INTERNETOWE MATERIAŁY DOWODOWE – NOWE METODY

Wykorzystywanie monitoringu Internetu
oraz narzędzi typu web crawler w gromadzeniu
i zapisywaniu dowodów w sprawach motywowanych
uprzedzeniami.

stowarzyszenie żydowskie czulent
Foundation EVZ Remembrance Responsibility Future
ISD Powering solutions to extremism and polarisation
CCOA Coalition to Counter Online Antisemitism

With support from Google.org

Wydawca
Jewish Association Czulent
ul. Sebastiana 36/1
31-051 Kraków
www.czulent.pl
office@czulent.pl
Kraków 2024
Edycja I.
ISBN: 978-83-972977-2-2

Redakcja merytoryczna: Joanna Grabarczyk-Anders
Autorzy: Joanna Grabarczyk-Anders, Jakub Kłosiński, Jędrzej Kupczyński

Wesprzyj naszą organizację, dokonując wpłaty na nasze konto:
Jewish Association Czulent
ul. Sebastiana 36/1
31-051 Kraków
NIP (tax ID): 6762300850
Konto bankowe: 42 1600 1462 1880 9351 6000 0001

Publikacja powstała w ramach projektu ”New Methods of Gathering Evidence on antisemitic crimes committed on Social Media” finansowanego przez The Coalition to Counter Online Antisemitism (CCOA).

Publikacja powstała w ramach projektu „Online antisemitism in Poland: establishment of a legal aid helpdesk, reporting and advocacy activities”, finansowanego z Fundacji Pamięć, Odpowiedzialność i Przyszłość, realizowanego przez Żydowskie Stowarzyszenie Czulent

Spis treści

1 Wstęp

W ostatnich latach obserwujemy niepokojący trend – ilość przestępstw motywowanych uprzedzeniami w Internecie stale rośnie. Media społecznościowe, fora dyskusyjne i inne przestrzenie cyfrowe, zamiast być miejscem wymiany myśli i budowania relacji z innymi, stały się narzędziem do szerzenia mowy nienawiści w tym do organizowania zmasowanych ataków na osoby, organizacje i grupy, w szczególności te należące do mniejszości.

Część tych działań stanowi przestępstwa motywowane uprzedzenia, które uderzają w podstawy równości i bezpieczeństwa społecznego. Osoby nimi pokrzywdzone – zarówno osoby indywidualne, organizacje jak i grupy społeczne – doświadczają nie tylko szkód psychologicznych, ale również społecznego wykluczenia, któremu towarzyszy strach o własne bezpieczeństwo. Reagowanie na tego typu incydenty jest kluczowe, aby wspierać osoby pokrzywdzone i chronić społeczności szczególnie wrażliwe przed eskalacją zagrożeń. Brak odpowiednich i zdecydowanych działań może prowadzić do normalizacji nienawiści w przestrzeni publicznej, na co nie ma miejsca w demokratycznym państwie.

Jednym z priorytetów w walce z przestępstwami motywowanymi uprzedzeniami jest ich monitorowanie i informowanie o nich organów ścigania (policji i prokuratury) a także nieuchronne karanie sprawców[1] oraz usuwanie treści nielegalnych z Internetu.

W dobie dynamicznego rozwoju Internetu jako organizacje monitorujące publikowane treści nielegalne nie jesteśmy już w stanie realizować naszych działań manualnie. Dlatego coraz większe znaczenie mają narzędzia do analizy i monitoringu treści, takie jak SentiOne i jemu podobne. Dzięki nim możliwe jest wykrywanie i dokumentowanie zorganizowanych kampanii nienawiści skierowanych do konkretnych osób, organizacji czy grup. A także gromadzenie materiału dowodowego w przypadkach przestępstw

1 Żydowskie Stowarzyszenie Czulent priorytetowo traktuje zastosowanie inkluzywnego i zrównoważonego języka. Publikacja napisana jest językiem prawniczym i jeśli było to możliwe dobierano zneutralizowane formy językowe i feminatywy. Rodzaj męskoosobowy zastosowano do rzeczowników liczby mnogiej.

publicznie popełnianych za pośrednictwem Internetu, Nowoczesne technologie odgrywają dziś kluczową rolę w dokumentowaniu naruszeń prawnych, zwłaszcza gdy sprawcy pozostają pozornie anonimowi.

Niniejsza publikacja jest swoistym przewodnikiem po świecie nowych technologii i ich wykorzystywania by stanowiły wsparcie do pociągnięcia sprawców przestępstw motywowanych uprzedzeniami do odpowiedzialność karnej. Wskazuje także jak osoby pokrzywdzone przestępstwem i organizacje mogą zapisywać trwale materiał dowodowy czy wykorzystywać materiały pochodzące z komercyjnych narzędzi często wykorzystywanych do celów marketingowych (social listening) do informowania policji i prokuratury o przestępstwach popełnianych na ich szkodę. Jest też przewodnikiem dla osób pokrzywdzonych, adwokatek i adwokatów, policjantek i policjantów czy prokuratorek i prokuratorów jak wykorzystywać dowody cyfrowe pochodzące z narzędzi typu crawler.

Publikacja ta powstała w oparciu o gromadzone latami doświadczenie w monitorowaniu treści o charakterze nienawistnym, wspierania osób pokrzywdzonych w procesie zbierania dowodów oraz składania zawiadomień o możliwości popełnienia przestępstwa przez osoby o nieustalonej tożsamości. Materiał, który przygotowaliśmy, powstał dzięki wiedzy i doświadczeniu Żydowskiego Stowarzyszenia Czulent oraz eksperckiej wiedzy prokuratorów. Praktyczne wskazówki zawarte w opracowaniu bazują na sprawdzonych metodach i realnych przypadkach, dzięki czemu stanowią skuteczne narzędzie w walce z przestępstwami z nienawiści w Internecie.

Dzięki współpracy międzysektorowej – przy użyciu technologii, wsparcia prawnego i odpowiedzialnego reagowania – możemy przyczynić się do stworzenia bezpieczniejszej przestrzeni cyfrowej dla wszystkich.

2 Wykorzystanie narzędzi do monitorowania Internetu przez ofiary i organizacje

Nielegalne treści o charakterze nienawistnym publikowane w Internecie mają swoich autorów, którzy ponoszą za nie odpowiedzialność. Jednakże fakt iż opublikowane zostały one w Internecie, niesie ze sobą wiele wyzwań związanych z identyfikacją autora, edytowaniem lub automatycznym usuwanie treści w stosunkowo krótkim czasie, co wymusza niejednokrotnie pozyskanie materiałów dowodowych w momencie zetknięcia się z treściami o charakterze nielegalnym. Dla większości osób pokrzywdzonych gromadzenie materiału dowodowego jest trudnym procesem zarówno emocjonalnie jak i technicznie; wymagającym wiedzy. Niestety jest to proces niezbędny by móc złożyć zawiadomienie o możliwości popełnienia przestępstwa. Zwiększenie liczby zawiadomień wraz ze zgromadzonym materiałem dowodowym pozwoli sprawniej karać sprawców, ale także wpływać na wymiar sprawiedliwości by traktowano te sprawy w sposób z należytą atencją.

Powszechnie dostępne narzędzia wykorzystywane do monitorowania Internetu oraz mediów społecznościowych przez organizacje w celu sprawdzania swojej skuteczności w docieraniu do odbiorców można wykorzystywać także do zbierania materiału dowodowego przez umiejętne wykorzystywanie i zmianę parametrów kierowanych zapytań. W ten sposób wprowadzając frazy np. nawołujące do nienawiści w stosunku do konkretnej osoby czy grupy osób, system wyszuka za nas konkretne treści. Dodatkowo wykorzystywanie zautomatyzowanych narzędzi pozwala Nam wyjść poza naszą bańkę informacyjną, która jest tworzona przez algorytmy social mediów. Pozwala zobaczyć duży wycinek internetowego dyskursu, ale także posiada swoje ograniczenie. Rozwiązania, które prezentujemy wyszukują tylko publiczne treści, nie dają możliwości byśmy poznali wpisy publikowane przez użytkownikach w wiadomościach prywatnych czy zamkniętych grupach lub osób, które np. ograniczyły widoczność swoich mediów społecznościowych tylko do grona najbliższych (takie możliwości daje użytkownikowi Facebook).

Żydowskie Stowarzyszenie Czulent wykorzystuje dziś narzędzia do monitoringu Internetu i mediów społecznościowych by:

- monitorować nienawistne treści i raportować społeczności o potencjalnych zagrożeniach;
- monitorować treści nawołujące do nienawiści mające charakter kryminalny oraz informować o nich wymiar sprawiedliwości;
- gromadzić materiał dowodowy dla osób pokrzywdzonych przestępstwem w Internecie.

3 Zabezpieczenie przez stronę postępowania publicznie dostępnych danych przetwarzanych przez platformy internetowe

Adres url

Każda opublikowana w Internecie treść ma indywidualny adres URL (Uniform Resource Locator) to unikalny adres internetowy, który wskazuje lokalizację treści w sieci. Innymi słowy to po prostu adres w Internecie, który wskazuje na konkretne miejsce, jak np. strona internetowa, zdjęcie, wideo czy komentarz. Jest jak adres domu, ale w sieci. Działa jak adres w GPS – wpisujesz go, a przeglądarka prowadzi cię do konkretnego miejsca.

Składa się z kilku części:

- Protokół: mówi, jak się połączyć (np. https://).
- Domena: nazwa strony (np. www.google.com).
- Ścieżka: dokładne miejsce w tej stronie (np. /szukaj).

Przykład: https://www.czulent.pl

Co ważne każdy komentarz na platformach, takich jak YouTube czy Facebook, Instagram ma swój własny adres. Dzięki temu możesz podać komuś link, który zaprowadzi go dokładnie do tego komentarza.

Jak znaleźć URL komentarza?

- Na YouTube: Kliknij czas pod komentarzem (np. „5 minut temu”), a URL zmieni się na ten prowadzący do komentarza.
- Na Facebooku: Kliknij czas lub datę pod komentarzem, a URL w przeglądarce pokaże link do niego.

W jaki sposób zapisać treść strony internetowej?

Najczęstszym sposobem prezentowania w postępowaniu karnym treści stron internetowych, która to treść ma znaczenie dowodowe, jest wykonanie zrzutów ekranu (np. za pomocą skrótu klawiszowego Win+prtsc bądź fn+ptrsc+spacja w systemie Windows; shift+cmd+3 w systemie macOS) i ich wydrukowanie lub zapisanie pliku jako pdf. Tę prostą metodę stosują zarówno przedstawiciele organów procesowych, jak i strony postępowania i ich pełnomocnicy czy obrońcy.

Choć w wielu przypadkach takie rozwiązanie będzie wystarczające, z pewnością nie jest ono najwygodniejsze. Jeśli konieczne jest zaprezentowanie rozbudowanej strony, np. zawierającej długi artykuł bądź wpis z licznymi komentarzami i całość tych treści ma znaczenie dowodowe, wykonywanie serii zrzutów ekranu jest czasochłonne, ponadto taka forma przedstawienia treści strony jest mało czytelna. Poniżej przedstawiamy kilka wygodniejszych rozwiązań, zaczynając od najprostszych, które sprawdzą się, gdy nie ma konieczności prezentowania podstron, kończąc na rozwiązaniu wymagającym instalacji dodatkowego oprogramowania, które pozwoli na zapisanie kompletnej treści rozbudowanej strony.

Zapisanie strony jako PDF

Wszystkie popularne przeglądarki dają możliwość zapisania strony w formacie PDF. Można to zrobić np. wybierając opcję „Drukuj" (np. za pomocą skrótu klawiaturowego Ctrl+P), a następnie w polu wyboru drukarki wskazać np. „Zapisz jako PDF" bądź „Microsoft Print to PDF". W ten sposób uzyskuje się plik zawierający całą treść strony, która była otwarta w chwili wyboru opcji „Drukuj", w tym część okien reklamowych. Plik ten może liczyć wiele stron, co stanowi jego przewagę nad „ręcznym" wykonywaniem zrzutów ekranu.

Zapisanie strony w postaci dokumentu HTML

W tym celu należy wybrać opcję „Zapisz jako" (np. za pomocą skrótu klawiaturowego Ctrl+S), a następnie wybrać sposób zapisu. Wybranie opcji „Zapisz jako typ: strona internetowa, kompletna" prowadzi do zapisania pliku HTML zawierającego całą zapisaną stronę, a dodatkowo do utworzenia folderu zawierającego pliki graficzne pochodzące z zapisanej strony, co w pojedynczych przypadkach może być przydatne. Podobnie jak w przypadku pierwszej opcji, nie zapiszemy w ten sposób podstron, a jedynie stronę, która była wyświetlana w chwili wybrania opcji „Zapisz jako".

Zastosowanie rozszerzenia, np. Save Page

Lepszy efekt (plik dostępny offline zawierający zapis strony o identycznym wyglądzie i układzie jak strona wyświetlana online) można uzyskać, korzystając z rozszerzeń do przeglądarki, np. Save Page

dla przeglądarki Google Chrome czy SingleFile dla przeglądarki Mozilla Firefox. W tym przypadku również przeglądarki Google Chrome czy SingleFile dla przeglądarki Mozilla Firefox. W tym przypadku również nie osiągnie się efektu tożsamego z zapisaniem dostępu do kompletnej strony offline – we wszystkich przypadkach hiperłącza zawarte na danej stronie nie będą aktywne w zapisanym pliku, więc uzyskujemy efekt zbliżony do opisanych na początku zrzutów ekranu – choć znacznie mniejszym nakładem pracy i w znacznie bardziej czytelnej formie.

Zapisanie kopii lustrzanej danej strony

W przeciwieństwie do pozostałych rozwiązań, to działanie pozwala na zapisanie kopii interesującej nas strony w postaci pliku HTML, z zachowaniem jej struktury (linków, podstron itp.). Kopia nie zawsze będzie jednak kompletna, gdyż dana strona może stosować ograniczenia w zakresie tego, jakie treści są dostępne dla robotów indeksujących – a takie roboty są wykorzystywane do tworzenia kopii lustrzanej. Obecnie takie ograniczenia stają się coraz bardziej powszechne, by utrudnić wykorzystywanie zawartości strony przez generatywną sztuczną inteligencję.

Wykonanie kopii wymaga użycia przeznaczonego do tego oprogramowania, np. HTTrack Website Copier. Jest to łatwe w obsłudze, otwarte oprogramowanie, które pozwala na zapisanie lokalnej kopii strony, dostępnej bez połączenia z internetem.

Jako ogólną zasadę można przyjąć, że każdy z opisanych wyżej sposobów zapisania strony WWW i jej przedstawienia organowi procesowemu (Policji, prokuraturze, sądowi) może być wystarczający. Zarazem w przypadku każdego z opisanych wyżej sposobów nie jest możliwe kategoryczne wykluczenie manipulacji treścią – innymi słowy, plik zapisany którykolwiek z opisanych sposobów nie może być traktowany jako niepodważalny dowód, że w danej chwili dana strona zawierała określone treści.

> Ze względów praktycznych, rozwiązaniem najmniej rekomendowanym jest zapisanie zrzutów ekranu. W ich przypadku ryzyko manipulacji treścią jest bowiem największe. Ponadto w przypadku konieczności przedstawienia bardziej rozbudowanych treści przemawiają za tym względy praktyczne – nakład pracy i mniejsza przejrzystość prezentowanych treści.

Wayback Machine

Więcej o tym rozwiązaniu na stronie nr. 52.

Jak zapisać treści z poszczególnych mediów społecznościowych

Facebook

Serwis ma wbudowaną funkcjonalność umożliwiającą użytkownikowi pobranie wszystkich informacji związanych z publikowanymi przez niego informacjami. W pojedynczych przypadkach może ona okazać się użyteczna na potrzeby postępowania karnego, np. gdy komentarz o znamionach przestępstwa został opublikowany pod postem osoby zainteresowanej ściganiem autora tego komentarza. W tym celu należy wybrać ***Ustawienia – Ustawienia i Prywatność***, następnie w sekcji ***Centrum kont*** wybrać zakładkę ***Informacje osobiste***, następnie ***Twoje informacje i uprawnienia***, a następnie ***Pobierz swoje informacje.***

Można jednak przyjąć, że znacznie częściej zawiadamiający lub pokrzywdzony nie jest autorem posta, pod którym pojawił się komentarz stanowiący przedmiot zawiadomienia, a tym samym nie jest on uprawniony do jego pobrania. W tej sytuacji serwis nie zapewnia wygodnego sposobu zapisywania posta ze wszystkimi komentarzami. Można więc posłużyć się opisanymi wyżej metodami zapisu treści strony internetowej, traktując wpis z komentarzami jak każdą inną stronę internetową. Pomocne może być w pierwszej kolejności zapisanie danego posta poprzez wybranie ikonki trzech kropek przy danym poście i opcję „Zapisz post". Jest on wówczas dostępny w menu po lewej stronie panelu użytkownika w zakładce „Zapisane". Po otwarciu tej zakładki i wybraniu danego posta należy rozwinąć wszystkie komentarze, a następnie zapisać stronę. W niektórych przypadkach pozwoli to jedynie na zapis bieżącej widocznej strony, na takiej samej zasadzie jak zrzut ekranu, nie zaś całej, wielostronicowej listy komentarzy. Pomocne może być ponowienie próby w innej przeglądarce.

Istnieją możliwości automatyzacji tego procesu przy użyciu zaawansowanych komend. Należy jednak przestrzec osoby niemające wiedzy z zakresu programowania przed wpisywaniem w konsoli (rozwijanej klawiszem F12) skryptów znalezionych na forach internetowych. Istnieje bowiem ogromne ryzyko, że taki skrypt w rzeczywistości posłuży atakującemu do uzyskania dostępu do naszego konta.

Istnieją także rozwiązania komercyjne do zapisywania i analizy postów, z których niektóre są dostępne w wersji darmowej z ograniczeniami. Przykłady takich produktów to: Exportcomments, ESUIT Comments Exporter for Facebook.

X

Standardowe sposoby zapisu danych można uzupełnić dzięki dedykowanym programom lub rozszerzeniom. Wśród komercyjnych rozwiązań można wymienić np. **readwise.io**. Przykładowym przydatnym rozszerzeniem do przeglądarki Google Chrome jest **TwCommentExport**. Aby pobrać plik CSV (plik tekstowy, w którym poszczególne kategorie danych są oddzielone przecinkami) zawierający szczegółowe dane dotyczące wszystkich komentarzy, należy skopiować adres URL danego posta, a następnie wkleić go w okno wyszukiwarki rozszerzenia TwCommentExport i wybrać „Start Export". Uzyskany w ten sposób plik nie jest wygodną graficzną prezentacją posta i komentarzy, jednak nadaje się do zastosowania narzędzi analitycznych. Należy jednak upewnić się, że wygenerowany plik zawiera wszystkie posty, które są istotne w postępowaniu karnym, gdyż może okazać się, że komentarze, które z powodu naruszenia zasad danej platformy zostały oznaczone jako niewłaściwe, są pomijane w pliku CSV.

Instagram

Podobnie jak w przypadku Facebooka, istnieje funkcjonalność pozwalająca na zapisanie wszelkich danych konta, do którego posiada się dostęp, co w niektórych wypadkach może okazać się wystarczające. Dostęp do ww. usługi znajduje się pod adresem instagram.com/download/request. Zapis danych może trwać do 48 godzin. Uporządkowane dane zostaną zapisane w folderze skompresowanym .zip, z podziałem m. in. na poszczególne interakcje użytkowników (komentarze, „polubienia" itp.). Dane są zapisywane domyślnie w postaci plików w formacie JSON.

WhatsApp

W komunikatorze tym istnieje możliwość wygenerowania raportu z całą zawartością naszego konta, w tym danymi dotyczącymi jego rejestracji, zdjęciem profilowym, numerem telefonu, wersją aplikacji, kontaktami, grupami, ustawieniami prywatności i in. Raport nie obejmuje jednak treści wiadomości ani przesyłanych plików. Dokładną instrukcję można znaleźć pod linkiem.

Wyeksportowanie pełnej treści czatu (w razie wyboru takiej opcji obejmującego również przesyłane pliki) jest możliwe po otwarciu danego czatu, wybraniu symbolu trzech kropek, zakładki „Więcej", a następnie „Eksportuj czat".

4 Wykaz skrótów i informacje wstępne

Stan prawny na: listopad 2024 r.

DSA - **Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE** (akt o usługach cyfrowych)

k.p.k. - **Ustawa z dnia 1 września 1998 r. Kodeks postępowania karnego, Dziennik Ustaw z roku 2024, poz. 37** (tekst jednolity ze zmianami)

p.k.e. - **Ustawa z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej, Dziennik Ustaw z roku 2024, poz. 1221**

Rozporządzenie e-evidence - **Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonywaniem kar pozbawienia wolności**

5 Wprowadzenie - dane informatyczne jako dowód w postępowaniu karnym

Dowody cyfrowe mają kluczowe znaczenie we współczesnym postępowaniu karnym. Szacuje się, że występują one nawet w 85% postępowań karnych prowadzonych w Europie[2]. Warto więc przyjrzeć się temu pojęciu, zwłaszcza w kontekście przestępstw motywowanych nienawiścią, popełnianych z wykorzystaniem Internetu.

Definicja i specyfika dowodu cyfrowego

Dowód cyfrowy (dowód elektroniczny, e-evidence) można zdefiniować jako każdy rodzaj informacji zapisanej lub przekazanej w formie elektronicznej, mającej znaczenie dowodowe[3]**.** W praktyce pod pojęciem tym mogą kryć się bardzo różnorodne rodzaje danych, takie jak przykładowo: **treść komunikacji** (e-mail, SMS, wymienianej za pomocą komunikatorów internetowych); dane abonenta lub użytkownika usług świadczonej drogą elektroniczną (np. dane przedstawione przy rejestracji konta na platformie Facebook lub X); czy wreszcie **dane o ruchu sieciowym** (informacja o adresie IP, z którego nawiązano sesję internetową, podczas której zaistniały istotne dowodowo zdarzenia) i inne.

W zależności od rodzaju danych, **administrowane są one przez różne podmioty**: osoby fizyczne, spółki i korporacje, podmioty publiczne. Z perspektywy śledczej istotne jest to, że do tych samych danych organy ścigania mogą uzyskać dostęp niekiedy na kilka sposobów. Przykładowo treści

2 Komisja Europejska, COMMISSION STAFF WORKING DOCUMENT IMPACT ASSESSMENT Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and Proposal for a Directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings, dokument nr 52018SC0118, źródło: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD:2018:118:FIN (data dostępu: 13/11/2024).

3 B. Flander, A. Erbežnik, Toolkit for Handling and Admissibility of Electronic Evidence Empowering Legal Practitioners to Critically Review E-Evidence from the Procedural Rights Perspective, Koper 2024, s. 57. Bardziej szczegółowa definicja wraz z rozważaniami nad zakresami pojęć “dowód cyfrowy”, “dowód elektroniczny”, “dane” i “informacje” - zob. P. Lewulis, Dowody cyfrowe – teoria i praktyka kryminalistyczna w polskim postępowaniu karnym, Warszawa 2021, s. 28-43.

publikowane przez użytkownika na portalu społecznościowym można uzyskać i zabezpieczyć na potrzeby postępowania zarówno z otwartego źródła informacji, czyli bezpośrednio z Internetu (o ile użytkownik udostępnia je publicznie), jak i od dostawcy danego medium społecznościowego, czy wreszcie od samego użytkownika, w przypadku uzyskania danych dostępowych do jego konta albo zabezpieczenia urządzeń elektronicznych, na których pozostaje on zalogowany do owego konta.

Z drugiej strony dane takie najczęściej **dostępne są tylko przez bardzo ograniczony czas** - przykładowo do momentu wykasowania ich przez użytkownika, a w przypadku danych telekomunikacyjnych do końca okresu retencji tych danych (który w Polsce wynosi 12 miesięcy, a w innych krajach najczęściej jest krótszy).

Co więcej, pozyskiwanie danych przez organy ścigania od dostawców usług sieciowych bywa znacząco utrudnione, czy to z uwagi na brak współpracy, brak instrumentów realnego egzekwowania wymiany informacji wobec podmiotów zagranicznych, ograniczony zakres dobrowolnej wymiany danych i istotną długotrwałość procedur międzynarodowej pomocy prawnej. Z kolei nawet zabezpieczenie urządzeń elektronicznych bezpośrednio od użytkownika nie otwiera automatycznie dostępu do wszystkich danych zgromadzonych na tych urządzeniach, czy też w powiązanych z nimi usługach sieciowych (trzeba bowiem wyjaśnić, że przykładowo treści publikowane na portalu społecznościowym nie są przechowywane bezpośrednio w pamięci telefonu, z którego dokonano publikacji, a na serwerze dostawcy danego medium, najczęściej zlokalizowanym za granicą). Wynika to z faktu, że urządzenia elektroniczne w większości przypadków chronione są hasłami lub zabezpieczeniami biometrycznymi, a użytkownik w żadnym wypadku nie jest zobowiązany do podawania tych haseł lub zdejmowania zabezpieczeń dla organów ścigania. Naturalnie policjant ma prawo zapytać użytkownika o hasło, a użytkownik może takiej informacji udzielić. Odbywa się to jednak na zasadzie dobrowolności, a jeżeli użytkownik odmówi podania hasła, to nie można wyciągać wobec niego żadnych negatywnych konsekwencji z tego powodu.

Aktywne działanie pokrzywdzonego lub zawiadamiającego na etapie jeszcze przed wszczęciem postępowania karnego może jednak doprowadzić do skutecznego zabezpieczenia przynajmniej części materiału dowodowego na potrzeby późniejszego postępowania.

Polska podstawa prawna - dane informatyczne traktowane analogicznie do rzeczy zgodnie z art. 236a k.p.k.

W k.p.k. brak wprost wyrażonej definicji dowodu cyfrowego lub dowodu elektronicznego. Nie jest to jednak luka prawna. O ile bowiem kodeks reguluje sposób przeprowadzenia podstawowych, typowych czynności dowodowych (jak przesłuchanie świadka, uzyskanie opinii biegłego itp.), to nie zawiera zamkniętego katalogu dowodów. Przeciwnie, przyjmuje się, że **dowodem może być każdy dopuszczalny przez prawo karne procesowe środek służący dokonaniu ustaleń mających znaczenie dla rozstrzygnięcia procesowego[4].**

Na potrzeby niniejszego opracowania **podstawowe znaczenie ma art. 236a k.p.k**., usytuowany w rozdziale 25., dotyczącym zatrzymania rzeczy i przeszukania. Zgodnie z art. 236a k.p.k. przepisy dotyczące zatrzymania rzeczy i przeszukania 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."*** Kodeks posługuje się zatem określeniem "dane informatyczne" i nakazuje traktować je analogicznie jak rzeczy fizyczne, które podlegają zabezpieczeniu w toku czynności przeszukania lub zatrzymania rzeczy.

"Dane informatyczne", o których mowa w art. 236a k.p.k., **obejmują w praktyce wszystkie rodzaje informacji zapisywanych i przetwarzanych w urządzeniach elektronicznych i sieciach komputerowych.** Dla pozyskania tych danych na potrzeby postępowania karnego niezbędne jest stwierdzenie, że mogą one stanowić dowód w sprawie (art. 217 § 1 k.p.k. w zw. z art. 236a k.p.k.), a w przypadku danych telekomunikacyjnych - że "mają znaczenie dla toczącego się postępowania" (art. 218 § k.p.k.). Uzyskanie tych danych wymaga wydania postanowienia przez prokuratora lub sąd (na etapie postępowania sądowego).

Ustawodawstwo międzynarodowe: DSA oraz Konwencja Rady Europy o cyberprzestępczości

W ustawodawstwie europejskim zdefiniowano **"dowód elektroniczny" jako dane abonenta, dane o ruchu lub dane dotyczące treści przechowywane przez usługodawcę, lub w imieniu usługodawcy, w formie elektronicznej.** "Usługodawcą" w tej definicji jest po prostu podmiot dostarczający usługi

4 Zob. np. T. Grzegorczyk, J. Tylman, Polskie postępowanie karne, Warszawa 2001, s. 435.

łączności elektronicznej, różne aplikacje i usługi online czy wreszcie usługi związane z administrowaniem domenami internetowymi. Definicja ta została zawarta w rozporządzeniu e-evidence[5], które wprawdzie zostało już uchwalone, jednak jego stosowanie rozpocznie się dopiero 18 sierpnia 2026 roku. Będzie ono miało ogromne znaczenie dla ułatwienia pozyskiwania danych przez organy ścigania bezpośrednio od dostawców usług elektronicznych, zwłaszcza tych mających siedzibę za granicą. Obejmie ono bowiem nie tylko podmioty zlokalizowane w Unii Europejskiej, lecz także (w szczególności) te, które swoje usługi świadczą na jej obszarze, choćby miały siedzibę w państwach trzecich.

Nie sposób mówić o przetwarzaniu danych informatycznych w Internecie bez omówienia unijnego aktu prawnego DSA (Digital Services Act - akt o usługach cyfrowych)[6]. Jest on stosowany bezpośrednio przez poszczególne kraje członkowskie UE (nie wymaga implementacji przy pomocy ustawy). Nie definiuje on "danych informatycznych", skupiając się na nieco innym pojęciu - "usługi pośredniej" ("intermediary service"). Oznacza ono w praktyce przekazywanie (transmitowanie) oraz przechowywanie i udostępnianie (w tym publicznie) informacji, danych, treści, komunikatów pochodzących od użytkowników sieci (Internet)[7].

DSA definiuje za to **"platformy internetowe"** jako usługi służące przechowywaniu i publicznemu rozpowszechnianiu danych pochodzących od użytkownika[8]. **W praktyce zatem media społecznościowe - platformy takie jak Facebook, X, TikTok - podlegają pod DSA jako "platformy internetowej"**, a ich dostawcy zobowiązani są stosować się do przepisów tego aktu prawnego. Szczególnie rygorystyczne przepisy dotyczą "bardzo dużych platform internetowych" ("very large online platforms" - VLOP), czyli takich, które posiadają przeciętnie co najmniej 45 milionów aktywnych użytkowników na miesiąc na obszarze Unii Europejskiej[9].

Na listę VLOP-ów obecnie wpisane zostały m.in.: Facebook, Instagram, LinkedIn, Snapchat, TikTok, X (dawny Twitter)[10], a zatem praktycznie wszystkie wiodące media społecznościowe.

---

5 Dokładnie: Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1543 z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonywaniem kar pozbawienia wolności (rozporządzenie e-evidence).

6 Pełna nazwa to: Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych).

7 Bardziej szczegółowa definicja legalna dostępna w art. 3 lit. g) oraz art. 4-6 DSA.

8 Dokładna definicja dostępna w art. 3 lit. i) DSA.

9 Dokładna definicja dostępna w art, 33 DSA.

10 Pełna lista dostępna na stronie Komisji Europejskiej: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (data dostępu: 20/11/2024)

O ile DSA ukierunkowane jest głównie na administrowanie rynkiem usług cyfrowych, to tzw. Konwencja budapesztańska (Konwencja Rady Europy o cyberprzestępczości)[11] wraz z protokołami dodatkowymi zaprojektowana została bezpośrednio na potrzeby zwalczania przestępstw komputerowych, w tym związanych z rasizmem i ksenofobią. Tych ostatnich kwestii dotyczy konkretnie pierwszy protokół dodatkowy do konwencji[12]. Polska ratyfikowała zarówno konwencję, jak i protokół dodatkowy.

Konwencja budapesztańska definiuje "dane informatyczne" ("computer data") w sposób szeroki, jako dowolne przedstawienie faktów, informacji lub pojęć w systemie komputerowy[13]. Sieć Internet jest rodzajem "systemu komputerowego" w rozumieniu tej konwencji. Z kolei pierwszy protokół dodatkowy obliguje, by uznawać za przestępstwa szereg zachowań związanych np. z dystrybuowaniem w "systemie komputerowym" rasistowskich i ksenofobicznych materiałów, grożeniem i znieważeniem, przez "system komputerowy", osób z uwagi na przynależność rasową, etniczną itp., negowaniem ludobójstw i zbrodni przeciwko ludzkości i inne[14].

11 Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie w dniu 23 listopada 2001 r.

12 Protokół dodatkowy do Konwencji Rady Europy o cyberprzestępczości dotyczący penalizacji czynów o charakterze rasistowskim lub ksenofobicznym popełnionych przy użyciu systemów komputerowych, sporządzony w Strasburgu w dniu 28 stycznia 2003 r.

13 Dokładna definicja dostępna w art. 1 Konwencji budapesztańskiej.

14 Szczegółowy opis czynów, które zgodnie z protokołem dodatkowym powinny stanowić przestępstwa, znajduje się w art. 3-7 tego protokołu. Warto wskazać, że Polska ratyfikowała ten protokół z dwoma zastrzeżeniami. Konkretnie skorzystała z zastrzeżenia, że dystrybucja materiałów rasistowskich i ksenofobicznych stanowić będzie przestępstwo jedynie, gdy materiały te nawołują do dyskryminacji związanej z przemocą lub nienawiścią; oraz że negowanie lub popieranie ludobójstwa lub zbrodni przeciwko ludzkości stanowić będzie przestępstwo, jedynie, gdy towarzyszy mu zamiar wywołania nienawiści, dyskryminacji lub aktów przemocy wobec jednostki lub grupy.

6 Rodzaj i zakres danych przetwarzanych przez platformy internetowe, w tym dostawców “mediów społecznościowych”

W części wstępnej przedstawiono definicję “platform internetowych” wyłaniającą się z DSA. Obecnie warto przyjrzeć się temu, jakie kategorie danych przetwarzane są przez dostawców takich platform (i innych usług internetowych), dzięki czemu możliwe będzie poznanie prawidłowej metodyki prowadzenia spraw karnych o przestępstwa z nienawiści, popełniane za ich pośrednictwem.

Kategorie danych przetwarzanych przez platformy internetowe

Dostawcy platform internetowych przetwarzają bardzo szeroki zakres danych informatycznych dotyczących użytkowników. Najogólniej można podzielić ja na dwie kategorie: content data (dane “treściowe” - dotyczące treści) i non-content data (pozostałe dane).

Pierwsza kategoria obejmuje treść informacji publikowanych, zamieszczanych czy przesyłanych przez użytkowników usługi, np. tekst w poście na Facebooku, zdjęcie przesłane do Instagrama, film opublikowany w serwisie YouTube, a także zawartość korespondencji elektronicznej wymienianej pomiędzy użytkownikami skrzynek e-mail lub komunikatorów internetowych, takich jak Messenger, WhatsApp, Signal czy Telegram[15].

Druga kategoria (non-content data) obejmuje:

1. **Dane abonenta/użytkownika** - czyli wszystkie dane identyfikujące klienta (użytkownika Internetu) i usługę, z której korzysta. Przykładowo dla użytkownika portalu Facebook będą to: imię, nazwiska, numer telefonu i pozostałe dane podane przy rejestracji konta, dane dotyczące płatności realizowanych przez klienta na rzecz Facebooka, ale także dane techniczne, np. o urządzeniach użytkownika powiązanych z tym kontem oraz związane z weryfikowaniem tożsamości klienta

15 Warto wiedzieć, że w przypadku Telegrama wymiana komunikatów pomiędzy dwoma użytkownikami jest tylko jedną z funkcjonalności, obok grup dyskusyjnych, grup przeznaczonych do umieszczania ogłoszeń, “kanałów” o charakterystyce zbliżonej do mikroblogów.

(co miałoby większe znaczenie przy usługach finansowych, takich jak bankowość internetowa i usługi płatnicze). Co jednak istotne, do kategoria ta nie obejmuje haseł lub innych środków uwierzytelniania zastępujących hasła. O ile zatem organy ścigania zasadniczo mogą uzyskiwać dane abonenta, to jednak nie ujawnią w ten sposób haseł do użytkowanych usług lub platform.

2. **Dane o ruchu (sieciowym)** - to zasadniczo dane związane z łącznością elektroniczną. Najważniejszymi z nich - z punktu widzenia efektywnego prowadzenia śledztwa - są adres IP i numer portu sieciowego użytkownika usługi internetowej, wraz z dokładną datą i godziną (co do sekundy) nawiązania połączenia z tą usługą. Przykładowo, jeśli jakiś użytkownik opublikowałby komentarz pod filmem na YouTube'ie, to dane o ruchu sieciowym oznaczałyby przede wszystkim adres IP urządzenia, z którego połączył się z Internetem pisząc ten komentarz, wraz z numerem portu sieciowego, a także dokładną datę i godzinę, w której połączył się z platformą YouTube. Ale nie tylko. Dane o ruchu sieciowym mogą objąć też szereg dalszych informacji związanych z realizowanym przez użytkownika połączeniem, takie jak: lokalizacja użytkownika, cechy oprogramowania i modele urządzeń, z których korzystał podczas połączenia. Takie szczegółowe dane nie muszą być jednak rejestrowane przez wszystkich usługodawców.

Okres przechowywania danych przez platformy internetowe

Jak już sygnalizowano, dane telekomunikacyjne przechowywane są zasadniczo przez okres 12 miesięcy (w Polsce). Wynika to wprost z ustawy p.k.e.[16]. Obowiązek ten dotyczy jednak tylko przedsiębiorców telekomunikacyjnych (jak dostawcy sieci Plus, Play, T-Mobile, Orange itp.), a nie platform internetowych lub innych usług sieciowych.

Jak długo platformy internetowe przechowują dane? To zależy od polityki konkretnej platformy. Zasadniczo dane przechowywane są tak długo, jak jest to potrzebne do dostarczenia użytkownikowi danej funkcji lub usługi. Przy czym w praktyce decyzja o przechowywaniu lub nieprzechowywaniu danych przez platformę ma przede wszystkim charakter biznesowy. A więc zazwyczaj dane użytkowników przechowywane są tak długo, jak długo ich przetwarzanie może generować korzyści ekonomiczne dla platformy[17]. **Nie ma zatem jednej konkretnej odpowiedzi na pytanie o to, jak długo platformy internetowe przechowują dane użytkowników.** Zależy to od rodzaju danych i polityki konkretnej

16 Konkretnie: art. 47 i nast. p.k.e.

17 Korzyści te mogą być czasem nieoczywiste. Przykładowo - platforma społecznościowa pozornie nie odnosi żadnych korzyści z tego, że przestrzeń dyskowa na jej serwerach zajmowana jest przez posty użytkownika sprzed dwudziestu lat. W praktyce jednak przetwarzania ogromu danych uzyskanych o tym użytkowniku w ostatnim dwudziestoleciu pozwala platformie na zaoferowanie skutecznych (płatnych) usług reklamowych różnym podmiotom trzecim - reklamodawcom.

platformy. Szczegółowe informacje o tym można uzyskać zapoznając się z regulaminem, polityką przetwarzania danych, zasadami prywatności lub innym analogicznym dokumentem obowiązujących dla danej platformy. Kilka przykładów dotyczących popularnych dostawców platform internetowych zostanie omówione poniżej.

Dostęp do danych wykasowanych przez użytkownika

Podobnie jest z dostępem do danych wykasowanych przez użytkownika, i to zarówno z perspektywy samego użytkownika, jak i organów ścigania. Poszczególne platformy i inni dostawcy usług internetowych mogą odrębnie kształtować swoje polityki w zakresie przechowywania takich danych, np. w przypadku usługi e-mail skasowane wiadomości najczęściej są w dalszym ciągu przechowywanie w folderze "kosz" i ulegają wykasowaniu dopiero po ręcznym "opróżnieniu kosza" albo z upływem określonego przez dostawcę usługi czasu.

Definitywne wykasowanie takich danych przez użytkownika najczęściej sprawia, że stają się one niedostępne także dla organów ścigania nawet wtedy, jeżeli we właściwym trybie zwrócą się o nie do platformy internetowej czy innego dostawcy. Z drugiej strony dostawca taki może określić pewne zdarzenia, które zadecydują o dalszym przechowywaniu danych pomimo ich wykasowania przez użytkownika. Może to mieć miejsce np. w razie podejrzenia naruszenia regulaminu platformy internetowej - gdy administrator weryfikuje zaistnienie tego naruszenia. Niektórzy dostawcy mogą też zastrzec, że ręczne wykasowanie danych przez użytkownika wcale nie oznacza ich pełnego usunięcia z serwerów platformy, a jedynie sprawia, że są one niedostępne do innych użytkowników. Zasadniczo jednak trzeba przyjąć, że ręczne wykasowanie treści przez użytkownika najczęściej doprowadzi do tego, że jej późniejsze zabezpieczenie przez organy ścigania nie będzie możliwe.

Przykładowe zasady przetwarzania danych przez dostawców popularnych usług sieciowych: FB, X, TikTok

Facebook należy do korporacji Meta[18], podobnie zresztą jak Instagram oraz komunikatory Messenger i WhatsApp. Portal X, poprzednio Twitter, kojarzony obecnie z Elonem Muskiem, jest własnością założonej przez niego, amerykańskiej spółki X Corp. Struktura własnościowa TikToka jest nieco bardziej skomplikowana, ale ostatecznie należy on do chińskiej spółki ByteDance Ltd., mającej siedzibę w Pekinie, choć formalnie zarejestrowanej na Kajmanach.

18 Meta Platforms Inc. z siedzibą w Stanach Zjednoczonych, poprzednio Facebook Inc.

Facebook[19]

Co do zasady platforma przetwarza dane użytkownika tak długo, jak jest to potrzebne do dostarczania usług i funkcjonalności. Co to w praktyce oznacza? To już zależy od kategorii danych i konkretnej sytuacji. Przykładowo dane logowania do konta użytkownika, czy też opublikowane przez użytkownika (i nieusunięte) zdjęcia i posty są przechowywane przez cały czas funkcjonowania konta użytkownika. Jednak Facebook zapisuje też historię aktywności użytkownika na platformie. Takie dane, o ile nie zostaną ręcznie usunięte, korporacja Meta przechowuje przez 6 miesięcy. To ograniczenie czasowe dotyczy jednak tylko danych, "które nie będą konieczne do tego, by wyświetlać Ci historię wyszukiwania, np. informacje o wykorzystywanym urządzeniu lub Twojej lokalizacji" - jak deklaruje Meta. Właściwe co to oznacza? Otóż sama historia wyszukiwania, dostępna z poziomu "Dziennika aktywności" na portalu Facebook, przechowywana jest przez cały czas funkcjonowania konta użytkownika, o ile nie zostanie ręcznie wykasowana. **Jednak informacja o adresie IP (i numerze portu sieciowego oraz pozostałych parametrach konkretnego połączenia użytkownika z platformą) zostaną automatycznie wykasowane po 6 miesiącach,** w przynajmniej tak wskazuje Meta.

W przypadku ręcznego wykasowania treści (postów, zdjęć) przez użytkownika, są one dostępne w folderze "kosz" na Facebooku przez 30 dni. Po tym czasie rozpoczyna się proces automatycznego usuwania. W praktyce proces ten (obejmujący usuwanie danych także z kopii zapasowych i systemów odzyskiwania danych po awarii) może trwać do 90 dni. Proces usuwania rozpocznie się wcześniej, jeżeli użytkownik ręcznie "opróżni kosz". Dostawca Facebooka zadbał jednak dobre "ukrycie" kosza na stronie platformy[20], więc przypuszczalnie nie wszyscy użytkownicy wiedzą w ogóle o jego istnieniu lub o możliwości jego ręcznego opróżnienia. W trakcie 90-dniowego procesu usuwania będą one już najprawdopodobniej niedostępne dla organów ścigania, nawet jeżeli zwrócą się we właściwym trybie do korporacji Meta.

Usunięcie konta przez użytkownika automatycznie inicjuje mogący trwać do 90-dni proces usuwania wszystkich danych użytkownika. W tej sytuacji dane użytkownika mogą być zachowane przez platformę tylko jeżeli zobowiązanie takie będzie wynikało z przepisów prawa. Jeżeli np. organy ścigania lub sąd we właściwym trybie zwrócą się do korporacji Meta o zamrożenie konkretnych danych określonego użytkownika, to usunięcie konta przez tego użytkownika nie spowoduje ich wykasowania po stronie platformy - będą one przechowywane aż do końca trwania okresu "mrożenia".

---

19 Opracowano na podstawie dokumentacji korporacji Meta aktualnej na listopad 2024 r.: Zasady Ochrony Prywatności: https://www.facebook.com/privacy/policy oraz dokumenty i strony, do których odnośniki znajdują się w tych zasadach

20 Na stronie głównej platformy na komputerze należy wybrać kafelek ze zdjęciem profilowym w lewym, górnym rogu, następnie "Ustawienia prywatności", następnie "Dziennik aktywności", a wreszcie w menu po lewej stronie wyszukać "Kosz".

X[21]

Okres przechowywania danych na X również zależy od rodzaju danych i konkretnej sytuacji. Dane profilowe i dane do logowania przechowywane są przez cały okres istnienia konta. Publikowane przez użytkownika treści, komentarze, interakcje z innymi użytkownikami również dostępne są przez cały czas funkcjonowania konta, o ile nie zostaną ręcznie wykasowane. Adres IP, z którego użytkownik korzysta podczas połączenia z platformą, i inne parametry połączenia sieciowego, X przechowuje przez okres 13 miesięcy. Z kolei informacje o treściach wyświetlanych przez użytkownika, w tym o reklamach, w które użytkownik kliknął, dostępne są przez 90 dni. Wszystkie te rodzaje danych lub część z nich może być jednak przechowywana dłużej, jeżeli administrator X weryfikuje ewentualne naruszenie regulaminu platformy lub zawiesi konto, albo gdy wynika to z zewnętrznych zobowiązań prawnych.

Na portalu X użytkownicy mogą kasować zarówno pojedyncze posty, jak i dezaktywować całe konto. Obecnie platforma nie posiada funkcjonalności jednorazowego kasowania wielu postów. A co dzieje się z wykasowanymi postami i czy można je odzyskać? Inaczej niż na Facebooku, platforma X nie zawiera folderu "kosz", a usunięcie posta ma skutek natychmiastowy i powoduje - jak deklaruje administrator portalu - usunięcie go z konta użytkownika, z linii czasu użytkowników śledzących to konto i z wyników wyszukiwania na platformie[22]. Czyli post taki stanie się niewidoczny dla użytkowników platformy. Administrator X sprytnie jednak pominął informację o tym, czy także dla niego samego treść posta stanie się niedostępna. W praktyce zatem trudno się zorientować, czy ręczne wykasowanie posta przez użytkownika powoduje rzeczywiście jego usunięcie na serwerach X, czy tylko uniemożliwienie wyświetlania go od strony użytkowników. Gdyby jednak nawet tak było, to możliwość uzyskania dostępu do wykasowanych już postów przez organy ścigania jest raczej wątpliwa.

Dezaktywacja konta przez pierwsze trzydzieści dni nie wywołuje w praktyce żadnych skutków dla danych powiązanych z tym kontem. W tym okresie bowiem użytkownik może się ponownie zalogować, co będzie równoznaczne z ponownym aktywowaniem konta. Dopiero po upływie tego 30-dniowego okresu konto zostanie trwale usunięte. Wówczas niedostępne będą też prywatne wiadomości użytkownika i jego publiczny profil. Administrator X będzie jednak przechowywał "pewne" dane dotyczące usuniętego konta (nie precyzuje w swoich dokumentach o jakie dane chodzi) w celach bezpieczeństwa.

Podobnie jak w przypadku Facebooka, wystąpienie przez organy ścigania o zamrożenie danych ustrzeże je przed usunięciem nawet jeżeli później użytkownik zdecyduje się na ich ręczne wykasowanie.

---

21 Opracowano na podstawie dokumentacji administratora X aktualnej na listopad 2024 r.: Polityka Prywatności: https://x.com/pl/privacy; https://help.x.com/pl/managing-your-account/how-to-deactivate-x-account; https://help.x.com/en/using-x/delete-posts.

22 https://help.x.com/en/using-x/delete-posts (data dostępu: 22/11/2024).

TikTok[23]

Także w tym wypadku okres przechowywania danych zależy od ich rodzaju i konkretnej sytuacji. Przy tym polityka prywatności TikToka została sformułowana nieco lapidarnie - można się z niej dowiedzieć niewiele ponad to, że dane użytkownika są przechowywane "tak długo, jak jest to konieczne do świadczenia usług". Jedynie przykładowo dla kategorii danych obejmujących: informacje z konta (dane użytkownika i dane do logowania); treści publikowane przez użytkownika; wiadomości - administrator platformy podaje, że przechowuje je tak długo, jak długo aktywne jest konto użytkownika. Brak informacji o tym, przez jaki czas dostępne są informacje o logowaniach użytkowników do platformy, takie jak adres IP i powiązane z nim parametry połączenia.

Usunięcie pojedynczych treści przez użytkownika TikToka jest możliwe. W takim wypadku dane nie ulegają jednak natychmiastowemu wykasowaniu, a są dalej przechowywane przez okres "do 30 dni", zwany okresem karencji. W tym okresie dane można wyświetlać w folderze ostatnio usuniętych postów, odzyskać i przywrócić do konta użytkownika. Byłyby zatem one dostępne także dla organów ścigania.

TikTok oferuje użytkownikom możliwość usunięcia konta bądź dezaktywowania konta. To pierwsze oznacza bezpowrotną utratę konta przez użytkownika. Dezaktywacja to z kolei zawieszenie konta z możliwością jego reaktywacji. W tym wypadku dane użytkownika nie są w ogóle kasowane. Potencjalnie więc organy ścigania mogą mieć do nich dostęp. W przypadku usunięcia konta rodzaj, zakres i czas usunięcia przez TikToka danych użytkownika są niejasne - dokumenty platformy tego nie precyzują. Należy jednak przypuszczać, że w tym wypadku dane nie będą już dostępne dla organów ścigania, nawet jeżeli wystąpią do TikToka we właściwej procedurze.

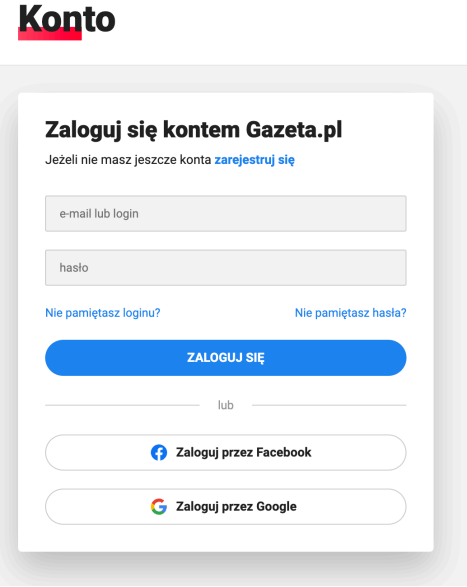
Co wynika z danych przetwarzanych przez platformy internetowe i jak ustalić tożsamość użytkownika na ich podstawie?

Niekiedy użytkownicy publikują w Internecie treści pod swoim pełnym, prawdziwym imieniem i nazwiskiem. Jeśli tak nie jest, tożsamość autora danego posta, komentarza, wpisu, filmu itp. trzeba ustalić na podstawie danych abonenckich i o ruchu sieciowym, przetwarzanych przez platformę internetową.

23 Opracowano na podstawie dokumentacji administratora X aktualnej na listopad 2024 r.: Polityka prywatności, https://www.tiktok.com/legal/page/eea/privacy-policy/pl; Prywatność i bezpieczeństwo, https://www.tiktok.com/community-guidelines/pl/privacy-security; także: https://support.tiktok.com/pl/using-tiktok/creating-videos/editing-posting-and-deleting; https://support.tiktok.com/pl/account-and-privacy/deleting-an-account/deleting-an-account.

Najprostszym, ale i najbardziej zawodnym sposobem na ustalenie tożsamości użytkownika danej treści jest pozyskanie przez organy ścigania danych abonenckich, o których była mowa powyżej. Dlaczego zawodnym? Trzeba pamiętać, że użytkownik publikujący przykładowo komentarz pod filmem na YouTube'ie wcale nie musi podawać swoich prawdziwych danych przy rejestracji na tej platformie. A niekiedy z konta jednego użytkownika może korzystać zupełnie inna osoba. A więc poprzestanie na danych abonenckich może być niewystarczające do ustalenia rzeczywistej tożsamości autora. Z drugiej strony wiele usług sieciowym umożliwia zarejestrowanie się i późniejsze logowanie "przez Facebook'a", "przez Google'a" lub z wykorzystaniem innego, istniejącego już konta użytkownika w innej usłudze. W takim wypadku dochodzi do powiązania ze sobą dwóch kont. Z perspektywy ustalenia tożsamości użytkownika sytuacja taka może być korzystna, bo konto użyte do uwierzytelnienia nowej usługi sieciowej często bywa takim, z którego użytkownik w życiu codziennym korzysta, i z którym powiązane są jego prawdziwe dane, ewentualnie inne informacje prowadzące do wykrycia jego tożsamości.

Przykład. Załóżmy, że artykułem na stronie internetowej Gazeta.pl pojawił się rasistowski komentarz. Aby umieszczać komentarze pod artykułami, niezbędne jest posiadanie konta Gazeta.pl. Konto można zarejestrować "ręcznie" - podając login, e-mail i hasło. Ale można też zalogować się poprzez powiązanie konta na Facebooku lub Google. Jeżeli użytkownik skorzystał z tej możliwości, to opublikowany przez niego, rasistowski komentarz będzie można powiązać z jego kontem na Facebooku lub Google. Jest szansa, że użytkownik na co dzień korzysta z tych kont i zawierają one jego prawdziwe dane. Nawet jeśli nie, to i tak mogą się tam znajdować informacje ułatwiające wykrycie jego tożsamości, np. zdjęcia z jego wizerunkiem opublikowane na Facebooku, informacja o kręgu "znajomych", w czy wreszcie dane karty płatniczej powiązanej z kontem.



Ilustracja 1. Zrzut ekranu z konto.gazeta.pl - dwie ścieżki logowania się do konta: przez login i e-mail lub przez jedno z powiązanych kont: na Facebooku albo na Google (data dostępu: 30/11/2024)

A co, jeżeli użytkownik podał swoje nieprawdziwe dane i nie skorzystał z możliwości powiązania konta? **Dlatego właśnie dane o adresie IP są takie ważne.** "IP" to skrót od angielskiego "Internet Protocol". Jest to ciąg cyfr (albo cyfr i liter w przypadku wersji szóstej protokołu IP), który:

- identyfikuje indywidualne urządzenie podłączone do sieci, np. do Internetu;
- a jednocześnie informuje o tym, jaki przedsiębiorca jest dostawcą Internetu dla konkretnego połączenia.

Omówmy to na przykładzie. Przykładowy adres IP (w wersji czwartej protokołu IP - wciąż najbardziej powszechnej) może wyglądać tak: **188.146.23.68**[24] . Załóżmy, że to jest właśnie adres IP, którym posłużył się użytkownik publikujący analizowany komentarz na YouTube'ie. Żeby rozszyfrować zawarte w nim dane, trzeba skorzystać z jednego z dostępnych w Internecie narzędzi analitycznych, takich jak CentralOps[25] . Analiza tego adresu da następujący wynik:

Ilustracja 2. Zrzut ekranu z centralops.net po wykonaniu analizy adresu IP: 188.146.23.68 (data dostępu: 20/11/2024)

24 Adres IP w wersji szóstej protokołu mógłby wyglądać przykładowo tak: 2001:0db8:0001:0000:0000:0ab9:C0A8:0102.

25 Dostępne pod adresem: centralops.net. Alternatywy to na przykład: https://www.whois.com/; https://whatismyipaddress.com/; https://ip-lookup.net/ i wiele innych.

Co wynika z wykonanej analizy? Że użytkownik adresu IP 188.146.23.68 korzysta z łącza internetowego, którego dostawcą jest T-Mobile. **Dostawcami Internetu mogą być operatorzy telekomunikacyjni,** np. dostawcy sieci Plus, Play, T-Mobile czy Orange (wówczas mowa o tzw. "Internet mobilny") albo **przedsiębiorcy dostarczający Internet do domu czy biura**, jak UPC, Vectra itp. (tzw. "Internet stacjonarny").

Stąd już tylko krok do poznania tożsamości osoby, która skorzystała z łącza internetowego. Ten krok polega na uzyskaniu **przez organy ścigania od operatora telekomunikacyjnego lub innego dostawcy Internetu danych klienta, z którym zawarto umowę**, w ramach której ów klient połączył się z Internetem korzystając z konkretnego adresu IP. Czyli - w omawianym przykładzie - jaki konkretnie abonent korzysta z usług telekomunikacyjnych świadczonych przez T-Mobile, w ramach których nawiązał połączenie z wykorzystaniem adresu IP 188.146.23.68.

Kierując pytanie (w formie postanowienia wydanego przez prokuratora lub sąd) do takiego dostawcy Internetu organy ścigania **uzyskają informację o konkretnej osobie (z imienia i nazwiska), która skorzystała z danego adresu IP.**

Trudności i problemy związane z ustaleniem tożsamości użytkownika na podstawie adresu IP i jak im przeciwdziałać

W poprzednim akapicie założono optymistycznie, że autor analizowanego komentarza na YouTube'ie jest dokładnie tą samą osobą, która zawarła z T-Mobile umowę na świadczenie usług telekomunikacyjnych, w ramach której nawiązała połączenie internetowe z adresu IP 188.146.23.68. Tak jednak wcale nie musi być.

1. Z numeru telefonu[26] zarejestrowanego na pewną osobę może w rzeczywistości korzystać inna osoba - członek rodziny, znajomy albo nawet osoba zupełnie obca.
2. Użytkownik numeru telefonu może udostępnić Internet innej osobie albo umieścić kartę SIM w routerze, tworząc w ten sposób sieć WiFi opartą na łączu mobilnym.
3. Tym bardziej w przypadku Internetu stacjonarnego - z tej samej sieci WiFi może korzystać większa grupa osób - rodzina, domownicy, pracownicy biura itp. Adres IP identyfikuje w gruncie rzeczy router, z którego użytkownicy sieci Wifi łączą się z Internetem, a nie urządzenie (komputer, telefon), które łączy się z tym routerem. **Trudność tę można niekiedy przezwyciężyć. Otóż sam router zapisuje w formie dziennika systemowego (tzw. logi/logi systemowe) informację o tym, jakie urządzenia i w jakim czasie łączyły się z nim w celu nawiązania połączenia z Internetem.**

26 Precyzyjnie - obowiązkowi rejestracji podlega karta SIM, a nie sam numer telefonu komórkowego opisywany skrótem MSISDN.

Mając zatem dostęp do routera[27] można ustalić, które konkretnie urządzenie nawiązało dane połączenie z Internetem. Z drugiej strony trzeba pamiętać, że - w zależności od modelu routera i ustawień użytkownika - logi mogą być przechowywane tylko przez ograniczony czas, mogą być "ręcznie" wykasowane przez użytkownika, mogą ulegać wykasowaniu wskutek wyłączenia routera (np. przy przerwie w dostawie prądu).

4. Także w przypadku podłączenia się do otwartej sieci Wifi (w miejscu publicznym, w kawiarni, na lotnisku itp.) adres IP posłuży jedynie identyfikacji podmiotu, który udostępnił otwartą sieć Wifi, a nie konkretnego użytkownika łączącego się z tą siecią (choć niektóre publiczne sieci WiFi mogą wymagać podania adresu e-mail lub innych danych w celu udostępnienia łącza internetowego; w takich wypadkach być może ustalenie tożsamości użytkownika okaże się możliwe; jest to uzależnione od tego, czy użytkownik posłużył się danymi, które rzeczywiście powiązane są z jego tożsamością oraz czy dane te w ogóle są w dalszym ciągu dostępne po stronie administratora sieci).
5. Użytkownicy mogą korzystać z oprogramowania służącego maskowaniu ich tożsamości w Internecie, takiego jak VPN (Virtual Private Network) albo TOR (The Onion Router). W obu wypadkach zestawienie połączenia internetowego odbywa się za pośrednictwem innych urządzeń o innych adresach IP niż urządzenie, z którego w rzeczywistości nawiązano połączenie. "Deanonimizacja" użytkownika, który skorzystał z VPN, jest teoretycznie możliwa w przypadku uzyskania tych danych od dostawcy usługi VPN, ale w praktyce jest to trudne do osiągnięcia. "Deanonimizacja" użytkownika sieci TOR wymaga specjalistycznej analizy danych o ruchu sieciowym na poziomie, który w większości spraw karnych jest całkowicie nieosiągalny.
6. Jeżeli upłynął okres retencji danych telekomunikacyjnych (wynoszący w Polsce 12 miesięcy), to operator telekomunikacyjny nie będzie w stanie zidentyfikować użytkownika korzystającego z danego adresu IP (dotyczy to "Internetu mobilnego").
7. Jednoznaczne zidentyfikowanie urządzenia łączącego się z Internetem po "łączu mobilnym" (dostarczanym przez operatora telekomunikacyjnej) wymaga znajomości nie tylko adresu IP, ale także numeru portu sieciowego. Tymczasem niektórzy dostawcy usług Internetowych (w tym i platformy internetowe) wcale nie gromadzą danych o numerach portów sieciowych. Ten problem nie istnieje w przypadku korzystania z "Internetu stacjonarnego".

---

27 Precyzyjnie - do panelu użytkownika/interfejsu użytkownika do obsługi danego routera. Uzyskanie takiego dostępu wymaga znajomości hasła. Choć warto zauważyć, że wielu użytkowników nigdy nie zmienia domyślnego hasła do panelu użytkownika i wówczas bardzo łatwo je poznać (jest ono zależne od producenta routera i modelu routera; często brzmi "admin" lub z zbliżony sposób). Wielu użytkowników w ogóle nie zdaje sobie sprawy z możliwości zmiany hasła do tego panelu. Dostęp do panelu użytkownika następuje poprzez wpisanie w pasku adresu przeglądarki internetowej adresu lub adresu IP wskazanego przez producenta routera zazwyczaj na naklejce znamionowej na dolnej stronie urządzenia (informację tę, podobnie jak informację o domyślnym haśle, można też zazwyczaj uzyskać ze strony internetowej pomocy technicznej producenta routera, np. http://tplinkwifi.net/).

7 Dostęp do danych przetwarzanych przez platformy internetowe dla organów ścigania.

Wprowadzenie

W toku postępowania karnego organ procesowy (np. policjant, prokurator lub sąd) gromadzi dowody, z których część może pozyskać bez żadnej sformalizowanej procedury (np. dołączenie do akt zdjęć, które dostarczył pokrzywdzony), zaś część wymaga zachowania wymogów określonych w przepisach k.p.k. i innych ustaw. Przykładowo, uzyskanie danych telekomunikacyjnych (np. wykazu połączeń danego numeru MSISDN w danym okresie czy danych abonenta, któremu przydzielono określony adres IP) może nastąpić wyłącznie na podstawie postanowienia sądu lub prokuratora i wyłącznie w przypadku, gdy wymaga tego dobro wymiaru sprawiedliwości[28].

W przypadku, gdy dowody istotne w postępowaniu karnym znajdują się poza granicami RP lub ich dysponentem jest podmiot zagraniczny, ich pozyskanie odbywa się na szczególnych zasadach. Tak jak oczywiste jest, że przedstawiciele polskich służb nie mogą, powołując się na przepisy k.p.k., przeprowadzić przeszukania miejsca znajdującego się poza terytorium Polski, tak nie powinno budzić zdziwienia, że zagraniczny podmiot nie wyda polskiemu organowi procesowemu danych lub przedmiotów wyłącznie w oparciu o polskie przepisy. Konieczność współpracy z władzami innych państw występuje bardzo powszechnie w przypadku postępowań dotyczących czynów popełnionych za pośrednictwem internetu. Uwaga ta dotyczy zarówno przestępstw polegających na publikacji określonej treści, gdy konieczne może być uzyskanie informacji od administratora zagranicznej platformy internetowej czy zagranicznego operatora telekomunikacyjnego, jak i przestępstw o zupełnie innej charakterystyce, np. ataków **ransomware**, w przypadku których infrastruktura wykorzystana do zaszyfrowania danych zaatakowanego podmiotu może obejmować serwer zlokalizowany za granicą. Wybór właściwej drogi do uzyskania dowodów będzie zależny od trzech czynników:

28 art. 180 § 1 k.p.k. w zw. z art. 226 k.p.k.

- **po pierwsze, od państwa, w którym znajduje się dany dowód** (np. gdzie zamieszkuje świadek, który musi zostać przesłuchany; gdzie zlokalizowany jest serwer C2 wykorzystany do ataku; gdzie ma siedzibę operator telefonii komórkowej, z którego usług sprawca korzystał, zamieszczając w internecie istotne treści; gdzie znajduje się siedziba lub oddział podmiotu administrującego platformę internetową, na której zamieszczono owe treści). Inne instrumenty prawne będą bowiem obowiązywały w przypadku państw Unii Europejskiej, a inne w przypadku państw trzecich. W przypadku niektórych państw szansa na uzyskanie jakichkolwiek danych w rozsądnym terminie będzie przy tym znikoma;
- **po drugie, od rodzaju dowodów, które mają zostać przeprowadzone**. Niektóre kategorie danych wymagają dochowania szczególnych formalności, przykładowo dominuje stanowisko, że uzyskanie danych objętych tajemnicą bankową od zagranicznego banku wymaga w pierwszej kolejności uzyskania zgody polskiego sądu na udzielenie informacji objętych tajemnicą, a dopiero potem wystąpienia do właściwych władz innego państwa. Inne dane z kolei można uzyskać bez zachowania jakichkolwiek formalności, np. jeśli w danym państwie istnieje możliwość przeglądania rejestru sądowego za pośrednictwem ogólnodostępnej, rządowej strony internetowej, dane uzyskane z takiego serwisu mogą stanowić materiał dowodowy w polskim postępowaniu karnym. Biorąc pod uwagę ogromny zasób informacji gromadzonych w publicznie dostępnych rejestrach, w wielu przypadkach może okazać się, że podstawowa analiza OSINT (tzn. rozpoznanie z ogólnodostępnych źródeł) pozwoli uniknąć długotrwałego oczekiwania na uzyskanie danych od władz innego państwa;
- **po trzecie, od polityki danego podmiotu, np. platformy internetowej**. Administratorzy niektórych serwisów odmawiają wydania jakichkolwiek danych przedstawicielom innych państw, co prowadzi do konieczności zwrócenia się we właściwym trybie do władz państwa, w którym dany podmiot ma siedzibę. W dalszej kolejności organ tego państwa uzyskuje dane i przekazuje je na potrzeby polskiego postępowania karnego. Inne platformy natomiast prezentują bardziej liberalne podejście, udostępniając przedstawicielom władz innych państw dane tak wrażliwe jak np. numer karty kredytowej, z której opłacono daną usługę, czy pełne dane posiadacza portfela kryptowalutowego, często nie wymagając przy tym nawet postanowienia – wystarczająca może być korespondencja e-mail z adresu w domenie rządowej.

Wybór właściwej formy współpracy międzynarodowej

Wniosek o udzielenie międzynarodowej pomocy prawnej

Podstawowym sposobem uzyskania dowodu znajdującego się za granicą lub w dyspozycji zagranicznego podmiotu jest skierowanie do władz danego państwa (w zależności od państwa – do organu

centralnego, np. właściwego ministerstwa, lub do organu procesowego, np. prokuratury) wniosku o udzielenie międzynarodowej pomocy prawnej. Spotykane bywa określanie takiego wniosku skrótem MLAT, pochodzącego od sformułowania **mutual legal assistance treaty**, tj. umowa o wzajemnej pomocy prawnej. W oparciu o konwencje międzynarodowe, których Polska jest stroną, a także o umowy dwustronne lub wielostronne, możliwe jest uzyskanie pomocy polegającej m. in. na przesłuchaniu świadka czy podejrzanego zamieszkującego w innym kraju, przeszukania lokalu położonego za granicą czy uzyskania dokumentacji. W przypadku przestępstw z nienawiści dowodem, który należy uzyskać za granicą, będzie zwykle informacja od administratora platformy internetowej bądź dane telekomunikacyjne. Kluczowe znaczenie dla wyboru właściwej procedury ma siedziba podmiotu, który jest dysponentem danych, które chcemy uzyskać na potrzeby postępowania karnego. Ustalenie podstawy prawnej wystąpienia do określonego państwa z wnioskiem o pomoc prawną należy do sądu lub prokuratora i nie jest konieczne wskazywanie takiej podstawy we wniosku dowodowym. Innymi słowy, jeśli domagamy się przeprowadzenia dowodu za granicą, nie musimy ustalać, jaki rodzaj porozumienia wiąże RP z danym krajem. Warto natomiast poświęcić czas na ustalenie:

- gdzie znajduje się siedziba podmiotu, od którego chcemy uzyskać dowód. Należy ustalić dokładny, aktualny adres, gdyż zdarza się, że po wielomiesięcznym oczekiwaniu na realizację pomocy prawnej organ procesowy uzyskuje odpowiedź, że dany podmiot nie ma siedziby pod wskazanym adresem. Pomocne mogą być w tym celu np. rejestry sądowe, które w wielu krajach są dostępne online. Warto też ustalić wszystkie możliwe formy kontaktu, w tym adresy e-mail, telefony, a nawet formularze kontaktowe – nie ma przeszkód, by funkcjonariusze służb zagranicznych, którzy będą wykonywali pomoc prawną, w razie potrzeby podjęli próbę kontaktu taką niestandardową drogą;
- czy dany podmiot dysponuje interesującymi nas danymi. Przykładowo, dana platforma może przyjąć zasadę, że w zależności od kategorii dowodu, który ma zostać wydany, wniosek należy kierować do jej centrali lub do oddziału terenowego, znajdującego się w innym kraju. Zapoznanie się z zasadami współpracy danej platformy może uchronić nas od sytuacji, w której wniosek zostanie skierowany do niewłaściwego kraju, prowadząc do straty czasu, a nawet do utraty danych. Wskazówki w tym zakresie, dotyczące popularnych platform, zostaną omówione w dalszej części niniejszego opracowania.

Europejski nakaz dochodzeniowy

W stosunkach pomiędzy państwami członkowskimi Unii Europejskiej, z wyjątkiem Irlandii i Danii, wnioski o pomoc prawną zostały zastąpione europejskimi nakazami dochodzeniowymi (END). Instrument ten pozwala na uproszczenie i znaczne przyspieszenie uzyskiwania dowodów na obszarze UE, m. in. ze względu na to, że END jest kierowany bezpośrednio do organu procesowego, nie zaś do władz centralnych. Ułatwia też bezpośredni kontakt (np. e-mailowy) pomiędzy prokuratorem lub sędzią wydającym

nakaz a funkcjonariuszem, który go wykonuje. Możliwość ta jest stosunkowo rzadko wykorzystywana, jednak nie ma przeszkód, by nawiązać taki kontakt, np. w celu przekazania dodatkowej, pilnej informacji, która może wpłynąć na realizację nakazu, lub w celu uzyskania kluczowych informacji bezpośrednio po przeprowadzeniu dowodów, jeszcze przed skierowaniem oficjalnej odpowiedzi do państwa wydającego END.

Na portalu Europejskiej Sieci Sądowej (https://www.ejn-crimjust.europa.eu/ejn2021/ AtlasChooseCountry) dostępne jest narzędzie Atlas Sądowy, które pozwala na łatwe ustalenie, do jakiego organu należy skierować END w określonym przypadku. Wybór właściwego adresata nakazu, jak już podkreślono, należy do organu procesowego, choć nie ma przeszkód, by samodzielnie zweryfikować, czy nie doszło do omyłkowego wskazania niewłaściwego organu, co wydłużyłoby uzyskanie dowodów.

Dobrowolne wydanie danych przez ich administratora

W wielu przypadkach występowanie z END lub wnioskiem o pomoc prawną nie jest konieczne, pomimo że dane istotne w postępowaniu karnym są administrowane przez podmiot zagraniczny. Coraz liczniejsze platformy przewidują bowiem udzielanie informacji zagranicznym organom procesowym bez pośrednictwa władz krajowych. Mogą w tym zakresie występować ograniczenia, np. dane z kategorii **non-content data** dana platforma udostępni w oparciu o postanowienie wydane przez zagranicznego prokuratora lub sąd, natomiast kategorię **content data** zastrzega dla organów krajowych i do ich uzyskania niezbędne jest skierowanie wniosku o pomoc prawną. Trzeba podkreślić, że wbrew stanowisku wyrażanym niekiedy przez przedstawicieli polskich organów procesowych, dane uzyskane w ten sposób, a więc niejako „nieoficjalnie" – bez pośrednictwa organu zagranicznego, stanowią pełnowartościowy materiał dowodowy. Nie ma żadnej racjonalnej przesłanki, by wiadomość e-mail zawierającą określone dane, przesłaną bezpośrednio polskiemu organowi, traktować jako mniej wartościową, niż gdyby została ona uzyskana w drodze realizacji wniosku o pomoc prawną.

Poniżej scharakteryzowano zakres informacji udzielanych dobrowolnie przez najważniejsze platformy należące do kategorii VLOPS.

Facebook (Meta Platforms)

W ramach platformy Facebook współpraca z organami wymiaru sprawiedliwości została rozproszona pomiędzy różne komórki organizacyjne, w zależności od tego, czego dotyczy zapytanie. Jak wynika z informacji udostępnionych przez administratora:

- w zakresie użytkowników platformy Facebook w Unii Europejskiej, informacji udziela Meta Platforms Ireland Ltd., Law Enforcement Response Team, Merrion Road, Dublin 4, D04 X2KP, Ireland

(nie dotyczy Traffic and Content Data, tj. danych o ruchu sieciowym oraz o zawartości profilu, treści wiadomości itp.).

- w zakresie płatności poprzez Meta Pay dokonanych w Unii Europejskiej, informacji udziela Meta Payments International Limited, Legal Department, Merrion Road, Dublin 4, D04 X2KP, Ireland
- w zakresie użytkowników platformy Facebook w USA, a także w zakresie Traffic and Content Data niezależnie od lokalizacji użytkownika, informacji udziela Meta Platforms Inc., 1601 Willow Road, Menlo Park California 94025, USA
- w zakresie płatności poprzez Meta Pay dokonanych w USA, informacji udziela Meta Payments Inc., Legal Department, 1601 Willow Road, Menlo Park California 94025, USA

Część danych, w tym informację o adresach IP, z których logowano się do profilu, o adresie e-mail, telefonie, a także imieniu, nazwisku i dacie urodzenia użytkownika, administrator udostępnia za pośrednictwem panelu **Law Enforcement Online Requests System** (LEORS). Dostęp do panelu może uzyskać każdy przedstawiciel organu procesowego (w tym prokurator, sędzia, policjant), wykorzystując imienny adres e-mail w domenie gov.pl. Standardowo do uzyskania odpowiedzi na żądanie konieczne jest dołączenie skanu postanowienia (np. o zwolnieniu z tajemnicy prawnie chronionej), przy czym nie ma potrzeby tłumaczenia go na język angielski. Konieczne jest jednak również wypełnienie formularza, zawierającego krótki opis powodów żądania – w języku angielskim.

Warto wskazać, że obecny poziom udzielania odpowiedzi za pośrednictwem LEORS w praktyce bardzo znacznie ogranicza kierowanie wniosków do Meta Platforms Ireland Ltd., bowiem jeśli jakaś informacja nie jest dostępna poprzez LEORS, tj. należy do kategorii **Traffic Data** lub **Content Data**, niezbędne jest skierowanie wniosku o pomoc prawną do władz USA w celu uzyskania informacji od Meta Platforms Inc. Wnioski do Meta Platforms Ireland Ltd. będą się więc ograniczały do **Preservation requests**, tj. wniosków o zabezpieczenie danych, oraz do **Emergency disclosure requests**, tj. Żądania ujawnienia informacji w nagłych wypadkach, choć i takie kategorie wniosków mogą zwykle zostać rozpoznane za pośrednictwem LEORS, który zawiera odpowiednie zakładki.

W ramach kategorii **Traffic Data** i **Content Data** możliwe jest natomiast uzyskanie bardzo szerokiego zakresu informacji, niemal wyczerpującego katalog danych posiadanych przez administratora na temat danego użytkownika. Niektóre informacje są jednak usuwane po upływie określonego czasu, zaś inne są przechowywane przez cały czas utrzymywania konta użytkownika. Bardziej szczegółowe dane w tym zakresie nie mogą zostać opublikowane w ogólnodostępnym opracowaniu. O ile organ procesowy nie chce, by użytkownik został powiadomiony o zapytaniu o jego profil ze strony organów państwowych, należy zastrzec to w formularzu lub we wniosku o pomoc prawną.

Instagram (Meta Platforms)

W ramach platformy Instagram informacji organom procesowym udzielają te same podmioty, co w przypadku platformy Facebook, tj. Meta Platforms Ireland Ltd., Meta Payments International Limited, Meta Platforms Inc. oraz Meta Payments Inc., przy czym podział zadań jest identyczny jak w przypadku Facebooka.

Również zakres danych udostępnianych w ramach dobrowolnej współpracy i w ramach międzynarodowej pomocy prawnej jest taki sam, jak w przypadku platformy Facebook. Do składania bezpośrednich wniosków do administratora platformy wykorzystuje się ten sam panel, tj. LEORS, zatem aktualne są wszystkie uwagi dotyczące jego obsługi, wskazane przy opisie platformy Facebook.

O ile organ procesowy nie chce, by użytkownik został powiadomiony o zapytaniu o jego profil ze strony organów państwowych, należy zastrzec to w formularzu lub we wniosku o pomoc prawną.

WhatsApp (Meta Platforms)

W przypadku komunikatora WhatsApp funkcjonują inne kanały komunikacji z organami procesowymi niż w przypadku pozostałych platform Meta. Dane użytkowników są administrowane przez następujące podmioty:

- dla użytkowników z Europejskiego Obszaru Gospodarczego, tj. UE oraz Norwegii, Szwajcarii i Liechtensteinu: WhatsApp Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland
- dla użytkowników z pozostałych obszarów: WhatsApp LLC, 1601 Willow Road, Menlo Park, California 94025, USA

Do uzyskiwania informacji w ramach dobrowolnej współpracy z organami procesowymi służy panel LEORS (Law Enforcement Online Request System), dostępny pod adresem https://www.whatsapp.com/records/login

Zabezpieczenie danych

Na zakończenie tej części opracowania warto wspomnieć o możliwości wystąpienia przez organ procesowy o zabezpieczenie danych na okres do 90 dni, który powinien być wystarczający dla organu do sporządzenia i przetłumaczenia oficjalnego wniosku o pomoc prawną / END. Obowiązek taki wynika z Konwencji Rady Europy o Cyberprzestępczości (tzw. Konwencji Budapesztańskiej), art. 16 i 29. Okres, przez jaki dany podmiot będzie przechowywał dane w oczekiwaniu na oficjalne żądanie ich wydania, jest zależny od prawa krajowego oraz od polityki danego przedsiębiorstwa (przykładowo, Meta przewiduje okres 90 dni, przy czym nie usuwa danych, dopóki profil użytkownika nie zostanie usunięty),

jednak konwencja przewiduje okres nie krótszy niż 60 dni. Należy przyjąć, że w sytuacji, w której dane nie są udostępniane na zasadzie dobrowolnej współpracy z wymiarem sprawiedliwości (a więc wymagane jest wystąpienie z wnioskiem o pomoc prawną / END), zawsze występuje ryzyko utraty danych. Dlatego za dobrą praktykę można uznać poprzedzenie takiego wniosku / END wystąpieniem (np. w formie e-maila bądź poprzez wybranie odpowiedniej zakładki w formularzu dla organów wymiaru sprawiedliwości) o zabezpieczenie danych na podstawie Konwencji o Cyberprzestępczości.

Zakres danych dostępnych z poziomu urządzenia użytkownika - w kontekście platform internetowych

Jak sygnalizowano w części wstępnej, dane publikowane na mediach społecznościowych zasadniczo "znajdują się" na serwerach dostawców tych usług - w centrach danych zlokalizowanych w różnych miejscach na świecie - a nie w pamięci urządzeń poszczególnych użytkowników. A jednak na urządzeniach osobistych (komputerach, telefonach) mogą znajdować się kopie tych danych lub pliki tymczasowe zawierające te dane, ewentualnie kopie zapasowe danych.

Zakres danych dostępnych z poziomu urządzenia jest niejednolity - zależy zarówno od rozwiązań technicznych zastosowanych przez daną platformę, jak i ustawień prywatności i własnych konfiguracji użytkownika. Trudno więc przedstawić generalne zasady.

Można pokusić się o stwierdzenie, że **komunikatory internetowe co do zasady przechowują kopię konwersacji "lokalnie", czyli w pamięci urządzenia. Oznacza to, że konwersacje na takich komunikatorach jak: Messenger, WhatsApp, Signal, nawet Telegram, czy wreszcie na komunikatorach powiązanych z np. TikTokiem, Instagramem, SnapChatem, częstokroć będzie można uzyskać z poziomu urządzenia użytkownika (o ile oczywiście możliwe okaże się "odblokowanie" tego urządzenia)**. Jest jednak kilka ważnych zastrzeżeń. Otóż użytkownik może sam skonfigurować usługę tak, aby wiadomości automatycznie się kasowały (oferuje to większość popularnych komunikatorów), ewentualnie ręcznie wykasować całą historię konwersacji. Wreszcie możliwa jest i taka sytuacja, a której użytkownik zdalnie wykasuje dane powiązane z jego kontem, logując się do tego konta z innego urządzenia. Stąd też niezbędne jest, aby zabezpieczone od uczestników postępowania urządzenia rozłączyć z siecią i wykonać ekstrakcję danych, zanim przedsięweźmie się z nimi jakiekolwiek dalsze działania.

Przykład. Załóżmy, że grupa użytkowników wymieniała się rasistowskimi komentarzami w ramach "społeczności" na WhatsAppie. Prawdopodobnie kopia tej konwersacji jest dostępna

na urządzeniach poszczególnych członków "społeczności". Jeżeli jednak telefon jednego z użytkowników zostanie zabezpieczony na potrzeby postępowania, to użytkownik ten wciąż będzie mógł zalogować się do swojego konta na innym urządzeniu. W takim wypadku będzie mógł również dokonać ingerencji w treść danych na swoim koncie. Przykładowo będzie mógł wykasować swoje wypowiedzi na "społeczności", zawierające rasistowskie komentarze. Takie działanie będzie skuteczne dla wszystkich urządzeń powiązanych z tym kontem i ile będą podłączone do Internetu. A zatem w celu uniemożliwienia użytkownikowi zdalnej ingerencji w zakres danych dostępnych na jego zabezpieczonym urządzeniu, należy je rozłączyć z Internetem, zabezpieczyć dostępne dane i ewentualnie dopiero w dalszej kolejności wykonywać z tym urządzeniem czynności wymagające dostępu do sieci.

Sytuacja jest nieco bardziej skomplikowana w przypadku treści publikowanych w portalach społecznościowych. Facebook i Instagram zasadniczo nie przechowują "lokalnie" (na urządzeniu użytkownika) treści opublikowanych postów. Oczywiście jeżeli danemu postowi towarzyszyły media (zdjęcie, grafika, film) załadowane z pamięci wewnętrznej urządzenia, to media te w dalszym ciągu będą dostępne na urządzeniu (chyba że użytkownik zdążył je ręcznie wykasować). Niezależnie jednak od tego w pamięci podręcznej urządzenia oraz w lokalnym pakiecie danych powiązanych z aplikacją dostępne są treści na bieżąco przetwarzane i dostarczane użytkownikowi przez daną platformę, a wśród nich mogą znajdować się ostatnio opublikowane przez użytkownika posty, komentarze, grafiki itp.

Przykład. Dostęp do danych przechowywanych w pamięci podręcznej można samemu sobie łatwo zilustrować. Wystarczy na telefonie z aplikacją Facebook (lub inną) uruchomić tryb samolotowy, a następnie uruchomić aplikację. Pomimo braku dostępu do sieci aplikacja wyświetli przetwarzane na bieżąco dane nawet z ostatnich kilku dni - w tym ostatnie treści dostarczone użytkownikowi. Wśród tych danych mogą być też posty samego użytkownika.

Podobnie w przypadku portalu "X" - zasadniczo aplikacja nie zapisuje "lokalnej" (na konkretnym urządzeniu) kopii opublikowanych danych, a jednak możliwy jest dostęp do pamięci podręcznej powiązanej z tą aplikacją, gdzie dane takie można znaleźć. Dokumenty dotyczące portalu "X" nie odnoszą się do tej kwestii bezpośrednio. Praktyka pokazuje, że zakres danych przetwarzanych w pamięci podręcznej może obejmować nawet wszystkie aktywności użytkownika (opublikowane posty), jednak dostęp do tych danych może być ograniczony. Przede wszystkim dane znajdujące się w pamięci podręcznej ze swej natury mają charakter tymczasowy, a ponadto dostęp do nich może wymagać specjalistycznego oprogramowania.

Oznacza to, że zakres danych "lokalnych" obejmujących treści opublikowane przez użytkowników portali społecznościowych jest dość wąski, zazwyczaj dane takie znajdują się w pamięci tymczasowej, a uzyskanie do nich dostępu może wymagać posłużenia się specjalistycznym oprogramowaniem.

Niezależnie od tego różne platformy internetowe mogą oferować wykonywanie kopii zapasowej, która może być przechowywana "lokalnie" - na urządzeniu użytkownika albo "w chmurze", czyli na serwerze dostawcy usługi sieciowej. Wykonywanie kopii zapasowej – w zależności od funkcjonalności danej usługi oraz konfiguracji użytkownika - może wymagać ręcznego wybrania tej opcji przez użytkownika albo dokonywać się automatyczne, w z góry określonych odstępach czasu. Jeżeli istnieje lokalna kopia zapasowa danych, to zawiera ona wszystkie treści opublikowane przez użytkownika i niewykasowane, według stanu na moment jej utworzenia. W takim wypadku dane te mogą być dostępne także dla organów ścigania, z poziomu urządzenia użytkownika, po jego zabezpieczeniu.

Przykład. Komunikator WhatsApp oferuje funkcjonalność utworzenia kopii zapasowej. Może to być zarówno kopia lokalna, jak i kopia zapisywana na dysku sieciowym usługi powiązanej z WhatsAppem, przykładowo na Google Drive. Można wybrać również opcję cyklicznego tworzenia kopii zapasowej. Kopia taka zawiera historię komunikacji na czatach, wraz z dołączanymi do nich multimediami.

8 Znaczenie dowodowe informacji uzyskanych i zabezpieczonych przy pomocy oprogramowania typu web crawler i do przetwarzania big data

Wprowadzenie

Źródłem informacji o aktywnościach w sieci noszących znamiona czynów zabronionych, w tym przestępstw z nienawiści, mogą być nie tylko publikacje dostrzeżone przez przedstawicieli organów procesowych czy innych użytkowników internetu, ale również – na znacznie większą skalę – posty czy komentarze wyselekcjonowane przez tzw. ***crawlery***, tzn. roboty (boty) indeksujące.

Charakterystyka robotów indeksujących (web crawlerów)

Zadaniem *crawlerów* jest zautomatyzowane pozyskiwanie treści ze stron internetowych, co poprzedzone jest analizą danej strony. *Crawlery* stanowią podstawę działania wyszukiwarek internetowych, jednak nie jest to ich jedyne przeznaczenie – w zależności od celu, do którego dostosowany jest dany robot, może on zbierać określone kategorie danych. Przykładowo, popularny robot hunter.io przeszukuje witryny internetowe w celu pozyskania danych biznesowych, w szczególności adresów e-mail, które są na nich umieszczone, nie tylko w zakładce "kontakt", ale w jakimkolwiek zasobie danej strony. Wykorzystanie tego rodzaju wyspecjalizowanych ***crawlerów*** może pozwolić na osiągnięcie lepszych wyników niż w przypadku ograniczenia się do wyszukiwarki internetowej.

Pojęcie ***web crawler*** odnosi się do niezwykle szerokiej gamy narzędzi internetowych o różnych zastosowaniach. Są wśród nich zarówno rozwiązania niebudzące zastrzeżeń natury etycznej (zaprogramowane w taki sposób, by nie spowalniać działania stron, respektujące istniejące na danej witrynie wyłączenia określonych treści spod działania robotów internetowych), jak i narzędzia o niepożądanym działaniu (np. służące do rozprzestrzeniania spamu) czy wreszcie służące do popełniania przestępstw (w tym ***crawlery*** zbierające dane wrażliwe, jak numery kart płatniczych, niezabezpieczone zbiory loginów i haseł itp., czy służące spowolnieniu lub wyłączeniu działania danej strony w ramach ataku typu DDoS).

Analiza dużych zbiorów danych publikowanych w internecie opiera się w istotnym stopniu na działaniu robotów indeksujących. Niektóre z nich zostały stworzone w celu wyszukiwania treści wskazanych przez użytkownika na portalach społecznościowych czy forach internetowych. Łatwo więc wyobrazić sobie ich potencjalne wykorzystanie przez podmioty analizujące zasoby sieciowe pod kątem publikowania treści mających cechy mowy nienawiści, np. przez organizacje społeczne. W niniejszym opracowaniu przeanalizujemy możliwości i wyzwania związane z wykorzystaniem takich narzędzi w postępowaniu karnym. Jako przykład posłuży komercyjne narzędzie SentiOne.

Charakterystyka działania SentiOne

Omawiany produkt, należący do polskiej spółki SentiOne sp. z o.o., służy do monitorowania zasobów internetu (***social listening***), m. in. na potrzeby kampanii marketingowych czy działań z zakresu PR. Wykorzystując algorytmy uczenia maszynowego, bazujące na potężnych zasobach danych treningowych, narzędzie to pozwala m. in. na wyselekcjonowanie publikacji internetowych zawierających określone słowa kluczowe, a także na pogrupowanie ich według sentymentu wypowiedzi, rozróżniając wypowiedzi o charakterze pozytywnym, neutralnym i negatywnym.

Z oczywistych względów omówienie zastosowań biznesowych tego i podobnych narzędzi leży poza obszarem niniejszego opracowania. Nie ulega jednak wątpliwości, że może ono posłużyć także w celu wyszukiwania treści stanowiących przedmiot zainteresowania postępowań karnych.

Przykładowo, możliwe jest sprawdzenie występowania określonego hasła (np. „Polacy") w zakreślonych datach. Wynik wyszukiwania można zawęzić do określonych platform (Facebook, Instagram, X, TikTok czy Reddit) lub określonych kategorii stron, np. portale, fora, blogi, recenzje, video. Uzyskane wpisy można pogrupować według kategorii, np. ograniczając się w dalszej analizie do tych wypowiedzi, które zostały ocenione przez program jako nacechowane negatywnie. Należy przy tym mieć na względzie, że przyporządkowanie to może być niedoskonałe i błędnie klasyfikować wypowiedzi, dlatego w danym przypadku konieczne może być przeanalizowanie wszystkich wypowiedzi, zaś ocenę wyrażonego w nich sentymentu można traktować jedynie pomocniczo.

> Warto w tym miejscu podkreślić, że roboty indeksujące co do zasady zbierają jedynie treści publiczne, a zatem nie mają dostępu np. do wpisów publikowanych w zamkniętych grupach czy umieszczanych przez użytkowników stosujących ograniczenia widoczności wpisów.

Pracę z narzędziem SentiOne można zakończyć poprzez wygenerowanie raportu, zawierającego wyselekcjonowane wypowiedzi. Można wyobrazić sobie wykorzystanie takiego raportu przy składaniu

zawiadomienia o przestępstwie, polegającym na publikowaniu treści wyczerpujących znamiona przestępstw, np. określonych w art. 256 k.k., dlatego konieczne jest omówienie związanych z tym zagadnień praktycznych.

Wykorzystanie w postępowaniu karnym raportu z monitoringu sieci na przykładzie SentiOne

Raport może zawierać pełną treść danego wpisu, wraz z datą i godziną publikacji i oznaczeniem autora. O ile chodzi o artykuł prasowy czy wpis na blogu jako autor wskazana jest osoba podpisana pod danym tekstem. Raport może też wskazywać na brak danych o autorze. Natomiast w przypadku wpisu lub komentarza w mediach społecznościowych, prezentowana jest nazwa profilu, z którego opublikowano daną treść. Tweety umieszczane na platformie X są dodatkowo opatrzone zindywidualizowaną nazwą użytkownika.

Warto zwrócić uwagę, że pozyskiwanie danych przez oprogramowanie typu ***web crawler*** od platform społecznościowych najczęściej odbywa się z wykorzystaniem infrastruktury informatycznej dostarczanej wprost przez administratora takiej platformy na potrzeby przedsiębiorców zajmujących się analizą big data, takich jak przykładowo dostawca programu SentiOne. Dostęp do takich danych odbywa się zatem na zasadach typowych dla komercyjnej, biznesowej współpracy pomiędzy dwoma przedsiębiorcami. Dopuszczalność takiej współpracy administratorzy platform internetowych gwarantują sobie odpowiednimi postanowieniami regulaminów swoich usług.

Nie ulega wątpliwości, że raport może stanowić wstęp do dalszego zbierania materiałów na potrzeby postępowania karnego. Przykładowo, wyselekcjonowane w nim komentarze, tweety czy publikacje nawołujące do nienawiści na tle różnic narodowościowych mogą zostać następnie odszukane na stronach źródłowych. Zawiadamiający bądź przedstawiciel organu procesowego może zapoznać się z zawartością danego profilu na platformie społecznościowej i potwierdzić, że dany wpis istnieje, co będzie prowadziło do dalszych czynności dowodowych, ukierunkowanych na utrwalenie treści tego wpisu oraz na ustalenie tożsamości osoby, która go opublikowała. W takiej sytuacji raport wygenerowany z wykorzystaniem SentiOne stanowi przede wszystkim punkt wyjścia do zebrania dowodów, które będą pochodziły ze stron źródłowych, dlatego nawet w razie uznania przez organ procesowy, że dokument prywatny w postaci raportu nie może stanowić podstawy ustaleń faktycznych, spełni on swoją rolę, gdyż zostanie potraktowany nie jako dowód, jako informacja o dowodach, które następnie zostaną uzyskane z właściwych platform.

Zupełnie inaczej wygląda sytuacja, gdy okaże się, że dany wpis figurujący w raporcie został usunięty jeszcze zanim zabezpieczono go w jakikolwiek inny sposób na potrzeby postępowania karnego.

Należy rozstrzygnąć kwestię, czy jeżeli raport wygenerowany z SentiOne będzie stanowił jedyne potwierdzenie, że na danym profilu opublikowano określoną treść, może to stanowić wystarczający dowód takiego faktu.

Odpowiadając na to pytanie, w pierwszej kolejności trzeba raz jeszcze odwołać się do obowiązującej w polskim porządku prawnym zasady swobodnej oceny dowodów, wynikającej z art. 7 k.p.k.:

Organy postępowania kształtują swe przekonanie na podstawie wszystkich przeprowadzonych dowodów, ocenianych swobodnie z uwzględnieniem zasad prawidłowego rozumowania oraz wskazań wiedzy i doświadczenia życiowego.

Zasada swobodnej oceny dowodów stanowi jeden z filarów polskiej procedury karnej, a omówieniu art. 7 k.p.k. poświęcono liczne monografie i fragmenty komentarzy. Jego wykładnia uwzględnia też bardzo bogate orzecznictwo sądów. Nie sposób streścić całego tego dorobku naukowego i orzeczniczego w kilku zdaniach na potrzeby niniejszej publikacji. Konieczne jest jednak odniesienie omawianej zasady do możliwości wykorzystania konkretnego dowodu, jaki miałby stanowić raport wygenerowany z użyciem narzędzia SentiOne czy też jakikolwiek analogiczny dokument, obrazujący rezultat działania robotów indeksujących.

Po pierwsze więc, raport taki może stanowić dowód w postępowaniu karnym, podobnie jak niemal każdy inny przedmiot czy zapis treści (z pewnymi wyłączeniami, określonymi m. in. w k.p.k., leżącymi poza przedmiotem tego opracowania). Dopuszczalność tego rodzaju dowodu w procedurze karnej potwierdza art. 393 § 3 k.p.k., zgodnie z którym możliwe jest odczytywanie na rozprawie sądowej wszelkich tzw. "dokumentów prywatnych", a zatem powstałych poza postępowaniem, wytworzonych przez podmioty prywatne.

Jeżeli raport zostanie uzyskany w toku postępowania (np. dostarczony prokuratorowi przez zawiadamiającego), podlega ocenie, której dokonuje organ procesowy: na etapie dochodzenia lub śledztwa – prokurator lub policjant, względnie przedstawiciel innej służby, zaś na etapie postępowania jurysdykcyjnego - sąd. W ramach tej oceny organ będzie ustalał między innymi, czy dany dowód został uzyskany w sposób legalny, czy jego wiarygodność nie budzi wątpliwości oraz jakie ustalenia faktyczne można w oparciu o niego poczynić (innymi słowy, co wynika z tego dowodu). Legalność dowodu w postaci omawianego raportu nie powinna budzić żadnych wątpliwości – stanowi on bowiem zestawienie treści publikowanych w internecie, bez jakichkolwiek ograniczeń dostępu dla osób trzecich. Należy jednak poświęcić więcej uwagi dwóm pozostałym zagadnieniom.

Czy wiarygodność raportu nie budzi wątpliwości?

Innymi słowy, czy w przypadku, gdy oryginalne treści zostały bezpowrotnie usunięte i nie ma możliwości uzyskania ich żadną inną drogą, raport stanowiący rezultat działania ***crawlera*** może stanowić dowód na to, że na danym profilu/stronie zamieszczono określoną treść?

W ocenie autorów opracowania należy na to pytanie udzielić odpowiedzi twierdzącej, z zastrzeżeniem jednak, że dopiero całokształt okoliczności danej sprawy będzie determinował możliwość wykorzystania danego dowodu do czynienia ustaleń faktycznych, czyli do stwierdzenia, jaki był przebieg istotnych zdarzeń, które bada się w postępowaniu karnym.

Raport zawiera treści pobrane w zautomatyzowany sposób z publicznie dostępnych profili społecznościowych i witryn internetowych. Treści te nie są w żaden sposób modyfikowane – skracane, uzupełniane czy edytowane. Wykorzystanie algorytmów sztucznej inteligencji w generowaniu raportu również nie ma żadnego wpływu na ocenę autentyczności jego treści, bowiem służy ono wyłącznie selekcjonowaniu treści oraz ich kategoryzowaniu pod względem tego, jaki sentyment wyraża dana wypowiedź (negatywny, neutralny czy pozytywny). Oczywiście to, w jaki sposób algorytm klasyfikuje daną wypowiedź, jest całkowicie bez znaczenia dla ustaleń w toku postępowania. Organ procesowy będzie samodzielnie dokonywał oceny, jaka była intencja autora wpisu, i to jego zadaniem będzie np. dostrzeżenie, że dany wpis ma charakter ironiczny czy prześmiewczy, co mogło nie zostać odzwierciedlone w raporcie.

Mierząc się z potencjalnymi problemami, jakie mogą wyniknąć w toku postępowań karnych, warto pochylić się nad zagadnieniem, czy organ procesowy powinien przedsięwziąć jakiekolwiek dodatkowe czynności, by ustalić, że treści generowane w raporcie nie zostały zmodyfikowane. Przykładowo, czy nie jest konieczne przeanalizowanie działania algorytmów, w oparciu o które działa SentiOne, by stwierdzić, że ograniczają się one do pobierania treści, bez ich modyfikowania? Czy nie jest w tym celu konieczne zasięgnięcie opinii biegłego, który zbada cały proces generowania raportu i wypowie się w kwestii niezmienności treści do niego pozyskiwanych?

Trzeba w tym miejscu zauważyć, **że powszechną praktyką organów procesowych jest opieranie ustaleń o rozwiązania techniczne, których organy te nie znają i nie rozumieją. Stwierdzenie to nie ma wbrew pozorom charakteru krytycznego, odnosi się raczej do specyfiki funkcjonowania w otoczeniu dynamicznego rozwoju technologii informacyjnej.** Przykładowo, w toku danego postępowania może zostać ustalone, że na określoną skrzynkę e-mail przesłano istotną w danym procesie wiadomość z innej skrzynki. Organ procesowy podejmie działania, aby ustalić, że wiadomość taka

faktycznie dotarła do adresata (np. dokona oględzin jego skrzynki e-mail), i że adres nadawcy wiadomości nie budzi wątpliwości (np. zbada nagłówek rozszerzony bądź, jeśli ma taką możliwość, zapozna się ze skrzynką, z której wiadomość została nadana). Jeśli konkluzje tych czynności będą jednoznaczne, organ poczyni ustalenie faktyczne, że ze skrzynki "A" przesłano wiadomość określonej treści na skrzynkę "B". Można jednak przyjąć za pewnik, że w niemal wszystkich przypadkach przedstawiciel organu procesowego (np. policjant, prokurator czy sędzia) ma bardzo ograniczoną (lub żadną) wiedzę w zakresie tego, jakie rozwiązania techniczne zastosowano, by wiadomość nadana z jednego konta dotarła w niezmienionej postaci do innego konta. Zarazem nie są autorom znane przypadki, aby organ procesowy powziął wątpliwość w tym zakresie, tj. by – bez wystąpienia szczególnych okoliczności – miał wątpliwość co do tego, że treść wiadomości dociera od nadawcy do odbiorcy w niezmienionej formie. Wątpliwości organu nie dotyczą rozwiązań technicznych stosowanych przez administratorów poczty elektronicznej, a zupełnie innych zagadnień, np. tego, czy możliwe jest ustalenie, kto posługiwał się kontem e-mail nadawcy w czasie wysłania e-maila.

Przykład ten, jak każda analogia, ma pewne słabości. Nie w każdym elemencie odpowiada on sytuacji poddawanej analizie, tj. kwestii niezmienności treści publikowanych w raporcie SentiOne. W szczególności trzeba mieć na względzie, że poczta elektroniczna jest na co dzień wykorzystywana przez przeważającą część populacji, zatem przedstawiciel organu procesowego, choćby nie miał wiedzy o zastosowanych rozwiązaniach technicznych, zna zasadę jej działania z własnego doświadczenia. Nie można tego powiedzieć o stosowaniu ***crawlerów*** pozyskujących dane z portali społecznościowych – nie jest to technologia na tyle rozpowszechniona, by przeciętny przedstawiciel organów procesowych miał jakiekolwiek zdanie na jej temat. Z drugiej jednak strony podobnych przykładów można sformułować bardzo wiele, np. jeśli na profilu społecznościowym zostało zamieszczone określone zdjęcie, przyjmuje się, że osoba mająca (uprawniony bądź nieuprawniony) dostęp do danego profilu umieściła to zdjęcie; jeśli dana osoba figuruje jako kontakt innej osoby w określonym komunikatorze, przyjmuje się, że musiała przez nią zostać dodana do kontaktów. W żadnym z tego typu przypadków organy procesowe nie podejmują decyzji o zasięgnięciu opinii biegłego, aby rozwiać ewentualne wątpliwości wynikające z braku wiedzy o technicznych rozwiązaniach stosowanych w danej aplikacji.

Warte rozważenia byłoby natomiast wystąpienie (przez zawiadamiającego bądź organ procesowy) do administratora lub twórcy danego programu, generującego omawiane raporty, z zapytaniem o kwestie budzące wątpliwości organu, np. o to, czy treści znajdujące się w raportach są w jakikolwiek sposób modyfikowane. Uzyskanie odpowiedzi, w miarę możliwości popartej opisem zastosowanych rozwiązań technicznych, powinno być wystarczające do potwierdzenia tej kluczowej kwestii.

Jakie ustalenia można poczynić w oparciu o raport?

W zależności od wybranego pakietu usług, SentiOne oferuje analizę danych historycznych sięgających do 3 lat wstecz. Zarazem opóźnienie w zbieraniu danych jest bardzo niewielkie, tj. ***crawler*** może umieścić w raporcie wpisy opublikowane zaledwie kilka sekund wcześniej. Oznacza to, że o ile dany wpis zawiera wskazane przez użytkownika słowo kluczowe, był dostępny publicznie i był zamieszczony w jakimkolwiek momencie na przestrzeni trzech lat przed wygenerowaniem raportu (choćby nawet został krótko potem usunięty), co do zasady powinien w nim zostać uwzględniony. Z doświadczeń użytkowników wynika, że możliwe są rezultaty fałszywie negatywne, tj. że raport nie obejmuje jakiegoś wpisu, który był dostępny w okresie objętym monitoringiem, natomiast nie ma możliwości, by w raporcie wystąpiły rezultaty fałszywie pozytywne, tj. by obejmował on wpisy czy publikacje, które w rzeczywistości nie były zamieszczone przez danego użytkownika. Ta ostatnia cecha raportów ma kluczowe znaczenie dla ich przydatności w postępowaniu karnym, bowiem stwierdzenie, że raporty mogą dostarczać błędnych wyników, wykluczałoby możliwość stosowania raportu jako samodzielnego dowodu na fakt opublikowania określonej treści. Takich konsekwencji nie niesie ze sobą sporadyczne pominięcie w raportach niektórych wpisów usuniętych przez autora, które może być wynikiem specyfiki działania crawlerów.

W ten sposób raport pozwala nie tylko na zautomatyzowane wyszukanie treści spełniających określone kryteria, ale też ułatwia osadzenie ich w kontekście. **Możliwe jest wykorzystanie omawianego narzędzia do analizy poszczególnych profili, dzięki czemu można łatwo wykazać, że dana treść publikowana na określonym profilu, nosząca cechy mowy nienawiści, nie ma charakteru incydentalnego, lecz towarzyszy jej wiele treści o podobnym charakterze. Rezultat ten można osiągnąć również poprzez ręczne sprawdzenie zawartości profilu (crawler nie ujawnia żadnych treści, które nie są dostępne dla postronnego użytkownika danej platformy), jednak wykorzystanie narzędzi analitycznych pozwala przyspieszyć ten proces**. Ma to znaczenie zwłaszcza w przypadku, gdy na analizowanym profilu zamieszczane są bardzo liczne wpisy.

Narzędzia analityczne, takie jak SentiOne, **pozwolą również na sprawniejsze dostrzeganie zależności pomiędzy różnymi profilami, co może przyczynić się do ustalenia, że są one administrowane przez ten sam podmiot lub przez osoby działające w porozumieniu lub według tego samego planu czy wytycznych**. Przykładowo, wyszukanie określonych słów kluczowych po zawężeniu okresu objętego analizą wykaże, że w krótkim czasie na różnych profilach opublikowano bardzo zbliżone treści. Powinno to stanowić impuls do dalszych badań, które mogą wykazać, że taka sytuacja (powielanie treści w niewielkim odstępie czasowym na wielu kontach) ma miejsce regularnie, co może prowadzić do wniosku, że profile te są powiązane, np. osobowo.

Tego rodzaju obserwacje będą miały istotne znaczenie w postępowaniu karnym, w którym zawsze niezbędne jest ustalenie zamiaru i motywacji sprawcy danego czynu. W każdym przypadku będzie ona miała wpływ na szkodliwość społeczną tego czynu, co przekłada się też na wymiar ewentualnej kary. Co więcej, w niektórych przypadkach ustalenie celu działania sprawcy decyduje o tym, czy określony czyn stanowi przestępstwo. Przykładowo, publiczne propagowanie ideologii nazistowskiej czy komunistycznej stanowi przestępstwo z art. 263 § 1a k.k. tylko wtedy, gdy ma na celu wpływanie na życie polityczne lub społeczne. Wreszcie warto przypomnieć, że większość czynów określonych w kodeksie karnym stanowi przestępstwo tylko wtedy, gdy zostaną popełnione umyślnie. Dlatego ustalenie kontekstu wypowiedzi, ujawnienie innych przykładów publikowania podobnych treści czy wykazanie działania w porozumieniu z inną osobą umieszczającą tożsame wpisy może mieć decydujące znaczenie dla skutecznego przeprowadzenia postępowania karnego.

Zarazem jednak trzeba pamiętać, że raport (przyjmując argumentację przedstawioną w poprzednim podrozdziale co do autentyczności wpisów wyszczególnionych w raporcie) dowodzi tylko jednej rzeczy, a mianowicie tego, że na określonym profilu w określonej dacie umieszczono wpis o określonej treści. W żadnym wypadku nie jest to wystarczające do stwierdzenia, że dana osoba dopuściła się przestępstwa, nawet jeżeli dany profil w sposób niebudzący żadnych wątpliwości można powiązać z określoną osobą. Postępowanie karne będzie bowiem wymagało rozprawienia się z potencjalnymi trudnościami, które w zależności od stanu faktycznego mogą polegać m. in. na:

- wykluczeniu wersji, że wpis został umieszczony przez inną osobę niż ustalony posiadacz konta (choć warto wspomnieć, że samo udostępnienie innej osobie swojego konta w celu umożliwienia jej opublikowania wpisu o znamionach przestępstwa można traktować jako pomocnictwo do przestępstwa, a w pewnych warunkach nawet jako współsprawstwo);

- ustaleniu, że posiadacz konta nie utracił do niego dostępu np. wskutek ataku hakerskiego (nie jest to zagrożenie wyłącznie teoretyczne - autorom niniejszego opracowania znane są postępowania karne prowadzone w związku z wpisami w mediach społecznościowych, co do których ustalono następnie, że zostały umieszczone po przełamaniu lub ominięciu zabezpieczeń do konta w tym celu, by skierować postępowanie karne przeciwko posiadaczom tych kont);

- wykazaniu w sposób niebudzący wątpliwości, że dane konto jest prowadzone przez określoną osobę; trzeba przy tym brać pod uwagę wariant, że utworzenie konta, a nawet jego prowadzenie przez dłuższy czas, mogło stanowić wyrafinowaną prowokację, ukierunkowaną na utratę reputacji przez daną osobę, a nawet na skierowanie przeciwko niej postępowania karnego.

> Autorom publikacji znany jest przykład utworzenia fałszywego profilu funkcjonariusza publicznego, opatrzonego jego imieniem, nazwiskiem i zdjęciem, na którym publikowano przez pewien czas treści mające wykazać jednoznacznie, że ich autorem jest ww. funkcjonariusz, a następnie rozpoczęto publikowanie treści o charakterze rasistowskim. Działanie to nie doprowadziło do skierowania postępowania karnego przeciwko ww. osobie, natomiast w istotny sposób zaszkodziło jej reputacji.

Postępowanie karne wymaga oczywiście rozstrzygnięcia wielu innych wątpliwości, w tym dotyczących stanu świadomości sprawcy, jego motywacji, stanu jego poczytalności i in., co jednak leży poza zakresem niniejszego opracowania. Dane zawarte w raporcie z monitoringu internetu mogą więc znacząco przyczynić się do ustalenia, jakie treści zostały opublikowane na danym profilu, jednak jest to zaledwie punkt wyjścia do dalszych ustaleń, które finalnie mogą skutkować przypisaniem przestępstwa określonej osobie.

Na zakończenie tej części opracowania warto wrócić raz jeszcze do zasadniczego pytania - czy wiarygodność raportu nie budzi wątpliwości? Jak wskazano, odpowiedź na nie jest zdaniem autorów twierdząca, jednak tylko z uwzględnieniem realiów konkretnej sprawy. O ile bowiem nie budzi wątpliwości to, że raport dostarczany przez SentiOne lub inne narzędzia monitorujące nie zmienia treści pobranych przez roboty indeksujące (a więc odzwierciedla rzeczywistą treść postów czy komentarzy), to trudno wyobrazić sobie sytuację, w której pojedynczy wpis, znajdujący się w raporcie z monitoringu, usunięty z danej witryny przed jego procesowym zabezpieczeniem, mógłby stanowić jedyny i wystarczający dowód do przedstawienia zarzutów danej osobie. Konieczne jest bowiem rozprawienie się ze wszystkimi wątpliwościami, pojawiającymi się na drodze pomiędzy zawiadomieniem o przestępstwie a wydaniem wyroku, z których zaledwie część opisano wyżej, a które niezwykle trudno byłoby rozwiać wyłącznie w oparciu o raport z monitoringu sieci.

Czynności organu procesowego po zapoznaniu się z raportem

Jak już sygnalizowano, kodeks postępowania karnego przewiduje bardzo niewiele ograniczeń w zakresie dopuszczalności dowodów i można w pewnym uproszczeniu wskazać, że niemal wszystkie materiały, które zawiadamiający jest w stanie przedstawić organowi procesowemu lub które organ procesowy jest w stanie legalnie uzyskać, będą mogły zostać zaliczone do materiału dowodowego (wyłączenia od tej zasady przewidują m. in. art. 171, art. 174, art. 178 i art. 178a k.p.k.). Dowodem może więc być raport z monitoringu mediów, zawierający treść publikacji internetowej, zrzut ekranu zawierający komentarz umieszczony na portalu społecznościowym, a nawet zeznanie świadka, który zrelacjonuje,

że przeczytał na danym portalu komentarz o określonej treści. Przepisy nie przewidują gradacji dowodów i nie sposób w oderwaniu od realiów konkretnej sprawy stwierdzić, że dana kategoria dowodów przeważy nad dowodami z innej kategorii.

Zarazem jednak każdy dowód może zostać uznany przez organ procesowy za nieprzydatny – choć dopuszczalny – jeśli na jego podstawie nie będzie można w sposób niebudzący wątpliwości czynić ustaleń faktycznych. Przykładowo, wspomniany zrzut ekranu może zostać zakwestionowany przez użytkownika danego profilu, który stwierdzi, że nigdy nie publikował takiej treści. Jeśli zrzut ekranu, przedstawiający zasadniczo bardzo niską wartość z uwagi na możliwość jego samodzielnego wytworzenia czy manipulacji autentycznym zrzutem, będzie jedynym dowodem na potwierdzenie, że dany komentarz faktycznie został opublikowany, należy przypuszczać, że sąd nie uzna takiego dowodu za wystarczający do stwierdzenia tego faktu. Innymi słowy, choć niemal każdy dowód jest dopuszczalny, to nie każdy przedstawia jakąkolwiek wartość w postępowaniu karnym. Jeżeli inny uczestnik postępowania (lub sąd, działając z urzędu) jest w stanie podważyć wiarygodność danego dowodu lub możliwość wyciągnięcia z niego określonych wniosków, może on pozostać bez żadnego wpływu na ustalenia faktyczne.

Poniżej zostaną zawarte porady, w jaki sposób można wzmocnić dowody, które zostaną wprowadzone do postępowania karnego, tak by zmniejszyć ryzyko ich podważenia i ułatwić wyciąganie na ich podstawie bardziej jednoznacznych wniosków.

Oględziny dokonane przez organ procesowy

Naturalnym dążeniem policjanta czy prokuratora po uzyskaniu informacji, że na określonej stronie internetowej znajduje się treść o znamionach przestępstwa, jest zweryfikowanie tego poprzez odwiedzenie tej strony. Wyłączając oczywiście przypadki, gdy uruchomienie danej witryny mogłoby np. rozpocząć pobieranie złośliwego oprogramowania, takie podejście należy uznać za prawidłowe, nie tylko ze względu na możliwość wstępnej weryfikacji informacji, uzyskanych zwykle z zawiadomienia o przestępstwie, ale też dlatego, że konieczne może się okazać podjęcie działań w celu zablokowania danej witryny.

Po stwierdzeniu, że na badanej stronie faktycznie znajdują się treści istotne dla postępowania karnego, funkcjonariusz zwykle przystępuje do oględzin, tj. zapoznaje się z wyglądem strony, jednocześnie sporządzając protokół, w którym określa czas, miejsce i warunki, w których dokonuje czynności, a także dokumentuje, jakie treści widoczne są po wprowadzeniu określonego adresu URL czy wybraniu określonego hiperłącza. Czynność taka może zostać również potraktowana jako eksperyment

procesowy, o którym mowa w art. 211 k.p.k. stanowiący pewnego rodzaju doświadczenie - co wydarzy się, gdy zaistnieją określone warunki. Z punktu widzenia wartości dowodowej to, czy potraktuje się daną czynność jako oględziny czy eksperyment, jest w tej sytuacji drugorzędne.

Działanie to może wydać się osobom niemającym styczności z postępowaniem karnym archaiczne i zbyteczne, przez co powoduje komentarze na temat "przepisywania internetu" itp. Faktycznie, automatyzm w działaniu organu procesowego w dokonywaniu oględzin prowadzi czasami do marnotrawienia czasu i daje kuriozalny efekt, np. wtedy, gdy protokół zawiera dokładny opis strony startowej popularnego serwisu społecznościowego czy wymienia wszystkie zakładki, choćby nie miały one żadnego znaczenia dla postępowania - takie zachowanie wynika najprawdopodobniej z traktowania oględzin strony internetowej tak jak oględzin rzeczy, co standardowo obejmuje opisanie wszystkich jej cech fizycznych.

Zarazem jednak w ocenie autorów praktyka protokolarnego potwierdzania, że dana strona zawiera określone treści, jest zasadniczo prawidłowa i pozwala na wyeliminowanie problemów, które mogą pojawić się w razie zaniechania takiej czynności procesowej jak eksperyment czy oględziny. Trzeba też mieć na względzie nakaz wynikający z art. 207 k.p.k., który stanowi, że w razie potrzeby dokonuje się oględzin miejsca, osoby lub rzeczy.

Przeprowadzenie czynności, w której protokolarnie stwierdzony zostaje fakt umieszczenia danej treści na stronie internetowej, pozwala na wytworzenie dokumentu urzędowego, który stanowi dowód tego, co zostało w nim urzędowo stwierdzone. Organ procesowy w sposób niezależny od stron postępowania stwierdza, czy dana treść faktycznie została umieszczona na określonej witrynie. Podważenie takiego dowodu jest niezwykle trudne i wymagałoby np. wykazania, że w czasie oględzin omyłkowo wprowadzono błędny adres, skorzystano z linku dostarczonego przez zawiadamiającego zamiast samodzielnego wyszukania strony bądź że z innych racjonalnych względów organ w rzeczywistości nie zweryfikował autentyczności zawiadomienia. Może tak się stać np. w przypadku, gdy oględziny mają charakter bardzo pobieżny i przedstawiciel organu ograniczy się do stwierdzenia w protokole, że na danej stronie faktycznie widnieją treści opisane w zawiadomieniu, jednak nie przytoczy ich ani nie udokumentuje w żaden sposób, np. poprzez wykonanie kopii danej witryny. Jeśli zawiadomienie dotyczy licznych, obszernych wpisów, taki sposób sporządzenia protokołu oględzin nie jest wystarczający do wykluczenia wątpliwości co do tego, jakie treści zostały umieszczone na analizowanej stronie. Prawidłowo przeprowadzone oględziny potwierdzą natomiast tę okoliczność, mającą fundamentalne znaczenie w postępowaniach o przestępstwa związane z mową nienawiści.

Skoro oględziny (lub eksperyment procesowy) mają tak istotne znaczenie w omawianych postępowaniach, rodzi się pytanie - czy w razie odstąpienia od nich postępowanie nie może być prowadzone? A w konsekwencji, czy jeśli dana treść została usunięta z internetu zanim organ procesowy protokolarnie stwierdził jej zamieszczenie na stronie, prowadzenie postępowania w sprawie takiego wpisu nie będzie możliwe?

Na oba te pytania należy odpowiedzieć przecząco, powołując się po raz kolejny na zasadę swobodnej oceny dowodów. **Jeśli zgromadzone w toku postępowania dowody będą wystarczające do jednoznacznego stwierdzenia, że wpis o znamionach przestępstwa został opublikowany, a przy tym znany będzie jego autor, pociągnięcie go do odpowiedzialności karnej będzie możliwe także wtedy, gdy oględziny nie zostaną przeprowadzone. Nie można abstrakcyjnie określić, jakie dowody powinny być zebrane, by w danej sprawie materiał dowodowy nie budził wątpliwości, gdyż zależy to od okoliczności konkretnego przypadku.** Można jednak zastosować jeden lub więcej z opisanych niżej sposobów (lub jakichkolwiek innych legalnych metod prowadzących do osiągnięcia tego samego celu), by wzmocnić materiał dowodowy. Część z poniższych rozwiązań jest dostępna tylko organowi procesowemu (jak uzyskanie informacji od administratora strony), część może zostać przeprowadzona zarówno przez zawiadamiającego, jak i przez organ, zaś część - jak sporządzenie protokołu notarialnego - nigdy nie będzie przeprowadzana przez organ procesowy, natomiast może z nich skorzystać zawiadamiający.

Uzyskanie informacji od administratora witryny

W zależności od tego, na jakiej stronie internetowej umieszczono określoną treść, może istnieć możliwość uzyskania przez organ procesowy od jej administratora dokładnej zamieszczonej treści (artykułu, posta, komentarza, grafiki itp.), wraz ze szczegółowymi danymi dotyczącymi użytkownika, który ją opublikował, takimi jak adres IP, login, adres e-mail itp. Podważenie przez przeciwnika procesowego takiej informacji, uzyskanej od niezależnego podmiotu, jakim jest administrator strony, byłoby z pewnością niezwykle trudne. Szczegółowe omówienie informacji, które są możliwe do uzyskania w zależności od platformy, na której opublikowano daną treść, znajduje się w rozdziale ***Rodzaj i zakres danych przetwarzanych przez platformy internetowe, w tym dostawców "mediów społecznościowych".***

Wykonanie kopii strony

Wykorzystując metody opisane w poprzednim rozdziale, można utworzyć plik stanowiący kopię strony. Wydaje się, że utworzenie kopii lustrzanej będzie przedstawiało większą wartość dowodową niż np. zapisanie strony w postaci pliku PDF, ze względu na to, że zachowanie w kopii lustrzanej dokładnej

struktury kopiowanej strony i pobranie wszystkich jej katalogów daje większe możliwości weryfikacji autentyczności takiej kopii niż ma to miejsce w przypadku pojedynczego pliku. Warto wskazać, że działanie to nie wymaga posiadania jakichkolwiek uprawnień i dlatego nie jest zastrzeżone dla organu procesowego, zatem warto zadbać o utworzenie kopii już na etapie składania zawiadomienia o przestępstwie.

Wayback Machine

Jednym z fascynujących zasobów internetu, mogącym znaleźć zastosowanie w postępowaniu karnym, jest archiwum cyfrowe Wayback Machine, prowadzone przez organizację non-profit Internet Archive, dostępne pod adresem archive.org. Ideą, jaka przyświecała twórcom tego narzędzia było zapobieganie utracie treści publikowanych w internecie, do których nie ma dostępu po edycji strony lub jej zamknięciu. Jego działanie opiera się na ***web crawlerach***, które regularnie indeksują ogólnodostępne treści, archiwizując w ten sposób zasoby internetu. Dotychczas zgromadzono ponad 100 petabajtów danych, dzięki którym możliwe jest np. sprawdzenie, jak zmieniał się wygląd i zawartość danej strony na przestrzeni lat. Może się więc okazać, że dana strona nie jest już dostępna, jednak jej zapis (w zakresie, w jakim strona nie uniemożliwiała działania robotów indeksujących) widnieje w Wayback Machine. W pewnych warunkach może więc być to sposób na odzyskanie treści, która została już usunięta, a która ma kluczowe znaczenie w postępowaniu karnym. Z tych względów przedstawiciele Policji i prokuratury dość powszechnie wykorzystują to narzędzie w swojej pracy.

Trzeba jednak podkreślić, że częstotliwość automatycznego zapisu danej strony może być niewielka, co więcej, w przypadku serwisów społecznościowych zapisanie kopii danego portalu nie prowadzi do zapisania kopii całej jego zawartości, w tym wszystkich postów widocznych publicznie, gdyż w bardzo krótkim czasie doprowadziłoby to do zwielokrotnienia zapisanych danych. Szansa, że w archiwum została zapisana strona zawierająca dokładnie ten post, który stanowi przedmiot zawiadomienia, jest niewielka.

> Serwis archive.org daje jednak możliwość samodzielnego wskazania strony do zapisania (funkcjonalność ta dostępna jest pod adresem https://web.archive.org/save). W ten sposób treść zostanie zabezpieczona przed usunięciem, bowiem możliwości podważenia wiarygodności zapisanej w ten sposób wersji strony są bardzo niewielkie - autorom nie są znane przypadki kwestionowania w postępowaniach karnych danych uzyskanych za pomocą Wayback Machine.

Notarialne poświadczenie treści strony

Jedną z metod zabezpieczenia treści zamieszczonych w sieci jest sporządzenie przez notariusza protokołu z otwarcia strony internetowej. W ten sposób powstaje dokument urzędowy, stwierdzający dokładną treść dostępną w chwili jego sporządzania, co należy uznać za metodę budzącą mniejsze wątpliwości niż samodzielne zabezpieczenie treści przez zawiadamiającego. Zarazem jednak praktyczne wykorzystanie tego instrumentu w postępowaniu karnym jest znikome - jest to rozwiązanie przyjęte raczej w postępowaniu cywilnym. Protokół notarialny nie ma bowiem żadnej przewagi nad protokołem sporządzonym przez organ procesowy, o ile ten ostatni został sporządzony wystarczająco starannie, co omówiono wyżej w tym rozdziale. Rozwiązanie w postaci notarialnego poświadczenia treści strony mogłoby zostać wykorzystane np. w sytuacji, gdy zawiadamiający spodziewa się, że treść może zostać usunięta jeszcze zanim zdąży on złożyć zawiadomienie o przestępstwie lub zanim zostaną przeprowadzone oględziny. Trzeba też brać pod uwagę, że organ procesowy może poddać stronę oględzinom z pewnym opóźnieniem, a zawiadamiający co do zasady nie ma wpływu na to, kiedy policjant czy prokurator przeprowadzi daną czynność.

Inne sposoby zabezpieczenia treści strony internetowej

Odwołując się po raz kolejny do zasady swobodnej oceny dowodów można stwierdzić, że do tego celu nadaje się każdy sposób, który sprawi, że zgodnie z zasadami prawidłowego rozumowania oraz wskazaniami wiedzy i doświadczenia życiowego będzie można uznać fakt umieszczenia danej treści na danej stronie za udowodniony. Przypuszczalnie osoby mające dużą wiedzę z zakresu technik informatycznych będą w stanie optymalnie dobrać narzędzie do potrzeb, wydaje się też, że w przyszłości możliwe byłoby wykorzystanie do takiego celu możliwości, jakie daje blockchain. **Jednak również sposoby niewymagające żadnego przygotowania technicznego mogą pozwolić na wzmocnienie materiału dowodowego, choćby w ten sposób, że zawiadamiający dokona nagrywania ekranu podczas uruchamiania danej strony (w urządzeniach z systemem Windows opcja dostępna jest standardowo pod skrótem klawiaturowym Windows+G), a nawet zarejestruje ekran kamerą czy uruchomi stronę w obecności świadków, którzy zapoznają się z nią, a ich zeznania będą stanowiły dowód uzupełniający kopię strony internetowej.** W ocenie autorów żadne z tych działań nie jest wymagane, aby zawiadomienie można było uznać za odpowiednio udokumentowane - wyliczenie tych pomysłów ma raczej na celu uświadomienie czytelnikowi, że katalog dowodów w postępowaniu karnym jest otwarty i jeśli zawiadamiający ma pomysł, choćby niestandardowy, jednak dopasowany do realiów konkretnej sprawy, na wzmocnienie materiału dowodowego, warto z niego skorzystać.

9 Zasady formułowania wniosków dowodowych

Wprowadzenie

W postępowaniu karnym wiele dowodów przeprowadza się z urzędu[29]. Oznacza to, że prokurator, policjant, sąd czy też inny organ prowadzący konkretne postępowanie na danym etapie samodzielnie decyduje o tym, aby pozyskać dany dowód.

Nie wyklucza to inicjatywy dowodowej stron postępowania, a wręcz przeciwnie. Strony mają prawo składać wniosku o przeprowadzenie dowodu[30], a organ procesowy (sąd, prokurator, policjant) ma obowiązek do takich wniosków się ustosunkować.

Kto w praktyce może złożyć wniosek dowodowy? Kodeks przyznaje to prawo stronom. Na etapie postępowania przygotowawczego (czyli przed wniesieniem aktu oskarżenia do sądu, gdy toczy się śledztwo lub dochodzenie) za strony uznaje się: pokrzywdzonego i podejrzanego[31]. Na etapie postępowania sądowego (po wniesieniu aktu oskarżenia do sądu, a przed wydaniem prawomocnego wyroku) stronami postępowania są: oskarżony, prokurator oraz oskarżyciel posiłkowy[32].

Organizacja społeczna może - w zależności od sytuacji - mieć status pokrzywdzonego i wówczas przysługują jej prawa strony, w tym do składania wniosków dowodowych.

---

29 Zgodnie z zasadą działania z urzędu, określoną w art. 9 k.p.k.

30 Zgodnie z art. 167 k.p.k.

31 Zgodnie z art. 299 § 1 k.p.k.

32 Zgodnie z art. 45 § 1 k.p.k., art. 55 k.p.k., art. 367 k.p.k. Prokurator występuje przed sądem jako "oskarżyciel publiczny". Niekiedy jednak "oskarżycielem publicznym" może być inny organ, np. Krajowa Administracja Skarbowa (w sprawach dotyczących przestępstw podatkowych). Zamiast oskarżyciela publicznego może zaś występować oskarżyciel prywatny (w sprawach ściganych z oskarżenia prywatnego, jak np. w sprawie o zniesławienie czy znieważenie) lub oskarżyciel posiłkowy (w sytuacji dwukrotnego umorzenia lub dwukrotnej odmowy wszczęcia postępowania przez prokuratora).

Do kogo kierować wniosek dowodowy?

Wniosek dowodowy należy kierować do organy, który prowadzi postępowanie na danym etapie.

W postępowaniu przygotowawczym takim organem jest **jednostka Policji prowadząca dochodzenie lub śledztwo oraz prokurator, który je nadzoruje**[33] **.** Właściwie nie ma różnicy, czy wniosek złoży się do Policji prowadzącej postępowania, czy do prokuratora, który je nadzoruje[34] - w obu wypadkach powstanie obowiązek ustosunkowania się do tego wniosku.

W postępowaniu sądowym takim organem jest **sąd.**

Co musi zawierać wniosek dowodowy?

Wniosek dowodowy nie jest pismem zupełnie swobodnym. Powinien on zawierać następujące elementy:

1. określenie dowodu, który miałby być przeprowadzony (obowiązkowo);
2. wskazanie okoliczności, które miałyby być udowodnione (obowiązkowo; jest to tzw. teza dowodowa);
3. określenie sposobu przeprowadzenia dowodu (fakultatywnie - można, ale nie trzeba)[35];
4. uzasadnienie (fakultatywnie - nie trzeba go umieszczać, ale jest to pożądane)[36].

Przykład: wnoszę o przesłuchanie w charakterze świadka Jana Kowalskiego na okoliczność tego, jakie osoby w okresie obejmującym dzień 12 listopada 2024 r., godz. 16:45, miały dostęp do łącza internetowego dostarczanego przez Dostawcę Internetu S.A. dla Jana Kowalskiego pod adresem ul. Uliczna 1/1 w Warszawie. | Uzasadnienie: nieustalony dotychczas użytkownik portalu "X" opublikował w dniu 12 listopada 2024 r., o godz. 16:45, z konta użytkownika o nazwie @Ogien123456789, post zawierający nawoływanie do nienawiści na tle różnic rasowych, o treści "(...)". W toku postępowania stwierdzono, że użytkownik ten dokonał publikacji postu korzystając z adresu IP należącego do puli Dostawcy

33 Zamiast Policji mogą występować w określonych kategoriach spraw inne organy, np. Straż Graniczna, Agencja Bezpieczeństwa Wewnętrznego, Naczelnik Urzędu Celno-Skarbowego itp.

34 Choć w niektórych wypadkach prokurator w ogóle nie występuje. Dotyczy to dochodzenia, które zakończyło się umorzeniem i wpisaniem sprawy do rejestru przestępstw; innego dochodzenia na pierwszym jego etapie - gdy Policja (inny organ) nie powiadomiła jeszcze prokuratora o jego prowadzeniu; dochodzeń w sprawach karnych-skarbowych (podatkowych) prowadzonych przez Krajową Administrację Skarbową.

35 Zgodnie z art. 169 k.p.k.

36 W piśmie procesowym uzasadnienie umieszcza się "w miarę potrzeby" - zgodnie z art. 119 § 1 pkt 3 k.p.k. Dołączenie uzasadnienia do wniosku dowodowego jest zasadne. W uzasadnieniu można wyjaśnić, dlaczego prowadzenie konkretnego dowodu w danej sprawie jest konieczne i jakie informacje może przynieść.

Internetu S.A., który świadczył usługę dostępu do Internetu dla Jana Kowalskiego pod adresem ul. Uliczna 1/1 w Warszawie. W dalszej kolejności ustalono, że pod adresem tym mieści się prowadzone przez Jana Kowalskiego biuro co-workingowe, a dostęp do łącza internetowego mogą mieć wszystkie przebywające tam osoby. W celu zweryfikowania tożsamości autora wymienionego postu niezbędne jest w pierwszej kolejności ustalenie kręgu osób, które miały dostęp do łącza internetowego Jana Kowalskiego w wymienionym biurze. W dalszej kolejności możliwe będzie zidentyfikowanie rzeczywistego autora wymienionego postu.

Jak widać na powyższym w przykładzie - wniosek dowodowy może zmierzać do wykrycia innych źródeł dowodowych[37] , które dopiero doprowadzą do wyjaśnienia okoliczności istotnych dla sprawy (autorstwa kwestionowanego posta na portalu "X"). Dołączenie uzasadnienia do wniosku jest zasadne. Gdyby tego uzasadnienia nie było, to organowi procesowemu "łatwiej" byłoby oddalić wniosek dowodowy z taką argumentacją, że Jan Kowalski prowadzi biuro, do którego ma dostęp wiele osób, a zatem "nie da się" ustalić, kto konkretnie jest autorem posta. Wyjaśnienie, że wniosek zmierza właśnie do ustalenia tego kręgu osób, co jest warunkiem wyjściowym do wytypowania sprawcy przestępstwa dopiero w dalszej kolejności, czyni mniej prawdopodobną perspektywę oddalenia wniosku.

W jednym piśmie procesowym można zawrzeć jeden lub więcej wniosków dowodowych, a także inne wnioski, oświadczenia i stanowiska. W praktyce rzadko spotyka się sytuację, w której jedno pismo procesowe zawiera tylko jeden wniosek dowodowy.

Pismo procesowe zawierające wniosek dowodowy powinno być opatrzone własnoręcznym podpisem[38].

Formułowanie tezy dowodowej

Ważne jest, aby teza dowodowa sformułowana została w sposób konkretny. Powinna ona wskazywać konkretne okoliczności, których ustalenie ma być możliwe dzięki przeprowadzeniu dowodu.

<u>Nie</u> jest właściwe poprzestawanie na ogólnikowych stwierdzeniach takich jak:

Przykład (błędna praktyka!): wnoszę o dopuszczenie owodu (...) na okoliczności sprawy.

37 Wniosek dowodowy może zmierzać do wykrycia lub oceny właściwego dowodu - art. 169 § 2 k.p.k.

38 Zgodnie z art. 119 § 1 pkt. 4 k.p.k. Dotychczas w doktrynie postępowania karnego, jak też w praktyce jego stosowania, zasadniczo nie akceptuje się podpisów elektronicznych, cyfrowych, składanych za pomocą "Profilu zaufanego" lub tym bardziej skanów podpisów odręcznych.

Przykład (błędna praktyka!): wnoszę o dopuszczenie dowodu (...) na okoliczności przestępstwa będącego przedmiotem zawiadomienia.

Przykład (błędna praktyka!): wnoszę o dopuszczenie dowodu (...) na okoliczności wskazane w zawiadomieniu[39].

Prawidłową praktyką jest formułowanie konkretnych też dowodowych, takich jak:

Przykład: wnoszę o dopuszczenie dowodu (...) na okoliczność tego, jakie osoby w okresie obejmującym dzień 12 listopada 2024 r., godz. 16:45, miały dostęp do łącza internetowego dostarczanego przez Dostawcę Internetu S.A. dla Jana Kowalskiego pod adresem ul. Uliczna 1/1 w Warszawie.

Przykład: wnoszę o wystąpienie do (...) na okoliczność ustalenia, z wykorzystaniem jakiego adresu IP, numeru portu sieciowego, w jakiej dokładnie dacie i godzinie (z dokładnością co do sekundy) na koncie użytkownika @Ogien123456789 na portalu "X" opublikowany został post o treści (...) z dnia 12 listopada 2024 r., z godz. 16:45.

Przykład: wnoszę o wystąpienie do (...) na okoliczność ustalenia klienta (ze wskazaniem imienia, nazwiska, ewentualnie nazwy i pełnych danych adresowych i kontaktowych) korzystającego z adresu IP (...), nr portu sieciowego (...) w dniu 12 listopada 2024 r., o godz. 16:45:23, dostarczanego przez Dostawcę Internetu S.A.

Błędne lub niestaranne sformułowanie tezy dowodowej może doprowadzić do oddalenia wniosku dowodowego nawet, jeżeli jego uwzględnienie w danej sprawie byłoby merytorycznie zasadne.

Jak organy ścigania postępują z wnioskiem dowodowym?

Jeżeli prokurator, policjant czy sąd **uwzględnia wniosek dowodowy, to nie ma obowiązku wydawać w tej kwestii żadnego formalnego rozstrzygnięcia**[40]**.** Niewydanie żadnego rozstrzygnięcia nie narusza w tym wypadku przepisów procedury karnej.

39 Ewentualnie odwołanie się do konkretnego fragmentu pisma procesowego, który zawierałby skonkretyzowaną tezę dowodową, mogłoby być poprawne. Jednak ogólnikowe odwołanie się do "okoliczności wskazanych w zawiadomieniu" jest błędne.

40 Wyjątkiem jest uwzględnienie przez sąd (na etapie postępowania sądowego) wniosku dowodowego strony, któremu inna strona sprzeciwia się. W tym wypadku sąd wydaje postanowienie - art. 368 § 1 k.p.k.

Jeżeli prokurator, policjant czy sąd **oddala wniosek dowodowy, to rozstrzyga w tej kwestii postanowieniem**[41]. A w jakiej sytuacji organ procesowy może oddalić wniosek dowodowy? Katalog takich sytuacji jest następujący:

1. przeprowadzenie dowodu jest niedopuszczalne;
2. okoliczność, która ma być udowodniona, nie ma znaczenia dla rozstrzygnięcia sprawy albo jest już udowodniona zgodnie z twierdzeniem wnioskodawcy;
3. dowód jest nieprzydatny do stwierdzenia danej okoliczności;
4. dowodu nie da się przeprowadzić;
5. wniosek dowodowy w sposób oczywisty zmierza do przedłużenia postępowania;
6. wniosek dowodowy został złożony po zakreślonym przez organ procesowy terminie, o którym strona składająca wniosek została zawiadomiona42.

Poza tymi sytuacjami oddalenie wniosku dowodowego jest niedopuszczalne. W szczególności nie można oddalić wniosku dowodowego na tej podstawie, że dotychczasowe dowody wykazały przeciwieństwo tego, co wnioskodawca zamierza udowodnić43.

Niektóre z tych podstaw do oddalenia wniosku dowodowego mają charakter ocenny. Organ procesowy może mieć odmienne zdanie niż autor wniosku dowodowego np. co do tego, czy dowód jest przydatny, czy też nie. Albo w zakresie tego, czy wniosek zmierza do przewlekania postępowania. Co zrobić, gdy autor wniosku nie zgadza się z rozstrzygnięciem o jego oddaleniu?

Kwestionowanie oddalenia wniosku dowodowego

Postanowienie o oddaleniu wniosku dowodowego nie podlega zaskarżeniu. Podstawowy sposób sprzeciwiania się decyzji organu procesowego jest więc w tym wypadku niedostępny.

Zasadne jest jednak **kwestionowanie oddalenia wniosku dowodowego w środku odwoławczym od decyzji kończącej postępowanie** (niekorzystnej dla autora wniosku). Takimi środkami odwoławczymi są: zażalenie (na postanowienie o umorzeniu lub odmowie wszczęcia postępowania) albo apelacja (na wyrok sądu).

Przykład: Stowarzyszenie ABC występuje jako pokrzywdzony w sprawie. Kieruje wniosek dowodowy do prokuratora. Prokurator wydaje postanowienie o oddaleniu tego wniosku dowodowego

41 Art. 170 § 3 k.p.k., art. 368 § 1 k.p.k.
42 Art. 170 § 1 k.p.k.
43 Art, 170 § 2 k.p.k.

z uwagi na fakt, że zmierza on w sposób oczywisty do przedłużenia postępowania. Następnie postępowanie to zostaje umorzone. W tej sytuacji zasadne jest podniesienie kwestii niezasadnego oddalenia wniosku dowodowego w zażaleniu na postanowienie o umorzeniu postępowania.

Jak skutecznie budować argumentację związaniu z oddaleniem wniosku dowodowego w środku zaskarżenia od decyzji kończącej?

Jeżeli jest to etap postępowania przygotowawczego (czyli mowa o zażaleniu na umorzenie lub odmowę wszczęcia postępowania), to zasadne jest odwołanie się do art. 297 k.p.k., który określa "cele postępowania przygotowawczego". Zgodnie z tym przepisem do celów postępowania przygotowawczego należy m.in.:

- ustalenie, czy został popełniony czyn zabroniony i czy stanowi on przestępstwo;
- wykrycie i w razie potrzeby ujęcie sprawcy;
- wyjaśnienie okoliczności sprawy, w tym ustalenie osób pokrzywdzonych i rozmiarów szkody;
- zebranie, zabezpieczenie i w niezbędnym zakresie utrwalenie dowodów dla sądu.

Można więc argumentować, że organ postępowania przygotowawczego nie zrealizował celów określonych w art. 297 k.p.k., przykładowo poprzez niewyjaśnienie okoliczności sprawy, niezebranie i niezabezpieczenie dowodów, a było to konsekwencją oddalenia zasadnego wniosku dowodowego strony postępowania.

Jeżeli jest to etap postępowania sądowego, to warto odwołać się do art. 366 k.p.k. Stanowi on, że przewodniczący (składu sędziowskiego) jest zobowiązany "baczyć", aby wyjaśnione zostały wszystkie istotne okoliczności sprawy. Analogicznie więc można argumentować w apelacji od wyroku, że sąd zaniechał wyjaśnienia "wszystkich istotnych okoliczności sprawy" w ten sposób, że oddalił zasadny wniosek dowodowy strony postępowania.

Kwestia nierozpoznania wniosku dowodowego przez organ procesowy

Jak kilkakrotnie wspomniano, organ procesowy (prokurator, policjant, sąd) ma obowiązek ustosunkować się do złożonego wniosku dowodowego. Może go uwzględnić (wówczas nie wydaje żadnego rozstrzygnięcia) albo oddalić (wówczas wydaje postanowienie). W praktyce nie jest jednak sytuacją niespotykaną, że rozpoznanie wniosku lub wniosków dowodowych organowi procesowemu umknie. Wówczas ani nie uwzględnia on wniosku, ani nie realizuje zawnioskowanego dowodu ani nie wydaje postanowienia o jego oddaleniu. Jak postąpić w tej sytuacji?

Sytuacja jest w gruncie rzeczy zbliżona do przypadku niezasadnego oddalenia wniosku dowodowego. Mianowicie **zasadne jest kwestionowanie faktu nierozpoznania wniosku dowodowego w środku zaskarżenia (zażaleniu, apelacji) od decyzji kończącej** (postanowienia o umorzeniu, o odmowie wszczęcia, wyroku). Dodatkowo jednak, poza argumentowaniem o niezrealizowaniu celów postępowania przygotowawczego lub niewyjaśnieniu wszystkich istotnych okoliczności sprawy, **warto podnieść jeszcze jeden zarzut. Właściwym jest podniesienie zarzutu naruszenia przez organ procesowy przepisu art. 170 § 3 k.p.k.,** zgodnie z którym oddalenie wniosku dowodowego winno nastąpić w formie postanowienia. Skoro bowiem organ nie przeprowadził danego dowodu, to można argumentować, że oddalił wniosek o jego przeprowadzenie, a jednak nie wydał w tej kwestii stosownego postanowienia, naruszając tym samym powołany przepis.

Uwaga! Jeżeli wniosek dowodowy obejmuje przeprowadzenie dowodu z dokumentów lub danych bezpośrednio załączonych przez autora wniosku, to sam fakt umieszczenia tych dokumentów lub danych w aktach sprawy świadczy o dopuszczeniu wnioskowanego dowodu. Ewentualne nieuwzględnienie informacji wynikających z tych dokumentów lub danych, czy też wyciągnięcie z nich błędnych wniosków, stanowi innego rodzaju uchybienie po stronie organu procesowego niż związane z kwestią rozpoznania wniosku dowodowego.

Autorzy:

Jakub Kłosiński – prokurator Prokuratury Okręgowej Warszawa-Praga, delegowany do Prokuratury Regionalnej w Warszawie (Wydział ds. Przestępczości Gospodarczej). Prowadził m. in. śledztwa dotyczące działalności transgranicznych zorganizowanych grup zajmujących się przestępczością samochodową i narkotykową. Aktualnie wykonuje obowiązki w Dziale ds. Cyberprzestępczości.

Jędrzej Kupczyński - Doktorant w Katedrze Kryminalistyki WPiA UW, prokurator w Prokuraturze Rejonowej Warszawa-Wola w Warszawie, absolwent Wydziału Prawa i Administracji Uniwersytetu Warszawskiej oraz Krajowej Szkoły Sądownictwa i Prokuratury. Do jego zainteresowań naukowych należy kryminalistyka, w szczególności mechanoskopia oraz zagadnienia mechanicznych zabezpieczeń mienia i taktyki włamań, a także nowe technologie w prawie karnym i kryminalistyce. Zawodowo związany z problematyką cyberprzestępczości, przestępczości inwestycyjnej i giełdowej. Obecnie przygotowuje rozprawę doktorską dotyczącą wykorzystania kamer nasobnych (kamer noszonych na mundurach) w pracy policyjnej i jako dowodu w postępowaniu karnym. Członek zespołu realizującego projekt naukowy “Kamery Nasobne w Pracy Organów Ścigania i Wymiaru Sprawiedliwości”. Z ramienia Ministerstwa Sprawiedliwości członek polsko-norweskiej, dwustronnej grupy roboczej dotyczącej biegłych sądowych. W wolnym czasie chodzi po górach, jeździ na rowerze, nurkuje z butlą i uprawia freediving.

Joanna Grabarczyk-Anders - ekspertka z dziesięcioletnim doświadczeniem w obszarze mowy nienawiści, przestępstw motywowanych uprzedzeniami oraz bezpieczeństwa w sieci. Jest współtwórczynią kampanii Hejtstop. Obecnie współpracuje jako ekspertka z Żydowskim Stowarzyszeniem Czulent. Od 2024 członkini Zespołu doradców przy Prokuratorze Generalnym do spraw przeciwdziałania mowie nienawiści oraz przestępstwom motywowanym uprzedzeniami. Jej ekspertyza obejmuje prowadzenie badań, analiz oraz sporządzanie raportów dotyczących skali incydentów motywowanych nienawiścią, stosowania treści nienawistnych w kampaniach wyborczych, usuwania nielegalnych treści przez serwisy IT oraz zjawisk dezinformacji w mediach społecznościowych. Specjalizuje się w zagadnieniach dotyczących underreportingu oraz litygacje strategicznych w organizacjach mniejszościowych. Jako wykwalifikowana trenerka w dziedzinie bezpieczeństwa w sieci, mowy nienawiści oraz przestępstw z motywacji uprzedzeń, prowadzi szkolenia dla różnych grup zawodowych, w tym dla policji, adwokatów, administratorów treści oraz organizacji mniejszościowych. Jej obszarem zainteresowań jest również odpowiedzialność administratorów sieci za treści, zabezpieczanie i gromadzenie materiału dowodowego oraz ustalanie tożsamości sprawców przestępstw.

Żydowskie Stowarzyszenie Czulent

Żydowskie Stowarzyszenie Czulent jest niezależną organizacją non profit, działającą na poziomie krajowym i międzynarodowym, angażującą się przede wszystkim w działania rzecznicze.

Nasza platforma gromadzi profesjonalistów ze społeczności żydowskiej zarówno w Polsce, jak i za granicą. Nasze działania rzecznicze obejmują aspekty polityczne, społeczne i prawne, które są realizowane przez wdrażanie innowacyjnych rozwiązań edukacyjnych oraz budowanie koalicji na rzecz otwartości, przeciwdziałania antysemityzmowi, rasizmowi i dyskryminacji.

Współpracujemy z instytucjami, administracją publiczną i organizacjami dialogu, by przyczynić się do zmiany postaw społeczeństwa oraz ustawodawstwa polskiego w obszarze tolerancji i zwalczania rasizmu.

Wśród naszych partnerów znajdują się m.in. Biuro Instytucji Demokratycznych i Praw Człowieka OBWE (ODIHR), American Jewish Committee Central Europe oraz National Democratic Institute. Czulent podejmuje kompleksowe inicjatywy mające przeciwdziałać antysemityzmowi, w ramach których są opracowywane analizy i raporty dotyczące zjawiska antysemityzmu w krajach Grupy Wyszehradzkiej, zajmuje się również działaniami z obszaru litygacji strategicznej. Prowadzi platformę zglosantysemityzm.pl, umożliwiającą raportowanie incydentów i przestępstw o charakterze antysemickim oraz wsparcie prawne dla osób nimi pokrzywdzonych. W ramach koalicji międzynarodowych – European Network on Monitoring Antisemitism (ENMA), Coalition to Counter Online Antisemitism (CCOA), European Network Countering Antisemitism Through Education (ENCATE) i European Network Against Racism (ENAR) – gromadzimy i promujemy dobre praktyki oraz rekomendujemy rozwiązania na poziomie europejskim.

stowarzyszenie
żydowskie
czulent