2017*, red. A. Skaržauskienė, N. Gudelienė), Red Hook, NY 2017, s. 403–404.

[45] J.P. Murphy, A. Fontecilla, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, „Richmond Journal of Law & Technology" 2013, vol. 19, s. 19; A. Parker, *Four Tips for Mining Social Media Evidence*, „Business Torts & Unfair Competition", 2019 vol. 26, no. 2, s. 24.

[46] J.W. Creswell, *Research design: qualitative, quantitative, and mixed methods approaches*, Thousand Oaks 2014, s. 129.

społecznościowych, które okazały się skuteczne? W jaki sposób ustalano w takich sprawach tożsamość sprawców w braku efektywnej współpracy międzynarodowej?

Wstępnej odpowiedzi na powyższe pytania można próbować udzielić na podstawie studium przypadków[47]. Analiza przeprowadzona w czerwcu 2022 r. objęła akta spraw karnych prawomocnie zakończonych w latach 2016–2018 w sądach rejonowych leżących we właściwości Sądu Okręgowego w Warszawie[48]. Konkretne sprawy zostały wyodrębnione do analizy na podstawie rezultatów wcześniejszych badań ilościowych realizowanych przez autora w 2019 r.[49] – z wcześniejszej próby wytypowano sprawy dotyczące przekroczenia granic wolności słowa w mediach społecznościowych. Ustalono łącznie jedenaście[50] takich spraw i wszystkie poddano analizie jakościowej (jedną z art. 255 k.k., sześć z art. 256 k.k. i cztery z art. 256 w zw. z art. 257 k.k.).

Postępowania były analizowane indywidualnie, bez z góry określonych zmiennych. Protokół badania (rozumiany jako procedura postępowania z danym przypadkiem)[51] zakładał szczegółowe zapoznanie się z aktami i odnotowywanie informacji o sposobie zachowania się sprawcy oraz wszystkich podejmowanych w postępowaniu działaniach i ich rezultatach – od powzięcia informacji o sprawie, do prawomocnego rozstrzygnięcia sądowego. Wyniki analizy opracowywane były na podstawie notatek badawczych przygotowanych w czasie przeglądu akt, przy czym żadne dane osobowe uczestników analizowanych postępowań nie były gromadzone.

Tak realizowana analiza ma swoje oczywiste ograniczenia. Wąski charakter próby o doborze celowym nie pozwala na łatwą generalizację rezultatów i porównywanie ich z wynikami innych badań, w szczególności z danymi ilościowymi. Jednakże, przyjęta metoda studium przypadków z założenia pozwala na przeprowadzenie badania na stosunkowo niedużej próbie wyłonionej w drodze doboru celowego[52]. Jest to także zgodne z ogólnymi założeniami badań jakościowych[53], których zamierzeniem jest przedstawienie pogłębionego opisu przypadków a nie ilościowa ich

[47] M. Łuczewski, P. Bednarz-Łuczewska, *Analiza dokumentów zastanych* [w:] *Badania jakościowe - metody i narzędzia*, red. D. Jemielniak, Warszawa 2012, s. 163–185; M. Strumińska-Kutra, I. Kołdakiewicz, *Studium przypadku* [w:] *Badania jakościowe – metody i narzędzia*, red. D. Jemielniak, Warszawa 2012, s. 1–37.

[48] Z wyjątkiem SR dla Warszawy-Żoliborza, którego Prezes nie wyraził zgody na przeprowadzenie badań.

[49] Szczegółowy przebieg zdarzeń nie był wówczas poddawany analizie ze względu na zdecydowanie bardziej ilościowy charakter badań i odmienny cel badawczy (związany ze sposobami ujawniania, zabezpieczania, analizy, prezentacji i oceny dowodów cyfrowych). Zawsze odnotowywano jednak podstawowe informacje o charakterystyce każdej sprawy, co pozwoliło na wyłonienie konkretnych sygnatur do dalszej analizy jakościowej. Pełen opis metodologii i rezultatów wspomnianego badania znajduje się w: P. Lewulis, op. cit., s. 211–257.

[50] Jedno postępowanie prowadzone z art. 255 k.k. wykluczono z badanej grupy przypadków ze względu na niepoczytalność sprawcy czynu, która silnie wpływała na jego motywację i *modus operandi*.

[51] M. Strumińska-Kutra, I. Kołdakiewicz, op. cit., s. 26.

[52] U. Flick, P. Tomanek, *Projektowanie badania jakościowego*, Warszawa 2012, s. 55–62; B. Flyvbjerg, *Pięć mitów o badaniach typu studium przypadku*, „Studia Socjologiczne" 2005, nr 2 (177).

[53] B. Flyvbjerg, op. cit.; D. Jemielniak, *Badania jakościowe – metody i narzędzia*, Warszawa 2012, s. xiii.

generalizacja. Akta spraw sądowych stanowią przy tym specyficzne, tzw. złożone[54] obiekty badawcze – zawierają (co do zasady chronologiczną) dokumentację rzeczywistych wydarzeń oraz ustaleń śledczych i jako takie „przypadki" dobrze poddają się analizie właściwej naukom społecznym. Kolejnym, celowo przyjętym ograniczeniem jest poddanie analizie wyłącznie spraw, w których proces wykrywczy zakończył się sukcesem organów ścigania. Z przeprowadzonej analizy wyłania się jedynie obraz postępowań skutecznych, co nie daje podstawy do wnioskowania o tym, jakie okoliczności udaremniłyby ściganie (wiadomo jednak, co nie jest w tym przeszkodą i jaka jest charakterystyka zdarzeń znajdujących finał sądowy). W przyszłych badaniach zdecydowanie warto jest dokonać analizy spraw zakończonych na etapie postępowania przygotowawczego ze względu na niewykrycie sprawcy, a niniejsza analiza jakościowa może stanowić odpowiedni punkt wyjścia w przyszłej konceptualizacji zamierzeń badawczych i w generowaniu hipotez.

PRZEBIEG POSTĘPOWAŃ – ANALIZA PRZYPADKÓW

Badane postępowania miały szereg elementów wspólnych. Wszystkie prowadzone były z zawiadomienia – najczęściej pochodzącego od jednej z organizacji pozarządowych prowadzących monitoring Internetu pod kątem mowy nienawiści. Wszystkie też dotyczyły wpisów (komentarzy) internetowych, które w swojej treści naruszały dozwolone granice wolności słowa. Przedmiotowe treści miały co do zasady wymowę wulgarnie rasistowską, ksenofobiczną, wzywającą do przemocy i nienawiści na tle religijnym lub etnicznym, albo nawoływały lub pochwalały popełnianie przestępstw. Precyzyjna treść tych wpisów została pominięta w niniejszym omówieniu – jej odtwarzanie jest zbędne w świetle celu analizy. We wszystkich sprawach ustalono rzeczywistą tożsamość przynajmniej jednej osoby, której sprawstwo było niesporne – wszystkie osoby, którym przedstawiono zarzuty, potwierdzały fakt zamieszczenia przez siebie wpisu (na ogół już podczas pierwszego przesłuchania w postępowaniu przygotowawczym). Co interesujące z dowodowo-kryminalistycznego punktu widzenia, w żadnym z analizowanych przypadków nie zabezpieczano dowodów cyfrowych ani nie powoływano biegłych (np. z zakresu informatyki). W żadnym z przypadków nie zaważyło to na rezultacie postępowania. Wszyscy doprowadzeni do odpowiedzialności sądowej sprawcy, jak wynikało z treści ich wyjaśnień, umieszczali swoje wpisy spontanicznie, pod wpływem emocji. Żaden z nich nie stosował technicznych zabiegów maskujących – swoją tożsamość co najwyżej próbowali nieskutecznie maskować przybranymi pseudonimami lub fałszywymi nazwiskami.

Cyberprzestrzenią zamieszczanych wpisów był przede wszystkim Facebook (w 6 z 11 spraw) oraz różne polskie portale informacyjne i rozrywkowe umożliwiające m.in. umieszczanie i komentowanie treści (wp.pl, wiocha.pl, gazeta.pl, sadistic.pl,

[54] T. Anwar, *Unfolding the Past, Proving the Present: Social Media Evidence in Terrorism Finance Court Cases*, „International Political Sociology" 2020, vol. 14, no. 4.

cda.pl). W postępowaniach dotyczących wpisów w polskich serwisach internetowych wszyscy sprawcy posługiwali się pseudonimami. Ich tożsamość była zawsze ustalana w ten sam, opisany wcześniej sposób: w drodze współpracy z administratorami domen internetowych i przedsiębiorcami telekomunikacyjnymi. Tak ustalonych abonentów usług telekomunikacyjnych przesłuchiwano w charakterze świadków – część z nich okazywała się sprawcami, część zaś wskazywała na inną osobę (najczęściej kogoś z domowników, członka rodziny lub znajomego, który miałby korzystać z danego urządzenia we wskazanym czasie), którą także przesłuchiwano. W rezultacie tych czynności uzyskiwano niebudzące wątpliwości przyznanie się do sprawstwa (tj. do faktu zamieszczenia wpisu w Internecie, niezależnie od jego oceny prawnokarnej, która bywała kwestionowana przez oskarżonych). Postępowania przygotowawcze w tych sprawach były jednak proste w przebiegu, choć niekoniecznie bardzo szybkie: od zgłoszenia zawiadomienia o popełnieniu przestępstwa do potwierdzenia tożsamości sprawcy w drodze przesłuchania upływało średnio 198 dni (mediana 203 dni).

Sześć spraw dotyczyło zachowań w zagranicznej platformie społecznościowej, tj. wpisów w portalu Facebook. Tylko w jednym z tych postępowań zwrócono się do administratora portalu o wydanie danych użytkownika – bezskutecznie (odnotowano jedynie brak odpowiedzi na przesłane żądanie). W aktach tych spraw umieszczane były jednak notatki służbowe uzasadniające bezcelowość występowania o dane do administratora portalu, w których stwierdzano m.in.: „władze amerykańskie konsekwentnie odmawiają wykonywania wniosków o pomoc prawną o czyny stypizowane w art. 212, 256, 257 i innych k.k., powołując się na okoliczność, że wykonanie takiej odezwy naruszyłoby porządek konstytucyjny Stanów Zjednoczonych Ameryki (…) ze względu na to, wniosek o międzynarodową pomoc prawną w niniejszej sprawie jest niecelowy”[55]. Albo: „Z uwagi na fakt, że siedziba podmiotu administrującego znajduje się na terenie USA, nie ma możliwości uzyskania adresu IP ani danych osób”[56]. Tożsamość podejrzanych we wszystkich tych przypadkach skutecznego ścigania ustalano w drodze analizy białowywiadowczej. Uwzględniano w niej informacje widniejących w profilu danego użytkownika – brzmienie imion, nazwisk, podane daty urodzenia, wskazywane miejsca pracy, dane osób z „listy znajomych”. Nie wszystkie dane osobowe podawane przez użytkowników były prawdziwe, ale żaden z profili nie był w pełni fałszywy. Umożliwiało to skuteczną analizę krzyżową z danymi pochodzącymi z dostępnych organom ścigania registratur (w szczególności z bazą PESEL). Czynności wykrywcze[57] prowadzone w ten sposób trwały śred-

[55] Notatka z 19 maja 2017 r. umieszczona w aktach sprawy o sygn. II K 867/17 (w Sądzie Rejonowym w Piasecznie).

[56] Notatka z 18 stycznia 2018 r. umieszczona w aktach sprawy o sygn. II K 1099/17 (w Sądzie Rejonowym dla Warszawy-Śródmieścia).

[57] Licząc od daty zawiadomienia o popełnieniu przestępstwa do potwierdzenia tożsamości sprawcy w drodze przesłuchania.

nio 133 dni (mediana 203). Całokształt tych działań w syntetyczny sposób opisano poniżej, z uwzględnieniem stanu faktycznego występującego w każdym z sześciu przypadków.

1) Przypadek pierwszy[58]: dotyczył komentarza umieszczonego z profilu o nazwie ekranowej „Jan Janina Kowadło"[59]. Na zdjęciu profilowym użytkownika widniały dwie osoby. Przeprowadzono „oględziny zawartości strony internetowej" (w trybie art. 207 k.p.k.), a w protokole oględzin opisany został wygląd strony internetowej którą wskazano w zawiadomieniu i stwierdzono, że „wśród wypowiedzi pod postem nie ujawniono komentarza o treści (…)". Do protokołu dołączono wydruki zrzutów ekranu z zawartością strony, z których wynika m.in., że funkcjonariusz realizujący oględziny prowadził je jako użytkownik zalogowany – z konta założonego na własne imię i nazwisko. Następnie dokonano sprawdzenia osób „Jan Kowadło" i „Janina Kowadło" w bazie PESEL – ustalono dwie osoby o takich danych, zameldowane pod tym samym adresem. Przesłuchany w charakterze świadka Jan K. potwierdził, że konta w portalu Facebook używa wspólnie z żoną, ale że to on zamieścił komentarz, który później skasował, i że nie pamięta jego treści. Wskazał, że nie chciał nikogo urazić, a komentarz umieścił pod wpływem wzburzenia i spożycia alkoholu. Przesłuchany w charakterze podejrzanego (po przedstawieniu mu zarzutu z art. 256 k.k.) – przyznał się do zarzuconego czynu i ponownie wyraził żal. Sprawa została zakończona wyrokiem warunkowo umarzającym postępowanie.
2) Przypadek drugi[60]: dotyczył komentarza w portalu Facebook umieszczonego przez użytkownika „Marian Maserati". W trybie art. 207 k.p.k. przeprowadzone zostały oględziny jego profilu ‑ w protokole opisano, że w profilu nie ma żadnych danych osobowych, że użytkownik ma 32 „znajomych", oraz że często publikuje na swoim profilu „treści wskazujące na negatywny stosunek do migrantów". Zdjęcie profilowe użytkownika sprawdzono także w wyszukiwarce obrazów Google Image Search – co prawda z wynikiem negatywnym, lecz warto podkreślić pomysłowość takiego sprawdzenia[61]. Do protokołu oględzin załączono wydruk całej zawartości profilu użytkownika wraz z historią publikowanych postów. Odnotowano, że w dostępnych Policji bazach danych nie istnieje osoba o personaliach „Marian Maserati". Zlecono natomiast przesłuchania w charakterze świadków łącznie pięciu osób, których dane (imiona i nazwiska) ustalono na podstawie listy „znajomych" podejrzewanego użytkownika oraz bazy PESEL. Dwie spośród tych pięciu osób zeznały, że przypisywane im profile nie należą do nich, zaś trzy pozostałe potwierdziły prawdziwość swo-

[58] W Sądzie Rejonowym dla m.st. Warszawy (sygn. III K 827/16).

[59] Wszelkie dane osobowe podawane w niniejszych opisach zostały zmienione. W przedstawionych opisach przypadków do stanu faktycznego dobrane zostały przykładowe imiona i nazwiska uczestników, dla zachowania czytelności przebiegu zdarzeń.

[60] W Sądzie Rejonowym w Piasecznie (sygn. II K 609/17).

[61] Wyszukiwanie obrazem umożliwia sprawdzenie, czy dane zdjęcie nie zostało wykorzystane w innym miejscu w Internecie dostępnym dla wyszukiwarki Google.

ich profili oraz „znajomość" z użytkownikiem „Marian Maserati" – znanym im faktycznie pod innym (prawdziwym) nazwiskiem. Na podstawie informacji od świadków ustalono jego tożsamość i miejscowość zamieszkania, który przesłuchany w charakterze świadka potwierdził zamieszczenie przez siebie komentarzy, a przesłuchany w charakterze podejrzanego przyznał się do zarzuconego mu czynu (z art. 256 w zb. z art. 257 kk), choć nie wyraził żalu. W trybie nakazowym został ukarany grzywną.

3) Przypadek trzeci[62]: zawiadomienie dotyczyło łącznie pięciorga użytkowników portalu Facebook komentujących treści. Ustalono prawdopodobną tożsamość trzech z nich, z czego jedną doprowadzono do odpowiedzialności sądowej, a w pozostałym zakresie postępowanie umorzono. W aktach sprawy pozostawiono szereg notatek dotyczących niemożliwości uzyskania danych użytkowników serwisu Facebook w drodze pomocy prawnej. W trybie art. 207 k.p.k. oględzinom poddano „profile osób zamieszczających komentarze na portalu FB" – w protokole opisano konta użytkowników, odnotowano dostępne publicznie dane i informacje o powiązaniach osobowych. Tego samego dnia sporządzona została także notatka opisująca „analizę danych zawartych na kontach FB" i porównanie ich z danymi z bazy PESEL. Dokonano krzyżowych porównań pomiędzy danymi z profili w portalu Facebook (imiona, nazwiska, daty urodzin, informacje o członkach rodziny) z bazą PESEL. Stwierdzono, że w przypadku części osób „brak jest możliwości ustalenia tożsamości" – np. stwierdzono, że w Polsce jest 50 osób o personaliach „Karina Nowak" (w tym 7 urodzonych w roku podanym przez podejrzewaną użytkowniczkę Facebooka). Ustalono jednak prawdopodobne dane osobowe trzech osób wymienionych w zawiadomieniu i przesłuchano je w charakterze świadków. Dwie z nich zaprzeczyły, jakoby wskazane profile w mediach społecznościowych należały do nich (argumentując, że „są inne osoby o takim nazwisku"). Przesłuchania świadków były realizowane w drodze pomocy prawnej przez inne jednostki terenowe Policji. Co interesujące, świadkom okazywano link (treść adresu URL) do podejrzewanego profilu a nie graficzną reprezentację profili. Tylko jeden z przesłuchiwanych potwierdził, że wskazany mu profil należy do niego, i że to on zamieścił wskazywany mu komentarz. Zeznał też: „nie wiem co mnie podkusiło, zrobiłem to, czytając inne wpisy podobnej treści, pod wpływem emocji. Żałuję". Przesłuchany w charakterze podejrzanego (pod zarzutem z art. 256 §1 w zb. z 257 kk) przyznał się do winy i odmówił składania wyjaśnień. Oskarżony został ukarany grzywną.

4) Przypadek czwarty[63]: postępowanie dotyczyło publicznego nawoływania do popełnienia przestępstwa w komentarzach zamieszczanych w portalu Facebook przez dwóch użytkowników („Jan Piotrowski" i „Janusz Novacki"). Przeprowadzone zostały oględziny (w trybie art. 207 k.p.k.) „strony internetowej o adresie

[62] W Sądzie Rejonowym w Piasecznie (sygn. II K 867/17).

[63] W Sądzie Rejonowym dla Warszawy-Śródmieścia (sygn. II K 1099/17).

logicznym (…)". W protokole oględzin opisano sposób wejścia na stronę, na której znajdowały się komentarze objęte zawiadomieniem, i dołączono do niego wydruk zrzutów ekranu. Z dołączonej notatki wynika też, że zgodnie z danymi z bazy PESEL w Polsce żyje 50 osób o imieniu i nazwisku „Jan Piotrowski" i że brak jest osób o danych podanych przez drugiego podejrzewanego użytkownika. Do administratora Facebooka (na amerykański adres spółki) przesłano postanowienie – wydane na podstawie art. 217 w zw. z art. 180 k.p.k. – z żądaniem wydania danych IP podejrzewanych użytkowników. Odpowiedzi na to postanowienie nigdy nie otrzymano, co stwierdzono też notatką służbową, po czym postępowanie umorzono z uwagi na niewykrycie sprawcy. Na skutek zażalenia złożonego przez pokrzywdzone osoby sąd nakazał śledczym: zwrócić się do europejskiego oddziału Facebooka o wydanie danych użytkownika „Jan Piotrowski" oraz zwrócić się o dane takiej osoby do spółki widniejącej w profilu jako „miejsce pracy" oraz do uczelni, również wymienionej w publicznym profilu użytkownika. W zakresie użytkownika „Janusz Novacki" umorzenie pozostało w mocy. W efekcie zwrócono się do Facebook Poland sp. z o.o. oraz do Facebook Ireland Ltd. (jako podstawę prawną przesłanych pism wskazano art. 15 §3 k.p.k. – pisma pozostały bez odpowiedzi). Zwrócono się także do uczelni i miejsca pracy wskazanych przez Jana Piotrowskiego w jego profilu. Odpowiedzi z obu tych miejsc wpłynęły do akt sprawy po dwóch dniach i zawierały dane Jana Piotrowskiego (w tym numer PESEL i adres zamieszkania). Przesłuchany w charakterze świadka potwierdził, że jest użytkownikiem wskazanego konta w portalu Facebook i że to on zamieścił przypisywany mu komentarz. Na etapie sądowym prowadzono spór co do karnomaterialnej kwalifikacji czynu, natomiast okoliczności faktyczne (tj. zamieszczenie komentarza przez oskarżonego) nie były kwestionowane[64]. W pierwszej instancji postępowanie zostało umorzone warunkowo, zaś sąd odwoławczy orzekł o uniewinnieniu.

5) Przypadek piąty[65]: dotyczył użytkownika „Michał Kowalski", z którego konta umieszczono nienawistny komentarz. W aktach zamieszczono notatkę służbową o treści: „wykonując czynności służbowe do sprawy (…) ustaliłem dane osobowe właściciela profilu 'Michał Kowalski', mając informacje z profilu FB – imię i nazwisko jego żony oraz datę jej urodzenia. Pełne dane zamieszczono w zał. teleadresowym". Ustalony z wykorzystaniem tych danych w bazie PESEL i przesłuchany w charakterze podejrzanego Michał Kowalski przyznał się do zarzuconego mu czynu z art. 256 §1 k.k. i odmówił składania wyjaśnień, zastrzegając, że jest je gotów złożyć przed sądem. Do sądu przesłany został wniosek o warunkowe umorzenie postępowania (notabene, w uzasadnieniu wniosku wskazano, że „podejrzany zrozumiał naganność swojego zachowania", choć faktycznie w aktach brak jest jego stanowiska w tej sprawie).

[64] Z tego powodu powtarzanie w tym miejscu argumentacji prawnej stron i sądu prowadzących do uniewinnienia jest niecelowe.

[65] W Sądzie Rejonowym dla Warszawy Mokotowa w Warszawie (sygn. XIV K 2/16).

6) Przypadek szósty[66]: dotyczył komentarza użytkowniczki Facebooka posługującej się nazwą ekranową „Maria Janina Górska" pod materiałem umieszczonym na stronie „showtime.pl" (komentarz pochodził z konta na Facebooku; taki sposób komentowania umożliwiała odpowiednia wtyczka na przedmiotowej stronie, co początkowo nie zostało dostrzeżone przez prowadzących postępowanie). Po wszczęciu dochodzenia przeprowadzono oględziny „strony internetowej showtime.pl" (w trybie art. 207 k.p.k.). W protokole oględzin stwierdzono, że „na przedmiotowej stronie nie odnotowano powyższego komentarza", po czym oględziny zakończono. Do administratora strony showtime.pl przesłano postanowienie „o zwolnieniu z tajemnicy służbowej i żądaniu wydania rzeczy" w zakresie danych podejrzewanego użytkownika, jednakże w odpowiedzi administrator wskazał, że nie posiada danych tej osoby, gdyż administratorem tych danych jest portal Facebook. O dane do portalu Facebook nie zwrócono się. Ustalono natomiast dane osobowe i adresowe Marii Janiny Górskiej w bazie PESEL – podane imiona i nazwisko okazały się prawdziwe. Przesłuchana w charakterze świadka potwierdziła, że korzysta z Facebooka i że to ona jest autorką przedmiotowego komentarza. Dodała też, że komentarz napisała pod wpływem emocji wywołanych treścią komentowanego artykułu oraz innego nagrania, które oglądała (nieustalonego w postępowaniu). Podkreśliła, że nie ma uprzedzeń do osób innych narodowości. Przesłuchana w charakterze podejrzanej (pod zarzutem z art. 265 §1 kk) przyznała się do winy i wyraziła żal. Postępowanie karne zostało warunkowo umorzone.

WNIOSKI

Z podjętej analizy wyłania się częściowo nieoczywisty przebieg skutecznych postępowań karnych skierowanych przeciwko sprawcom mowy nienawiści w mediach społecznościowych. Istotne w badanych sprawach było przede wszystkim to, czy platforma społecznościowa, z której korzystał sprawca działający w Polsce, jest administrowana przez podmiot leżący w polskich granicach jurysdykcyjnych (czynnik obiektywny), a jeżeli nie, to czy możliwe było ustalenie tożsamości sprawcy na podstawie informacji na jego temat ujawnionych publicznie (czynnik subiektywny). Wiążą się z tym dwie różne, choć niewykluczające się wzajemnie taktyki wykrywcze: oparta na danych przekazywanych przez podmioty trzecie oraz oparta na analizie informacji ze źródeł otwartych. Wśród najistotniejszych wniosków z przeprowadzonej analizy należy wskazać następujące:

Po pierwsze, w sprawach dotyczących wpisów na polskich stronach internetowych skuteczne działania wykrywcze prowadzono tylko na podstawie danych uzyskiwanych od ich administratorów domen i przedsiębiorców telekomunikacyjnych. Wszyscy użytkownicy polskich stron internetowych występowali pod pseudonimami, co nie miało wpływu na proces wykrywczy. Podstawy prawne kierowanych do nich

[66] W Sądzie Rejonowym dla Warszawy-Śródmieścia w Warszawie (sygn. II K 1026/16).

postanowień nie zawsze były prawidłowe – w szczególności mylono zakres art. 217 i 281 k.p.k., choć nie miało to faktycznego wpływu na realizację żądań przez ich adresatów.

Po drugie, we wszystkich mających finał sądowy sprawach dotyczących wpisów w portalu Facebook podejrzanych ustalano tylko na podstawie informacji osobistych na ich temat dostępnych w profilach użytkownika, weryfikowanych w bazie PESEL. Przydatne informacje obejmowały imiona i nazwiska (często prawdziwe i unikalne), dane o miejscu pracy lub ukończonej szkole (do których można było zwrócić się o dane osobowe), dane członków rodziny i daty urodzenia (umożliwiające sprecyzowanie wyszukiwani w bazie PESEL), dane osobowe „znajomych" (pozwalające na ich przesłuchanie w celu ustalenia tożsamości podejrzewanej osoby). O ile zatem przybrane (fałszywe) dane osobowe nie ochronią sprawcy przed odpowiedzialnością za wpisy na stronach polskich, mogą skutecznie uniemożliwić jego ściganie, jeżeli działał na stronach zagranicznych. Warto dostrzec, że funkcjonariusze prowadzący analizowane postępowania wykazywali się niekiedy pomysłowością w stosowaniu tej taktyki. Co więcej, postępowania realizowane w ten sposób były przeciętnie szybsze (średnio o około dwa miesiące) od tych, w których tożsamość sprawców ustalano w drodze analizy danych o połączeniach internetowych sprawców.

Po trzecie jednak, finał sądowy znajdowały wyłącznie takie sprawy, w których podejrzany przyznawał się do sprawstwa. Jeżeli podejrzewany użytkownik zagranicznych mediów społecznościowych zaprzeczał związkom ze zdarzeniem – postępowanie przeciwko niemu nie było kontynuowane. We wszystkich analizowanych postępowaniach oskarżeni przyznawali się do dokonania wpisu, nawet jeśli kwestionowali jego prawnokarny charakter.

Po czwarte, zeznania świadków, wyjaśnienia podejrzanych i proste wydruki treści stron internetowych (a i to nie zawsze, gdyż w analizowanych przypadkach były i takie, gdzie komentarze zostały wcześniej usunięte) stanowiły najczęściej jedyne, ale wystarczające podstawy ustaleń faktycznych w badanych postępowaniach dotyczących zagranicznych mediów społecznościowych. Nie wykorzystywano innego materiału dowodowego. W szczególności w żadnej sprawie nie badano urządzeń w poszukiwaniu dowodów cyfrowych ani nie powoływano biegłych. Nie wiadomo, jakie byłyby rezultaty tych samych postępowań, gdyby podejrzani przyjęli bardziej konfrontacyjną, obronną postawę w swoich sprawach. Tym bardziej więc to właśnie przesłuchania stanowiły kluczową czynność dowodową. Ich taktyka była często przemyślana – pytania zadawane były od kwestii ogólnych (np. kto korzysta z danego urządzenia, czy przesłuchiwany korzysta ze wskazanych stron, kont użytkownika) po szczegółowe (np. czy to przesłuchiwana osoba zamieściła dany wpis) w sposób nie zdradzający zbyt wcześnie przyczyn przesłuchania co mogłoby zaalarmować podejrzanego i wywołać chęć złożenia wyjaśnień niezgodnych z prawdą.

Ogólnym wnioskiem jest zaś to, że finał sądowy znajdowały sprawy o podstawowym, nieskomplikowanym przebiegu. Skuteczność ścigania przestępstw z nienawiści popełnianych w cyberprzestrzeni uzależniona jest od wyborów dokonywanych przez sprawcę: czy działał na polskich, czy zagranicznych stronach, czy zachował anonimowość swojego konta, a wreszcie – czy i w jaki sposób zaprzeczył swojemu sprawstwu w toku przesłuchania. Poniekąd sposób świadczy to o (niezawinionej) bezsilności organów ścigania, co nie napawa optymizmem. Niewykluczone, że przyszłe lub trwające procesy prawotwórcze i społeczne będą miały pozytywny wpływ na omówioną problematykę, a tymczasem warto analizować dostępne metody wykrywcze i harmonizować je.

BIBLIOGRAFIA

AKTY PRAWNE:

Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (tekst jednolity Dz. U. z 2022 r., poz. 1375, ze zm.).
Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (tekst jednolity Dz. U. z 2022 r., poz. 1138, ze zm.).
Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tekst jednolity Dz. U. z 2020 r., poz. 344).
Ustawa z dnia 16 lipca 2004 – Prawo telekomunikacyjne (tekst jednolity Dz.U. z 2022 r., poz. 1648, ze zm.).

LITERATURA:

Aichner T. i in., *Twenty-Five Years of social media: A Review of Social Media Applications and Definitions from 1994 to 2019,* „Cyberpsychology, Behavior, and Social Networking" 2021, vol. 24, no. 4.
Anwar T., *Unfolding the Past, Proving the Present: Social Media Evidence in Terrorism Finance Court Cases*, „International Political Sociology" 2020, vol. 14, no. 4.
Błaszczyk M., *Odpowiedzialność za przestępstwa „mowy nienawiści" stypizowane w art. 256 § 1 i 257 k.k. – wybrane problemy normatywne i praktyczne*, „Studia Iuridica" 2021, nr 88. Chabiera A., Klotz M., *Dowody z mediów społecznościowych w sprawach dotyczących przestępstw z nienawiści – praktyka polskich organów ścigania*, [w:] *Media społecznościowe w postępowaniu karnym*, red. P. Waszkiewicz, Warszawa 2022.
Chlebowicz P., Filipkowski W., *Analiza kryminalna: aspekty kryminalistyczne i prawnodowodowe*, Warszawa 2011.
Creswell J.W., *Research design: qualitative, quantitative, and mixed methods approaches*, Thousand Oaks 2014.
Czekalska M., Krawczyk *K., Media społecznościowe jako narzędzie pracy polskiej policji. Wyniki badań kwestionariouszowych*, [w:] *Media społecznościowe w pracy organów ścigania*, red. P. Waszkiewicz, Warszawa 2021.Dębniak H., Rabczuk S., *Wybrane aspekty prawne pozyskiwania danych z mediów społecznościowych przez polskie organy ścigania*, „Problemy Współczesnej Kryminalistyki" 2019, t. 23.
Flick U., Tomanek P., *Projektowanie badania jakościowego*, Warszawa 2012.
Flyvbjerg B., *Pięć mitów o badaniach typu studium przypadku*, „Studia Socjologiczne" 2005, nr 2 (177).
Hoffmeister T., *The Challenges of Preventing and Prosecuting Social Media Crimes*, „Pace Law Review" 2015, vol. 35 no. 1.
Jemielniak D., *Badania jakościowe – metody i narzędzia*, Warszawa 2012.
Karasek P., *Social Media Intelligence as a tool for immigration and national security purposes*, „Przegląd Bezpieczeństwa Wewnętrznego" 2018, nr 19 (10).
Krysztofiuk G., *Europejski nakaz dochodzeniowy*, „Prokuratura i Prawo" 2015, nr 12.

Lebiedowicz A., *Wybrane aspekty prawnokarne, kryminalistyczne i kryminologiczne cyberprzestępczości*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2022, nr 1 (45).
Lebiedowicz A., *Wykorzystanie białego wywiadu w działalności Policji i prokuratury*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2021, nr 1 (41).
Lewulis P., *Collecting Digital Evidence from Online Sources: Deficiencies in Current Polish Criminal Law*, „Criminal Law Forum" 2022, nr 33 (1).Lewulis P., *Dowody cyfrowe – teoria i praktyka kryminalistyczna w polskim postępowaniu karnym*, Warszawa 2021.
Lewulis P., *O rozgraniczeniu definicyjnym pomiędzy przestępczością „cyber" i „komputerową" dla celów praktycznych i badawczych*, „Prokuratura i Prawo" 2021, nr 3. Łuczewski M., Bednarz-Łuczewska P., *Analiza dokumentów zastanych [w:] Badania jakościowe – metody i narzędzia*, red. D. Jemielniak, Warszawa 2012.
M. Strumińska-Kutra, I. Kołdakiewicz, *Studium przypadku*, [w:] *Badania jakościowe – metody i narzędzia*, red. D. Jemielniak, Warszawa 2012.
Mądrzejowski W., „Biały wywiad" w Policji [w:] Biały wywiad: otwarte źródła informacji -- wokół teorii i praktyki, red. W. Filipkowski, W. Mądrzejowski, Warszawa 2012,
Müller K., Schwarz C., *Fanning the Flames of Hate: Social Media and Hate Crime*, „Journal of the European Economic Association" 2021, vol. 19, no. 4.
Murphy J.P., Fontecilla A., *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, „Richmond Journal of Law & Technology" 2013, vol. 19.Nojeim G., *When Other Governments Want Your Stuff: Rules of the Road for Cross-Boarder Law Enforcement Demands*, „Georgetown Law Technology Review" 2016, vol. 1.
Ocieczek G., Samiczak K., *Przestępstwa z nienawiści*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2022, nr 2 (46).
Olber P., *Europejski nakaz dochodzeniowy jako mechanizm współpracy międzynarodowej w sprawach karnych na rzecz zwalczania cyberprzestępczości*, „Przegląd Policyjny" 2020, nr 1 (137).
Opitek P., Choroszewska A., *Uzyskiwanie dowodów cyfrowych z zagranicy w sprawach karnych - stan obecny i procedowane zmiany (cz. I)*, „Prokuratura i Prawo" 2020, nr 9.
Opitek P., *Wybrane aspekty pozyskiwania dowodów cyfrowych w sprawach karnych*, „Prokuratura i Prawo" 2018, nr 7–8.
Parker A., *Four Tips for Mining Social Media Evidence, „Business Torts & Unfair Competition"*, 2019, vol. 26, no. 2.
Patel P. i in., *A theoretical review of social media usage by cyber-criminals*, [w:] 2017 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore 2017. P. Szymański, P. Zalewski., *Aktywność zorganizowanych grup przestępczych w cyberprzestrzeni w czasach pandemii – analiza wybranych podatności i metod anonimizacji*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury" 2022, nr 1 (45).
Rabczuk, S., *Pozyskiwanie danych pochodzących z mediów społecznościowych – perspektywy dla polskich organów ścigania w kontekście rozporządzenia e-evidence*, [w:] *Media społecznościowe w postępowaniu karnym*, red. P. Waszkiewicz, Warszawa 2022.
Saramak B., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Warszawa 2015.
Sloan L., Quan-Haase A., *The Sage handbook of social media research methods*, Los Angeles – London, 2017.
Stromczyński B., Waszkiewicz P., *Biały wywiad w praktyce pracy organów ścigania na przykładzie wykorzystania serwisów społecznościowych*, „Prokuratura i Prawo" 2014, nr 5.
Taberski D., *Postępowania w sprawach o oszustwa popełnione za pośrednictwem Internetu*, „Prokuratura i Prawo" 2018, nr 6.
Tomaszewska-Michalak M., *Prawne aspekty pozyskiwania informacji w Internecie*, „Studia Politologiczne" 2019, t. 54.
Troia V., *WHOIS*, [w:] *Hunting Cyber Criminals: A Hacker's Guide to Online Intelligence Gathering Tools and Techniques*, Wiley 2020.

Waszkiewicz P., *Media społecznościowe w postępowaniu karnym*, Warszawa 2022.
Williams J., *Legal and ethical issues surrounding open-source research for law enforcement purposes*, [w:] *4th European Conference on Social Media (ECSM 2017): Vilnius, Lithuania, 3-4 July 2017*, red. A. Skaržauskienė, N. Gudelienė, NY 2017.
Yar M., E-*Crime 2.0: the criminological landscape of new social media*, „Information & Communications Technology Law" 2013, vol. 21 no. 3.
Ziółkowska A., *Biały wywiad jako narzędzie uzupełniające czynności z zakresu techniki kryminalistycznej*, „Acta Universitatis Lodziensis. Folia Iuridica" 2018, t. 82.

STRONY INTERNETOWE:

https://datareportal.com/reports/digital-2022-global-overview-report,
https://about.fb.com/news/2021/10/facebook-company-is-now-meta/,
https://about.facebook.com/company-info/,
https://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/,
https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52018PC0225,
https://www.facebook.com/records/login/.

Determining the identity of social media users in Poland: prosecuting hate speech in cyberspace – a case study

SUMMARY

Some cybercrimes are relatively easy to prosecute, while others are almost impossible. This often depends on the perpetrator's modus operandi. When it comes to hate speech or other prohibited content posted on social networking sites, the effectiveness of basic investigative activities relying on data provided by the site administrator is limited. This article presents the results of a qualitative analysis of selected cases of legally concluded criminal proceedings concerning crossing the limits of freedom of expression on the Internet, where prosecution was successful and the real perpetrator was identified and brought to justice. In the analyzed cases, all perpetrators who posted on websites run by Polish entities were identified effectively, due to the cooperation between law enforcement authorities, website administrators, and telecommunications entities. On the other hand, the perpetrators of hate speech on foreign social networking sites (e.g. Facebook) were identified with basic Open-Source Intelligence techniques analysis, based on data publicly available in the perpetrators' profiles (such as names and surnames, workplaces, and details of family and friends). This article provides descriptions of the facts and the course of proceedings in the analyzed cases, illustrating various variants of how the identity of the perpetrator through the analysis of publicly available data may be established.

Key words: social media, hate speech, cybercrime, OSINT