Czasopismo Prawa Karnego i Nauk Penalnych
Journal of Criminal Law and Penal Studies
ISSN: 1506-1817 e-ISSN: 2719-6569
Rok/Volume XXVII: 2023 Zeszyt/No. 4

Jakub Retyk[1]

Wykorzystywanie dowodów z mediów społecznościowych w postępowaniu karnym a konstytucyjne prawo do prywatności

Use of Social Media Evidence in Criminal Proceedings vs. the Constitutional Right to Privacy

1. Wstęp

Media społecznościowe stanowią jeden z podstawowych sposobów komunikacji w XXI w. Zgodnie z badaniem *Digital 2022: Poland*[2], przeprowadzonym w lutym 2022 r., w Polsce istnieje ok. 27 mln użytkowników (nie można określić dokładnej liczby osób fizycznych) *social mediów*. Ponadto warto zauważyć, że aż 55,2% Polaków[3] nie sprawdza tego, jakie informacje podlegają przetwarzaniu z wykorzystaniem mediów społecznościowych. Przeprowadzone badania potwierdzają tezę o braku świadomości co do możliwości usunięcia treści i zaufaniu, że usunięte informacje nie podlegają odzyskaniu. Oczywiście przekonanie to jest błędne, jednakże prowadzi do wyjątkowej śmiałości w publikowaniu treści przez niektóre jednostki, w rezultacie czego aktywność w Internecie coraz częściej dostarcza materiału dowodowego organom ścigania. Przekonały się o tym chociażby osoby publikujące groźby pod postem litewskiej pary homoseksualnej, które to komentarze doprowadziły do sprawy przed Europejskim Trybunałem Praw Człowieka[4] (dalej: ETPC).

[1] Jakub Retyk – student kierunku prawo, Uniwersytet Warszawski / law student, University of Warsaw; ORCID: 0000-0002-3825-0203; ✉ jakub.retyk@gmail.com.

[2] S. Kemp, *Digital*…

[3] S. Cyrankiewicz-Gortyńska, *Wyniki*…

[4] Wyrok Europejskiego Trybunału Praw Człowieka z dnia 14 stycznia 2020 r. w sprawie Beizaraz i Levickas przeciwko Litwie, skarga nr 41288/15.

Ponadto niejako naturalnym procesem jest zwiększanie udziału dowodów z mediów społecznościowych, w szczególności z konwersacji prowadzonych przy użyciu tych mediów, w postępowaniu karnym, skoro to właśnie ta forma staje się dominującym sposobem komunikacji. W drodze przykładu, na początku października 2023 r. polskim światem internetowych twórców oraz ich obserwujących wstrząsnęła sprawa pedofilii wśród znanych „influencerów", nazwana PandoraGate, w której to materiał dowodowy właśnie pochodzi z wiadomości wykorzystywanych przy użyciu komunikatorów takich jak Messenger[5]. Polski ustawodawca nie zdecydował się jednak na odrębne uregulowanie kwestii pozyskiwania dowodów z *social mediów*, dlatego też otwarte pozostaje jedno z fundamentalnych pytań o granicę możliwości ich wykorzystania. Warto również podkreślić, że sfera udostępnianych treści w mediach społecznościowych może podlegać pod reżim ochrony jednej z naczelnych wartości konstytucyjnych, jaką jest prawo do prywatności. Wychodząc naprzeciw przedstawionej problematyce, niniejsze opracowanie ma na celu przybliżyć kwestie relacji pomiędzy prawem do prywatności a możliwością wykorzystywania dowodów z *social mediów* w postępowaniu karnym poprzez próbę odpowiedzi na pytanie, czy ochrona prawa do prywatności może uzasadniać ograniczenie pozyskiwania materiału dowodowego z *social mediów*.

Odpowiedź na zadane powyżej pytanie będzie udzielana przy wykorzystaniu dyrektywy proporcjonalności rozumianej jako konieczność zachowania odpowiedniej proporcji pomiędzy środkiem, jakim jest ograniczenie danego prawa lub wolności, a celem rozumianym jako szeroko pojęty interes publiczny, wraz z wprowadzeniem odpowiednich instrumentów ochronnych przed nadmierną i dyskrecjonalną ingerencją władz państwowych w prawa i wolności jednostki. Pierwszy etap odpowiedzi stanowi potwierdzenie hipotezy, że mimo braku wyraźnej regulacji w Kodeksie postępowania karnego[6], obecne normy procesowe nie wykluczają dopuszczalności wykorzystywania dowodów z *social mediów* w postępowaniu karnym. Następnie konieczne jest zdefiniowanie prawa do prywatności oraz określenie sfery życia prywatnego

[5] M. Czubaszek, *To jest*...

[6] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, Dz.U. 2022, poz. 1375, 1855, tekst jedn. ze zm., dalej: Kodeks postępowania karnego, k.p.k.

w *social mediach*. Wreszcie ostatni etap stanowi odpowiedź na następujące pytania:

1) Czy konwersacje grupowe są objęte tajemnicą korespondencji i czy można zaliczyć je do sfery życia prywatnego?
2) Czy organy publiczne powinny mieć dostęp do całej konwersacji, czy jedynie do jej części?
3) Czy organy ścigania mogą zamieszczać w bazach danych treści dostępne w mediach społecznościowych?

1.1. Definicje używanych w tekście pojęć

Współczesny świat cyfrowy zapewnia szeroką gamę form partycypacji społecznej w Internecie. Dlatego też dla celów poniższego opracowania konieczne jest przyjęcie jednolitej definicji zarówno samych *social mediów* (zamiennie stosuje się pojęcie „media społecznościowe"), jak i dowodów z *social mediów*. Ogólnie przyjęta definicja mediów społecznościowych zawiera w sobie zarówno serwisy społecznościowe (np. Facebook lub Twitter), komunikatory (np. Messenger), jak i serwisy streamingowe (np. Twitch czy TikTok). Ze względu na oczywistą różnorodność pośród *social mediów*, dla celów niniejszego artykułu pojęcie to zostało zawężone do jednego komunikatora oraz dwóch serwisów społecznościowych, tj. Facebooka, Instagrama[7] oraz Messengera[8]. Platformy te zostały wybrane, ponieważ utrzymują się jako najpopularniejsze spośród pozostałych komunikatorów i serwisów społecznościowych w Polsce i Unii Europejskiej[9].

W kwestii definicji dowodu z *social mediów* należy na wstępie zauważyć, że pojęcie można zaliczyć do szerszej instytucji dowodów cyfrowych. Za P. Lewulisem dowód cyfrowy stanowi: „informację o znaczeniu dowodowym dla postępowania wynikającą z danych binarnych przetwarzanych elektronicznie (tj. z danych w formie cyfrowej)"[10]. Jak dalej wskazuje P. Lewulis, definicja ta jest szeroka i mieści w swojej treści m.in. wiadomości e-mail, dokumenty zapisane na komputerze czy wypowiedzi

[7] Za pomocą którego, poza publikowaniem zdjęć wraz z ich opisami, użytkownicy również mogą wysyłać między sobą wiadomości, tak jak w przypadku komunikatorów.
[8] Historycznie komunikator ten był częścią Facebooka, obecnie jest on subsydiarnym elementem Facebooka, lecz jego posiadanie nie jest konieczne, aby korzystać z serwisu.
[9] Tak wynika z przywoływanego już raportu: S. Kemp, *Digital*...
[10] P. Lewulis, *Dowody*..., s. 58.

publikowane na portalach społecznościowych[11]. Dlatego też niniejszy artykuł ogranicza pojęcie dowodów z *social mediów* do dowodów cyfrowych, których źródłem są informacje transmitowane przez użytkowników następujących trzech platform: Facebook, Instagram, Messenger. Ostatnim kluczowym elementem definicyjnym, porządkującym cały poniżej przedstawiony wywód, jest definicja pojęcia „wykorzystywania dowodu". Zgodnie z definicją dostępną w internetowej wersji *Słownika języka polskiego*, słowo „wykorzystywać" oznacza użyć coś dla osiągnięcia jakiegoś celu[12]. Naczelnym celem postępowania karnego *sensu largo* jest ocena, czy doszło do popełnienia danego przestępstwa oraz ew. następstwa w zakresie skazania sprawcy czynu zabronionego. Tym samym autor na potrzeby niniejszego tekstu przyjmuje, że „wykorzystanie" obejmuje trzy etapy:

a) zabezpieczenie dowodu (a właściwie jego źródła jako nośnika informacji),
b) przeprowadzenie dowodu,
c) ocena dowodu dokonana przez odpowiedni organ, która to przyczynia się do ustalenia właściwego stanu faktycznego.

1.2. Klasyfikacje dowodów cyfrowych w podziale na dowody rzeczowe i osobowe

Celem odpowiedzi na pierwsze pytanie postawione we wstępie należy również wskazać, jakie miejsce zajmują dowody cyfrowe w klasycznym podziale na dowody rzeczowe oraz dowody osobowe. Kluczowy punkt odniesienia dla dalszych rozważań stanowi orzeczenie Sądu Najwyższego z dnia 13 października 2021 r.[13] dot. charakteru dowodowego środków pieniężnych zgromadzonych na rachunku bankowym. Wyrok ten spotkał się jednak z istotną krytyką ze strony części doktryny, która to nie zgadzała się ze stanowiskiem Sądu Najwyższego wskazującym na brak cech dowodu rzeczowego w przypadku rachunków bankowych[14]. Orzeczenie to również doprowadziło do zmian legislacyjnych w postaci nowego art. 236b k.p.k., który nakazuje traktować środki na rachunku bankowym jako rzecz lub przedmiot.

---

[11] P. Lewulis, *Dowody*..., s. 59.
[12] *Wykorzystywać*…
[13] Wyrok Sądu Najwyższego z dnia 13 października 2021 r., I KZP 1/21.
[14] Zob. M. Kurowski, *Glosa*…, s. 131–142.

Zgodnie z główną tezą tego judykatu dwa kryteria decydują o przynależności danego źródła dowodowego do grupy dowodów rzeczowych:

a) przedmiot istnieje fizycznie – posiada przymiot „materialności" (tak jak w przypadku prawa cywilnego „rzeczy ruchome") oraz
b) posiada właściwości indywidualizujące go – ma utrwalone ślady przestępstwa.

O ile pierwsze kryterium nie budzi wątpliwości, o tyle należy rozwinąć drugie z nich. Korzystając z dorobku cywilistyki oraz przedstawionej powyżej konstatacji Sądu Najwyższego, można zauważyć pewną pośrednią analogię pomiędzy dowodami cyfrowymi a rzeczami oznaczonymi co do gatunku. Celem wytłumaczenia tej tezy w niniejszym tekście wprowadzono dwa pojęcia: kopiowania oraz powielania. Dowody rzeczowe, które stanowią pośredni odpowiednik rzeczy oznaczonych co do tożsamości, można kopiować, ale nie można powielać, np. nóż ze śladami krwi może zostać sfotografowany czy narysowany, ale to, co czyni go wyjątkowym na tle innych noży, to indywidualizujące go właściwości w postaci krwi oraz ew. odcisków palców sprawcy. Tak samo dokument może zostać sfotografowany, ale to oryginalny podpis na nim czyni go wyjątkowym. Inaczej jest jednak w przypadku dowodów cyfrowych, które to mogą być powielane i każda z form „powielonych" ma właściwości indywidualizujące np. pendrive czy wydruk rozmów z danego komunikatora. Reasumując powyższe, dowody cyfrowe stanowią odrębną od dowodów rzeczowych grupę o charakterze *sui generis*. Prowadzi to do odpowiednich implikacji na gruncie k.p.k., w szczególności w zakresie zabezpieczania takich dowodów, co zostało opisane poniżej.

2. Dopuszczalność dowodów z *social mediów* w postępowaniu karnym

Zgodnie z wykładnią art. 7 Kodeksu postępowania karnego, statuującego jedną z podstawowych zasad procesowych – zasadę swobodnej oceny dowodów, wszelkie materiały, które nie zostały wskazane przez ustawodawcę jako dowody niedopuszczalne, mogą zostać przedstawione w toku postępowania. Zasada swobodnej oceny dowodów stanowi wsparcie naczelnej zasady polskiego procesu karnego, jaką jest zasada prawdy materialnej. Dlatego też normy kodeksowe „nie zawierają żadnych dyrektyw, które nakazywałyby określone ustosunkowanie się do

konkretnych dowodów, jak również przepisy te nie wprowadzają różnic w zakresie wartości dowodowej poszczególnych dowodów”[15]. Ogólną normą stwierdzającą niedopuszczalność danego dowodu i jednocześnie ograniczającą powyższą zasadę wynikającą z art. 7 k.p.k. jest art. 170 § 1 pkt. 1 k.p.k., zgodnie z którym dowód niedopuszczalny „rozumiany jest jako ten, którego przeprowadzenie jest sprzeczne z zakazami dowodowymi oraz ten, którego przedmiotem ma być okoliczność niemogąca w ogóle stanowić przedmiotu dowodu jak, na przykład treść prawa krajowego”[16]. Powyższe normy wskazują wyraźnie na otwarty katalog dowodów w procesie karnym, tym samym konstatuje się o dopuszczalności wykorzystania dowodów z *social mediów*. Problemem może okazać się sposób wprowadzenia dowodów z mediów społecznościowych do postępowania karnego na obu jego stadiach. W tym kontekście należy zwrócić uwagę na dwa aspekty: praktyczny, związany ze stroną techniczną zabezpieczenia i przedstawienia dowodów oraz prawny, dotyczący podstaw procesowych umożliwiających wprowadzenie dowodów. Obie te kwestie są doniosłe prawnie i mogą przesądzić o ocenie wartości dowodowej dokonywanej przez organy postępowania.

2.1. Strona techniczna zabezpieczenia i przedstawienia dowodów

W zakresie pierwszej kwestii doktryna prawa karnego zwraca uwagę na pewne niebezpieczeństwo związane z możliwością matactwa przy przedstawianiu tychże dowodów[17]. Współczesne programy komputerowe nie tylko umożliwiają obróbkę zrzutu ekranu, pozwalającą na przedstawienie danej konwersacji bez odpowiedniego kontekstu, ale także na wygenerowanie wypowiedzi przez inne osoby. Po wpisaniu odpowiedniej frazy można z łatwością znaleźć w przeglądarce internetowej poradniki nt. wytwarzania fałszywych konwersacji prowadzonych np. na Messengerze czy innych powszechnie używanych komunikatorach, do celów chociażby humorystycznych[18]. Równie łatwo można uzyskać dostęp do generatorów tzw. *deep fake'ów*, czyli technologii umożliwiającej tworzenie fałszywych nagrań wideo lub głosowych z wykorzystaniem

[15] J. Skorupka, w: *Kodeks*..., s. 35.
[16] P. Waszkiewicz, H. Dębniak, S. Rabczuk, *Wybrane*..., s. 116.
[17] K. Skraba, I. Strzałkowski, *Media*..., s. 116.
[18] Zob. celem przykładu: M. Majchrzycki, *Jak tworzyć*...

wizerunku jakiejkolwiek osoby na świecie. Oczywiście powstają w tym zakresie programy komputerowe, które przynajmniej w pewnym stopniu pomagają odróżnić fakty od fikcji, jednak są to oprogramowania nowe i niedoskonałe[19]. Podjęta problematyka rzetelności dowodów z *social mediów* jest o tyle istotna dla doktryny prawa, że nie wypowiedział się w tej materii dotychczas Sąd Najwyższy, a sami sędziowie, wedle badań przeprowadzonych w 2021 r.[20], odnoszą się do tychże dowodów z dużą ostrożnością, traktując je niejako „posiłkowo".

Dlatego też uzyskiwanie dowodów z mediów społecznościowych powinno zostać poprzedzone sprawdzeniem tzw. adresu IP, co jest konieczne, aby potwierdzić tożsamość sprawcy. W przypadku odwrotnej kolejności podjętych działań może okazać się, że ktoś prowadzi konwersacje bądź publikuje dane treści, podszywając się pod inną osobę. Ponadto należałoby też ustalić odpowiedniego użytkownika sprzętu elektronicznego. Poza problemem związanym z fałszywymi kontami, taki sposób zabezpieczania dowodów jest istotny ze względu na oprogramowania szpiegujące, które umożliwiają korzystanie z wszelkich funkcji danego urządzenia. Takim oprogramowaniem jest chociażby okryty złą sławą system Pegasus, który umożliwia korespondowanie za pomocą komunikatorów bez możliwości wykrycia faktycznej ingerencji osoby trzeciej (nie-użytkownika danego urządzenia) w konkretną konwersację lub publikowane w serwisach treści. Właściwym więc są założenia *Metodyki prowadzenia spraw dotyczących przestępstw z nienawiści popełnianych z wykorzystaniem internetu*[21], wydanej już w 2014 r. przez Prokuratora Generalnego, zobowiązujące organy ścigania m.in. do: utrwalenia treści i obrazów poprzez skopiowanie plików źródłowych oraz ekranów; ustalenia numeru IP, ISP oraz kopii źródłowych logów dotyczących nadania numeru IP. Jednakże organy ścigania stosują mniej rzetelną praktykę od przedstawionej w *Metodyce*… oraz w Wytycznych Komendanta Głównego Policji[22] wskazujących na sposób przeprowadzenia przeszukania oraz

[19] Zob. celem przykładu: M. Ciesielski, *Jak generuje*…

[20] M. Tomaszewska-Michalak, B. Stromczyński, K. Skraba, S. Rabczuk, P. Waszkiewicz, *Facebook*..., s. 183–184.

[21] M. Tomaszewska-Michalak, B. Stromczyński, K. Skraba, S. Rabczuk, P. Waszkiewicz, *Facebook*..., s. 119.

[22] Wytyczne Nr 3 Komendanta Głównego Policji z dnia 30 sierpnia 2017 r. w sprawie wykonywania niektórych czynności dochodzeniowo-śledczych przez policjantów, Dz. Urz. KGP 2017, poz. 59 ze zm.

oględzin wszelkich dowodów cyfrowych. Zgodnie bowiem z badaniami przeprowadzonymi przez P. Lewulisa zazwyczaj dowody cyfrowe utrwalone są w formie niepoświadczonych wydruków (uzyskanych zazwyczaj od podmiotów zewnętrznych) i również w takiej formie wprowadzone są na dalsze etapy postępowania[23]. Poza wspomnianymi wydrukami organy ścigania wykorzystują instytucję przeszukania, oględzin oraz wydania danych przez podmiot zewnętrzny (art. 236a k.p.k.). W zakresie przeszukania P. Lewulis wskazuje, że co do zasady zabezpieczeniu podlega wyłącznie sprzęt elektroniczny, a funkcjonariusze nie wykonują dodatkowych czynności mających na celu stworzenie kopii danych na nim zawartych[24]. Przedmiotem oględzin był albo dysk optyczny zawierający dane, albo strona internetowa traktowana jako rzecz – co, jak wskazano powyżej, nie jest adekwatne. Równie istotne jest to, że w przebadanych sprawach co do zasady nie wykorzystywano wiedzy specjalistycznej biegłych z zakresu informatyki[25].

Warto również zasygnalizować, że już na etapie zabezpieczania dowodów cyfrowych może dojść do konfliktu pomiędzy ochroną prawa do prywatności a zasadą prawdy materialnej, ponieważ wymienione czynności ingerują w sferę intymności danej jednostki. Na przykładzie braku dokonywania kopii danych zawartych na nośniku – sprzęcie elektronicznym: z jednej strony ten sposób postępowania może uniemożliwiać dojście do prawdy materialnej na wypadek, gdyby nośnik został nieodwracalnie uszkodzony, z drugiej jednak strony stworzenie kopii ingerowałoby dodatkowo w prawo do prywatności bez wyraźnej podstawy prawnej umożliwiającej podjęcie takich czynności. Ponadto dowody cyfrowe mogą zostać uzyskane przez organy ścigania właśnie z wykorzystaniem programów szpiegujących. Od 2018 r. Federalne Biuro Śledcze USA prowadziło operację o skali międzynarodowej pod kryptonimem Trojan Shield[26]. W ramach tej akcji FBI wprowadziło do obrotu prawie 12 tys. urządzeń – specjalnych telefonów, które miały zainstalowaną aplikację Anom. Program ten funkcjonował jak portal społecznościowy zapewniający pełną anonimowość swoim użytkownikom zajmującym się handlem i przemytem narkotyków. Dzięki tej akcji FBI nie musiało dodatkowo

[23] P. Lewulis, *Dowody*..., s. 245.
[24] P. Lewulis, *Dowody*..., s. 241.
[25] P. Lewulis, *Dowody*..., s. 243.
[26] United States Attorney's Office Southern District of California, *FBI's Encrypted*...

poszukiwać i zabezpieczać dowodów, ponieważ sami handlarze i przemytnicy dostarczali ich poprzez wzajemne przesyłanie sobie zdjęć w ramach aplikacji. Operacja została zakończona w 2021 r., a w październiku 2022 r. Sąd Okręgowy w Tarnowie skazał czternaście osób z Polski właśnie na podstawie danych dostarczonych z Anom[27]. Obrońcy skazanych zapowiedzieli złożenie apelacji, której podstawą ma być nielegalne uzyskanie dowodów przez organy ścigania. Warto w tym miejscu podkreślić, że obecne brzmienie art. 168a k.p.k. co do zasady umożliwia korzystanie z tzw. „owoców zatrutego drzewa"[28], co już na tym etapie ogranicza prawo do prywatności w przypadku konfliktu z zasadą prawdy materialnej.

2.2. Prawne aspekty wprowadzania do procesu dowodów z mediów społecznościowych

Pomimo wielu nowelizacji karnych na przestrzeni ostatnich 10 lat prawodawca nie zdecydował się na przyjęcie osobnej regulacji dotyczącej sposobów wprowadzenia do konkretnego procesu karnego dowodów z mediów społecznościowych. Jedynie pozornie problematykę zmaterializowania dowodu z *social mediów* wydaje się regulować Kodeks postępowania karnego. Ustawa przewiduje w art. 236a pewną szczątkową normę, której treść warto w tym miejscu przytoczyć: „Przepisy rozdziału niniejszego [Rozdział 25. Zatrzymanie rzeczy. Przeszukanie – J.R.] stosuje się odpowiednio do dysponenta i użytkownika urządzenia zawierającego dane informatyczne lub systemu informatycznego, w zakresie danych przechowywanych w tym urządzeniu lub systemie albo na nośniku znajdującym się w jego dyspozycji, lub użytkowaniu, w tym korespondencji przesyłanej pocztą elektroniczną". Pojęcie „system informatyczny" znajdujące się w niniejszej normie spotkało się ze sporą rozbieżnością w doktrynie. Przykładowo R. Stefański zdefiniował to pojęcie jako „część systemu przetwarzania danych, który zawiera się w systemie informacyjnym; jest realizowany dzięki technologii komputerowej, a jego celem jest wspieranie procesów zarządzania w przedsiębiorstwie i pozyskiwanie, przetwarzanie, gromadzenie oraz udostępnianie informacji"[29]. Inaczej M. Nawacki, który przedstawił dość daleko idącą tezę, wedle której

[27] M. Baran, *Apelacje*...
[28] Zob. M. Gabriel-Węglowski, *Teoria*..., pogląd nr 1.
[29] R.A. Stefański, S. Zabłocki, w: *Kodeks*..., s. 778.

„desygnaty pojęciowe terminów «użytkownik» i «dysponent» obejmują praktycznie wszystkie osoby i podmioty wykorzystujące jakikolwiek współczesny sprzęt elektroniczny i logujące się do Internetu”[30]. Inną kwestią budzącą pewne kontrowersje stanowi utrwalanie „korespondencji przesyłanej pocztą elektroniczną”. Już w 2004 r. A. Lach zauważył, że kontrola przesyłania poczty elektronicznej „może być traktowan[a] w sposób zbliżony do rozmowy telefonicznej, w innych zaś do przesyłania tradycyjnej poczty”[31]. Istotą powyższych rozważań jest refleksja nad aktualnością art. 236a k.p.k. Zdaniem autora niniejszego tekstu literalna wykładnia, szczególnie pojęcia „systemu informatycznego” i „poczty elektronicznej”, nie wskazuje na możliwość zastosowania normy wynikającej ze wskazanego przepisu k.p.k. do mediów społecznościowych. Ten sposób wykładni prowadziłby do rozszerzenia stosowania art. 236a k.p.k., co byłoby niezgodne z Konstytucją[32], jako że przyzwalałoby na pozaustawową ingerencję w prawo do prywatności poprzez możliwość uzyskania dostępu do treści zastrzeżonych dla pewnego grona odbiorców, co wynika np. z korespondencji prowadzonej przy użyciu komunikatorów.

Ponadto autor niniejszego tekstu stoi na stanowisku, że w zakresie wprowadzenia dowodu z *social mediów* do postępowania kluczową rolę odgrywa instytucja biegłego. Na wstępie warto zauważyć, że obecne przepisy wymagają, aby osoba wpisana jako biegły na listę biegłych prowadzoną przez sądy okręgowe (poza ogólnymi przesłankami, jak wiek) posiadała „teoretyczne i praktyczne wiadomości specjalne w danej gałęzi nauki, techniki, sztuki, rzemiosła, a także innej umiejętności, dla której ma być ustanowiona”[33]. Poświadczenie tej wiedzy wymagane jest jedynie poprzez opinie pracodawcy lub organizacji zawodowej w przypadku wolnego zawodu. Ponadto ostateczna ocena, czy posiadana przez jednostkę wiedza na temat wiadomości specjalnych została właściwie wykazana, należy do prezesa sądu okręgowego[34]. Niezależ-

30 M. Nawacki, w: *Kodeks*..., s. 1267.

31 A. Lach, *Dowody*...

32 Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997, nr 78, poz. 483; z 2001, nr 28, poz. 319; z 2006, nr 200, poz. 1471; z 2009, nr 114, poz. 946, dalej: Konstytucja RP, Konstytucja.

33 Zgodnie z § 12 ust. 1 pkt. 3 rozporządzenia Ministra Sprawiedliwości z dnia 24 stycznia 2005 r. w sprawie biegłych sądowych, Dz.U. 2005, nr 15, poz. 133 ze zm.

34 Zgodnie z § 12 ust. 2 rozporządzenia Ministra Sprawiedliwości w sprawie biegłych sądowych, Dz.U. 2005, nr 15, poz. 133 ze zm.

nie od instytucji biegłego sądowego, sąd zawsze może powołać biegłego *ad hoc*, czyli zgodnie z art. 195 k.p.k. osobę, która ma odpowiednią wiedzę w danej dziedzinie. Taki sposób unormowania ogólnie instytucji biegłego w procedurze karnej spotyka się z istotną krytyką w doktrynie ze względu na brak rzetelności wykonywanej przez biegłych pracy[35]. Niezależnie jednak od oceny *de lege lata*, organy ścigania i sądy powinny korzystać szeroko z wiedzy biegłych w przypadku wykorzystywania dowodów z *social mediów*. Osoby posiadające wiedzę specjalistyczną z zakresu informatyki powinny być obecne już przy zabezpieczeniu materiałów dowodowych, aby uchronić uzyskiwane dowody przed kontaminacją np. poprzez zapewnienie właściwego rozszerzenia przy zapisywaniu treści z serwisów społecznościowych. Ponadto, pomimo że zgodnie z przepisami k.p.k. ostateczna ocena dowodów należy do sędziego, to na etapie postępowania sądowego celem zachowania należytej staranności dowody z *social mediów* powinny podlegać ocenie biegłego co do ich prawdziwości. Można postawić tezę, że zasadniczo zawód sędziowski nie wiąże się z posiadaniem specjalistycznej wiedzy z zakresu informatyki. Co więcej, przy obecnym prymacie zasady prawdy materialnej sędzia powinien z urzędu zlecić badanie prawdziwości przedstawionych dowodów z mediów społecznościowych.

3. Definicja i zakres prawa do prywatności

Celem udzielenia odpowiedzi na pytania związane z przedstawioną we wstępie problematyką należy przybliżyć pojęcie „prawa do prywatności". Prawo to normowane jest jednakowo na gruncie krajowym, europejskim, a także międzynarodowym. Relewantne dla poniższego opracowania będzie przedstawienie norm wynikających z Konstytucji Rzeczpospolitej oraz Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności[36]. Warto podkreślić, że powyższe akty prawne zawierają w sobie zupełnie rozbieżne wzorce, co wynika z poglądu orzecznictwa ETPC, że EKPC stanowi „żywy instrument", który należy interpretować w sposób dynamiczny – nadążający za „duchem czasu". Co istotne, to właśnie

[35] Zob. przykładowo A. Szaplonczay, *Wadliwe*..., s. 225.

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

ETPC, a nie polski Sąd Najwyższy rozstrzygał dotychczas o prawie prywatności w *social mediach* w związku z postępowaniem karnym, rozbudowując tym samym wzorzec konwencyjny. Warto również wspomnieć, że prawo to zarówno na gruncie Konstytucji, jak i EKPC nie ma charakteru bezwzględnego i może ulec ograniczeniu na gruncie ustawowym.

Prawo do prywatności zostało zawarte w art. 47 Konstytucji[37], która to jest normą o szerokiej pojemności, mieszczącą w sobie zarówno prawo do ochrony życia prywatnego czy prawo do ochrony czci, jak również prawo do samostanowienia. Co prawda, jak wskazuje systematyka Konstytucji, jest to prawo o charakterze subsydiarnym oraz uzupełniającym do prawa do decydowania o swoim życiu osobistym, jednakże jego szczególny charakter został potwierdzony poprzez uwzględnienie tegoż prawa w art. 233 ust. 1 Konstytucji – normy dozwalającej na ograniczenie niektórych praw podczas stanu wyjątkowego albo stanu wojennego, o ile tylko „ograniczenia te odpowiadają stopniowi zagrożenia i zmierzają do jak najszybszego przywrócenia normalnego funkcjonowania państwa”[38]. Dla dalszych rozważań istotne jest określenie konstytucyjnej wykładni elementu składowego prawa do prywatności – ochrony sfery życia prywatnego.

Definicja sfery życia prywatnego stanowi kwestię sporną w doktrynie. Przykładowo P. Sarnecki wskazuje na następujący sposób wskazania desygnatów tegoż pojęcia: „częściowo można ją zdefiniować poprzez przeciwstawienie jej sferze życia «nieprywatnego» – czyli «publicznego» (w tym: «politycznego») lub «społecznego» jednostki – a więc sferze, w której następuje jej aktywne angażowanie się w różnorodne interakcje z innymi. (…) Przestawanie w kręgu rodziny bądź przyjaciół czy bliskich znajomych pozostaje w sferze życia prywatnego; bardzo podobne przestawanie z grupą innych osób – już nie”[39]. W kontrze do przedstawionego poglądu M. Wild co prawda zgadza się z definiowaniem „sfery życia prywatnego” poprzez antonimy, lecz wyraża sprzeciw wobec poglądu, iż desygnatem pojęcia jest „przebywanie w kręgu rodziny bądź przyjaciół”[40]. Jako przykład rewidujący pogląd P. Sarnackiego autor wskazuje,

[37] Pełne brzmienie art. 47 Konstytucji: „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym”.

[38] M. Florczak-Wątor, w: *Konstytucja*..., komentarz do art. 233, teza 1.

[39] P. Sarnecki, w: *Konstytucja*..., komentarz do art. 47, teza 3.

[40] M. Wild, *Konstytucja*..., komentarz do art. 47.

że: „nie sposób np. uznać, że uczestniczenie w spotkaniach anonimowych alkoholików (osób niepowiązanych raczej więzami przyjaźni) nie jest objęte sferą życia prywatnego”[41]. Następnie M. Wild proponuje następujący sposób zdefiniowania sfery życia publicznego, z którym należy się zgodzić ze względu na jego uniwersalny charakter:

> Innymi słowy, należy raczej rozważać, czy ze względu na sytuację jednostki jej prawo do bycia pozostawioną samą (*right to be let alone*) rzeczywiście powinno ustąpić, niż domagać się dodatkowego uzasadnienia dla objęcia ochroną autonomii jednostki poszczególnych sfer życia jednostki. Jak trafnie przyjęto w wyr. Sądu Apelacyjnego w Warszawie z 12.11.2013 r. (I ACA 906/13) jednostka, jako podmiot obdarzony autonomią woli, ma prawo samodzielnie wyznaczać obszar swojej prywatności, w szczególności wytyczać granice dostępności swojego życia osobistego dla innych[42].

Artykuł 8 EKPC, będący wzorcem prawa do prywatności dla ETPC, ma – podobnie jak art. 47 Konstytucji – szeroki zakres przedmiotowy dotyczący literalnie: poszanowania życia prywatnego i rodzinnego, ochrony miru domowego oraz tajemnicy korespondencji. Norma ta adresowana jest do władz państwowych, które to zobowiązane są do nieingerowania w sposób arbitralny w prywatność jednostek (negatywny wymiar prawa) oraz zapewnienia jednostkom skutecznego poszanowania ich prawa w relacji horyzontalnej (pozytywny wymiar prawa). Marek Antoni Nowicki, powołując się na wyrok ETPC z dnia 16 lipca 2014 r. w sprawie Hämäläinen przeciwko Finlandii[43], zwraca uwagę na to, że: „wymagania w stosunku do władz różnią się w zależności od wchodzącego w grę konkretnego aspektu życia prywatnego lub rodzinnego oraz od praktyki i sytuacji w danym państwie”[44]. Z orzecznictwa ETPC jako elementy istotne, określające pozytywne obowiązki państwa, można wymienić m.in.: „ocenę czy chodzi o fundamentalne wartości” albo „stopień spójności praktyk administracyjnych i prawnych w systemie krajowym” czy też „zakres i charakter obowiązków władzy publicznej”[45]. Jak wskazano wyżej, sfera życia prywatnego została poprzez orzecznictwo ETPC tak rozszerzona, że nie da się jej zdefiniować w sposób wyczerpujący.

---

41 M. Wild, *Konstytucja*..., komentarz do art. 47.

42 M. Wild, *Konstytucja*..., komentarz do art. 47.

43 Wyrok Europejskiego Trybunału Praw Człowieka z dnia 16 lipca 2014 r. w sprawie Hämäläinen przeciwko Finlandii, skarga nr 37359/09.

44 M.A. Nowicki, *Wokół*..., s. 801.

45 M.A. Nowicki, *Wokół*..., s. 802.

Marek Antoni Nowicki zwraca uwagę[46], iż ETPC podkreślił również, że pojęcie to obejmuje takie elementy jak: identyfikacja płciowa, orientacja seksualna i życie seksualne, prawo do poszanowania decyzji w sprawie posiadania dziecka, imię i nazwisko albo elementy związane z prawem do wizerunku, a także informacje osobiste, w związku z którymi zainteresowani mogą w sposób uprawniony oczekiwać, że nie będą publikowane bez ich zgody, w tym dane medyczne odnoszące się do stanu zdrowia i leczenia.

4. Prawo do prywatności a sfera mediów społecznościowych

Istotny element łączący całość rozważań na temat prawa do prywatności stanowi reinterpretacja tegoż prawa ze względu nową potencjalną sferę prywatności powstałą w Internecie – *social mediach*. Trywializmem byłoby poprzestać na stwierdzeniu, że prawo to zostało zredefiniowane ze względu na rozwój świata wirtualnego. Pod tym względem orzecznictwo krajowe, jak i międzynarodowe nie jest aktualne w stosunku do kolejnych nowopowstałych platform komunikacyjnych. Ochrona prawa do prywatności w Internecie jest oparta na „prawie do bycia zapomnianym". Pojęcie to należy co prawda do porządku UE[47], jednakże zostało również wprowadzone do orzecznictwa strasburskiego wraz z wyrokiem w sprawie M.L. i W.W. przeciwko Niemcom z 2018 r.[48] Poprzez „prawo do bycia zapomnianym" należy rozumieć instytucję, która umożliwia zarządzanie danymi przechowywanymi przez podmioty zewnętrzne. W zakresie tej definicji mieści się zarówno uprawnienie do usunięcia danych z baz danych danego podmiotu, ale również żądanie usunięcia konta w mediach społecznościowych czy żądanie trwałego usunięcia publikowanych treści przez jednostkę, której te treści dotyczą. „Prawo do bycia zapomnianym" stanowi swoistą metanormę składającą się z dwóch aspektów: ochrony danych pozyskiwanych przez podmioty obsługujące

---

46 M.A. Nowicki, *Wokół…*, s. 803.

47 Prawo do bycia zapomnianym zostało zdefiniowane w preambule rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

48 Wyrok Europejskiego Trybunału Praw Człowieka z dnia 28 czerwca 2018 r. w sprawie M.L. i W.W. przeciwko Niemcom, skargi nr 60798/10 i 65599/10.

tzw. *Big Data*[49] oraz ochrony i prawa do zarządzania treściami publikowanymi. O ile obie te kwestie pozostają prawnie relewantne, o tyle na potrzeby niniejszego opracowania przybliżona zostanie tylko druga z nich.

Drugi aspekt prawa do prywatności w *social mediach* stanowi *lex specialis* do ogólnej zasady o prawie do samostanowienia, ustalając prawo do zarządzania treściami publikowanymi w mediach społecznościowych – prawo do autonomii informacyjnej. Indywiduum powinno móc decydować o tym, jakie informacje chce upublicznić, a po upublicznieniu powinno mieć prawo do ich trwałego usunięcia. Prawo to ma charakter zarówno wertykalny, jak i horyzontalny, więc jednostka ma słuszne oczekiwania, aby informacje z jej sfery życia prywatnego zostały usunięte na jej żądanie również przez pozostałych użytkowników. Równie istotna jest możliwość decydowania o kręgu osób, którym dane indywiduum udostępnia dane treści. Warto podkreślić, że orzecznictwo ETPC nie nadaje temu prawu charakteru bezwzględnego tak jak samemu prawu do prywatności ogólnie[50]. Najczęściej w tej materii ETPC rozpatrywał sprawy związane z konfliktem wolności wypowiedzi z „prawem do bycia zapomnianym"[51].

5. Ograniczenie pozyskiwania dowodów z *social mediów* ze względu na prawo do prywatności

Zasada prawdy materialnej, poza wskazanymi w Kodeksie postępowania karnego przypadkami, powinna również podlegać innym ograniczeniom opartym o prawo do prywatności w aspekcie prawa do prywatności w *social mediach*. Ze względu na to, że polski ustawodawca nie określił zasad dowodzenia związanych z dopuszczeniem dowodów z mediów społecznościowych, to konieczne jest zaczerpnięcie z orzecznictwa ETPC i Sądu Najwyższego oraz poprzez analogię wskazanie pewnego relewantnego kryterium, jakim powinny kierować się organy władzy publicznej, aby nie naruszyć jednego z podstawowych praw jednostki.

---

[49] *Big data* oznacza zbiory danych, które są zbyt duże lub zbyt złożone, aby mogło sobie z nimi poradzić tradycyjne oprogramowanie do przetwarzania danych.

[50] Ograniczenie prawa do prywatności zostało szczegółowo opisane w opracowaniu Europejskiego Trybunału Praw Człowieka, *Guide*...

[51] Patrz np. wyrok Europejskiego Trybunału Praw Człowieka z dnia 17 kwietnia 2014 r. w sprawie Brosa przeciwko Niemcom, skarga nr 5709/09.

Dlatego też celem ustrukturyzowania odpowiedzi na przedstawioną problematykę należy zadać następujące pytania:

1) Czym jest sfera życia prywatnego w mediach społecznościowych?
2) Czy konwersacje grupowe są objęte tajemnicą korespondencji i czy można zaliczyć je do sfery życia prywatnego?
3) Czy organy publiczne powinny mieć dostęp do całej konwersacji, czy jedynie do jej części?
4) Czy organy ścigania mogą zamieszczać w bazach danych treści dostępne w mediach społecznościowych?

Współczesne media społecznościowe, zgodnie z wymaganiami prawa do zarządzania treściami publikowanymi, przyznają dyskrecjonalność swoim użytkownikom co do tego komu i co upubliczniają. Jednakże utrudniony jest dychotomiczny podział na sferę publiczną i prywatną, ponieważ, rozpatrując przykład Facebooka, osoba z niego korzystająca może wybrać, czy udostępnia dane informacje całej społeczności, osobom, które ma „w znajomych" oraz wybranym jednostkom, które ma „w znajomych". Tym samym utworzony zostaje potrójny krąg znajomości, co również rewiduje przedstawione przez P. Sarneckiego rozumienie sfery prywatności, skoro możemy wydzielić treści nawet wśród „osób znajomych". Częściowo do tej problematyki odnosi się wyrok ETPC w sprawie Egill Einarsson przeciwko Islandii:[52]

> Sąd Najwyższy [Islandii – J.R.] w wyroku z 20 listopada 2014 r. stwierdził, że zmienione zdjęcie wraz z podpisem było dostępne nie tylko dla *followersów* X na *Instagramie*, ale także dla innych użytkowników tego medium. Sąd stwierdził, że tak czy inaczej, zostało ono udostępnione publicznie (…). Trybunał nie widzi powodu, by nie zgodzić się z oceną Sądu Najwyższego w tej kwestii. W tym względzie Trybunał uważa za istotne przypomnienie swojego wcześniejszego orzecznictwa, w którym uznał, że ze względu na swoją dostępność oraz zdolność do przechowywania i przekazywania ogromnych ilości informacji Internet odgrywa ważną rolę w zwiększaniu dostępu społeczeństwa do wiadomości i ułatwianiu rozpowszechniania informacji w ogóle[53].

Sprawa Egill Einarsson przeciwko Islandii dotyczyła kobiety, która jak twierdziła, przypadkowo udostępniła post na Instagramie nie tylko

---

[52] Wyrok Europejskiego Trybunału Praw Człowieka z dnia 7 listopada 2017 r. w sprawie Einarsson przeciwko Islandii, skarga nr 24703/15, pkt 46.

[53] Wyrok Europejskiego Trybunału Praw Człowieka z dnia 7 listopada 2017 r. w sprawie Einarsson przeciwko Islandii, skarga nr 24703/15.

dla „osób ją obserwujących" (*followersów*), ale dla całej społeczności. Tym samym ETPC przesądził, że treści udostępniane wybranej tylko części społeczności stanowią sferę życia prywatnego. To, co również należy rozważyć, to kwestia dotycząca tego, czy liczba osób znajdujących się w gronie *facebookowych* „znajomych" czy *instagramowych „followersów"* ma znaczenie w kontekście wyznaczenia granic sfery życia prywatnego. Zdaniem autora tekstu, jeśli dana osoba ma relatywnie dużą liczbę „znajomych" czy „obserwujących", jaką może stanowić liczba powyżej 250 osób, to wykorzystując pogląd M. Wilda[54], taka osoba publikuje treści w sposób powszechnie dostępny, mimo że jest to ograniczone do tychże np. 252 osób. Sama możliwość zawężenia kręgu jednostek, którym upowszechniane są informacje, nie przesądza o tym automatycznie, że dana publikacja przynależy do sfery życia prywatnego. Liczba 250 osób została podana jako pewna próba obiektywizacji tegoż kryterium, lecz należy wskazać, iż naruszenie prawa do prywatności powinno być zawsze badane *ad causum*, uwzględniając m.in. takie czynniki jak charakter profilu danego użytkownika, relacje z osobami znajdującymi się w większości w znajomych oraz wrażliwość udostępnianej treści. Z całą pewnością można stwierdzić, że treści dostępne całkowicie publicznie stanowią sferę życia publicznego, niezależnie od liczby osób „znajomych" czy „*followujących*" – to jedynie może przyczynić się do bezprawności bądź oceny społecznej szkodliwości. Tak samo treści zawężone do grona osób bliskich takich jak rodzina czy bliscy przyjaciele stanowią treści należące do sfery życia prywatnego. Dodatkowo, niezależnie od liczby grona odbiorców treści z serwisów społecznościowych, uzyskanie treści zaadresowanych do konkretnego grona osób poprzez chociażby „prośbę o dodanie do grona znajomych" wystosowaną przez organy ścigania do konkretnego użytkownika, nie jest zgodne z prawem. Zgodnie z art. 304 § 1 zd. 1 k.p.k. każdy, kto dowiedział się o popełnieniu przestępstwa ściganego z urzędu, ma społeczny obowiązek zawiadomić o tym organy ścigania. Tym samym obecne normy przewidują wystarczające zabezpieczenie przed bezkarnością w *social mediach*. Jednakże wyjątkiem od przedstawionej powyżej sytuacji jest stworzenie fałszywego konta, które w ramach kradzieży tożsamości podaje się pod inną osobę. W tej sprawie wypowiedział się ETPC w wyroku z dnia 14 września 2021 r.

[54] M. Wild, *Konstytucja*..., komentarz do art. 47.

w sprawie Volodnia przeciwko Rosji[55]. Na gruncie teoretycznym można byłoby ogólnie zakwestionować to, że prawo do prywatności obejmuje również fałszywe konta na Facebooku, skoro to konto ze względu na swój charakter nie prezentuje rzeczywistej sfery życia prywatnego, a jedynie rzeczywistość stworzoną przez pewną jednostkę. Jednakże pod względem praktycznym byłoby to niezwykle utrudnione, żeby stwierdzić, czy dany profil jest relatywnie nieprawdziwy.

Bardziej skomplikowana wydaje się kwestia konwersacji grupowych np. w aplikacji Messenger. Nie budzi kontrowersji korespondencja z dziesięcioma osobami, jednak zgodnie ze standardami aplikacji w takiej konwersacji może partycypować do 120 osób. Racjonalne wydaje się więc uznanie, że w tymże przypadku co prawda nie będzie obowiązywał standard odpowiedni dla tajemnicy korespondencji, ale dla ochrony sfery życia prywatnego. Warto zauważyć, że w zasadzie ta forma komunikacji (poza nazwą i stylem pisania) nie różni się za bardzo od publikowanych postów na profilu społecznościowym. Implikuje to ponownie, że organy ścigania, które uzyskują dostęp do takich informacji, działają w ramach szarego bądź czarnego wywiadu, a czynnością odpowiednią dla uzyskania powinno być ponownie przeszukanie. Warto jednak wspomnieć, że liczba nie jest jedynym kryterium obiektywnym, ponownie *ad causum* należy w szczególności zwrócić uwagę na cel powstania konwersacji grupowej i próbę jak najdokładniejszego ustalenia powiązań osób w niej uczestniczących. Przykładowo inny standard będzie dotyczył konwersacji studentów prawa, a inny konwersacji rodzinnej.

Ostatnią kwestią jest możliwość zamieszczania w policyjnej bazie danych informacji pozyskanych z *social mediów*. W tej kwestii wypowiedział się wyjątkowo Sąd Najwyższy. Co prawda wyrok Sądu Najwyższego z dnia 4 czerwca 2003 r.[56] dotyczył prawa do wizerunku, jednakże – jako że jest to prawo związane z ochroną życia prywatnego – tezy orzeczenia mogą znaleźć analogiczne zastosowanie. Zgodnie z uzasadnieniem przedstawionym przez sąd, należy uznać, że w przypadku, gdy dana osoba nie ma przynajmniej statusu osoby podejrzanej bądź dana jednostka przestaje znajdować się w kręgu zainteresowań organów ścigania, to informacje o niej pozyskane z *social mediów* (szczególnie te

[55] Wyrok Europejskiego Trybunału Praw Człowieka z dnia 14 września 2021 r. w sprawie Volodina przeciwko Rosji, skarga nr 40419/19.

[56] Wyrok Sądu Najwyższego z dnia 4 czerwca 2003 r., I CKN 480/01.

o charakterze prywatnym) powinny zostać usunięte. W tym miejscu należy zasygnalizować problematykę „osoby podejrzanej", a w zasadzie brak zdefiniowania tego pojęcia na gruncie k.p.k. To prowadzi do tego, że informacje dotyczące indywiduum o takim statusie, mimo że nie jest stroną postępowania (co więcej, może nie mieć świadomości o takim toczącym się postępowaniu), są udostępniane innym osobom w fazie postępowania *in rem*.

6. Wykorzystywanie dowodów z *social mediów* bez naruszania prawa do prywatności

Należy podkreślić (co wykazano już powyżej), że obecny stan prawny umożliwiający prawie pełne wykorzystywanie tzw. owoców zatrutego drzewa przesądza o wyższości prawdy materialnej nad prawem do prywatności. Organy ścigania mogą wykorzystywać dowody pozyskane poprzez szary bądź czarny wywiad, np. wchodząc w interakcję bezpośrednio z osobą podejrzaną, i taki materiał będzie stanowił dalej dowód w sprawie. Ten istotny aspekt procesowy należy podkreślić, lecz niniejszy tekst nie ma na celu pogłębiania problematyki owoców zatrutego drzewa wraz z postulatami *de lege ferenda* w tym zakresie. To, co jednak autor tekstu chciałby zaproponować, to konkretny postulat, aby przepisy procedury karnej uniemożliwiały wykorzystywanie dowodów właśnie z zakresu szarego bądź czarnego wywiadu, które to zostały uzyskane bez postanowienia sądu takiego jak w przypadku innych podsłuchów. Jednakże w ramach obecnego stanu prawnego należy zwrócić uwagę na dwie istotne kwestie z zakresu wykorzystywania dowodów z mediów społecznościowych.

Pierwsza z nich dotyczy osoby, której prawo do prywatności jest naruszane. Taka jednostka powinna mieć prawo do bezpośredniego uczestniczenia (oczywiście w miarę praktycznych możliwości) w zabezpieczaniu danego materiału dowodowego z nośnika elektronicznego należącego do niej. Czynności te również powinny odbywać się bez konieczności zatrzymywania rzeczy w postaci danego sprzętu elektronicznego. Tylko przeszukiwanie np. telefonu celem odnalezienia publikowanych treści w serwisie społecznościowym przy obecności osoby, która te treści publikowała, zapewnia takiej osobie jakiekolwiek poczucie, iż organy ścigania nie wykroczą w trakcie postępowania zabezpieczającego

poza to, co jest konieczne z pespektywy prawdy materialnej. W przeciwnym razie mogą pojawić się uzasadnione zarzuty, że organy procesowe uzyskały dostęp do pełnej treści konwersacji bądź jej tak szerokiej części, która jedynie pośrednio będzie relewantna dla postępowania, tym samym naruszając zasadę proporcjonalności. Ponadto takie dowody powinny zostać powielone w jak najmniejszym stopniu, tzn. jeśli można wykonać kopię na np. pendrive danych z serwisu społecznościowego, to powinno się na tym poprzestać i nie wykonywać dodatkowo wydruku tych danych. Równie istotne jest to, aby tam, gdzie nie było to konieczne dla ustalenia prawdy materialnej, organy ścigania starały się anonimizować dane osób „postronnych", czyli takich, które nie będą uczestnikami postępowania. Dodatkowo inne dane wrażliwe nierelewantne dla ustaleń faktycznych konkretnej sprawy powinny również zostać w miarę możliwości utajnione. Szczególne standardy zabezpieczania dotyczą przestępstw przeciwko wolności seksualnej zarówno dorosłych, jak i małoletnich. W takim przypadku, jeśli w danej konwersacji występują zdjęcia intymne, to powinno się jedynie odnotować fakt ich przesłania wraz z opisem. Ponadto na obu etapach postępowania podejrzany lub odpowiednio oskarżony powinien mieć możliwość wystąpienia z obligatoryjnym dla organu procesowego wnioskiem o powołanie biegłego celem zasięgnięcia opinii, czy dane dowody z *social mediów* mogą być uznane za wygenerowane bądź czy doszło w związku z nimi do innych istotnych manipulacji.

Drugi aspekt dotyczy wykorzystywania dowodów w zakresie sędziowskiej oceny zebranego materiału dowodowego z mediów społecznościowych. Przede wszystkim zgodnie z zasadą bezpośredniości *sensu largo* sędzia powinien mieć możliwość oceny źródła np. skopiowanego na odpowiedni dysk optyczny, a nie wyłącznie wydruku. Nawet w przypadku tzw. dowodów prywatnych dana osoba powinna zadbać o to, aby nie przedstawiać wyłącznie wydruków, lecz nośników z bezpośrednim źródłem dowodowym. Zasada prawdy materialnej wymaga, aby nie tylko uzyskać sam dowód, ale również określić cały kontekst sytuacyjny umieszczenia danego dowodu, m.in. sposób jego uzyskania czy jego właściwości. Dlatego też takie źródło powinno zawierać szerszy kontekst sytuacyjny w postaci np. innych zamieszczonych pod danym postem komentarzy czy całości wątku prowadzonej z użyciem komunikatora rozmowy. Źródło zawierające całokształt informacji na temat powstania

danych treści w serwisie społecznościowym czy komunikatorze umożliwia ocenę bezprawności oraz społecznej szkodliwości danego zachowania. Dodatkowo sędzia niejako z urzędu powinien powołać biegłego na okoliczność sprawdzenia prawdziwości dowodu z *social mediów*, jeśli nie zostało to uczynione na wcześniejszym etapie postępowania. Jeżeli takie źródło dowodowe budziłoby jakiekolwiek uznane wątpliwości, to sąd nie powinien brać go w żadnym stopniu pod uwagę.

7. Zakończenie

Jak wykazano powyżej, z pomocą wykładni Konstytucji i EKPC wraz z orzecznictwem ETPC i Sądu Najwyższego istnieje możliwość stworzenia obiektywnych kryteriów możliwości ingerencji w prawo do prywatności w *social mediach* na gruncie postępowania karnego. Wymaga ono rozważenia wielu czynników, zaczynając od dostępu do danych treści, poprzez badanie więzi pomiędzy osobą udostępniającą dane informacje a adresatem, kończąc na sposobach i zakresie zabezpieczenia treści z prowadzonych konwersacji. *De lege lata*, normy procedury karnej nie przewidują szczególnej procedury dla wykorzystywania dowodów cyfrowych, w tym dowodów z mediów społecznościowych. Taki stan rzeczy powoduje istotne rozbieżności, przede wszystkim przy zabezpieczaniu źródeł dowodowych, które to mogą prowadzić do kontaminacji materiału oraz uniemożliwią ustalenie stanu faktycznego zgodnie z główną zasadą prawdy materialnej. Ponadto ze względu na zagrożenia związane z nowymi technologiami materiał dowodowy zebrany z *social mediów* powinien zostać zbadany już na etapie zabezpieczania przez biegłego sądowego pod kątem jego prawdziwości – podejrzany, jak i oskarżony powinien mieć zagwarantowane prawo obligujące do powołania biegłego na tę okoliczność, a sąd na etapie postępowania sądowego powinien z urzędu powoływać biegłego w tym zakresie, jeśli jego wiedza nie została wykorzystana wcześniej.

Odpowiedzi na pozostałe pytania umożliwiły wypracowanie jednolitego testu możliwości wykorzystania dowodów z mediów społecznościowych bez bezprawnej ingerencji w sferę życia prywatnego jednostki. W pierwszej kolejności należy rozważyć, czy publikowane treści mogą należeć do sfery życia prywatnego. Jeżeli dana osoba publikuje treści dla wybranego grona odbiorców, to należy rozważyć, czy osoby będące

adresatami danych treści można uznać za krąg osób bliskich. Jeśli nie, to można pozyskać treści „fałszywie prywatne" poprzez próbę uzyskania zgody na dodanie do kręgu adresatów. W kwestii konwersacji grupowych istnieje standard ochrony życia prywatnego, a nie tajemnicy korespondencji, jednakże należy *ad casum* badać relacje znajdujące się między członkami danej konwersacji. Dalej, zarówno treści publikowane poprzez konwersację, jak i post w mediach należy zabezpieczać zgodnie z zasadą proporcjonalności, w tym gwarantując osobie pokrzywdzonej, jak i podejrzanemu bądź oskarżonemu możliwość wzięcia udziału w czynności zabezpieczania materiału dowodowego znajdującego się na nośniku elektronicznym. Dodatkowo takie dowody powinny być powielone w jak najmniejszym stopniu, a także niektóre dane wrażliwe i osobowe nierelewantne dla sprawy powinny zostać zanonimizowane. Takimi danymi są np. intymne zdjęcia, które to co do zasady nie powinny w ogóle ulegać zabezpieczeniu (poza wyjątkowymi sytuacjami, gdy np. są relewantne dla stwierdzenia popełnienia czynu), jedynie fakt ich istnienia należy odnotować w protokole z przeprowadzonej czynności. Za to sąd na etapie postępowania sądowego powinien mieć możliwość przede wszystkim zapoznania się z bezpośrednim źródłem dowodowym, a nie wyłącznie z wydrukami czy protokołami z oględzin. Ponadto sąd powinien móc zapoznać się z całym kontekstem sytuacyjnym przedstawionego dowodu. Wreszcie, wraz z zakończeniem prowadzonego postępowania (w tym po uprawomocnieniu się wyroku) bądź gdy jednostka w fazie *in rem* przestanie znajdować się w kręgu zainteresowania organów ścigania, to uzyskane i przechowywane dane powinny zostać bezwzględnie usunięte z policyjnej bazy danych. Tylko powyższe postępowanie jest w stanie w obecnym stanie prawnym zapewnić jednostce brak nieuzasadnionej lub nieproporcjonalnej ingerencji w jej prawa.

Summary

The Code of Criminal Procedure provides neither a separate legal basis for the inclusion of social media evidence into the trial, nor the actual standards and manner of its preservation. The sphere of social media publications may, to some extent, fall under the protection of the right to private life. One of the fundamental issues of limiting the ability to obtain and use these sources of evidence in the course of criminal proceedings remains open. Significantly, the issue related to possible evidentiary limitations arising from the sphere of private life has not been considered so far. The definition of the sphere

of private life, in the case of social media, needs to be reinterpreted by leaving open the key questions regarding the element that prejudges the public or private nature of the relevant information.

Keywords

criminal law, limitations of the right to privacy, social media evidence, criminal procedure, substantive truth

Bibliography

Baran M., *Apelacje od wyroków dla narkotykowego gangu*, „Temi.pl" z 5 kwietnia 2023 r., < https://www.temi.pl/tarnow/apelacje-od-wyrokow-dla-narkotykowego-gangu >.

Ciesielski M., *Jak generuje się deepfake i jak można z nim walczyć? Oto najgłośniejsze przypadki zastosowania*, „Forsal.pl" z 26 maja 2023 r., < https://forsal.pl/lifestyle/technologie/artykuly/8722398,jak-generuje-sie-deepfake-i-jak-mozna-z-nim-walczyc-oto-najglosniejsze-przypadki-zastosowania.html >.

Cyrankiewicz-Gortyńska S., *Wyniki raportu nt. „Bezpieczeństwa w social mediach"*, „Dziennik Warto Wiedzieć" z 28 lipca 2018 r., < https://wartowiedziec.pl/serwis-glowny/styl-zycia/47175-wyniki-raportu-nt-bezpieczenstwa-w-social-media >.

Czubaszek M., *To jest przemoc i pedofilia, nie „dramka". #MeToo na polskim YouTube*, „OKO.press" z 8 października 2023 r., < https://oko.press/stuu-gargamel-gonciarz-pandora-gate-czy-zmieni-internet >.

FBI's Encrypted Phone Platform Infiltrated Hundreds of Criminal Syndicates; Result is Massive Worldwide Takedown, komunikat prasowy United States Attorney's Office Southern District of California z 8 czerwca 2021 r., < https://www.justice.gov/usao-sdca/pr/fbi-s-encrypted-phone-platform-infiltrated-hundreds-criminal-syndicates-result-massive >.

Florczak-Wątor M., w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, red. P. Tuleja, LEX/el. 2021.

Gabriel-Węglowski M., *Teoria „owoców zatrutego drzewa" a dopuszczalność przeprowadzania dowodów w postępowaniu karnym*, Lex/el. 2021.

Guide on case-law of the Convention – Data protection, komunikat prasowy Europejskiego Trybunału Praw Człowieka, „ECHR.COE" z 31 sierpnia 2022 r., < https://echr.coe.int/Documents/Guide_Data_protection_ENG.pdf >.

Kemp S., *Digital 2022: Poland*, „DataReportal" z 15 lutego 2022 r., < https://datareportal.com/reports/digital-2022-poland >.

Kulesza C., *Pojęcie i rodzaje dowodów*, w: *Wykład prawa procesowego*, red. P. Kruszyński, Białystok 2012.

Kurowski M., *Glosa do uchwały Sądu Najwyższego z dnia 13 października 2021 r., I KZP 1/21*, „Prokuratura i Prawo" 2022, nr 2.

Lach A., *Dowody cyfrowe w postępowaniu karnym, wybrane zagadnienia praktyczne i teoretyczne*, „CBKE e-biluetyn" 2004, nr 2, < http://www.bibliotekacyfrowa.pl/Content/24720/PDF/Dowody_cyfrowe_w_postepowan.pdf >.

Majchrzycki M., *Jak tworzyć fałszywe posty i wiadomości na Facebooku*, „download.net.pl" z 8 stycznia 2019 r., < https://www.download.net.pl/jak-tworzyc-falszywe-posty-i-wiadomosci-na-facebooku/n/6162/ >.

Nawacki M., w: *Kodeks postępowania karnego. Tom I. Komentarz. Art. 1-424*, red. D. Drajewicz, Warszawa 2020.

Nowicki M.A., *Wokół Konwencji Europejskiej. Komentarz do Europejskiej Konwencji Praw Człowieka*, Warszawa 2021.

Sarnecki P., w: *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, t. II, red. L. Garlicki, M. Zubik, Warszawa 2016.

Skorupka J., w: *Kodeks postępowania karnego. Komentarz*, red. J. Skorupka, Warszawa 2021.

Skraba K., Strzałkowski I., *Media społecznościowe jako źródła dowodu w polskim procesie karnym. Badanie orzecznictwa Sądów Apelacyjnych i Sądu Najwyższego*, w: *Media społecznościowe w pracy organów ścigania*, red. P. Waszkiewicz, Warszawa 2021.

Stefański R.A., Zabłocki Z., w: *Kodeks postępowania karnego. Tom II. Komentarz do art. 167-296*, red. R.A. Stefański, S. Zabłocki, Warszawa 2019.

Szaplonczay A., *Wadliwe opinie biegłych jako przyczyna pomyłek sądowych w polskim procesie karnym. Sygnalizacje możliwości naprawczych*, „Studia Prawnicze. Rozprawy i Materiały" 2019, nr 1.

Tomaszewska-Michalak M., Stromczyński B., Skraba K., Rabczuk S., Waszkiewicz P., *Facebook est regina probationum? Ocena dowodów pochodzących z mediów społecznościowych przez sędziów w świetle badań eksploracyjnych*, w: *Media społecznościowe w postępowaniu karnym*, red. P. Waszkiewicz, Warszawa 2022.

Waszkiewicz P., Dębniak H., Rabczuk S., *Wybrane aspekty dopuszczalności dowodów pochodzących z mediów społecznościowych w postępowaniu karnym ujęcie porównawcze*, w: *Media społecznościowe w pracy organów ścigania*, red. P. Waszkiewicz, Warszawa 2021.

Wild M., *Konstytucja RP, t. I. Komentarz*, red. M. Safjan, L. Bosek, Warszawa 2016.

Wykorzystywać, w: *Słownik języka polskiego PWN*, < https://sjp.pwn.pl/sjp/wykorzystac;2539475.html >.