UCZELNIA PAŃSTWOWA
im. Jana Grodka w Sanoku

MATERIAŁY POKONFERENCYJNE



ZWALCZANIE PRZESTĘPCZOŚCI INTERNETOWEJ

SANOK 2025

REDAKCJA GRZEGORZ MATYNIAK

ZWALCZANIE PRZESTĘPCZOŚCI INTERNETOWEJ

MATERIAŁY POKONFERENCYJNE

REDAKCJA
GRZEGORZ MATYNIAK

UCZELNIA PAŃSTWOWA
im. Jana Grodka w Sanoku

Sanok 2025

Wydawca: Uczelnia Państwowa im. Jana Grodka w Sanoku
Redakcja: Grzegorz Matyniak
Projekt okładki: Wojciech Pilszak/AI
Opracowanie typograficzne: Marcin Stach

© Copyright by
Uczelnia Państwowa im. Jana Grodka w Sanoku
ul. Mickiewicza 21, 38-500 Sanok
www.up-sanok.edu.pl

Poglądy wyrażone w artykułach nie zawsze są zgodne z poglądami Redaktora i Wydawcy. Opublikowane referaty nie były poddane korekcie językowej przez Wydawcę i są publikowane w postaci dostarczonej przez Autorów.

ISBN 978-83-61802-62-4

SANOK 2025

Spis treści

Grzegorz Matyniak
Słowo wstępne 5

Paweł Baraniecki
Smartfon i „biling" nie są jedynymi źródłami informacji 11

dr Jarosław Biegański
Rola pojedynczego punktu kontaktowego FinCERT.pl w przeciwdziałaniu cyberprzestępczości finansowej 23

Arkadiusz Czak
Wizualizacja danych w analizie kryminalnej: zastosowanie aplikacji yEd Graph Editor w tworzeniu diagramów relacyjnych 41

Józef Druć
Podsłuch i monitoring oraz prosty sprzęt do wykrywania ukrytych urządzeń 69

Jacek Garbaczewski
Nie ma portu? I co z tego! Jak dojść do użytkownika końcowego, kiedy wszyscy mówią, że się nie da 95

Artur Kubiak
Kryptowaluty a ich wykorzystanie w procederze oszustw inwestycyjnych . . . 117

Grzegorz Matyniak
Czy biegły jest od wykrywania sprawców i z czego to może wynikać? 157

Wojciech Pilszak
Otwarte źródła informacji jako wsparcie inwigilacji realizowanej w środowisku cyfrowym 165

Marek Stawarczyk
O manipulacjach w obrazie cyfrowym 177

Tomasz Typrowicz
Metody oraz zakres gromadzenia, przetwarzania i analizy danych mogących stanowić materiał dowodowy stosowane w Placówkach Straży Granicznej 195

inż. Ireneusz Wasiewicz
Tajemnice zawodowe w Polsce – czyli rzecz o pragmatyce procesowej przy zabezpieczaniu nietypowych i wrażliwych dowodów cyfrowych 209

Teresa Wierzbowska, Zbigniew Taraś
Skuteczność zgłoszeń naruszeń treści audio video (AV) – raport z badania 251

Słowo wstępne

Szanowni Państwo,

oddawana do Państwa rąk publikacja jest pierwszą – a żywię nadzieję, że nie ostatnią – jaka pojawia się po piętnastu konferencjach organizowanych dla funkcjonariuszy służb państwowych zwalczających przestępczość związaną z szeroko pojętymi Internetem i telekomunikacją.

Uczelnia Państwowa im. Jan Grodka w Sanoku była w dniach 5–6 września 2024 r. miejscem jubileuszowej XV konferencji przybliżającej zagrożenia związane z użytkowaniem nowoczesnych technologii oraz metod zwalczania działalności osób wykorzystujących nowinki techniczne do działań niezgodnych z prawem, której organizatorem był Zakład Bezpieczeństwa Wewnętrznego Instytutu Nauk Społecznych. Tematem przewodnim konferencji było: **Zwalczanie przestępczości związanej z dostępem do Internetu. Zasady procesowe związane z zabezpieczaniem i analizą materiału dowodowego w sprawach internetowych.**

Konferencja – której początki sięgają roku 2009 – jest przeznaczona zgodnie z przyjętymi założeniami dla funkcjonariuszy wszystkich służb mundurowych zajmujących się w ramach codziennych obowiązków zwalczaniem szeroko pojętego zjawiska cyberprzestępczości. Tym razem w murach sanockiej uczelni pojawiło się ponad 180 funkcjonariuszy Policji garnizonu podkarpackiego, placówek Straży Granicznej wchodzących w skład nie tylko Bieszczadzkiego Oddziału Straży Granicznej, ale również innych oddziałów tej formacji w kraju, w tym Wyższej Szkoły Straży Granicznej w Koszalinie. Oczywiście przykładem lat poprzednich nie zabrakło również przedstawicieli Krajowej Administracji Skarbowej z terenu całego kraju, analityków i informatyków śledczych oraz biegłych sądowych z zakresu informatyki śledczej i niezależnych ekspertów z tego zakresu, którzy to nieodpłatnie chcieli podzielić się ze słuchaczami swoją wiedzą oraz swoim doświadczeniem.

Wszyscy uczestnicy konferencji otrzymali numizmat upamiętniający XV konferencję, który – mam nadzieję – okaże się ciekawą i miłą pamiątką dla obecnych na konferencji licznych słuchaczy, a dla zbieraczy numizmatów białym krukiem z uwagi na liczbę wybitych egzemplarzy.

Prelegentami w tej jubileuszowej edycji byli:

Paweł Baraniecki – ekspert niezależny,

Michał Barbaś – ekspert niezależny,

dr Jarosław Biegański – p.o. dyrektora Zespołu Bezpieczeństwa Banków Związku Banków Polskich,

Mateusz Chrobok – ekspert niezależny,

nadkom. Arkadiusz Czak – oficer KAS, Zachodniopomorski Urząd Celno-Skarbowy w Szczecinie,
Józef Druć – emerytowany funkcjonariusz Dolnośląskiego Urzędu Celno-Skarbowego we Wrocławiu, ekspert niezależny,
Mateusz Górka oraz **Artur Gałęski** – Dział ds. współpracy z organami ścigania, Allegro sp. z o.o.,
Hubert Hager – oficer Bundespolizei oraz ZITiS z Monachium,
Wojciech Kiszka – ekspert Biura Analiz Bank Pekao SA,
mł. insp. dr Bartłomiej Kowalski – naczelnik Wydziału dw z Przestępczością Gospodarczą KWP w Rzeszowie,
Artur Kubiak – emerytowany oficer Policji, dyrektor Działu Bezpieczeństwa ZondaCrypto,
Jakub Kupniewski oraz **Zbigniew Taraś** – Stowarzyszenie Sygnał,
Mariusz Łucyk – ekspert niezależny,
Grzegorz Matyniak – emerytowany oficer Policji, biegły sądowy SO w Krośnie z zakresu informatyki śledczej oraz analizy danych, nauczyciel akademicki Uczelni Państwowej im. Jana Grodka w Sanoku,
Jakub Pepłoński – ekspert niezależny,
Wojciech Pilszak – emerytowany oficer Policji, prezes zarządu e-Detektywi sp. z o.o., biegły sądowy z zakresu informatyki śledczej i analizy kryminalnej,
Marek Stawarczyk – biegły sądowy z zakresu informatyki i informatyki śledczej SO w Krośnie,
Ireneusz Wasiewicz – ekspert niezależny z zakresu informatyki śledczej,
Tomasz Wawrzkowicz – specjalista ds. współpracy z organami ścigania, Grupa Olx.

Celem konferencji, jak założono od samego początku, było praktyczne poszerzenie wiedzy z zakresu szeroko pojętej cyberprzestępczości oraz jej zapobiegania przez funkcjonariuszy różnych służb na co dzień zajmujących się zmaganiami z tą formą coraz szerzej wykorzystywanej – niestety – działalności przestępczej. Wśród wystąpień nie zabrakło tematów związanych z kryptowalutami – a nawet można by powiedzieć, że często się przewijały – zarówno ze śledzeniem ich przepływu, jak i z możliwościami ich procesowego zabezpieczania. Poruszono tematy dotyczące naruszania prawa autorskiego i praw pokrewnych w sieci, w tym nowych trendów i metod kradzieży sygnału telewizyjnego i zwalczania tego zjawiska. Dyskutowano również o możliwościach technicznych i prawnych zabezpieczania danych stanowiących lub mogących stanowić dowód w prowadzonych postępowaniach karnych.

Prelegenci poruszali również tematy związane z wykorzystywaniem narzędzi informatycznych pozwalających na analizę i obróbkę zarówno materiałów wideo, jak

i zdjęć zabezpieczanych w ramach prowadzonych postępowań przygotowawczych i ich procesowego wykorzystania.

Na konferencji po raz pierwszy – i mamy nadzieję, że nie ostatni – pojawił się przedstawiciel organów ścigania z zagranicy. Tym razem był to Hubert Hager, oficer Budnespolizei oraz ZITiS z Monachium, którego wystąpienie dostarczyło ciekawych spostrzeżeń w temacie zagadnień związanych z możliwościami badania m.in. kart SIM i zapisywanych na nich danych oraz nośników pamięci przybierających różnego rodzaju formy i kształty.

Po raz kolejny możliwości współpracy sektora bankowego z organami ścigania przedstawił Jarosław Biegański, p.o. dyrektora Zespołu Bezpieczeństwa Banków Związku Banków Polskich.

Swój warsztat pracy oraz interesujące case study przedstawili też biegli sądowi z zakresu informatyki śledczej biorący udział w konferencji.

Z bardzo ciekawym wystąpieniem o tytule „Chciałbym być przestempcom, ale nie wiem jak" na temat przeglądu rosyjskiego darknetu zaprezentowali się po raz pierwszy na konferencji w Sanoku (a już mamy nadzieję, że nie ostatni) Mateusz Chrobok i Michał Barbaś i od razu zdobyli wielkie zainteresowanie i uznanie uczestników.

Innym interesującym wystąpieniem był temat związany z metodyką śledzenia dystrybucji środków finansowych przez rachunki bankowe, jaki przedstawił Mariusz Łucyk. Z kolei Arkadiusz Czak przedstawił narzędzia Open Source, jakimi można prowadzić analizę zdjęć i materiałów wideo zarówno na potrzeby prowadzonych czynności procesowych, jak i operacyjno-rozpoznawczych, a które pozwalają zaoszczędzić czas. Ważną i ciekawą pozycją, jaką mogą wykorzystywać funkcjonariusze wszystkich służb, była mająca swoją polską premierę po uzyskaniu przez Centrum Kompetencyjne Kontroli Gier Hazardowych ZUCS w Szczecinie pisemnej zgody organizacji GAFILAT publikacja *Przewodnik po istotnych aspektach i właściwych krokach w zakresie dochodzenia, identyfikacji, zajmowania i konfiskaty aktywów wirtualnych*.

Zasygnalizowano również pojawiające się wątpliwości i uwagi związane z zabezpieczaniem, badaniem i analizowaniem materiału dowodowego oraz prowadzeniem postępowań przygotowawczych, w tym z trudnościami, z jakimi na co dzień mierzą się organy ścigania, dążąc do zapewnienia nam bezpieczeństwa i ścigając sprawców przestępstw. Próbowano wyjaśnić występujące nieraz niejasności lub rozbieżności w interpretacji obowiązków poszczególnych uczestników procesu karnego, jak też pomocników organów w tym procesie, jakimi są biegli sądowi.

Mając na uwadze, że wydarzenie to odbyło się po raz piętnasty, warto być może krótko przybliżyć jego historię. W roku 2009 Komenda Powiatowa Policji w Sanoku

zorganizowała po raz pierwszy szkolenie dla funkcjonariuszy Policji i to nie tylko tych sanockich, ale również z innych jednostek dawnego województwa krośnieńskiego. Wzmianki o tych początkach znajdziemy w archiwalnych numerach „Tygodnika Sanockiego" (nr 40 z 2009, nr 35 z 2011).



e-Policja

Policjanci się szkolą. Hotel „Kmicic" w Czartażu gościł uczestników warsztatów dotyczących szeroko rozumianych zagadnień piractwa komputerowego, ochrony własności intelektualnej oraz współpracy pomiędzy przedstawicielami pokrzywdzonych, a organami ścigania.

Policjanci z uwagą słuchali wykładów zaproszonych gości.

Szkolenie zorganizowano z inicjatywy Edwarda Zajdla, szefa sanockiej Policji. W zajęciach uczestniczyło około 60 funkcjonariuszy z kilku jednostek, działających na terenie dawnego województwa krośnieńskiego. Mali oni okazję wysłuchać wykładów, które prowadzili m.in.: biegli sądowi, przedstawiciele portali internetowych (nasza-klasa.pl), producenci oprogramowania komputerowego (Microsoft), czy organizacji zajmujących się ochroną praw autorskich.

– Były to prelekcje dotyczące głównie sposobów i technik zabezpieczania dowodów elektronicznych, które bardzo łatwo można stracić. Czasami wystarczy nawet niewłaściwe wyłączenie komputera i dowód jest już praktycznie nie do odzyskania. Musimy iść z duchem czasu, stąd inicjatywa tego typu szkoleń – powiedział o warsztatach Grzegorz Matyniak, naczelnik Wydziału Dochodzeniowo-Śledczego KPP w Sanoku. (bb)



O cyberprzestępczości i zagrożeniach w sieci

Wykonanie elektronicznej obrączki „Krynitanki".

I – przytaczając klasyka – tak to się zaczęło. I trwa do dziś. Prelegenci, którzy pojawiali się na sanockich spotkaniach, każdorazowo poruszali różne zagadnienia związane z przeciwdziałaniem przestępczości komputerowej (jak nazywano ją początkowo), przestępczości internetowej czy – jak ostatnio – cyberprzestępczości w każdej jej postaci. Bo to nie tylko oszustwa związane z handlem w sieci, nie tylko pornografia dziecięca, grooming, ale również naruszenia prawa autorskiego, groźby karalne, znieważenia w Internecie czy też pranie brudnych pieniędzy i wyłudzenia potężnych kwot pod hasłem pseudo inwestycji.

W trakcie tych edycji pojawiły się też okolicznościowe numizmaty związane ze szczególnymi edycjami konferencji. Był to rok 2018 (X edycja) oraz wspomniany rok 2024 (XV edycja). Na rewersie każdego z numizmatów umieszczone zostały nazwiska tych prelegentów, którzy wnieśli największy wkład w kolejne edycji konferencji. Wizerunki tych numizmatów pozwalam sobie zamieścić poniżej.



Czy będzie to trwało nadal? To pytanie, pozwolą Państwo, pozostawię bez odpowiedzi.

Chociaż jeżeli będzie potrzeba, będą chętni prelegenci, którzy będą chcieli podzielić się swoją wiedzą i doświadczeniem, to idea szkoleń non-profit dla zapewniających nam bezpieczeństwo funkcjonariuszy różnych służb (nie tylko Policji) na Uczelni Państwowej w Sanoku będzie trwać nadal. Oczywiście jeśli będą chętni do poszerzania swojej wiedzy i umiejętności. Konferencja, co widać na przestrzeni czasu, nie jest zamknięta dla przedstawicieli żadnego z organów ścigania.

W tym miejscu chciałbym złożyć swoje podziękowania tym wszystkim, którzy przez ten okres pojawili się w Sanoku i nigdy – co ważne – nie odrzucili skierowanego do nich zaproszenia. Są wśród tych wszystkich Szanownych Prelegentów osoby, na których pomoc mogę liczyć do chwili obecnej, jak i tacy, których niestety nie ma już z nami.

Pozwolą Państwo, że nazwiska osób związanych z konferencjami przywołam w tym momencie (kolejność przypadkowa):

Wojciech Pilszak, Jakub Pepłoński, Paweł Baraniecki, Arkadiusz Czak, Jarosław Biegański, Krzysztof Janiszewski, Artur Kubiak, Witold Budzisz, Jan Bałdyga, Maciej Pajęcki, Wojciech Kiszka, Tomasz Wawrzkowicz, Marek Stawarczyk, Ireneusz Wasiewicz, Jacek Garbaczewski, Marcin Ochociński, Mariusz Tokarski, Eugeniusz Trybalski, Krzysztof Czarnacki, Zbigniew Taraś, Jakub Kupniewski, Mateusz Górka, Józef Druć, Huber Hager, Mateusz Chrobok, Michał Barbaś, Maciej Kołodziej, Tomasz Typrowicz, Piotr Preisner, Tomasz Zaborowski, Marlena Kruczek-Sekuła, Ewelina Wojciechowska, Mateusz Górka i inni.

Nie mogę też – z chęci zachowania przyzwoitości – nie wspomnieć o śp. Janie Kmiecińskim, który w pierwszych latach konferencji służył lokalem, a do końca był „dobrym duchem spotkań".

Mamy rok 2025 i pomimo padających kiedyś z mojej strony stwierdzeń, że XV edycja będzie ostatnią, zbliża się nasze XVI spotkanie – a może nawet będą Państwo na tym spotkaniu, jakie odbędzie się w dniach 4–5.09.2025 r. (jak niektórzy stali bywalcy mówią – cyklicznych spotkań wrześniowych) – i nadal się spotykamy.

Wygląda na to, że dzięki namowom takich samych pozytywnie zakręconych osób, po poszerzeniu grona odbiorców mogących skorzystać z wiedzy i doświadczenia innych (przy zachowaniu tych samych kryteriów udziału) oraz przy nieco innej formie reklamowania to cykliczne wydarzenie na sanockiej Alma Mater (na którym z każdym kolejnym rokiem i każdą kolejną edycją wzrasta zarówno liczba prelegentów, jak i uczestników) na stałe zagościło na mapie Polski jako ważne miejsce spotkań, podczas których dochodzi do wymiany doświadczeń zarówno ekspertów, biegłych sądowych, funkcjonariuszy służb mundurowych (Policji, Straży Granicznej, CBA i Krajowej Administracji Skarbowej), jak i pracowników sektora prywatnego, którzy zajmują się bezpieczeństwem użytkowników cyberprzestrzeni.

Grzegorz Matyniak

Paweł Baraniecki[1]

Smartfon i „biling" nie są jedynymi źródłami informacji

Abstrakt

W pierwszej części artykułu wykazano zasadność pozyskiwania wiedzy o warunkach w jakich powstały ślady elektroniczne spowodowane użyciem popularnych urządzeń elektronicznych. Zastosowanie tej wiedzy zmniejsza prawdopodobieństwo błędnego wnioskowania, może tez zmniejszyć nakład pracy.

W drugiej, zaś wskazano na urządzenia mobilne będące źródłami danych o aktywności użytkownika inne niż smartfon.

Słowa kluczowe

Warunki świadczenia usługi telekomunikacyjnej, mobilne urządzenia elektroniczne, mobilne źródła śladów elektronicznych.

Wstęp

Artykuł podzielono na dwie części. W pierwszej z nich skupiono się na nowoczesnych usługach telekomunikacyjnych, w drugiej zaś, zwrócono uwagę na inne niż smartfon mobilne urządzenia elektroniczne, które mogą być źródłem wartościowych informacji.

Usługi telekomunikacyjne są coraz to bardziej skomplikowane. Dane poddane przez operatora telekomunikacyjnego retencji[2] coraz częściej nie pozwalają na jednoznaczną weryfikację hipotezy śledczej. W takich przypadkach pomocne mogą być informacje o warunkach świadczenia usługi telekomunikacyjnej, bądź poszukiwanie informacji u innych źródeł.

Celem tej publikacji jest wykazanie potrzeby zdobywania wiedzy o warunkach świadczenia usług telekomunikacyjnych i świadczonych drogą elektroniczną, a także pozyskiwania i analizy danych zebranych w pamięciach mobilnych urządzeń elektronicznych, tak aby poprzez zastosowanie uzyskanej wiedzy, zminimalizować prawdopodobieństwo błędnego wnioskowania.

[1] Paweł Baraniecki – wielokrotny prelegent na konferencjach naukowych dotyczących problematyki cyberprzestępczości. Specjalizuje się w zagadnieniach związanych z bezpieczeństwem w telekomunikacji, dowodami elektronicznymi zarówno od strony technicznej jak i prawnej, a także mechanizmach współpracy pomiędzy organami ścigania a operatorami telekomunikacyjnymi. Przez wiele lat odpowiadał w Polkomtel Sp. z o.o. za systemy wspomagające realizację obowiązków prawnych operatora (Pismak, Navigator...). Kontakt z Autorem: barpast@gmail.com

[2] Obowiązek prawny narzucony ustawą Prawo Komunikacji Elektronicznej z dnia 9 sierpnia 2024 Dz. U. 2024 poz. 1221 (dalej PKE).

Część I. Usługi telekomunikacyjne

Karty SIM o wielu numerach IMSI i wielu przyporządkowanych do nich numerach MSISDN

Od kilkunastu lat są używane karty SIM, które mają kilka numerów IMSI i/lub przyporządkowanych[3] jest do niej kilka numerów MSISDN. Jednym z biznesowych powodów używania takich kart jest świadczenie przez przedsiębiorcę telekomunikacyjnego[4] usług telekomunikacyjnych w roamingu. Dla takiego przedsiębiorcy tańsze jest wykorzystanie w roamingu numeracji IMSI z puli obsługującego go operatora telekomunikacyjnego od samodzielnego zawierania umów roamingowych.

Kilka numerów MSISDN jest przypisywany do kart SIM, na przykład, w modelu biznesowym „w każdym państwie masz lokalny numer". Przez co użytkownik unika opłat za rozmowy w roamingu.

Zgodnie z obowiązującym prawem funkcjonariusze podmiotów uprawnionych[5] mogą od operatora telekomunikacyjnego uzyskać wykaz połączeń w danym czasie (tzw. „bilingu") dla jednego z parametrów:

a) MSISDN;
b) IMSI;
c) IMEI.

Brak wiedzy o używaniu kart SIM do których przypisano po kilka numerów IMSI, czy MSISDN, a w konsekwencji zamówienie „bilingu" dla pojedynczego parametru da niepełne informacje o użyciu urządzenia, w którym zainstalowano kartę SIM np. smartfonu.

Tabela nr 1. Zestawienie „braków" w informacji o użyciu karty SIM dla pojedynczego parametru

„Biling po IMSI"	„Biling po MSISDN"	„Biling po IMEI"
Tylko dane o użyciu karty SIM dla wskazanego pojedynczego IMSI. Będą dane o wszystkich MSISDN przyporządkowanych do danego IMSI. NIE będzie danych o używaniu karty SIM korzystającej z innego IMSI	Tylko dane o użyciu karty SIM dla wskazanego pojedynczego MSISDN. Będą dane o wszystkich IMSI do których przyporządkowano dany MSISDN. NIE będzie danych o używaniu karty SIM korzystającej z innego MSISDN	Będą dane o użyciu karty SIM dla wszystkich IMSI i MSISDN.

[3] Numer MSISDN nie jest zapisywany na karcie SIM.
[4] Przedsiębiorca telekomunikacyjny nie ma własnej infrastruktury sieciowej.
[5] Lista podmiotów uprawnionych jest określona w PKE. Jest to lista zamknięta.

W tabeli nr 1 zestawiono jakie zestawy danych przekaże operator telekomunikacyjny w zależności od żądania. Przy braku wiedzy o korzystaniu z karty SIM do której przyporządkowano więcej niż jeden numer MSISDN, czy IMSI jest praktycznie pewność popełnienia błędu z powodu niepełnej informacji. W „bilingach" po IMSI, lub MSISDN będą to błędy spowodowane niepełnym zestawem danych. Zaś „biling po IMEI" – niemal na pewno – zostanie zinterpretowany jako korzystanie z kilku kart SIM u jednym urządzeniu.

Jak mitygować ryzyko błędnych wniosków?

W omawianym tu przypadku konieczna jest wiedza o stosowaniu karty SIM z przypisanymi do niej wieloma numerami IMEI i/lub MSISDN. Właściwego przedsiębiorcę, lub operatora telekomunikacyjnego należy zapytać o: czy w konkretnym przypadku jest świadczona usługa z przyporządkowaniem wielu numerów IMSI i/lub MSISDN do jednej karty SIM? Jeśli tak to należy zażądać „bilingu" dla wszystkich zmultiplikowanych numerów (po IMSI i po MSISDN).

e-SIM – wirtualne karty SIM

W ostatnich latach na rynku usług telekomunikacyjnych używane są coraz częściej wirtualne karty SIM, tzw. e-SIM. W urządzeniu np. telefonie nie ma fizycznej karty SIM. Tym samym urządzenie korzystające z wirtualnej karty SIM staje się urządzeniem końcowym (zakończeniem sieci). Wirtualna karta SIM wnosi kilka nowych możliwości, które warto znać, by móc je uwzględnić w budowaniu i weryfikacji hipotez śledczych. I tak karta e-SIM:

1. Może działać na kilku, różnego typu urządzeniach (bez fizycznego przenoszenia). Np.: smartfon, smartwatch, czy tablet;
2. Jedno urządzenie może obsługiwać kilka kart e-SIM, a przełączenie między nimi jest proste;
3. Kilka urządzeń może być przypisanych do różnych kart e-SIM o tym samym numerze MSISDN;
4. Może współpracować z materialną kartą SIM o tym samym numerze MSISDN.

Właściwość opisana w punkcie 1 (powyżej) oznacza, że przejęcie przez funkcjonariusza urządzenia końcowego (smartfon, tablet itp.) nie pozbawia jego właściciela możliwości dalszego korzystania z usług telekomunikacyjnych świadczonych z wykorzystaniem danej karty e-SIM.

Funkcjonalność opisana w punkcie 2 (powyżej) pozwala na kupowanie kart e-SIM u różnych dostawców. To oznacza istotne utrudnienie w zdobyciu wiedzy o komunikowaniu się, zwłaszcza w innych państwach.

Usługa opisana w punktach 3 i 4 (powyżej) jest świadczona w Polsce. Najczęściej karty SIM o tym samym MSISDN są instalowane w smartfonie i smartwatch'u. Przychodzące rozmowy, czy SMS można odebrać na każdym z urządzeń przy ich znacznym oddaleniu od siebie. To komplikuje analizę lokalizacji urządzenia.

Opisane tu funkcjonalności oparte na nich usługi generują nowe scenariusze połączeń (kilka kart SIM z tym samym numerem MSISDN), które będą miały swoją manifestację w kombinacji rekordów jakie są poddawane retencji.

Utrudnienia spowodowane postępem technologicznym

- Technologia LTE skokowo zwiększyła szybkość transmisji danych w telekomunikacji mobilnej.
- W tym samym czasie zaczął się tryumf smartfonów udostepniających szereg usług – także świadczonych drogą elektroniczną.

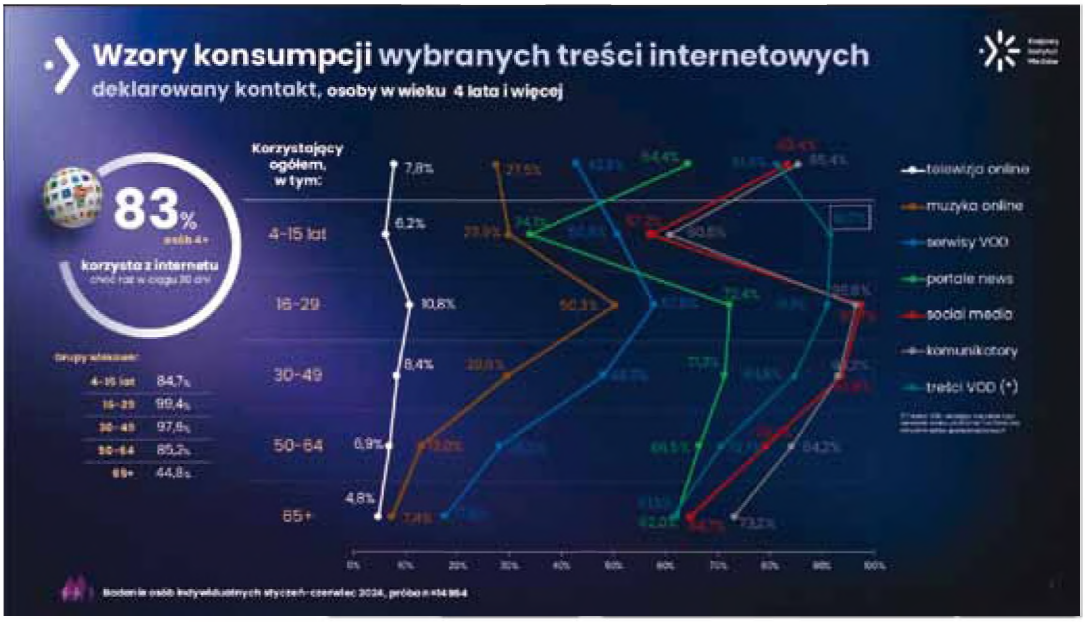
Te dwa czynniki doprowadziły do przeniesienia znacznej ilości połączeń głosowych, SMS i MMS do komunikatorów. To powoduje:

- brak informacji o dużym ułamku ogólnej liczby połączeń głosowych, SMS i MMS realizowanych za pomocą komunikatorów (brak informacji o aktywności użytkownika urządzenia mobilnego);
- logarytmicznego wzrostu objętości informacji dotyczącej transmisji danych. Przy czym dane retencyjne nie wskazują ani usługi, ani adresu docelowego. Ilość danych utrudnia analizę.

Według raportu mobirank.pl[6] z komunikatorów w pierwszym półroczu 2024 roku korzystało ponad 85% użytkowników telefonów.

Zmiany w sposobie użytkowania Internetu w pierwszej połowie 2024 roku pokazano na rysunku nr 1.

[6] https://mobirank.pl/2024/10/09/jak-korzystalismy-z-uslug-medialnych-w-polsce-w-1-polowie-2024-roku/ dostęp 20-05-2024.



Rysunek nr 1. Źródło: https://mobirank.pl/2024/10/09/jak-korzystalismy-z-uslug-medialnych-w-polsce-w-1-polowie-2024-roku / dostęp 20-05-2024

To powoduje deprecjację przydatności danych poddanych retencji. Korzystanie z komunikatora nie jest usługą telekomunikacyjną (nie ma obowiązku retencji danych), a najpopularniejsze komunikatory (aplikacje) są własnością podmiotów spoza EU. Pozyskanie danych od tych podmiotów jest skomplikowane i czasochłonne, a czasem niemożliwe.

Do tego dochodzi zmiana platformy technologicznej (w trakcie połączenia, i/lub w kolejnym połączeniu) w sposób niezauważalny dla użytkownika, a mającej istotny wpływ na informacje o połączeniu, zawarte w danych retencyjnych[7]. Mowa tu o zmianach platform technologicznych:

- CS na VoWi-Fi lub VoLTE dla połączeń głosowych;
- PS na Wi-Fi;
- dla SMS użycie platformy RCS[8][9].

[7] Dane retencyjne – dane o połączeniu poddane retencji. Obowiązek prawny.

[8] RCS – Rich Communication Services – model obsługi wiadomości w sieciach mobilnych objęty standardem GSMA.

[9] Zwłaszcza gdy tylko jeden interlokutor korzysta z platformy RCS.

Niepełna wiedza stwarza ryzyko błędnego wnioskowania

Brak wiedzy o zastosowaniu karty e-SIM, bądź brak wiedzy o konstrukcji usług telekomunikacyjnych świadczonych w oparciu o możliwości technologii opartej na wirtualnych kartach SIM, stwarza ryzyko niemożności stworzenia modelu odtwarzającego zdarzenia będące przedmiotem zainteresowania danej służby. Jeżeli dodamy do tego:

- niemożność pozyskania od operatora telekomunikacyjnego informacji o:
- połączeniach realizowanych za pośrednictwem komunikatora,
- wykorzystania smartfonu połączonego z Internetem za pomocą hotspotu Wi-Fi;
- trudności w interpretacji danych pozyskanych od operatora telekomunikacyjnego opisujących połączenia, podczas których doszło do zmiany platformy technologicznej;

to nietrudno wyobrazić sobie sytuację gdy analiza danych retencyjnych pozyskanych od operatora telekomunikacyjnego zakończy się wynikiem nieoznaczonym.

W Tabeli nr 2 jest zestawienie informacji, jakie należy pozyskać od dostawcy usług telekomunikacyjnych i źródła tej informacji. Wydaje się konieczne pozyskanie na wstępie od dostawcy usług telekomunikacyjnych informacji o tym jakie usługi telekomunikacyjne i w jakiej technologii są świadczone w konkretnym przypadku. Do tego dostosować zamówienia danych dokumentujących korzystanie z usług telekomunikacyjnych i dane o sposobie świadczenia/ korzystania z usług.

Tabela nr 2. Zestawienie informacji jakie można uzyskać od dostawcy usług telekomunikacyjnych i ich źródeł.

Informacja	Źródło	Uwagi
Jakie usługi telekomunikacyjne są świadczone w konkretnym przypadku.	Dostawca usług telekomunikacyjnych (pytania niestandardowe[1]) 1. Umowa o świadczenie usług telekomunikacyjnych. 2. Wykaz usług uruchomionych dla danej karty SIM. 3. Regulamin świadczenia usług telekomunikacyjnych.	Ad 2. Według bazy HLR stan na konkretną datę. Ewentualnie wykaz zmian.
W jakiej technologii/na jakich platformach technologicznych są świadczone poszczególne usługi telekomunikacyjne w ramach badanego przypadku.	Dostawca usług telekomunikacyjnych (pytanie niestandardowe).	

Informacja	Źródło	Uwagi
Jakie karty SIM i jakiego typu posiada abonent/użytkownik	Dostawca usług telekomunikacyjnych (pytanie niestandardowe; dane abonenckie).	
Tzw. „biling" dla parametrów wytypowanych na podstawie wiedzy o usługach i sposobie ich świadczenia.	Dostawca usług telekomunikacyjnych (pytanie standardowe).	Po jednym pytaniu standardowym dla bilingu po danym parametrze
Marka i typ urządzenia	Internet/Producent na podstawie numeru IMEI	Pozwala ocenić, które z zakupionych usług są możliwe do zrealizowania na danym urządzeniu.
Które zakupionych usług telekomunikacyjnych są dostępne w okolicy, gdzie zarejestrowano aktywność urządzenia końcowego	Dostawca usług telekomunikacyjnych, Internet.	Np. nadal nie wszędzie dostępne jest LTE. W takim obszarze transmisja obrazu jest co najmniej utrudniona.

Wnioski do części I

1. Dane retencyjne nie zawierają informacji o połączeniach realizowanych za pomocą komunikatorów.
2. Wirtualne karty SIM (e-SIM) udostępniają nowe funkcjonalności umożliwiające szybkie i łatwe przenoszenie usług telekomunikacyjnych pomiędzy urządzeniami końcowymi.
3. Bez systematycznego uzupełniania wiedzy o nowych technologiach i usługach oraz biznesowych modelach ich świadczenia zimniejsza się możliwość wykorzystania śladów elektronicznych w analizie śledczej.

Część II Inne urządzenia mobilne

Jakie urządzenia?

Obok smartfonów, tabletów, czy laptopów w powszechnym użyciu są inne urządzenia mobilne, których użycie wytwarza ślady elektroniczne. Ślady te można zbierać, zabezpieczać i analizować. Mowa tu o urządzeniach takich jak:

- smartwatche, opaski sportowe itp.;
- pojazdy wypożyczane „na minuty" (samochody, rowery, hulajnogi);
- karty płatnicze;

[10] Każdy z wiodących operatorów telekomunikacyjnych udostępnia informacje w trybach: niestandardowym/ tekstowym i automatycznym obejmujące pytania standardowe (bilingi, dane abonenckie).

- samochody i tzw. „piloty do samochodów".

Aby artykuł nie stał się nowelą tylko wspomnę o:

- routerach mobilnych (obsługują także SMS),
- odtwarzaczach mp3,
- dyktafonach,
- nawigacjach i kamerach samochodowych.

Urządzenia te rzadziej używane od 4 pierwszych.

Smartwatche, opaski sportowe

Urządzenia te niemal cały czas są z człowiekiem. Oprócz połączeń głosowych i SMS wykonują:

- mierzą czas;
- lokalizacje wg GPS;
- zliczają kroki;
- mierzą tętno;
- pozwalają na finansowe transakcje bezgotówkowe;

i to wszystko zapisują w swojej pamięci.

Pojazdy wypożyczane „na minuty"

Samochody, rowery, hulajnogi. Do ich wypożyczenia trzeba mieć zainstalowaną na smartfonie odpowiednią aplikację. Te pojazdy komunikują się z „centralą" oznaczając:

- telefon osoby wypożyczającej i jej kartę płatniczą/BLIK;
- początek i koniec trasy (czas, miejsce wg GPS).
- historię usług świadczonych dysponentowi danego numeru MSISDN i/lub numer karty płatniczej/BLIK'a

Dysponentem tych danych jest operator usługi. Czas przechowywania danych nie może być krótszy od czasu, w którym można skutecznie złożyć reklamację.

Karty płatnicze

Zawierają dane gdzie (terminal) i kiedy dokonano operacji finansowej, jak była ona autoryzowana. Często karty są wirtualne powiązane ze smartwatchem, czy smartfonem.

Samochody

Od kilkunastu lat są w nich używane urządzenia elektroniczne, które tworzą i zapisują dane.

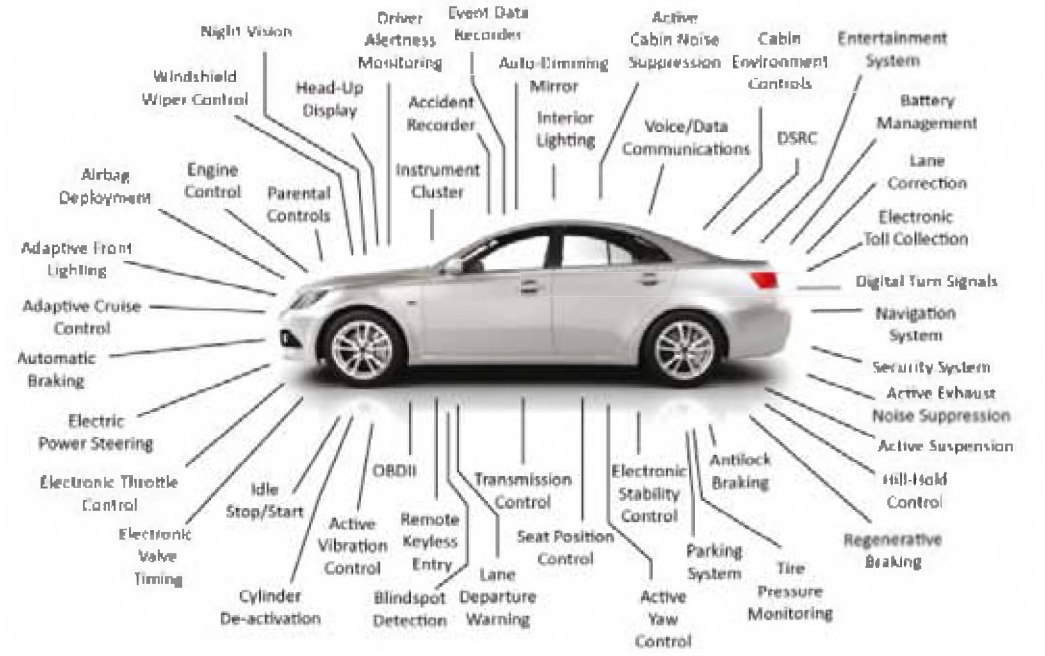
To urządzenie mobilne chcę opisać nieco bliżej.

Samochód

W Polsce, pod koniec 2023 roku było zarejestrowanych około 20 milionów samochodów osobowych[11]. Ponad 700 na 1000 mieszkańców. Udział tych bez elektroniki jest coraz to mniejszy.

Urządzeń elektronicznych montowanych w samochodzie przybywa. Pod koniec XX wieku pojawiły się sterowane elektronicznie zapłon i wtrysk paliwa. Później z roku na rok kolejne nowości takie jak ABS, stabilizacja toru jazdy, immobilajzer....

Na rysunku nr 2 przedstawiono poglądowy zestaw urządzeń elektronicznych w samochodzie z początku lat dwudziestych XXI wieku. Każdy z tych układów jest donorem danych, zapisywanych w jednej z kilku pamięci umieszczonych w samochodzie.



Rysunek nr 2. Urządzenia elektroniczne w samochodzie osobowym.
źródło: https://www.chipsetc.com/uploads/1/2/4/4/1244189/6873681_1_orig.png dostęp 20-05-2025

Wiele danych jest zbieranych przez producenta. Pozwala mu to optymalizować koszty serwisu i ... je odsprzedawać.

[11] https://portalstatystyczny.pl/samochody-w-polsce/ dostęp 20-05-2025.

Link https://vehicleprivacyreport.com prowadzi do strony, na której po wprowadzeniu numeru VIN[12] uzyskuje się informacje o danych zbieranych z konkretnego egzemplarza przez producenta samochodu, a także o aplikacjach służących do integracji smartfonu z samochodem.

Portal ten dostarcza też informacje o politykach udostępniania zebranych danych.

Jakie dane są zapisywane w pamięciach samochodu?

Dane te można pogrupować następująco:

1. Czas pokładowy.
   Pozwala na uszeregowanie chronologiczne zdarzeń i może odpowiedzieć na pytanie kiedy coś się zdarzyło. Uwaga: ten czas może się różnić od czasu urzędowego.
2. Praca. silnika.
   Czas włączenia i zatrzymania, obroty, przełożenie, ciśnienie oleju…
3. Komunikaty. Wszystko co samochód wyświetla, bądź sygnalizuje głosowo; w tym prędkość wg prędkościomierza, użycie kierunkowskazów, awaryjnego hamowania…
4. Rejestr zdarzeń:
   a. drzwi, okna;
   b. fotele, pasy;
   c. gaz/hamulec;
   d. …;
5. Urządzenia podłączone do:
   a. USB;
   b. Bluetooth;
   c. Wi-Fi;
   d. gniazda zapalniczki.
6. Używane media.
   Tu są informacje o korzystaniu z telefonów, streamingu, technologii radiowych, aplikacji (np. AndroidAuto, AppleCar) adresów IP…
7. Dane nawigacyjne:
   a. współrzędne GPS;
   b. prędkość, inna niż prędkość podana w sekcji „Komunikaty". Różnica większa od podanej we wzorze homologacyjnym jest przesłanką do wnioskowania o manipulowaniu dystansem poprzez obniżenie ciśnienia w oponach.
   c. Czas GPS.

[12] VIN (Vehicle Identyfication Number) – unikalny numer przypisywany do samochodu, pozwala na jednoznaczną identyfikację pojazdu.

8. Masa osoby na fotelu.
   Fotele ważą pasażera, by komputer mógł wyznaczyć moment inicjacji napinaczy pirotechnicznych pasów i poduszek.
9. Układy wspomagania i bezpieczeństwa.
   Dane w tej sekcji pokazują na sposób jazdy, stopień panowania nad samochodem. Np. częste uruchamianie się kontroli pasa ruchu może świadczyć o zakłóconej psychomotoryce kierowcy lub poświęcaniu uwagi innym czynnościom.

Ważnym jest określenie jaki czas jest czasem pokładowym. W zależności od woli właściciela i samochodu może to być czas synchronizowany z wzorcem czasu, ustawiony ręcznie itd.

Smartfon w samochodzie

Od wielu lat samochody są wyposażone w układ głośnomówiący zapewniający prowadzenie rozmów telefonicznych bez trzymania telefonu w dłoni. Do tego wystarczy zwykłe sparowanie „po bluetooth". Później po każdym włączeniu silnika następuje automatyczne nawiązanie łączności samochód ←→ smartfon i kopiowanie do pamięci samochodu:

- rejestru połączeń głosowych;
- „kontaktów".

Jeżeli smartfon został połączony z samochodem poprzez aplikację AndroidAuto/ AppleCar to do pamięci samochodu kopiowane są dane wszystkich aplikacji jakie są udostępnione na ekranie samochodu. Standardowo są to programy do wymiany poczty elektronicznej, SMS, kalendarz...

W sytuacji kiedy nie można wykonać akwizycji danych z telefonu warto spróbować pozyskać je z samochodu, z którym „sparowano" telefon.

Dostęp do danych zapisanych w samochodzie

Pełny dostęp do danych zapewni biegły/ekspert wyposażony w odpowiednie oprogramowanie i sprzęt do ich akwizycji i zabezpieczenia.

Można wystąpić do producenta samochodu o udostepnienie danych. Wspomniana strona https://vehicleprivacyreport.com dostarcza informacji o zakresie informacji zbieranych przez producenta.

Dane eksploatacyjne i serwisowe można pozyskać także za pomocą programów diagnostycznych. Programy takie są dostępne:

- w ASO[13] i innych serwisach samochodowych;
- w Internecie – najmniejszy zakres danych.

[13] ASO – Autoryzowany Serwis Obsługi – warsztaty samochodowe certyfikowane przez producenta samochodów.

Wnioski do części II

1. Powszechność elektronicznych urządzeń tworzących i zapisujących ślady elektroniczne powoduje niezwracanie na nie uwagi i zapominanie o pozostawionych śladach.
2. Źródłami informacji o aktywności danej osoby mogą być urządzenia elektroniczne jakie są w jej dyspozycji.
3. Najczęściej używanymi mobilnymi urządzeniami elektronicznymi są: smartfon, często ze smartwatch'em i samochód. W swoich pamięciach zapisują one bogactwo danych.

dr Jarosław Biegański[1]

Rola pojedynczego punktu kontaktowego FinCERT.pl w przeciwdziałaniu cyberprzestępczości finansowej

FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa
Związek Banków Polskich

Wprowadzenie

Wraz z rozwojem technologii wykorzystywanej do świadczenia usług finansowych, szczególnie w kanałach elektronicznych, coraz częściej dochodzi do wykorzystywania działalności banków do popełniania przestępstw. Cyberprzestępczość i cyberbezpieczeństwo w dobie świadczenia usług płatniczych w sposób zdalny stały się słowami odmienianymi przez wszystkie przypadki. Z punktu widzenia bezpieczeństwa finansowego istotne jest bieżące analizowanie zagrożeń i podatności, aby stale analizować ryzyko utraty bezpieczeństwa informacji, działać prewencyjnie na czynniki ryzyka i w razie potrzeby maksymalnie skrócić czas reakcji na incydent. Analizując zagrożenia należy zwrócić szczególną uwagę na zjawisko cyberprzestępczości, w tym popełnianej z wykorzystaniem usług finansowych, świadczonych w środowisku elektronicznym. Należy przyjąć, że korzystanie z owoców przestępstwa jest głównym czynnikiem motywującym sprawców do podejmowania nieuczciwej aktywności. Przerwanie procesu czerpania korzyści z nielegalnej działalności jest istotnym elementem wspólnej reakcji sektora finansowego i organów ścigania mającym na celu naprawienie krzywd wyrządzonych przez sprawców ofiarom przestępstw. Działanie takie powinno mieć także charakter odstraszający i zniechęcający. W niniejszym artykule podjęto temat usprawnienia reakcji sektora bankowego we współpracy z organami ścigania na przestępstwa popełniane z wykorzystaniem usług finansowych. Działania takie powinny podlegać procesowi stałego doskonalenia w ramach wspólnych inicjatyw partnerstwa publiczno-prywatnego.

Pojęcie cyberbezpieczeństwa i cyberprzestępczości

W literaturze przedmiotu funkcjonuje wiele definicji cyberbezpieczeństwa, w tym legalne na poziomie ustawy lub rozporządzenia UE. Zwykle w środowisku naukowym

[1] Jarosław Biegański, szef FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP, opiekun merytoryczny i współorganizator studiów podyplomowych z zakresu przeciwdziałania cyberprzestępczości finansowej na Uniwersytecie WSB Merito w Poznaniu, https://orcid.org/0000-0002-4689-5909 (przyp. autora).

i regulacyjnym koncentrowano się na technicznym ujęciu cyberbezpieczeństwa rozumianego jako bezpieczeństwo systemów teleinformatycznych. W ten sposób zdefiniowano cyberbezpieczeństwo w ustawie o krajowym systemie cyberbezpieczeństwa z 5 lipca 2018 r., w której cyberbezpieczeństwo określono jako *odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy*[2]. Nieco inaczej pojęcie cyberbezpieczeństwa zdefiniował Parlament Europejski wskazując w rozporządzeniu z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa), że cyberbezpieczeństwo oznacza *działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami*[3], jednocześnie definiując cyberzagrożenie jako *wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób*[4]. Warto zwrócić uwagę, że definicja zawarta w rozporządzeniu UE zwróciła uwagę na podmiot bezpieczeństwa: „użytkowników takich systemów oraz innych osób".

W niniejszym artykule skoncentrowano się na cyberbezpieczeństwie w aspekcie nauk społecznych, które definiują bezpieczeństwo kładąc nacisk na jego podmiotowość. Jeżeli przyjąć za Andrzejem Czupryńskim[5], że podmiotem bezpieczeństwa jest człowiek jako obiekt, któremu należy zapewnić bezpieczeństwo, można na podstawie definicji bezpieczeństwa A. Czupryńskiego wyprowadzić definicję cyberbezpieczeństwa w kontekście nauk społecznych. Jeżeli A. Czupryński wskazał, że *bezpieczeństwo definiowane w znaczeniu wąskim oznacza zdolność jego podmiotu do przeciwstawienia się zagrożeniom, a w kontekście szerokim oznacza zdolność podmiotu bezpieczeństwa do przetrwania i jego rozwoju*[6], to koncentrując się na wąskim znaczeniu termin cyberbezpieczeństwo można analogicznie

[2] Ustawa z dnia 5 lipca 2028 r. o krajowym systemie cyberbezpieczeństwa, tekst jednolity (Dz.U. 2024 poz. 1077), art.2 ust. 4.

[3] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881, art.2 ust. 1, (Dz.U. L 151/2019, s. 15).

[4] Tamże, art.2 ust. 8.

[5] dr hab. Andrzej Czupryński – był pracownikiem naukowo-dydaktycznym Akademii Obrony Narodowej i Wszechnicy Polskiej i zastępcą dyrektora Regionalnego Centrum Badań nad Bezpieczeństwem; autor i współautorem licznych opracowań naukowych z obszaru obronności i bezpieczeństwa; obszar zainteresowania naukowego i działalności dydaktycznej: nauki o obronności, nauki o bezpieczeństwie, nauki o polityce, metodologia badań (przyp. autora); zob. https://cnbop.pl/app/uploads/2024/11/Bezpieczenstwo-Teoria-Badania-Praktyka.pdf; https://orcid.org/0000-0002-0519-4989 (dostęp 11.07.2025).

[6] A. Czupryński, *Bezpieczeństwo w ujęciu teoretycznym,* [w:] Czupryński A., Wiśniewski B., Zboina J. (red.), *Bezpieczeństwo. Teoria – Badania – Praktyka,* Józefów 2015, s. 15.

zdefiniować jako zdolność (podmiotu bezpieczeństwa) do przeciwstawienia się zagrożeniom w cyberprzestrzeni. Pojęcie cyberprzestrzeni funkcjonuje już w świecie regulacji i oznacza przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami[7]. Jeżeli uznać, że najważniejszym podmiotem cyberbezpieczeństwa jest człowiek to jego zdolność do reagowania na zagrożenia w cyberprzestrzeni świadczyć może o stanie jego bezpieczeństwa, postrzeganym jako budowanie odporności na cyberzagrożenia. Jeżeli wziąć pod uwagę fakt, że cyberbezpieczeństwo podmiotu bezpieczeństwa może zostać naruszone przez cyberprzestępczość, to zdaniem autora zdefiniowanie cyberbezpieczeństwa jako zdolności do reagowania na zagrożenia w cyberprzestrzeni będzie pojęciem koncentrującym się na faktycznym stanie bezpieczeństwa podmiotu. Posługiwanie się wyłącznie definicją ustawową (z ustawy o krajowym systemie cyberbezpieczeństwa) może spowodować, że podmiot bezpieczeństwa nie do końca będzie świadomy, że cyberbezpieczeństwo może także zależeć od niego. Intencją zdefiniowania cyberbezpieczeństwa jako **zdolności do przeciwstawienia się zagrożeniom w cyberprzestrzeni** jest uniknięcie założenia, że cyberbezpieczeństwo jest tylko domeną profesjonalistów w aspekcie nauk technicznych, którzy to profesjonaliści w dziedzinie cyberbezpieczeństwa mają zapewnić odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

Specyfiką zagrożeń pojawiających się wraz z wykorzystaniem technologii teleinformatycznych jest brak fizycznego kontaktu z przestępcą. Brak wyraźnie zdefiniowanego przeciwnika może rozmywać ostrość i realizm dostrzegania zagrożeń, a tym samym sposób reagowania na nie. Może to także wpłynąć na zmniejszenie potrzeby tworzenia i utrzymywania stosownego systemu bezpieczeństwa[8]. Brak świadomości zagrożeń jest poważną podatnością. Taka sytuacja może utrudniać podejmowanie racjonalnych wysiłków służących budowaniu odporności oraz inicjowaniu reakcji na zagrożenia, które mogą się zmaterializować w postaci incydentów bezpieczeństwa.

Z naruszeniem cyberbezpieczeństwa ściśle związane jest pojęcie cyberprzestępczości. Przedstawiając kontekst cyberprzestępczości Jerzy Kosiński[9] wskazał, że cyberprzestępczość jest jednym z cyberzagrożeń, które obejmują nieuprawnione zachowania skierowane na uzyskanie dostępu, pozyskanie,

[7] zob. Ministerstwo Cyfryzacji, *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, s. 28.

[8] Za J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015, s. 18.

[9] Jerzy Kosiński – dr hab. inż., prof. AMW, dyrektor Morskiego Centrum Cyberbezpieczeństwa Akademii Marynarki Wojennej w Gdyni, zob. https://orcid.org/0000-0003-3823-4526; https://cyber24day.pl/osoby/dr-hab-inz-jerzy-kosinski-prof-amw/ (dostęp 12.07.2025).

manipulowanie lub utratę integralności, poufności i dostępności danych, aplikacji czy systemu komputerowego[10]. Analizując pojęcie cyberprzestępczości należy wskazać na brak definicji cyberprzestępstwa w akcie rangi ustawy. Zapytany o legalną definicję pojęcia cyberprzestępczości ChatGPT[11] odpowiedział: *W polskim systemie prawnym pojęcie „cyberprzestępczości" nie zostało wprost zdefiniowane w żadnym akcie prawnym, w tym w Kodeksie karnym ani w ustawach szczególnych dotyczących cyberbezpieczeństwa*, a dalej ChatGPT wskazał, że *w* ***Kodeksie karnym (Dz.U. 1997 nr 88 poz. 553 ze zm.)*** *znajdują się przepisy penalizujące konkretne czyny uznawane za cyberprzestępstwa (np. hacking, phishing, nielegalny dostęp do systemu informatycznego), ale nie ma tam definicji „cyberprzestępczości" jako pojęcia ogólnego. Przykłady takich przepisów:*

- *art. 267 – nieuprawnione uzyskanie dostępu do informacji,*
- *art. 268 – niszczenie, uszkadzanie lub zmiana informacji w systemie komputerowym,*
- *art. 269a – zakłócanie pracy systemów informatycznych,*
- *art. 287 – oszustwo komputerowe*[12].

ChatGPT dopytany o aktualność analizy udzielił odpowiedzi: *Analiza, którą Ci przedstawiłem, opiera się na stanie prawnym* ***obowiązującym w Polsce na dzień 27 czerwca 2025 r.****, czyli na datę dzisiejszą*[13]. Warto w tym miejscu wskazać, że ChatGPT nie był do końca precyzyjny, ponieważ w polskim systemie prawnym można odnaleźć zdefiniowane pojęcie cyberprzestępczości, co zostało wykazane w kolejnym akapicie niniejszego artykułu.

Na odniesienie się do pojęcia cyberprzestępczości można natrafić analizując zadania Centralnego Biura Zwalczania Cyberprzestępczości (dalej także CBZC), w których wskazuje się, że CBZC jako jednostka organizacyjna Policji służby zwalczania cyberprzestępczości odpowiedzialna jest za realizację zadań w zakresie rozpoznawania i zwalczania **przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej** oraz zapobiegania tym przestępstwom, a także wykrywania i ścigania sprawców tych przestępstw[14]. W polskim systemie prawnym wprowadzono definicję cyberprze-

[10] Zob. J. Kosiński, *Paradygmaty cyberprzestępczości*, Warszawa 2015, s. 14.

[11] ChatGPT – zaawansowany model językowy sztucznej inteligencji opracowany przez OpenAI, zob. https://pl.wikipedia.org/wiki/ChatGPT (dostęp 11.07.2025).

[12] ChatGPT, treść promptu (podpowiedzi): „w jakim polskim akcie prawnym zdefiniowano pojęcie cyberprzestępczości?" (dostęp 11.07.2025).

[13] ChatGPT, treść promptu: „wg stanu prawnego na jaki dzień zostały przedstawione te analizy?" (dostęp 11.07.2025).

[14] Zob. policja.pl, *Zadania Centralnego Biura Zwalczania Cyberprzestępczości,* https://cbzc.policja.gov.pl/bzc/o-cbzc/podstawowe-zadania/5,Zadania-Centralnego-Biura-Zwalczania-Cyberprzestepczosci.html (dostęp 7.07.2025).

stępczości w akcie rangi rozporządzenia, a konkretnie pojęcie to zostało określone w regulaminie wewnętrznym urzędowania powszechnych jednostek organizacyjnych prokuratury. Regulamin definiuje **cyberprzestępczość jako przestępstwa z wykorzystaniem Internetu oraz zaawansowanych technologii i systemów informatycznych**[15].

Serwis internetowy policja.pl informuje, że *cyberprzestępczość stanowi jedno z największych i najbardziej rozwijających się zagrożeń dla bezpieczeństwa obywateli naszego kraju. Jest zjawiskiem narastającym i niebezpiecznym. Skuteczna walka z zagrożeniami płynącymi z sieci możliwa jest wyłącznie w warunkach, gdy organy ścigania nie ustępują cyberprzestępcom zarówno w technologii jak i w umiejętnościach.*

Zwalczanie cyberprzestępczości powinno się opierać na ograniczaniu skutków jej wpływu na społeczeństwo oraz identyfikowaniu zagrożeń pochodzących z sieci. Głównym celem jest tworzenie bezpieczniejszej cyberprzestrzeni[16].

CBZC wskazało jako jeden z motywów swojego działania ograniczanie skutków wpływu cyberprzestępczości na społeczeństwo i właśnie temu aspektowi reagowania na cyberprzestępczość poświęcony został główny wątek tego artykułu.

Krajobraz zagrożeń z perspektywy Europolu

Europol[17] jako Agencja Unii Europejskiej ds. Współpracy Organów Ścigania analizuje tendencje przestępczości w UE. Podstawą działalności agencji jest analiza. Analitycy kryminalni Europolu należą do najlepiej wyszkolonych w Europie. Wykorzystują oni najnowocześniejsze narzędzia, aby codziennie wspierać postępowania przygotowawcze prowadzone przez organy ścigania w państwach członkowskich[18]. W celu określenia aktualnego krajobrazu zagrożeń poddano analizie raport Europolu, dotyczący oceny zagrożenia przestępczością zorganizowaną w Internecie: „Internet Organised Crime Threat Assessment IOCTA 2024". *Tegoroczny*[19] *raport uwypukla istotne trendy w obszarach przestępczości, takich jak*

[15] Zob. Rozporządzenie Ministra Sprawiedliwości z dnia 7 kwietnia 2016 r. – Regulamin wewnętrzny urzędowania powszechnych jednostek organizacyjnych prokuratury (Dz. U. z 2016 r., poz. 508), § 29 ust. 2 pkt 2.

[16] Policja.pl, https://cbzc.policja.gov.pl/bzc/o-cbzc/podstawowe-zadania/5,Zadania-Centralnego-Biura-Zwalczania-Cyberprzestepczosci.html (dostęp 7.07.2025).

[17] The European Union Agency for Law Enforcement Cooperation – agencja Unii Europejskiej, której głównym celem jest wspieranie współpracy między organami ścigania państw członkowskich UE w walce z poważną przestępczością zorganizowaną, cyberprzestępczością i terroryzmem, https://www.europol.europa.eu/about-europol (dostęp 13.07.2025).

[18] Zob. https://www.europol.europa.eu/about-europol:pl (dostęp 13.07.2025).

[19] Pomimo faktu, że w tytule raportu jest rok 2024, w treści komentarze często odnoszą się do roku 2023 (przyp. autora).

cyberataki, wykorzystywanie seksualne dzieci oraz oszustwa internetowe i płatnicze. Niedawne działania organów ścigania skłoniły grupy ransomware do rozłamu i rebrandingu pod różnymi szyldami. Co więcej, ciągłe zamykanie forów i platform handlowych w darknecie skróciło cykl życia witryn przestępczych. Ta niestabilność, w połączeniu z rosnącą liczbą oszustw, przyczyniła się do fragmentacji i namnażania się cyberzagrożeń[20].

Raport w czwartym rozdziale dedykowanym oszustwom w Internecie (*Online and payment fraud schemes*) podaje, że schematy oszustw internetowych i związanych z płatnościami stanowią rosnące zagrożenie przestępczością w UE i poza jej granicami, prowadząc do tego, że miliony obywateli UE stają się celem ataków, a kradzione są miliardy euro. Oszustwa inwestycyjne oraz przejęcia służbowej korespondencji e-mail (BEC) pozostają najczęściej występującymi formami oszustw internetowych. Coraz bardziej dostępne stają się usługi typu „phishing-as-a-service", a cyfrowy skimming (iniekcja złośliwego oprogramowanie na stronie internetowej sklepu) stanowi kolejne poważne zagrożenie, szczególnie dla sprzedawców internetowych (*e-merchantów*)[21].

Z analizy treści rozdziału nr 4 raportu IOCTA 2024 wynika, że do najpoważniejszych zagrożeń zidentyfikowanych przez Europol w roku 2023 należały:

- **phishing** jako główny wektor ataku, umożliwiający wyłudzenia danych uwierzytelniających, kart płatniczych czy danych osobowych; ataki były prowadzone poprzez złośliwe e-maile, SMS-y lub fałszywe strony internetowe podszywające się pod prawdziwe instytucje;
- **przejęcia kont** (ang. *account takeover*) – sytuacje, w których cyberprzestępca zdobył dostęp do konta ofiary (bankowego lub e-mailowego) i wykorzystał je do dalszych oszustw czy wyłudzeń; często do takiego ataku dochodziło z wykorzystaniem narzędzi zdalnego dostępu do komputera ofiary, na co pokrzywdzony wyraził zgodę pod wpływem manipulacji;
- **oszustwa inwestycyjne**, **business email compromise (BEC)** oraz **oszustwa romantyczne** (tzw. *romance scam*) jako kluczowe schematy przestępcze, prowokujące ofiary do błędnych decyzji poprzez fałszywe okazje inwestycyjne, podszywanie się pod zaufanych partnerów biznesowych lub stworzenie fikcyjnych więzi emocjonalnych w celu wyłudzenia środków finansowych;

[20] Zob. https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024 (dostęp 13.07.2025).

[21] Zob. Europol, *Internet Organised Crime Threat Assessment IOCTA 2024*, s. 27 https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf (dostęp 13.07.2025).

- **cyfrowy skimming** jako technologia służąca do kradzieży danych kart płatniczych osób odwiedzających strony e-commerce; zagrożenie wykorzystujące działalność sprzedawców internetowych w celu niezauważonego instalowania złośliwego kodu;
- **ataki na bankomaty** od fizycznych manipulacji (skimmery, nakładki) po ataki zdalne na oprogramowanie bankomatów;
- **połączenie oszustw internetowych z procederem prania pieniędzy** umożliwiającym cyberprzestępcom poprzez konta mułów (ang. *money mules*) legalizację skradzionych środków[22].

Wspólna reakcja sektora bankowego i organów ścigania na cyberprzestępczość

Strategia reagowania na cyberprzestępczość może przejawiać się zarówno w ściganiu sprawców przestępstw, jak i w ściganiu środków finansowych (określana jako strategia *follow the money*). Faktem jest, że do popełniania cyberprzestępstw wykorzystuje się działalność instytucji finansowych, a obecnie, to jest od roku 2024, najczęstszym schematem realizowanym przez sprawców przestępstw finansowych jest nakłanianie płatnika do realizacji płatności na jego własną szkodę. Socjotechniczna manipulacja w roku 2024 była przyczyną trzech na cztery zgłoszone transakcje oszukańcze. Według danych NBP w drugim półroczu 2024 r. *dokonano 32,0 tys. oszustw z wykorzystaniem polecenia przelewu (więcej o 3,7% w porównaniu z I półroczem 2024 r.) o wartości 282,8 mln zł (wzrost o 2,9%).* ***Liczba oszustw wynikających z nakłonienia zmanipulowanego płatnika do realizacji przelewu wzrosła*** *względem I półrocza o 17,2% (do 23,7 tys.), zaś ich wartość o 20,8% (do 213,8 mln zł).* ***Oszustwa te stanowiły 74,0% liczby oraz 75,6% wartości wszystkich transakcji oszukańczych z wykorzystaniem polecenia przelewu.*** *Średnia wartość jednego oszukańczego przelewu w II półroczu 2024 r. wyniosła 8 844,1 zł (spadek o 0,8% względem poprzedniego półrocza)*[23]. Mając świadomość tych danych w artykule podjęto próbę wykazania, że na ograniczenie zjawiska transakcji oszukańczych może wpłynąć zdecydowana i natychmiastowa reakcja sektora bankowego we współpracy z organami ścigania.

Dla procesu reakcji na przestępstwo kluczowy jest czas pozyskania wiedzy o incydencie. Jeżeli reakcja ma być skuteczna trzeba dać szanse organom ścigania i instytucjom finansowym na podjęcie odpowiednich działań. O zainicjowaniu

[22] Zob. Europol, *Internet Organised Crime Threat Assessment IOCTA 2024*, s. 28-31 https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf (dostęp 13.07.2025).

[23] NBP, *Ocena funkcjonowania polskiego systemu płatniczego w II półroczu 2024 r.*, https://nbp.pl/wp-content/uploads/2025/05/Ocena-II-polrocze-2024-r.pdf (dostęp 12.07.2025).

procesu powinien jak najszybciej zdecydować pokrzywdzony. Zgłoszenie przez pokrzywdzonego powinno w pierwszej kolejności dotyczyć poinformowania banku lub innej instytucji finansowej, z wykorzystaniem usług której doszło do popełnienia przestępstwa. Przykładowo jeżeli przestępstwo miało postać oszustwa polegającego na wprowadzeniu w błąd pokrzywdzonego, który udostępnił przestępcom swój rachunek bankowy lub umożliwił dokonanie płatności poprzez udostępnienie danych uwierzytelniających i zatwierdzenie płatności w sposób przewidziany w umowie ramowej o usługę płatniczą, to w takiej sytuacji pokrzywdzony jak najszybciej powinien zgłosić fakt przestępstwa do banku, w którego usługach bankowości elektronicznej zostały zlecone kwestionowane płatności. Dla celów badanego zagadnienia pominięto fakt rozważeń związanych z zagadnieniem prawnym, kto powinien ponieść odpowiedzialność finansową za transakcje dokonane w wyniku oszustwa (często do oszukańczych transakcji przyczynia się sam pokrzywdzony zatwierdzając je w usługach bankowości elektronicznej bez wystarczającej staranności). Z punktu widzenia interesu cyberprzestępców zagadnienie poniesienia odpowiedzialności za wyłudzone płatności nie ma znaczenia. Mają natomiast znaczenie wszelkie działania ograniczające skuteczność ataku, a w szczególności każde ograniczenie korzyści finansowej sprawców. Dla efektywnej reakcji najskuteczniejsze jest jak najszybsze prawidłowe poinformowanie przez pokrzywdzonego o wszystkich okolicznościach mających związek z oszustwem. Ukrywanie kłopotliwych działań przez ofiarę może tylko opóźnić skuteczność reakcji. Ważne jest przełamanie bariery wstydu przez pokrzywdzonego. Zgłoszenie przestępstwa powinno być priorytetem. Rzetelna informacja o zaistniałych okolicznościach może przyczynić się do zidentyfikowania sprawców i odzyskania utraconych środków. **Zaleca się, aby po poinformowaniu banku jak najszybciej poinformować organy ścigania.** W praktyce obserwuje się także odwrotną kolejność, najpierw informowane są organy ścigania w postaci zawiadomienia a kolejno instytucja finansowa. Należy docenić fakt, że organy ścigania podejmują wspólne działania z sektorem finansowym. Brak informacji o tym, w jaki sposób i na jakie konto (na jaki rachunek płatniczy) zostały przekazane pozyskane w wyniku przestępstwa środki znacząco może opóźnić proces ich odzyskania. Ustalenie wszelkich okoliczności może mieć istotne znaczenie dla ustalenia sprawców. Z punktu widzenia odzyskania utraconych środków najbardziej pilne jest uruchomienie procesów związanych ze śledzeniem przepływów finansowych w celu zatrzymania zleceń płatniczych realizowanych przez sprawców.

W tym celu Związek Banków Polskich podjął działania związane z powołaniem do życia pojedynczego punktu kontaktowego, prowadzonego przez FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP (dalej także FinCERT.pl lub Bankowe Centrum Cyberbezpieczeństwa). FinCERT.pl – BCC ZBP funkcjonuje w ramach

Komitetu Cyberbezpieczeństwa Banków jako jednostka operacyjna, która gromadzi, analizuje oraz przekazuje w ramach sektora bankowego i we współpracy z organami ścigania oraz innymi instytucjami, informacje dotyczące zidentyfikowanych zagrożeń oraz o incydentach o charakterze przestępczym, godzących w bezpieczeństwo banków oraz ich klientów[24]. W raporcie z dnia 14 lutego 2018 r. ENISA (Agencja Unii Europejskiej ds. Cyberbezpieczeństwa) uznała Bankowe Centrum Cyberbezpieczeństwa ZBP za ISAC (Centrum Wymiany i Analizy Informacji) polskiego sektora bankowego[25]. Zorganizowanie pojedynczego punktu kontaktowego dla organów ścigania i instytucji finansowych ma na celu usprawnienie procesu reakcji na incydent. Projekt ten zyskuje na znaczeniu szczególnie w sytuacji, gdy brakuje informacji na temat przepływu środków finansowych kontrolowanych przez sprawców cyberprzestępstw. Sektor finansowy i organy ścigania mogą wspólnie reagować, jeżeli będą potrafiły odpowiedzieć na pytania: co się stało, kiedy, skąd i dokąd zostały przekazane środki finansowego, a konkretnie jakie są numery rachunków wykorzystywane przez sprawców oraz z wykorzystaniem jakich danych zostały uruchomione usługi finansowe. Pokrzywdzony nie zawsze potrafi wskazać co się stało i do kogo zostały uruchomione oszukańcze płatności. W pozyskaniu takich informacji powinna pomóc instytucja finansowa, która prowadzi rachunek płatniczy, z którego na skutek działań przestępców została zainicjowana płatność. Dla usprawnienia pozyskania tego rodzaju informacji w momencie składania zawiadomienia przez pokrzywdzonego organy ścigania powinny wykorzystać wzór upoważnienia (załącznik 1)[26], który banki mają obowiązek respektować. W przypadku zastosowania upoważnienia istnieje możliwość pozyskania potrzebnych informacji stanowiących tajemnicę bankową na zasadach określonych w art. 104 ust. 3 prawa bankowego[27]. W tym miejscu należy nadmienić, że rozwiązaniem najefektywniejszym jest sytuacja, kiedy pokrzywdzony pozyska te informacje zanim zgłosi się do organów ścigania. Szablon upoważnienia jest rezultatem prac ekspertów skupionych wokół Komitetu Cyberbezpieczeństwa Banków ZBP we współpracy z przedstawicielami Komendy Głównej Policji i Prokuratury Krajowej i został uznany za obowiązujący banki standard na podstawie Rekomendacji Zarządu Związku Banków Polskich z dnia 24 października 2023 r.

[24] Zob. ZBP, *Cyberbezpieczeństwo banków i ich klientów,* https://zbp.pl/Dla-Bankow/Cyberbezpieczenstwo/Cyberbezpieczenstwo-bankow-i-ich-klientow (dostęp 11.07.2025).

[25] Zob. ENISA, *Information Sharing and Analysis Center (ISACs) – Cooperative models,* s. 49 https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models/ (dostęp 11.07.2025).

[26] ZBP, *Załącznik do Rekomendacji Zarządu Związku Banków Polskich z dnia 24 października 2023 r.*

[27] Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz.U.2024.0.1646 t.j.), art. 104 ust. 3.

Jeżeli organy ścigania posiadają informację o okolicznościach przestępstwa, do którego doszło z wykorzystaniem usług finansowych, mają możliwość skorzystania z tzw. „formularza blokadowego" opracowanego przez Bankowe Centrum Cyberbezpieczeństwa we współpracy z Biurem Zwalczania Przestępczości Ekonomicznej Komendy Głównej Policji (załącznik 2). Zastosowanie formularza blokadowego pozwala dokonać zamrożenia środków pochodzących z przestępstwa na podstawie art. 106a ust.3 prawa bankowego[28]. Warunkiem jest jak najszybsze przekazanie informacji na skrzynkę pojedynczego punktu kontaktowego: alert@fincert.pl.

Analiza studiów przypadków

Na potrzeby uzasadnienia, że procesy realizowane przez FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP mogą chronić pokrzywdzonych przed utratą środków finansowych na skutek cyberprzestępstw wybrano do analizy dwa studia przypadków[29].

Sprawa typu BEC (business email compromise)

Komenda Powiatowa Policji po przyjęciu zawiadomienia od przedstawiciela lokalnego przedsiębiorcy w toku prowadzonego postępowania ustaliła, że z pokrzywdzonym nawiązał kontakt sprawca, który podszył się pod firmę, mającą wykonać uprzednio zamówioną przez przedsiębiorcę usługę. Kontakt z przedsiębiorcą nastąpił z wykorzystaniem poczty elektronicznej i miał dotyczyć odebrania płatności za znaną przedsiębiorcy usługę. Przedsiębiorca po dokonaniu przelewu zorientował się, że płatność została wykonana na inne konto niż rachunek bankowy jego kontrahenta. Policja po odebraniu zawiadomienia wykorzystała pojedynczy punkt kontaktowy: alert@fincert.pl, dzięki któremu w trybie natychmiastowym w sposób zapewniający bezpieczeństwo informacji została przekazana wiadomość o oszustwie z wykorzystaniem międzybankowych systemów wymiany informacji Związku Banków Polskich. Docelowo informacja trafiła do banku, który prowadził rachunek kontrolowany przez sprawcę – odbiorcę wyłudzonej płatności. W wyniku prowadzonych działań zabezpieczono kwotę blisko 120.000 zł, co stanowiło 100% potencjalnej straty.

Oszustwo z wykorzystaniem ogłoszeniowego serwisu internetowego

Komisariat Policji po przyjęciu zawiadomienia od pokrzywdzonej ustalił, że z pokrzywdzoną nawiązał kontakt sprawca po ogłoszeniu przez pokrzywdzoną

[28] Tamże, art. 106a ust. 3.

[29] Na podstawie badań własnych autora – Szefa FinCERT.pl – BCC ZBP.

w serwisie internetowym zamiaru sprzedaży przedmiotu stanowiącego własność pokrzywdzonej. Sprawca przedstawiając się jako potencjalny kupujący, oświadczył, iż opłacił firmę kurierską, a pokrzywdzona otrzymała mailem link do strony internetowej celem potwierdzenia transakcji. Po kliknięciu w nieznany link pokrzywdzona zalogowała się do bankowości internetowej, jak sądziła własnego banku. Następnie w toku kolejnego połączenia telefonicznego inny sprawca podający się za przedstawiciela firmy kurierskiej przekonał pokrzywdzoną do podania treści komunikatów sms, które dotyczyły potwierdzenia transakcji przelewu na rachunek obcy. Na skutek manipulacji pokrzywdzona podała kody SMS do trzech transakcji wychodzących z jej rachunku, co spowodowało w sumie obciążenie jej konta bankowego kwotą ponad 60.000 zł. System antyfraudowy banku, w którym pokrzywdzona miało konto wysłał do pokrzywdzonej alert o konieczności dodatkowej weryfikacji dla części dokonanych płatności. Alert spowodował zgłoszenie telefoniczne przez pokrzywdzoną reklamacji do jej banku oraz zawiadomienie organów ścigania. Dzięki uruchomieniu procesu z wykorzystaniem pojedynczego punktu kontaktowego FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP nawiązało kontakt z bankiem pokrzywdzonej, ustaliło szczegóły rachunku odbiorcy oszukańczych płatności i uruchomiło procedurę blokadową we współpracy z bankiem odbiorcy płatności. Na skutek współpracy banku pokrzywdzonej, samej pokrzywdzonej, organów ścigania oraz banku odbiorcy wyłudzonej płatności zabezpieczono w obu bankach 100% potencjalnej straty (część kwoty skierowana do dodatkowej weryfikacji w procesie antyfraudowym nie opuściła banku pokrzywdzonej, a część kwoty potencjalnej straty została zatrzymana w banku odbiorcy płatności).

Konkluzje

W obu przypadkach doszło do pozbawienia sprawców owoców przestępstwa dzięki przygotowaniu z wyprzedzeniem odpowiednich procesów, które zostały uruchomione w odpowiednim momencie. Jest to dowód na to, że sektor finansowy wspólnie z organami ścigania uzyskał zdolność do przeciwstawienia się sprawcom cyberprzestępstw, którzy pomimo skutecznego ataku na pokrzywdzonych zostali skutecznie zneutralizowani przez profesjonalnie przygotowane służby bezpieczeństwa. Czynniki, które miały wpływ na taki rezultat działań to:

- świadomość pokrzywdzonych, że padli ofiarą oszustwa i ich prawidłowa reakcja, polegająca na zawiadomieniu organów ścigania bez zbędnej zwłoki;
- adekwatna do sytuacji reakcja organów ścigania i wiedza jak zadziałać (procedury zostały wcześniej przygotowane, zakomunikowane i przećwiczone, dzięki warsztatom z udziałem banków i organów ścigania oraz dzięki koordynującej

roli Biura Zwalczania Przestępczości Ekonomicznej KGP i Wydziałów do Walki z Przestępczością Gospodarczą Komend Wojewódzkich Policji);
- profesjonalna reakcja sektora bankowego z wykorzystaniem pojedynczego punktu kontaktowego FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa ZBP – reakcja była możliwa dzięki przygotowanym procesom i wykorzystaniu podstaw prawnych do takiego działania: artykułu 106a ust.3 prawa bankowego (możliwość zablokowania środków, co do których istnieje uzasadnione podejrzenie, że pochodzą z przestępstwa) oraz artykułu 106d ust.1 prawa bankowego (możliwość przetwarzania informacji stanowiących tajemnicę bankową przez ustawowo upoważniony krąg podmiotów w przypadkach uzasadnionych podejrzeń, o których mowa w art. 106a ust. 3 prawa bankowego).

Podsumowanie

W artykule przedstawiono wybrany aspekt przeciwdziałania cyberprzestępczości finansowej. Mianowicie skoncentrowano się na roli FinCERT.pl – Bankowego Centrum Cyberbezpieczeństwa w integrowaniu współpracy sektora bankowego z organami ścigania w celu ograniczenia skutków finansowych popełnionych przestępstw, do których doszło z wykorzystaniem usług finansowych oferowanych przez banki lub innych dostawców usług płatniczych. Wykazano, że jest możliwe skuteczne pokrzyżowanie szyków sprawcom przestępstw dzięki wcześniej uzgodnionym, przygotowanym, wdrożonym i przećwiczonym procedurom i procesom. Kluczem do sukcesu jest spójna i szybka reakcja sektora finansowego, jego klientów oraz organów ścigania w sytuacji wykrycia przestępstwa popełnionego z wykorzystaniem usług finansowych. Odzyskiwanie środków pochodzących z przestępstw jest ważnym elementem przeciwdziałania cyberprzestępczości finansowej, a budowanie procesów pozwalających na wymianę informacji i skuteczne zamrażanie środków pochodzących z przestępstwa to dowód tworzenia trwałej zdolności do reakcji na cyberzagrożenia.

Dla porządku należy wspomnieć, że rola Bankowego Centrum Cyberbezpieczeństwa nie kończy się na funkcjonowaniu pojedynczego punktu kontaktowego. Inne inicjowane przez FinCERT.pl – BCC ZBP działania w obszarze bezpieczeństwa finansowego to w szczególności:
- realizowany wspólnie przez ZBP i KIR projekt Sektorowego Centrum Usług AML (realizacja idei sektorowej reakcji na procesy prania pieniędzy);
- projekty edukacji eksperckiej (warsztaty i ćwiczenia cyberbezpieczeństwa, organizowanie konferencji naukowych oraz studiów podyplomowych w obszarze przeciwdziałaniu cyberprzestępczości finansowej);

- komunikaty i ostrzeżenia o aktualnych zagrożeniach, publikowane na stronie fincert.pl;
- powoływanie eksperckich grup roboczych w celu opracowania standardów i rekomendacji na rzecz bezpieczeństwa usług finansowych;
- koordynowanie grup operacyjnych tzw. *task force*, nakierowanych na pomoc organom ścigania w wykryciu sprawców cyberprzestępstw, popełnianych z wykorzystaniem usług finansowych;
- projekt wspólnych audytów dostawców usług ICT w celu efektywnego budowania odporności cyfrowej sektora bankowego;
- bieżąca analiza podatności i zagrożeń oraz dzielenie się tymi informacjami z wykorzystaniem międzybankowych systemów wymiany informacji ZBP.

Bibliografia

1. ChatGPT, https://pl.wikipedia.org/wiki/ChatGPT (dostęp 11.07.2025).
2. Czupryński A., Bezpieczeństwo w ujęciu teoretycznym, [w:] Czupryński A., Wiśniewski B., Zboina J. (red.), Bezpieczeństwo. Teoria – Badania – Praktyka, Józefów 2015.
3. ENISA, Information Sharing and Analysis Center (ISACs) – Cooperative models, s. 49 https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models/ (dostęp 11.07.2025).
4. Europol, https://www.europol.europa.eu/about-europol (dostęp 13.07.2025).
5. Europol, https://www.europol.europa.eu/about-europol:pl (dostęp 13.07.2025).
6. Europol, https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024 (dostęp 13.07.2025).
7. Europol, Internet Organised Crime Threat Assessment IOCTA 2024, https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf (dostęp 13.07.2025).
8. Kosiński J., Paradygmaty cyberprzestępczości, Warszawa 2015.
9. Ministerstwo Cyfryzacji, Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022.
10. NBP, Ocena funkcjonowania polskiego systemu płatniczego w II półroczu 2024 r., https://nbp.pl/wp-content/uploads/2025/05/Ocena-II-polrocze-2024-r.pdf (dostęp 12.07.2025).
11. Policja.pl, Zadania Centralnego Biura Zwalczania Cyberprzestępczości, https://cbzc.policja.gov.pl/bzc/o-cbzc/podstawowe-zadania/5,Zadania-Centralnego-Biura-Zwalczania-Cyberprzestepczosci.html (dostęp 7.07.2025).

12. Rozporządzenie Ministra Sprawiedliwości z dnia 7 kwietnia 2016 r. – Regulamin wewnętrzny urzędowania powszechnych jednostek organizacyjnych prokuratury (Dz. U. z 2016 r., poz. 508).
13. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 (Dz.U. L 151/2019).
14. Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (Dz.U.2024.0.1646 t.j.), art. 104 ust. 3.
15. Ustawa z dnia 5 lipca 2028 r. o krajowym systemie cyberbezpieczeństwa, tekst jednolity (Dz.U. 2024 poz. 1077).
16. ZBP, Cyberbezpieczeństwo banków i ich klientów, https://zbp.pl/Dla-Bankow/Cyberbezpieczenstwo/Cyberbezpieczenstwo-bankow-i-ich-klientow (dostęp 11.07.2025).
17. ZBP, Załącznik do Rekomendacji Zarządu Związku Banków Polskich z dnia 24 października 2023 r.

Załącznik 1

....
(imię i nazwisko) *(miejscowość i data)*

.....

.....
(adres)

.....
(PESEL)

.....
(nr tel., adres e-mail)

Upoważnienie

Na podstawie art. 104 ust. 3 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz.U.2020.1896 t.j.), podpisan(y/a) .....
upoważniam ..... do przekazywania wszelkich
(nazwa banku)

informacji, w tym objętych tajemnicą bankową dotyczących mo(jego/jej/ich):

- rachunk(u/ów) bankow(ego/ych) nr:
  .....
- kart(y) płatnicz(ej/ych) nr:
  .....
- produkt(u/ów) bankow(ego/ych): .....
  .....

wyłącznie na potrzeby czynności sprawdzających/postępowania przygotowawczego* o sygn.: .....
prowadzonego(ych) przez .....
(pełna nazwa jednostki Policji/Prokuratury prowadzącej sprawę)

w związku ze zdarzeniem: .....
.....
.....

....
(czytelny podpis osoby odbierającej oświadczenie) *(podpis osoby upoważniającej – zgodny z kartą wzoru podpisu w banku)*

*Adnotacje urzędowe***

.....
.....
.....

*Niepotrzebne skreślić
**Adnotacje urzędowe dotyczące np.: zmiany sygnatury sprawy, zmiany jednostki prowadzącej postępowanie

Załącznik 2

Informacja dotycząca uzasadnionego podejrzenia wykorzystania rachunku bankowego do działalności przestępczej

wysłać na: **alert@fincert.pl**

		miejscowość / data
PRIORYTET: /zaznaczyć właściwy/		
	PILNY	
	ZWYKŁY	
ZNAK SPRAWY:		
Wnioskodawca:		
Adresat:	Dyrektor Zespołu Bezpieczeństwa Banków, Związek Banków Polskich, ul. Leona Kruczkowskiego 8, 00-380 Warszawa	
I. Informacja o sprawie:		
a) Podstawa prawna skierowania informacji		
b) Sygnatura prowadzonego postępowania		
c) Kwalifikacja prawna (przestępstwo objęte postępowaniem)		
d) Data, czas zdarzenia		
e) Miejsce ujawnienia zdarzenia:		
f) Data, czas i miejsce zawiadomienia organów ścigania		
g) Jednostka Policji przyjmująca zawiadomienie:		
h) Rodzaj instrumentu płatniczego, do którego sprawca uzyskał dostęp		
i) Wysokość strat:		
j) Jednostka prokuratury właściwa do blokady rachunku (dla jednostki kierującej wniosek)		
Informacje o okolicznościach popełnionego przestępstwa:		

II. Rachunki wykorzystane do działalności przestępczej (RS):		
1. rachunek (RS-1)		
Numer rachunku bankowego RS		
Numer rozliczeniowy banku/nazwa banku		
Dane transakcji:	Numer rachunku bankowego z którego dokonano przelewu na RS	
	Nazwa odbiorcy:	
	Tytuł operacji:	
	Nr referencyjny operacji	
	Data operacji:	
	Data księgowania:	
	Kwota operacji (Waluta)	
	Numer transakcji BLIK (jeśli wykorzystano BLIK)	
	Dane dodatkowe BLIK:	

2. Rachunek (RS-2) – *dodać jeśli występuje*

III. Dane identyfikujące podmiot pokrzywdzony:							
Lp.	Imię i nazwisko/ nazwa podmiotu	Forma prawna działalności	PESEL	NIP/REGON/ KRS	Numer dowodu osobistego/ paszportu/ zagranicznego dokumentu identyfikującego	Data urodzenia	Inne dane identyfikujące (np. adres IP, adres zamieszkania, adres prowadzonej działalności gospodarczej)
1.							

IV. Treść wniosku:
Z uwagi na uzasadnione podejrzenie, że zgromadzone na wskazanych rachunkach RS-1 i RS-2 wartości pieniężne w całości lub w części pochodzą lub mają związek z przestępstwem [bądź istnieje uzasadnione podejrzenie popełnienia przestępstw na szkodę banku lub jego klienta] proszę o przeprowadzenie analizy oraz rozważenie możliwości zablokowania środków zgromadzonych na rachunku na podstawie art. 106a ust. 3 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe.

V. Dane kontaktowe Osoby merytorycznie zajmującej się sprawą/koordynatora	
a) Imię i Nazwisko	
b) Stanowisko służbowe	
c) Telefon komórkowy	
d) e-mail	
e) Reprezentowany podmiot (wraz z adresem)	

....

ID służbowe/podpis wykonującego pieczęć i podpis przełożonego/dyżurnego jednostki

Arkadiusz Czak[1]

Wizualizacja danych w analizie kryminalnej: zastosowanie aplikacji yEd Graph Editor w tworzeniu diagramów relacyjnych

Streszczenie/Abstract

Artykuł przedstawia zastosowanie edytora grafów yEd Graph Editor w analizie grafowej danych śledczych, ze szczególnym uwzględnieniem relacji typu obiekt-obiekt oraz typologii krawędzi. Omówiono proces przygotowania danych wejściowych (CSV, Excel), strukturyzację węzłów i relacji, automatyczne układy diagramów oraz eksport do formatów wektorowych (SVG, GraphML). Opisano trzy autorskie aplikacje wspierające integrację z yEd: konwerter Excel2yEd (generowanie plików grafowych z tabel), yEd2Excel (ekstrakcja danych z diagramów) oraz SVG Converter (tworzenie ikon dla wizualizacji semantycznej). Zaprezentowane rozwiązania umożliwiają interoperacyjność między środowiskami analitycznymi a wizualizacyjnymi oraz wspierają eksplorację relacji w danych nieustrukturyzowanych.

Słowa kluczowe: yEd Graph Editor, analiza grafowa, import danych, SVG, GraphML, relacje węzłowe, interoperacyjność narzędziowa

Wprowadzenie: Analiza relacyjna w kontekście kryminalistyki

Współczesne działania operacyjne i analizy kryminalne wymagają coraz częściej zastosowania narzędzi umożliwiających identyfikację, wizualizację oraz interpretację relacji zachodzących między osobami, zdarzeniami, przedmiotami i lokalizacjami. Jednym z kluczowych sposobów prezentacji tych relacji są tzw. diagramy połączeń (ang. link analysis diagrams), które odwzorowują struktury w formie grafów – skierowanych lub nieskierowanych – składających się z węzłów (reprezentujących obiekty) i krawędzi (reprezentujących powiązania między nimi)

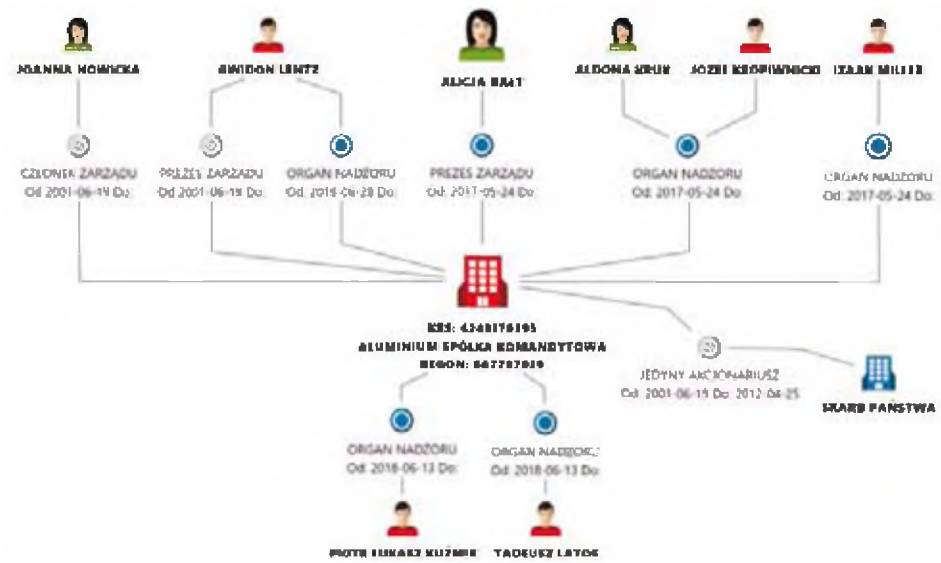
Z punktu widzenia metod analitycznych, podejście to zakorzenione jest w teorii grafów oraz analizie sieci społecznych (SNA – **Social Network Analysis).** Analiza sieci społecznych (SNA) staje się coraz bardziej wartościowym narzędziem dla służb policyjnych próbujących zrozumieć złożone relacje w ramach grup przestępczych. Wykorzystanie diagramów połączeń umożliwia śledczym wizualizację i interpretację powiązań między osobami, lokalizacjami, zdarzeniami i przedmiotami, przekształcając surowe dane w użyteczną informację operacyjną[2].

[1] Arkadiusz Czak – oficer Zachodniopomorskiego Urzędu Celno-Skarbowego w Szczecinie.

[2] Cramer, C., & Hochleitner, R. (2018). Visualizing criminal networks: A case study of social network analysis in law enforcement. Police Practice and Research , 19(6), 547–563.

Zastosowanie technik wizualizacji sieci pozwala policji ujawniać ukryte struktury w organizacjach przestępczych, identyfikować kluczowe osoby, śledzić przepływ zasobów i informacji oraz nawiązywać powiązania między incydentami a podejrzanymi.[3]

Ich skuteczność została potwierdzona w licznych opracowaniach empirycznych, zarówno na gruncie krajowym, jak i międzynarodowym[4]. W Polsce zagadnienie analizy relacyjnej w działaniach policyjnych i antykorupcyjnych rozwijane jest m.in. przez Centralne Biuro Antykorupcyjne oraz Krajową Szkołę Sądownictwa i Prokuratury[5].



Obraz 1. https://gazeta.policja.pl/997/archiwum-1/2022/numer-23-112022-r/225150,Analiza-kryminalna-w-PG.html

Diagramy połączeń (ang. link charts) to graficzne przedstawienie relacji między elementami, takimi jak osoby, miejsca, pojazdy czy firmy, które stanowią jedno z kluczowych narzędzi analizy kryminalnej. Stanowią one nieodzowną część zarówno analizy operacyjnej, jak i strategicznej, umożliwiając organom ścigania efektywne rozpoznanie i zrozumienie działań grup przestępczych oraz planowanie odpowiednich

[3] Cramer, C., & Hochleitner, R. (2018). Visualizing criminal networks: A case study of social network analysis in law enforcement. Police Practice and Research, 19 (6), 547–563. https://doi.org/10.1080/15614263.2017.1395747.

[4] Skaliński, Z. (2021). Praktyczne wykorzystanie analizy sieci społecznej (SNA) w analizie śledczej.

[5] Lebiedowicz, A. (2023). Wykorzystanie analizy kryminalnej w działalności organów ścigania. Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury, Zeszyt 4 (52)/2023.

działań.[6] Znaczenie diagramów połączeń jest wielowymiarowe i obejmuje szereg kluczowych funkcji:

1. Wizualizacja relacji w strukturach przestępczych

Graficzne odwzorowanie powiązań pomiędzy podejrzanymi, ofiarami, miejscami zdarzeń i dowodami rzeczowymi odgrywa istotną rolę poznawczą w analizie śledczej. Umożliwia ono identyfikację wewnętrznej organizacji grup przestępczych, w tym struktury hierarchicznej, kierunków przepływu informacji oraz kluczowych aktorów (węzłów centralnych) pełniących funkcje liderów, pośredników lub wykonawców.

2. Przekład złożonych danych na formę wizualną

Obszerne zbiory danych tekstowych – takie jak bilingi telefoniczne, meldunki operacyjne czy zapisy z baz informacyjnych – bywają trudne do bezpośredniego przetworzenia. Diagramy połączeń umożliwiają przekształcenie tych nieczytelnych treści w przejrzyste struktury graficzne, ułatwiające zarówno wewnętrzną analizę zespołów śledczych, jak i prezentację ustaleń przed organami procesowymi.

3. Konsolidacja danych pochodzących z różnych źródeł

Reprezentacje wizualne sprzyjają integracji informacji pochodzących z wielu niezależnych źródeł – m.in. rejestrów policyjnych, monitoringu, systemu PESEL, KRS czy notatek operacyjnych. Umożliwia to budowanie spójnych, wielowymiarowych modeli analitycznych, które można aktualizować w miarę postępu śledztwa.

4. Analiza czasowo-przestrzenna zdarzeń

Graficzne odwzorowanie relacji w układzie chronologicznym i przestrzennym pozwala odtworzyć przebieg zdarzeń i rozpoznać potencjalne wzorce działania. Diagramy pomagają zidentyfikować momenty kulminacyjne, punkty styczne między sprawcami oraz lokalizacje o podwyższonym ryzyku, wspierając planowanie działań operacyjnych.

5. Wsparcie w profilowaniu sprawców

Analiza powiązań między zdarzeniami, osobami i miejscami umożliwia uchwycenie charakterystycznych cech modus operandi sprawcy. Diagramy sieciowe ujawniają powtarzające się schematy działania, co sprzyja łączeniu pozornie odrębnych spraw i zwiększa skuteczność ich wykrywania.

6. Optymalizacja działań operacyjnych

Graficzne modele relacyjne ułatwiają typowanie osób do obserwacji, identyfikację węzłów komunikacyjnych oraz lokalizacji intensywnej aktywności przestępczej. Dzięki temu możliwe staje się skuteczniejsze planowanie obserwacji, zatrzymań czy działań prewencyjnych.

[6] Ratcliffe, J. H. (2016). Intelligence-led policing (2nd ed.). Routledge. str. 138.

7. Funkcja dokumentacyjna i dowodowa

Diagramy mogą pełnić funkcję nie tylko analityczną, lecz również dokumentacyjną. Są wykorzystywane w raportach operacyjnych, analizach końcowych, a także jako materiał uzupełniający w postępowaniach sądowych. Ich przejrzysta forma graficzna sprzyja zrozumieniu złożonych układów zależności przez osoby niezaangażowane bezpośrednio w analizę.

8. Ujawnianie luki informacyjnych

Zastosowanie diagramów relacyjnych sprzyja ujawnianiu braków w materiale dowodowym – tzw. „pustych pól", czyli miejsc, gdzie oczekiwane powiązania nie zostały jeszcze ustalone lub relacje pozostają niewyjaśnione. Takie wizualnie zidentyfikowane luki mogą stanowić istotny sygnał dla analityków do pogłębionej eksploracji danego obszaru, prowadząc do uzupełnienia danych, weryfikacji hipotez roboczych bądź identyfikacji nowych kierunków śledczych[7].

Warto jednak podkreślić, że diagramy nie stanowią celu samego w sobie – są narzędziem pomocniczym w procesie analizy i służą przede wszystkim lepszemu zrozumieniu jej wyników.[8]

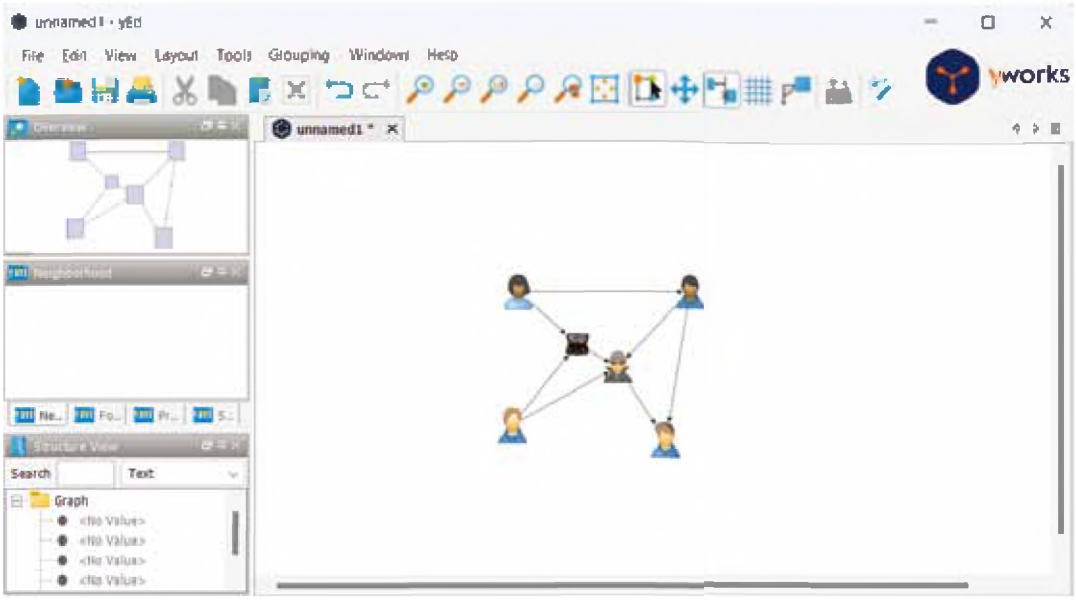
Najczęściej wykorzystywane przez funkcjonariuszy służb narzędzia do tworzenia diagramów w analizie kryminalnej to:

- i2 Analyst's Notebook (IBM),
- Maltego,
- Microsoft Visio,
- Gephi,
- LINK,
- yEd Graph Editor.

[7] Nawarecki, E., Kisiel-Dorohinicki, M., & Dobrowolski, G. (2012). Doskonalsza analiza kryminalna dzięki aplikacji informatyków z AGH. Akademia Górniczo-Hutnicza.

[8] Grzegorz Mazgaj (2025). Operacyjna Analiza Kryminalna str. 18.

yEd – narzędzie do tworzenia diagramów i wizualizacji powiązań



Czym jest yEd? yEd Graph Editor to darmowy, wieloplatformowy program służący do tworzenia przejrzystych diagramów, sieci powiązań i wykresów[9]. Jest szczególnie użyteczny w analizie kryminalnej, analityce biznesowej, edukacji czy zarządzaniu projektami. Oficjalna strona: https://www.yworks.com/products/yed[10]

yEd wyróżnia się następującymi funkcjami wspierającymi analizę graficzną:

1. Tworzenie różnorodnych diagramów – yEd obsługuje szeroką gamę typów diagramów, takich jak diagramy UML (klas, obiektów), BPMN, diagramy przepływów, sieci semantyczne, mapy myśli, diagramy relacji jednostek i wiele innych.
2. Import danych – umożliwia import własnych danych z arkuszy kalkulacyjnych Excel (.xls, .csv) oraz plików XML/GraphML, co pozwala szybko tworzyć diagramy na podstawie gotowych zestawów danych.

[9] yWorks GmbH, *yEd Graph Editor – Create high-quality diagrams quickly and easily*, [online], dostęp: https://www.yworks.com/products/yed [dostęp: 14 czerwca 2025].

[10] yWorks GmbH, *yEd Graph Editor Manual*, [online], dostęp: https://www.yworks.com/products/yed/documentation [dostęp: 14 czerwca 2025].

3. Automatyczne układanie elementów – zaawansowane algorytmy automatycznego rozmieszczania węzłów i krawędzi dbają o czytelność i estetykę diagramów, eliminując krzyżowanie się połączeń i chaos wizualny.
4. Bogata paleta elementów i personalizacja – oferuje szeroki wybór kształtów, typów połączeń, możliwość dodawania własnych grafik (JPG, PNG, SVG) oraz ikon, a także edycję atrybutów każdego elementu, co pozwala tworzyć niestandardowe i dopasowane diagramy.
5. Opis i pozycjonowanie elementów – pozwala na dodawanie etykiet, wielowierszowego tekstu, HTML, wielu etykiet na jednym elemencie oraz automatyczne pozycjonowanie etykiet dla zachowania czytelności. Eksport diagramów – umożliwia eksport do popularnych formatów graficznych i dokumentów, co ułatwia dalsze wykorzystanie diagramów w raportach i prezentacjach.
6. Narzędzia ułatwiające pracę z diagramami – potężne funkcje wyszukiwania i zaznaczania elementów, możliwość pracy z wieloma diagramami jednocześnie, skróty klawiaturowe, podgląd wydruku oraz dopasowywanie paneli interfejsu do potrzeb użytkownika.
7. Wieloplatformowość i stabilność – aplikacja działa na systemach Windows, Linux i macOS, wymaga jedynie środowiska Java, co zapewnia szeroką dostępność i stabilną pracę[11].

Do najważniejszych atutów programu yEd, decydujących o jego przydatności w zastosowaniach analitycznych i edukacyjnych, należą:

1. Darmowe i wieloplatformowe – yEd jest bezpłatnym programem działającym na systemach Windows, Linux i macOS dzięki środowisku Java, co zapewnia szeroką dostępność.
2. Intuicyjny i przyjazny interfejs użytkownika – ułatwia szybkie tworzenie i edycję diagramów, nawet osobom bez specjalistycznej wiedzy.
3. Szerokie wsparcie dla różnych typów diagramów – umożliwia tworzenie m.in. diagramów UML, BPMN, diagramów powiązań, map myśli, drzew genealogicznych, diagramów przepływów czy sieci semantycznych.
4. Automatyczne układanie elementów – zaawansowane algorytmy automatycznego rozmieszczania węzłów i krawędzi dbają o czytelność i estetykę diagramów, eliminując krzyżowanie się połączeń.
5. Import danych z różnych źródeł – pozwala na szybkie wczytanie danych z arkuszy kalkulacyjnych Excel (.xls, .csv) oraz plików XML/GraphML, co przyspiesza tworzenie diagramów na podstawie gotowych zestawów danych.

[11] yWorks. (2025). yEd Graph Editor – Features and Capabilities. [online], dostęp: https://www.yworks.com/products/yed [dostęp: 14 czerwca 2025].

6. Bogata paleta elementów i możliwość personalizacji – oferuje szeroki wybór kształtów, typów połączeń, a także opcję dodawania własnych grafik (JPG, PNG, SVG) i ikon, co pozwala tworzyć niestandardowe diagramy.
7. Eksport do wielu formatów – diagramy można zapisać jako bitmapy lub grafikę wektorową w formatach PNG, JPG, SVG, PDF czy SWF, co ułatwia ich dalsze wykorzystanie w raportach, prezentacjach czy dokumentach.
8. Funkcje ułatwiające pracę z diagramami – m.in. automatyczne pozycjonowanie etykiet, podpowiedzi, obsługa wielu etykiet i tekstów HTML, rozbudowane narzędzia wyszukiwania i wybierania elementów, a także możliwość pracy z wieloma diagramami jednocześnie.
9. Stabilność i wydajność – yEd radzi sobie zarówno z prostymi, jak i bardzo złożonymi diagramami, co czyni go uniwersalnym narzędziem do różnorodnych zastosowań.
10. Wsparcie społeczności i dokumentacja – dostępna jest zintegrowana pomoc oraz aktywne forum użytkowników, co ułatwia rozwiązywanie problemów i poznawanie nowych funkcji.
11. Nie wymaga instalacji dodatków – działa „od ręki"[12].

Pomimo wielu zalet, program yEd posiada również pewne ograniczenia funkcjonalne, które mogą wpływać na zakres i efektywność jego zastosowania w bardziej zaawansowanych projektach analitycznych. Do najważniejszych z nich należą:

1. Brak dedykowanych funkcji GIS – yEd nie jest systemem GIS, więc nie oferuje zaawansowanych narzędzi do analizy przestrzennej, takich jak dokładne mapowanie geograficzne, analiza warstw czy integracja z danymi GPS. To ogranicza jego zastosowanie w przypadku, gdy potrzebna jest szczegółowa wizualizacja przestrzenna zdarzeń.
2. Ograniczona automatyzacja analizy danych – Choć yEd pozwala na automatyczne układanie diagramów, nie posiada wbudowanych funkcji analitycznych, takich jak wykrywanie wzorców, klasteryzacja czy zaawansowane algorytmy analizy sieci społecznych. Wymaga to ręcznej interpretacji i analizy przez użytkownika.
3. Brak funkcji współpracy online – yEd jest aplikacją desktopową i nie oferuje natywnej funkcji pracy zespołowej w czasie rzeczywistym ani integracji z platformami chmurowymi, co może utrudniać współpracę wielu analityków nad jednym projektem.
4. Ograniczone możliwości personalizacji interfejsu – Interfejs yEd jest prosty i intuicyjny, ale nie pozwala na głęboką personalizację ani dostosowanie do

[12] yWorks. (2025). yEd Graph Editor – Features and Capabilities. [online], dostęp: https://www.yworks.com/products/yed [dostęp: 14 czerwca 2025].

bardzo specyficznych potrzeb użytkownika, co może być wadą w bardziej zaawansowanych projektach.

5. Brak wsparcia dla dużych baz danych w czasie rzeczywistym – Przy bardzo rozbudowanych i dynamicznie zmieniających się zbiorach danych yEd może mieć problemy z wydajnością, a także nie obsługuje bezpośredniego połączenia z bazami danych w czasie rzeczywistym.
6. Brak zaawansowanego wsparcia technicznego – jako darmowe narzędzie yEd oferuje ograniczone wsparcie techniczne, co może być problemem w przypadku wystąpienia błędów lub potrzeby dostosowania oprogramowania do specyficznych wymagań.

Przykłady zastosowania yEd w analizie kryminalnej

Współczesna analiza kryminalna opiera się w dużej mierze na zdolności do identyfikowania, odwzorowywania i interpretowania relacji zachodzących pomiędzy różnymi uczestnikami i elementami zdarzeń przestępczych. Złożoność struktur organizacji przestępczych, mnogość źródeł informacji oraz konieczność szybkiego reagowania sprawiają, że skuteczne narzędzia wizualizacji relacji stają się nieodzownym elementem pracy analityków. Jednym z takich narzędzi jest program yEd, który umożliwia tworzenie przejrzystych diagramów powiązań, stanowiących podstawę do pogłębionej analizy operacyjnej i dochodzeniowej.

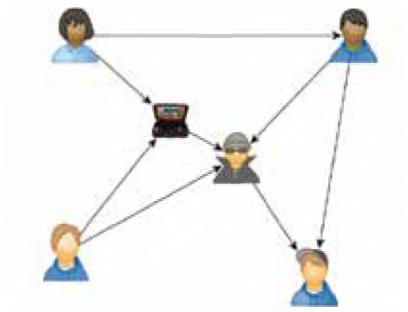


Diagram 1. Identyfikacja powiązań między osobami, zdarzeniami i obiektami

1) Tworzenie diagramów relacji (link charts) w yEd

Program yEd umożliwia tworzenie tzw. diagramów relacji, czyli graficznych sieci (link charts), które obrazują powiązania między różnymi elementami śledztwa, takimi jak podejrzani, ofiary, świadkowie, miejsca zdarzeń czy dowody. Dzięki temu narzędziu można w sposób czytelny i przejrzysty przedstawić złożone struktury przestępcze, co jest szczególnie istotne w przypadku organizacji o rozbudowanej hierarchii i wielu powiązaniach, np. gangów czy grup handlujących narkotykami.

2) Ułatwienie zrozumienia złożonych struktur przestępczych

Graficzne przedstawienie relacji pozwala na szybkie rozpoznanie centralnych postaci, ich ról oraz sposobu komunikacji i współpracy w grupie przestępczej. Wizualizacja sieci kontaktów umożliwia także identyfikację kluczowych węzłów i słabych punktów w strukturze, co jest niezbędne do planowania skutecznych działań operacyjnych i śledczych.

3) Funkcjonalność yEd w praktyce analitycznej

W yEd proces tworzenia map powiązań jest intuicyjny i elastyczny. Użytkownik może łatwo dodawać węzły reprezentujące różne podmioty, takie jak osoby, firmy, numery telefonów czy lokalizacje. Następnie łączy je krawędziami, które symbolizują relacje, np. kontakty, spotkania, wspólne przebywanie w tym samym miejscu lub przepływy finansowe. Takie podejście pozwala na dynamiczne budowanie i modyfikowanie sieci w zależności od napływających informacji.

4) Znaczenie wizualizacji dla efektywności analizy

Wizualne mapy powiązań pozwalają na integrację i kojarzenie danych pochodzących z różnych źródeł, co jest kluczowe przy dużej ilości informacji. Ułatwiają one śledczym i analitykom szybkie dostrzeżenie wzorców działania, powtarzających się schematów i anomalii, które mogłyby pozostać niezauważone przy analizie wyłącznie tekstowej. Ponadto, diagramy są nieocenione podczas prezentacji wyników śledztwa przed innymi funkcjonariuszami, prokuratorami czy sądami, gdyż ułatwiają zrozumienie skomplikowanych powiązań i argumentację dowodową.

Porządkowanie danych śledczych. Integracja danych z różnych źródeł

W trakcie prowadzenia śledztwa organy ścigania gromadzą ogromne ilości informacji pochodzących z różnych źródeł, takich jak notatki operacyjne, bilingi telefoniczne, monitoring wizyjny, rejestry połączeń czy zapisy GPS. Dane te często mają różnorodny format i są rozproszone, co utrudnia ich analizę i kojarzenie. Porządkowanie tych informacji polega na ich przekształceniu w spójną i czytelną formę, która umożliwia szybkie dostrzeżenie powiązań i wzorców.

1) Rola yEd w porządkowaniu i wizualizacji danych

Program yEd znacząco ułatwia ten proces, oferując możliwość importu danych z popularnych formatów, takich jak pliki Excel czy GraphML. Dzięki temu analitycy mogą szybko załadować duże zbiory informacji i automatycznie wygenerować diagramy powiązań, co znacznie przyspiesza tworzenie map relacji i eliminuje konieczność ręcznego wprowadzania danych.

2) Znaczenie porządkowania danych dla skuteczności analizy

Porządkowanie i wizualizacja danych pozwalają na:

1. eliminację chaosu informacyjnego i redukcję nadmiaru danych,
2. szybkie wykrywanie istotnych powiązań i anomalii,

3. lepsze planowanie działań operacyjnych i śledczych,
4. wsparcie podejmowania decyzji na podstawie kompleksowego obrazu sytuacji.

Tworzenie materiałów pomocniczych dla dochodzeń i sądu z wykorzystaniem yEd

Jednym z kluczowych elementów pracy analitycznej w kontekście śledztw kryminalnych jest nie tylko generowanie wiedzy na podstawie danych, lecz także jej skuteczne przekazywanie innym uczestnikom procesu dochodzeniowego – od funkcjonariuszy operacyjnych, przez prokuratorów, po sędziów. W tym zakresie istotną rolę odgrywają przejrzyste i czytelne materiały wizualne, które mogą służyć jako narzędzia pomocnicze w planowaniu działań, prezentacji ustaleń czy argumentacji dowodowej. Program yEd, dzięki swoim rozbudowanym funkcjom eksportu, formatowania i prezentacji diagramów, umożliwia przygotowanie wysokiej jakości materiałów graficznych, które znajdują zastosowanie zarówno w raportach śledczych, jak i w dokumentacji procesowej.

1) Eksport diagramów do różnych formatów

yEd umożliwia eksportowanie stworzonych diagramów do wielu popularnych formatów plików, takich jak PDF, PNG, SVG, JPG czy nawet SWF. Eksport do formatu PDF i SVG jest szczególnie wartościowy, ponieważ pozwala na zachowanie wysokiej jakości grafiki w formie wektorowej, co oznacza, że diagramy pozostają czytelne niezależnie od powiększenia. Format PNG i JPG z kolei umożliwiają łatwe wstawianie diagramów do raportów, prezentacji czy dokumentów tekstowych.

2) Wsparcie dla raportów śledczych i prezentacji

Diagramy wygenerowane w yEd mogą być wykorzystywane jako materiały pomocnicze podczas odpraw operacyjnych, analiz śledczych czy prezentacji w sądzie. Graficzne przedstawienie powiązań, schematów działania przestępców lub przepływów finansowych znacznie ułatwia zrozumienie skomplikowanych informacji przez funkcjonariuszy, prokuratorów oraz sędziów. Wizualizacje te wspierają argumentację dowodową i pomagają w klarownym przedstawieniu złożonych relacji między podmiotami.

3) Dodatkowe możliwości i narzędzia wspierające

yEd oferuje także automatyczne układanie elementów diagramu, co pozwala na estetyczne i czytelne rozmieszczenie węzłów i krawędzi bez konieczności ręcznego dopasowywania. Ponadto, diagramy można wzbogacać o opisy, etykiety i kolory, co dodatkowo ułatwia interpretację danych.

Wspieranie profilowania i łączenia spraw z wykorzystaniem yEd

W procesie analizy kryminalnej jednym z kluczowych zadań jest identyfikacja cech wspólnych dla różnych przestępstw oraz wykrywanie wzorców działania, które

mogą wskazywać na tożsamość sprawcy. Szczególne znaczenie w tym kontekście ma tzw. profilowanie kryminalne, polegające na przewidywaniu cech i zachowań nieznanego sprawcy na podstawie obserwowanych śladów i schematów działań. Narzędzia do analizy grafowej, takie jak yEd, pozwalają na przedstawienie tych wzorców w sposób graficzny, co znacząco ułatwia ich rozpoznawanie i interpretację. Wizualizacja powiązań między osobami, miejscami, narzędziami przestępstwa i charakterystycznymi cechami modus operandi umożliwia łączenie pozornie odrębnych zdarzeń oraz zawężenie kręgu podejrzanych. W niniejszym fragmencie omówiono możliwości wykorzystania programu yEd w kontekście profilowania i integracji informacji dochodzeniowych w spójną strukturę analityczną.

1) Graficzne powiązanie wspólnych cech modus operandi i kontaktów

W analizie kryminalnej kluczowe jest identyfikowanie wspólnych cech modus operandi, czyli charakterystycznych sposobów działania sprawców, oraz powiązań między nimi. Program yEd pozwala na tworzenie diagramów, które wizualizują te powiązania – łącząc węzły reprezentujące różne sprawy, osoby, narzędzia czy miejsca zdarzeń. Dzięki temu można graficznie ukazać, które elementy łączą poszczególne przestępstwa, co ułatwia wykrywanie wzorców i powiązań.

2) Znaczenie profilowania w śledztwach

Profilowanie kryminalne to metoda wykorzystywana do przewidywania cech nieznanego sprawcy na podstawie zachowań zaobserwowanych w miejscu zdarzenia. Jego podstawą jest analiza modus operandi oraz cech charakterystycznych zachowań przestępczych. Dzięki temu można zawęzić krąg podejrzanych, określić motywy działania, a także połączyć ze sobą pozornie niezwiązane sprawy[13]. Programy do analizy grafowej, takie jak yEd, wspierają ten proces, umożliwiając łączenie informacji z różnych źródeł w jeden spójny model relacyjny. Graficzne przedstawienie takich połączeń ułatwia identyfikację sprawców[14].

Przygotowanie danych do analizy grafowej w programie yEd w kontekście analizy kryminalnej

Współczesna analiza kryminalna coraz częściej opiera się na metodach analizy relacyjnej, w tym technikach grafowych. Narzędziem szeroko stosowanym w tym obszarze jest program yEd, umożliwiający tworzenie oraz analizę grafów reprezentujących złożone sieci powiązań. Skuteczne wykorzystanie tego

[13] B. Hołyst, *Kryminalistyka*, Warszawa 2020, LexisNexis, s. 568–575.

[14] A. Łozińska-Piekarska, T. Dąbrowski, *Profilowanie kryminalne jako nowoczesna i skuteczna technika zwalczania przestępczości i sposób poszerzenia kompetencji pracowników zatrudnionych w organach ścigania i w wymiarze sprawiedliwości*, „Edukacja Ustawiczna Dorosłych" 2023, nr 3(122), s. 123–138.

oprogramowania wymaga odpowiedniego przygotowania danych wejściowych, co obejmuje kilka kluczowych etapów.

1) Zbieranie i selekcja danych

Podstawą analizy grafowej jest zebranie danych o relacjach zachodzących między obiektami zainteresowania – osobami, zdarzeniami, miejscami czy przedmiotami. Dane te powinny pochodzić z wiarygodnych i zróżnicowanych źródeł, takich jak bazy danych organów ścigania, informacje telekomunikacyjne, monitoring wizyjny, media społecznościowe czy rejestry publiczne[15]. Kluczowe znaczenie ma selekcja informacji istotnych dla analizy, przy zachowaniu ich spójności i kompletności.

2) Strukturyzacja danych

Zgromadzone dane należy przekształcić do struktury umożliwiającej ich reprezentację w postaci grafu, w którym wyróżnia się dwa podstawowe elementy: wierzchołki (nodes) i krawędzie (edges). Wierzchołki reprezentują obiekty (np. osoby, miejsca, przedmioty), natomiast krawędzie odzwierciedlają relacje lub interakcje pomiędzy nimi[16].

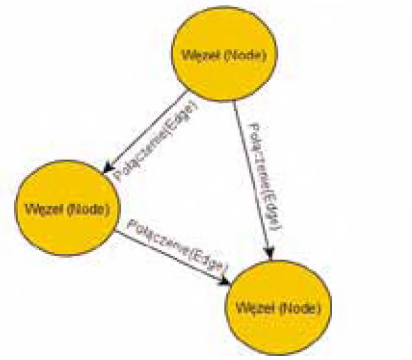


Diagram 2 Przykładowy graf

Wyróżnia się następujące typy krawędzi:

- **krawędzie nieskierowane** – oznaczające relację symetryczną, przedstawiane jako linie bez strzałek;
- **krawędzie skierowane (łuki)** – wskazujące kierunkowość relacji, np. nadanie połączenia telefonicznego;
- **pętle** – relacje wewnętrzne, gdzie obiekt jest powiązany sam ze sobą (np. osoba podejmująca działanie wobec siebie)[17].

[15] J. Ratcliffe, *Intelligence-Led Policing*, 2nd ed., London 2016, Routledge, s. 101–123.

[16] D. Easley, J. Kleinberg, *Networks, Crowds, and Markets: Reasoning about a Highly Connected World*, Cambridge 2010, Cambridge University Press, s. 39–67.

[17] R. Diestel, *Graph Theory*, 5th ed., Berlin 2017, Springer, s. 4–9.

Strukturalizacja danych w tym modelu pozwala na późniejszą analizę relacji społecznych, zależności czasowych czy hierarchii organizacyjnych, co jest istotne w badaniu struktur przestępczych[18].

3) Formatowanie danych do importu

Skuteczne wykorzystanie programu yEd Graph Editor w analizie grafowej wymaga uprzedniego przygotowania danych w odpowiednim formacie, umożliwiającym ich automatyczne przekształcenie w strukturę grafową. Program yEd obsługuje import danych z plików w formatach takich jak CSV, Excel (.xlsx, .xls), GraphML oraz XML, co pozwala na dużą elastyczność w zakresie integracji z różnymi źródłami informacji.

Aby możliwy był poprawny import danych, konieczne jest ich przedstawienie w formie ustrukturyzowanej tabeli, w której każda kolumna odpowiada precyzyjnie określonemu atrybutowi, przypisanemu do wierzchołków (nodes) lub krawędzi (edges). Taki schemat zapewnia jednoznaczność reprezentacji i umożliwia programowi yEd właściwe odwzorowanie relacji.

Podstawowe kolumny opisujące wierzchołki (nodes):

- ID – unikalny identyfikator obiektu (np. numer osoby, kod instytucji, oznaczenie dowodu rzeczowego); jego unikalność jest warunkiem spójności grafu;
- Label (etykieta) – nazwa obiektu, która będzie wyświetlana na diagramie (np. imię i nazwisko, adres, symbol zdarzenia);
- Type (typ) – klasyfikacja semantyczna obiektu (np. „osoba", „miejsce", „zdarzenie"), umożliwiająca różnicowanie wizualne węzłów.

Podstawowe kolumny opisujące krawędzie (edges):

- Source (źródło) – identyfikator wierzchołka początkowego relacji (zgodny z kolumną ID w tabeli węzłów);
- Target (cel) – identyfikator wierzchołka końcowego relacji;
- Relation type (typ relacji) – opis semantyczny charakteru powiązania (np. „kontakt telefoniczny", „udział we wspólnym zdarzeniu", „wspólne miejsce pobytu").

Kolumny dodatkowe (opcjonalne, ale istotne analitycznie):

- Weight (waga) – wartość liczbowa opisująca intensywność lub częstotliwość relacji (np. liczba połączeń telefonicznych, kwota przelewu, liczba wspólnych wizyt);
- Timestamp (znacznik czasu) – data lub dokładna godzina wystąpienia danej relacji, umożliwiająca analizę temporalną (np. sekwencje zdarzeń, powtarzalność działań);
- Atrybuty kontekstowe – wszelkie dodatkowe informacje, które mogą mieć znaczenie interpretacyjne (np. status osoby: podejrzany, ofiara, świadek; lokalizacja zdarzenia; krótki opis kontekstu interakcji).

[18] C. Morselli, *Inside Criminal Networks*, New York 2009, Springer, s. 67–95.

Prawidłowe przygotowanie danych w tej strukturze jest warunkiem nie tylko poprawnego zaimportowania ich do środowiska yEd, ale również ich dalszej obróbki analitycznej, w tym automatycznego układania grafów, klasyfikowania węzłów czy grupowania relacji według atrybutów. Zaniedbanie w zakresie formatowania danych może prowadzić do błędnej interpretacji diagramów oraz utraty ich wartości poznawczej[19].

4) Import danych i wizualizacja

Po przygotowaniu danych możliwy jest ich import do yEd. Program oferuje szereg automatycznych układów (layoutów), które pozwalają na czytelną organizację grafu – m.in. układ hierarchiczny, siatkowy, organiczny czy kołowy. Każdy z nich odpowiada innemu typowi struktury i pozwala na wydobycie określonych właściwości grafu, takich jak zależności nadrzędności, rozmieszczenie przestrzenne, intensywność relacji czy kierunkowość powiązań. Wstępna wizualizacja pozwala na szybkie rozpoznanie struktur dominujących, obszarów o wysokiej gęstości relacji oraz potencjalnych węzłów centralnych, co stanowi podstawę dalszej analizy.

5) Edycja grafu i analiza wizualna

yEd umożliwia dalszą edycję grafu: ręczne dodawanie lub usuwanie węzłów i relacji, edycję etykiet, stylizację elementów (np. kolorowanie w zależności od typu), a także grupowanie obiektów (np. powiązanych z daną lokalizacją). W ten sposób użytkownik może dostosować graficzne odwzorowanie sieci do potrzeb konkretnego dochodzenia[20].

6) Eksport i dalsze przetwarzanie

Gotowy graf można zapisać w różnych formatach (np. SVG, PDF, GraphML) oraz zintegrować z innymi narzędziami analitycznymi (np. Gephi, Cytoscape, R). Umożliwia to przeprowadzanie zaawansowanych analiz ilościowych i temporalnych, a także prezentację wyników w raportach operacyjnych[21].

Programy wspomagające uzupełnienie funkcjonalności programu yEd

Chociaż yEd Graph Editor stanowi wszechstronne i intuicyjne środowisko do tworzenia oraz edycji diagramów relacyjnych, jego funkcjonalność nie obejmuje wielu operacji kluczowych z punktu widzenia praktycznej analizy danych śledczych i organizacyjnych. W szczególności ograniczenia dotyczą:

[19] G. Brandes, U. Brandes, „Visual Representations of Network Structures", *IEEE Transactions on Visualization and Computer Graphics* 2005, vol. 11(5), s. 545–557.

[20] K. Borgatti et al., *Analyzing Social Networks*, 2nd ed., London 2018, SAGE Publications, s. 144–168.

[21] A. Perer, B. Shneiderman, "Balancing Systematic and Flexible Exploration of Social Networks", *IEEE Transactions on Visualization and Computer Graphics* 2006, vol. 12(5), s. 693–700.

- braku zautomatyzowanych mechanizmów przekształcania danych tabelarycznych w strukturę grafową,
- niewystarczających możliwości eksportu danych z diagramów do dalszej analizy ilościowej,
- braku wsparcia dla personalizacji ikon i symboliki dostosowanej do specyfiki analizy kryminalnej.

Z tych względów niezbędnym stało się opracowanie narzędzi uzupełniających, które integrują yEd z procesem przetwarzania danych źródłowych oraz umożliwiają ich szybką wizualizację i eksplorację. Powstałe rozwiązania mają na celu:

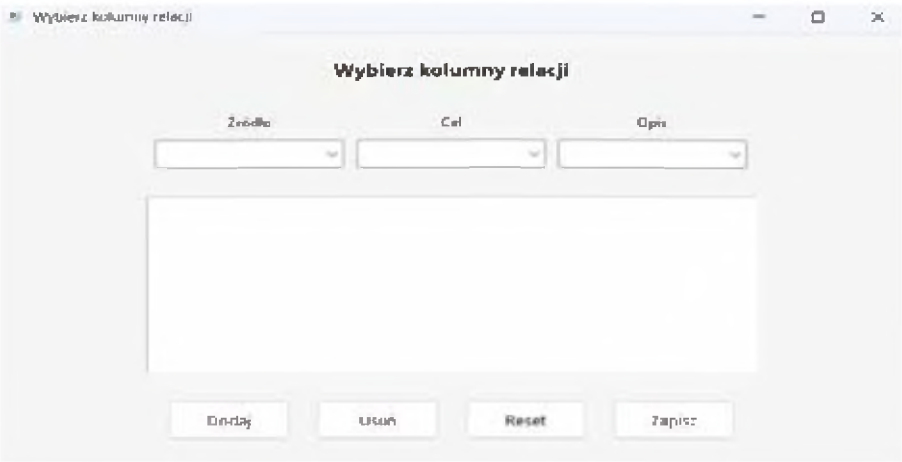
- usprawnienie przygotowania danych do analizy grafowej,
- automatyzację procesów konwersji między formatami (Excel, GraphML, CSV),
- rozszerzenie możliwości wizualnych poprzez obsługę niestandardowych ikon w formacie SVG.

Zaprojektowane zostały trzy autorskie aplikacje, które stanowią uzupełnienie funkcjonalności programu yEd w zakresie zastosowań śledczych, analitycznych oraz edukacyjnych. Każde z nich odpowiada na konkretne potrzeby praktyczne, niewystarczająco zaadresowane przez natywne możliwości edytora grafów:

- Excel2yEd_by_Czaku_2025 – narzędzie umożliwiające automatyczne przekształcanie danych tabelarycznych do postaci grafowej, zgodnej ze strukturą akceptowaną przez yEd Graph Editor;
- Konwerter yEd → Excel/CSV – aplikacja przeznaczona do translacji diagramów zapisanych w formacie GraphML na struktury tabelaryczne (Excel, CSV), co pozwala na dalszą analizę ilościową oraz integrację z zewnętrznymi narzędziami analitycznymi;
- SVG Converter – program służący do konwersji grafik rastrowych (JPG, PNG, BMP) do formatu SVG, wspieranego przez yEd, co umożliwia tworzenie dedykowanych ikon i wzbogacenie warstwy wizualnej diagramów o elementy semantycznie powiązane z analizowanymi kategoriami obiektów.

Każde z narzędzi odpowiada na konkretne potrzeby pojawiające się w toku pracy analitycznej i uzupełnia standardowe możliwości edytora grafów, czyniąc go pełnoprawnym środowiskiem analizy relacyjnej.

Aplikacja „EXCEL2YED_BY_CZAKU_2025" – funkcjonalność i zastosowania w modelowaniu struktur relacyjnych



Efektywne odwzorowanie złożonych relacji występujących w danych tabelarycznych – takich jak zależności organizacyjne, przepływy informacji czy sieci komunikacyjne – często wymaga ich transformacji do postaci grafowej. O ile arkusze kalkulacyjne (np. Microsoft Excel) doskonale nadają się do gromadzenia i filtrowania danych, to nie zapewniają one natywnego mechanizmu ich przestrzennej wizualizacji.

W odpowiedzi na tę lukę opracowano aplikację **Excel2yEd_by_Czaku_2025**, umożliwiającą bezpośrednie przekształcenie danych zawartych w plikach Excel (.xlsx) w strukturę grafu możliwą do zaimportowania w programie yEd Graph Editor. Narzędzie to funkcjonuje jako konwerter relacji tabelarycznych do plików zawierających węzły i krawędzie, zgodnie z logiką formatów stosowanych w analizie sieciowej[22].

Program pozwala na wieloetapową konfigurację procesu konwersji:

- wybór języka interfejsu (pięć wersji: PL, EN, DE, RU, CS),
- selekcję pliku wejściowego Excel (.xlsx),
- wybór arkusza w przypadku plików wieloarkuszowych,

[22] Lebiedowicz, A. (2023). Wykorzystanie analizy kryminalnej w działalności organów ścigania. Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury, Zeszyt 4 (52)/2023.

- wskazanie kolumn odpowiadających za źródło, cel oraz opcjonalny opis relacji (atrybuty semantyczne),
- dodanie wielu niezależnych relacji, każdej z własną parą kolumn.

W wyniku działania aplikacji generowany jest plik Excel zawierający trzy zakładki:

1. **nodes** – lista unikalnych elementów (identyfikatorów węzłów),
2. **edges** – relacje typu źródło → cel z opcjonalnymi etykietami,
3. **brak_relacji** – zestawienie niekompletnych danych (jeśli występują).

Zastosowane biblioteki (`pandas`, `openpyxl`, `xlsxwriter`, `json`) gwarantują interoperacyjność z innymi narzędziami analitycznymi i zapewniają automatyczną walidację struktury danych[23].

Dzięki możliwości integracji z innymi narzędziami analitycznymi oraz funkcji automatycznej walidacji struktury danych, aplikacja może być z powodzeniem wykorzystywana w różnorodnych kontekstach badawczych i praktycznych, związanych z analizą relacji, procesów organizacyjnych i wzorców współpracy. Jej zastosowania obejmują między innymi:

1. Analiza struktur organizacyjnych i komunikacyjnych

Aplikacja umożliwia modelowanie struktur formalnych i nieformalnych w organizacjach. Przykładowe zastosowania obejmują mapowanie hierarchii zarządzania, analizę przepływu dokumentów lub informacji, wykrywanie luk w systemach raportowania[24].

2. Analiza współpracy i interakcji

W środowiskach projektowych czy zespołach zadaniowych istotne jest zrozumienie schematu komunikacji i powiązań między osobami lub jednostkami. Aplikacja pozwala identyfikować m.in.: centralnych uczestników procesu, segmenty sieci o słabej komunikacji, struktury modularne i wzorce współdziałania.

3. Transformacja danych do wizualizacji i eksploracji

Dzięki generowaniu danych w postaci gotowej do importu do yEd, aplikacja znacząco skraca czas potrzebny na tworzenie diagramów relacyjnych. Znajduje to zastosowanie w analizie przypadków kryminalnych (osoby → kontakty → zdarzenia), raportach audytowych i projektowych, wizualizacji danych społecznych i marketingowych.

Z uwagi na swoją funkcjonalność, prostotę obsługi oraz możliwość integracji z różnymi środowiskami analitycznymi, aplikacja znajduje zastosowanie zarówno w pracy profesjonalistów, jak i użytkowników niewyspecjalizowanych technicznie.

[23] McKinney, W. (2010). *Data Structures for Statistical Computing in Python*. Proc. of the 9th Python in Science Conference.

[24] Tamże.

Narzędzie adresowane jest do szerokiego grona odbiorców, obejmującego między innymi:

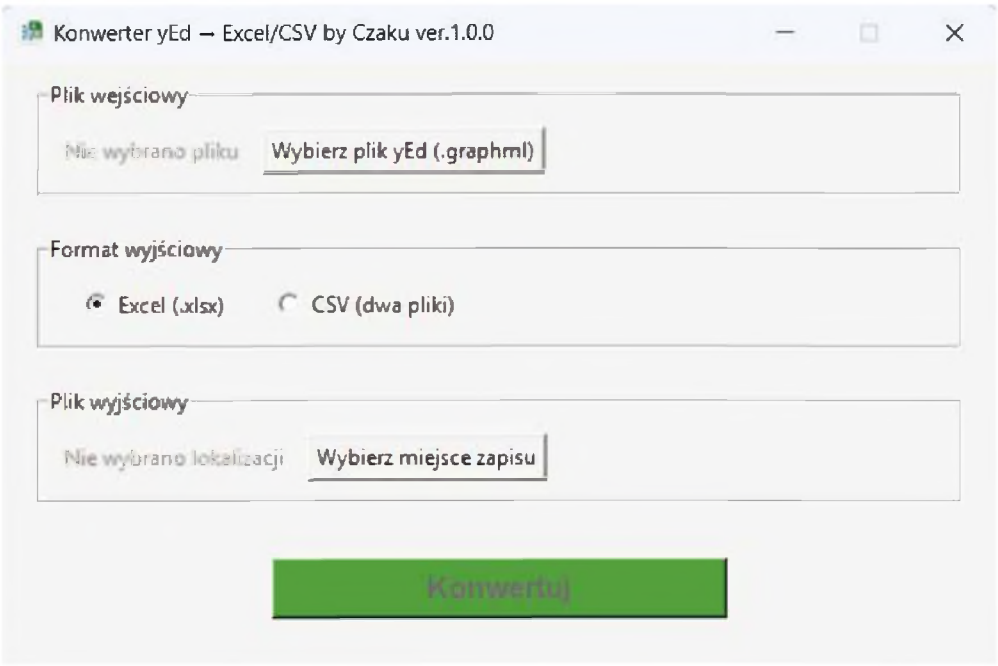
- analityków danych i specjalistów ds. compliance,
- funkcjonariuszy służb śledczych i analityków kryminalnych,
- naukowców pracujących z danymi relacyjnymi,
- osób odpowiedzialnych za optymalizację procesów organizacyjnych,
- studentów i dydaktyków przedmiotów związanych z analizą sieci, zarządzaniem i informatyką społeczną.

Konstrukcja interfejsu pozwala na korzystanie z programu również osobom nieposiadającym kompetencji programistycznych. Jednocześnie aplikacja może być stosowana jako wstępny moduł przygotowania danych do dalszych analiz eksploracyjnych – np. w Gephi, NetworkX czy Cytoscape.

Aplikacja **Excel2yEd_by_Czaku_2025** stanowi funkcjonalne narzędzie transformacji danych tabelarycznych do struktury grafowej, dedykowanej do dalszego przetwarzania w edytorze yEd. Zapewnia zgodność ze standardami reprezentacji sieciowej, wspiera wielojęzyczność oraz automatyzuje proces selekcji relacji. Dzięki temu wpisuje się w nurt narzędzi wspomagających analizę wizualną struktur relacyjnych oraz organizacyjnych, zarówno w zastosowaniach akademickich, jak i profesjonalnych.

Link do programu:
https://e.pcloud.link/publink/
show?code=XZaFNtZNEsaCMsmQXRuR1xQNlpjNk5aXKwk

Funkcjonalność i działanie aplikacji yEd2Excel do konwersji plików GRAPHML



Współczesna analiza grafowa, zarówno w kontekście informatyki śledczej, jak i analizy procesów organizacyjnych, wymaga nie tylko wizualizacji struktur sieciowych, lecz również skutecznego przetwarzania danych źródłowych. W odpowiedzi na potrzebę translacji plików diagramów tworzonych w programie yEd Graph Editor do formatów danych tabelarycznych opracowano aplikację yEd2Excel, która umożliwia konwersję plików w formacie GraphML do postaci arkuszy Excel (.xlsx) lub plików CSV.

Aplikacja została zaprojektowana jako lekkie narzędzie desktopowe, wykorzystujące język Python i biblioteki takie jak `pandas`[25] do zarządzania strukturą danych oraz `xml.etree.ElementTree` do przetwarzania dokumentów XML. Interfejs użytkownika został zrealizowany w oparciu o bibliotekę `Tkinter`,

[25] McKinney, W. (2010). *Data Structures for Statistical Computing in Python*. In Proceedings of the 9th Python in Science Conference (pp. 51–56).

co czyni program funkcjonalnym i przyjaznym nawet dla użytkowników bez doświadczenia programistycznego.

Architektura aplikacji i proces działania

Program działa w oparciu o schemat przetwarzania danych, który obejmuje selekcję pliku wejściowego w formacie `.graphml`, wybór preferowanego formatu wyjściowego (Excel lub CSV), oraz określenie lokalizacji zapisu wyników. Plik `.graphml` jest następnie analizowany w celu ekstrakcji dwóch podstawowych struktur grafowych: węzłów (nodes) i krawędzi (edges). Dane te zostają przetworzone i zapisane w formie tabelarycznej:

- W przypadku formatu Excel tworzony jest jeden plik z dwoma arkuszami – „Nodes" oraz „Edges".
- W przypadku CSV generowane są dwa odrębne pliki, odpowiadające każdej ze struktur.

Mechanizm działania programu uwzględnia obsługę błędów na poziomie użytkownika – w przypadku problemów (np. niepoprawna struktura XML, brak wymaganych znaczników), użytkownik otrzymuje odpowiedni komunikat informacyjny. Z kolei przy zakończeniu konwersji generowany jest komunikat sukcesu, co wpływa na przejrzystość procesu i ergonomię obsługi.

Elementy techniczne i specyfika implementacji

Kluczowym aspektem technologicznym programu jest obsługa przestrzeni nazw wykorzystywanych w standardzie GraphML oraz jego rozszerzeniach stosowanych przez yEd (np. `y:ShapeNode`, `y:EdgeLabel`), co umożliwia poprawne wydobycie danych semantycznych zawartych w diagramach. Dane są przetwarzane w strukturach słownikowych Pythona, a następnie konwertowane na obiekty `DataFrame`, co pozwala na dalszą analizę i zapis w formatach XLSX lub CSV.

Interfejs użytkownika zawiera intuicyjnie rozmieszczone komponenty: ramki, przyciski, radiobuttony i okna dialogowe. Co istotne, logika programu blokuje możliwość rozpoczęcia procesu konwersji bez uprzedniego wskazania pliku źródłowego oraz formatu docelowego, co zapobiega błędom wynikającym z niepełnej konfiguracji.

Projektując aplikację „Konwerter yEd → Excel/CSV by Czaku", założono jej uniwersalność i funkcjonalność w kontekście praktyk analitycznych, które obejmują szerokie spektrum dziedzin: od bezpieczeństwa wewnętrznego po zarządzanie wiedzą w organizacjach. Głównym celem było umożliwienie translacji danych wizualnych (zawartych w plikach GraphML) do formatów analitycznych obsługiwanych przez standardowe oprogramowanie biurowe.

1) Analityka śledcza i kryminalna

W pracy analityków kryminalnych i funkcjonariuszy służb bezpieczeństwa kluczowe znaczenie ma szybka identyfikacja relacji między osobami, miejscami i zdarzeniami. Narzędzia takie jak yEd pozwalają na ich wizualizację, jednak same diagramy nie są wystarczające do przeprowadzenia głębokiej analizy ilościowej. Konwersja do Excela lub CSV umożliwia:

- analizę centralności w sieci kontaktów[26],
- wykrywanie węzłów o wysokim stopniu połączeń (hubów),
- korelację relacji z danymi czasowymi lub geolokalizacyjnymi[27].

W takim ujęciu aplikacja stanowi pomost między narzędziami wizualnymi a metodami statystycznymi wykorzystywanymi m.in. w analizie sieci społecznych (SNA)[28].

2) Zarządzanie projektami i procesami

W organizacjach komercyjnych oraz instytucjach publicznych coraz częściej wykorzystuje się diagramy przepływu (flow charts) oraz mapy procesów do modelowania działalności operacyjnej[29]. Przekształcenie ich do struktury tabelarycznej umożliwia:

- analizę zgodności procesów z procedurami (compliance checking),
- identyfikację miejsc przeciążenia (bottlenecks) w strukturze organizacyjnej,
- integrację z innymi systemami analizy danych, takimi jak Power BI czy Tableau[30].

Dla menedżerów i specjalistów ds. zarządzania jakością narzędzie to może być wykorzystywane do mapowania i optymalizacji procesów.

3) Zastosowania edukacyjne i badawcze

Dla dydaktyków, studentów kierunków technicznych, socjologicznych czy bezpieczeństwa wewnętrznego aplikacja może pełnić rolę narzędzia dydaktycznego, umożliwiającego ćwiczenia z zakresu:

- budowy i interpretacji grafów,
- przetwarzania danych z diagramów do baz danych,
- przygotowania danych wejściowych do dalszych analiz (np. klasteryzacji, klasyfikacji)[31].

---

[26] Wasserman, S., & Faust, K. (1994). *Social Network Analysis: Methods and Applications*. Cambridge University Press.

[27] Chainey, S., & Ratcliffe, J. (2013). *GIS and Crime Mapping*. Wiley.

[28] Borgatti, S. P., Everett, M. G., & Johnson, J. C. (2018). *Analyzing Social Networks*. SAGE Publications.

[29] Dumas, M., La Rosa, M., Mendling, J., & Reijers, H. A. (2018). *Fundamentals of Business Process Management*. Springer.

[30] Few, S. (2012). *Show Me the Numbers: Designing Tables and Graphs to Enlighten*. Analytics Press.

[31] Freeman, L. C. (2004). *The Development of Social Network Analysis: A Study in the Sociology of Science*. Empirical Press.

Jest to także użyteczne narzędzie w projektach badawczych wymagających manualnego lub półautomatycznego przygotowania danych grafowych z materiałów źródłowych.

4) Użytkownicy bez kompetencji programistycznych

Jednym z celów projektowych była maksymalna dostępność narzędzia dla użytkowników nieposiadających umiejętności kodowania. Prosty interfejs oparty na Tkinterze pozwala na szybkie wykonanie złożonych operacji bez potrzeby znajomości formatu GraphML czy bibliotek Python[32]. Dzięki temu narzędzie może być z powodzeniem stosowane przez:

- specjalistów ds. administracji publicznej,
- pracowników biurowych,
- konsultantów sporządzających raporty z analiz struktur organizacyjnych lub komunikacyjnych.

5) Interdyscyplinarność i elastyczność

Aplikacja może być zintegrowana z innymi narzędziami, np. poprzez dalsze przetwarzanie danych w arkuszach kalkulacyjnych, import do systemów bazodanowych (np. MySQL) czy eksport do narzędzi eksploracji danych. Jej elastyczność sprawia, że może być wdrażana zarówno w małych zespołach badawczych, jak i w dużych organizacjach[33].

W kontekście wizualizacji sieci i struktur relacyjnych, coraz większą wagę przywiązuje się do czytelności, symboliki i jednoznaczności elementów graficznych reprezentujących węzły i krawędzie w diagramach. Dotyczy to zwłaszcza sytuacji, w których standardowe zestawy ikon oferowane przez edytory grafów (np. yEd) okazują się niewystarczające lub niedostosowane do specyfiki analizowanego zagadnienia.

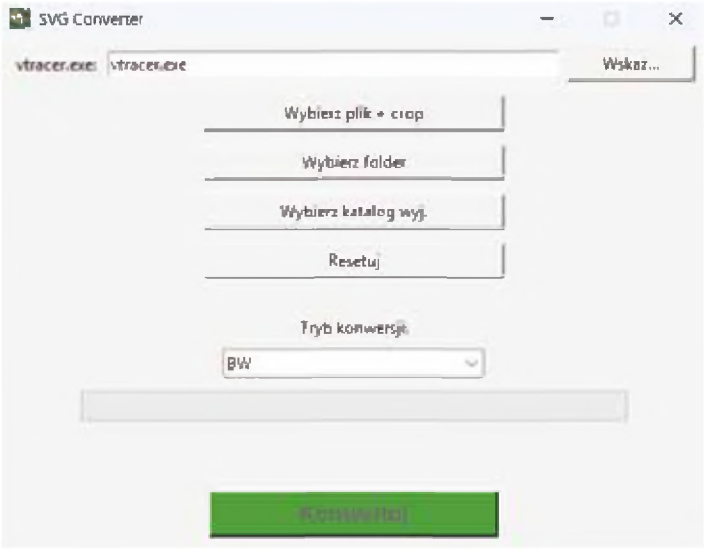
Link do programu:

https://e.pcloud.link/publink/show?code=XZoFNtZKYWf1Wm48g49opF97wUHER4MSb1V

[32] McKinney, W. (2010). *Data Structures for Statistical Computing in Python*. In Proceedings of the 9th Python in Science Conference (pp. 51–56).

[33] Kitchin, R. (2014). *The Data Revolution: Big Data, Open Data, Data Infrastructures and Their Consequences*. SAGE.

Aplikacja „SVG CONVERTER" – funkcjonalne narzędzie do przetwarzania grafiki na potrzeby systemów diagramowych



Współczesna wizualizacja danych i struktur wymaga nie tylko skutecznych metod analizy, lecz także precyzyjnych narzędzi graficznych, które umożliwiają generowanie elementów o wysokiej jakości estetycznej i funkcjonalnej. Jednym z istotnych aspektów projektowania diagramów – w tym również sieciowych – jest możliwość integracji niestandardowych ikon i symboli.

Aplikacja **SVG Converter** została zaprojektowana z myślą o konwersji standardowych obrazów rastrowych (w formatach PNG, JPG, BMP) do formatu wektorowego SVG, zgodnego z wymaganiami edytora diagramów **yEd Graph Editor** oraz innych narzędzi wspierających grafiki skalowalne.

Program umożliwia przekształcenie pojedynczego obrazu lub całej kolekcji plików graficznych do formatu SVG. Użytkownik może przed konwersją wykonać kadrowanie (crop), co pozwala precyzyjnie wyselekcjonować fragment obrazu, który będzie wykorzystany jako ikona. Dodatkowe funkcje obejmują:

- **Dwa tryby przetwarzania**:
  - *BW (black & white)* – konwersja kontrastowa, idealna do ikon funkcjonalnych;
  - *COLOR* – z zachowaniem koloru, przy wsparciu zewnętrznego narzędzia `vtracer.exe`.[34]
- **Skalowanie** – możliwość ustawienia żądanej wielkości wynikowej grafiki SVG.
- **Konwersja wsadowa** – przetwarzanie całych folderów z grafikami, co wspiera pracę seryjną np. przy tworzeniu bibliotek ikon.

[34] vTracer – narzędzie do konwersji rastrów na SVG. https://github.com/visioncortex/vtracer.

- **Przejrzysty interfejs graficzny** oparty na komponentach `Tkinter`, bez konieczności znajomości formatów SVG czy narzędzi graficznych.

Aplikacja znajduje zastosowanie w wielu obszarach działalności, w których istotna jest wizualna reprezentacja informacji:

1. Personalizacja diagramów w systemach typu yEd

SVG Converter umożliwia tworzenie ikon dostosowanych do kontekstu danej analizy. Dzięki temu możliwa jest np. identyfikacja osób, dokumentów, urządzeń czy lokalizacji na podstawie odpowiednio przekształconych grafik.

2. Zastosowania dydaktyczne i edukacyjne

W kontekście edukacyjnym program wspomaga nauczycieli i uczniów w przygotowaniu materiałów wizualnych – np. ikon do map myśli, infografik, projektów multimedialnych. W odróżnieniu od klasycznych edytorów grafiki wektorowej, nie wymaga on znajomości formatów XML/SVG ani umiejętności rysowania obiektów.

3. Prototypowanie i dokumentacja systemowa

Program przydatny jest również w działaniach związanych z projektowaniem systemów IT i dokumentowaniem architektury systemowej, gdzie ikony wykorzystywane są jako elementy diagramów przepływu informacji, zależności funkcjonalnych czy interfejsów użytkownika.

4. Wizualizacja danych internetowych i publikacje cyfrowe

Pliki SVG wygenerowane przez aplikację mogą być osadzane w dokumentach HTML lub publikacjach PDF, zapewniając wysoką jakość skalowania i kompatybilność z nowoczesnymi przeglądarkami. Program umożliwia szybkie przygotowanie ilustracji do publikacji online.

Ze względu na uniwersalność zastosowań oraz intuicyjny interfejs, aplikacja SVG Converter może być wykorzystywana przez przedstawicieli różnych środowisk zawodowych i edukacyjnych, których potrzeby koncentrują się wokół przetwarzania, personalizacji oraz integracji grafiki wektorowej. Do potencjalnych grup użytkowników należą w szczególności:

- użytkownicy yEd poszukujący możliwości personalizacji węzłów i symboli;
- nauczyciele akademiccy i uczniowie przygotowujący grafiki dydaktyczne i prezentacyjne;
- graficy nieprofesjonalni, którzy nie korzystają z zaawansowanych narzędzi typu Adobe Illustrator czy Inkscape;
- twórcy stron internetowych potrzebujący lekkich, skalowalnych grafik;
- analitycy i inżynierowie systemowi, którzy dokumentują diagramy przepływu i zależności funkcjonalnych.

Zaletą programu jest jego niezależność od środowisk zewnętrznych i prostota obsługi, co predestynuje go do użytku również w środowiskach edukacyjnych i administracyjnych.

SVG Converter to praktyczne i elastyczne narzędzie umożliwiające konwersję obrazów rastrowych na grafikę wektorową SVG, z przeznaczeniem do dalszej obróbki, prezentacji lub integracji z diagramami. Dzięki funkcjom przycinania, skalowania, wyboru trybu konwersji oraz wsadowego przetwarzania, aplikacja odpowiada na potrzeby szerokiej grupy użytkowników w zakresie przystępnego przetwarzania grafiki cyfrowej.

Link do programu:
https://e.pcloud.link/publink/
show?code=XZHpNtZxWW9t7p43S4xgORgoTSLjHoWCu0V

Podsumowanie

Analiza grafowa w kontekście kryminalistyki zyskuje coraz większe znaczenie jako narzędzie wspierające proces wykrywania, dokumentowania i interpretacji złożonych relacji między osobami, zdarzeniami i obiektami. Program yEd Graph Editor, dzięki funkcjom automatycznego układu, możliwości importu danych oraz eksportu do licznych formatów, stanowi praktyczne i szeroko dostępne narzędzie analityczne wykorzystywane w śledztwach operacyjnych, analizie sieci przestępczych i prezentacjach procesowych. Kluczowe znaczenie ma tu jednak nie tylko sam program, lecz także jego rozszerzenia funkcjonalne. Opracowane aplikacje wspierające – Konwerter yEd → Excel/CSV, Excel2yEd_by_Czaku_2025 oraz SVG Converter – umożliwiają odpowiednio: transformację plików GraphML do formatów analitycznych, tworzenie struktur grafowych z danych tabelarycznych oraz przekształcanie grafiki rastrowej do formatu SVG, który może być wykorzystany w yEd jako spersonalizowana ikonografia. Zastosowanie ikon SVG znacząco zwiększa przejrzystość diagramów i poprawia semantyczną interpretację węzłów, co jest szczególnie istotne w analizach śledczych oraz dydaktyce. Dzięki tej triadzie narzędzi yEd przestaje być jedynie edytorem grafów, a staje się kompletnym środowiskiem wspierającym profesjonalną analizę relacyjną – interdyscyplinarną, elastyczną i dostępną również dla użytkowników bez zaawansowanego zaplecza technicznego.

Bibliografia

1. Borgatti K., Everett M.G., Johnson J.C., *Analyzing Social Networks*, 2nd ed., London 2018, SAGE Publications, s. 144–168.
2. Borgatti S.P., Everett M.G., Johnson J.C. (2018). *Analyzing Social Networks*. SAGE Publications.
3. Brandes G., Brandes U., „Visual Representations of Network Structures", *IEEE Transactions on Visualization and Computer Graphics* 2005, vol. 11(5), s. 545–557.
4. CBA, *Analiza relacyjna w działalności operacyjnej CBA*, Centralne Biuro Antykorupcyjne, Warszawa 2021.
5. Chainey S., Ratcliffe J. (2013). *GIS and Crime Mapping*. Wiley.
6. Cramer C., Hochleitner R. (2018). Visualizing criminal networks: A case study of social network analysis in law enforcement. *Police Practice and Research*, 19(6), 547–563. https://doi.org/10.1080/15614263.2017.1395747
7. Cross R., Parker A., *The Hidden Power of Social Networks: Understanding How Work Really Gets Done in Organizations*, Harvard Business Review Press, Boston 2004.
8. Czaku, *Excel2yEd_by_Czaku_2025 – narzędzie konwersji danych tabelarycznych do grafów*, eCloud 2025, [online] https://e.pcloud.link/publink/show?code=XZaFNtZNEsaCMsmQXRuR1xQNlpjNk5aXKwk (dostęp: 15.06.2025).
9. Czaku, *Konwerter yEd → Excel/CSV – ekstrakcja danych z diagramów GraphML*, eCloud 2025, [online] https://e.pcloud.link/publink/show?code=XZoFNtZKYWf1Wm48g49opF97wUHER4MSb1V (dostęp: 15.06.2025).
10. Czaku, *SVG Converter – konwersja grafiki rastrowej do SVG dla yEd*, eCloud 2025, [online] https://e.pcloud.link/publink/show?code=XZHpNtZxWW9t7p43S4xgORgoTSLjHoWCu0V (dostęp: 15.06.2025).
11. Diestel R., *Graph Theory*, 5th ed., Berlin 2017, Springer, s. 4–9.
12. Dumas M., La Rosa M., Mendling J., Reijers H.A. (2018). *Fundamentals of Business Process Management*. Springer.
13. Easley D., Kleinberg J., *Networks, Crowds, and Markets: Reasoning about a Highly Connected World*, Cambridge 2010, Cambridge University Press, s. 39–67.
14. Freeman L.C., *The Development of Social Network Analysis: A Study in the Sociology of Science*, Empirical Press, Vancouver 2004.

15. Gazeta Policyjna, „Analiza kryminalna w PG", [online] https://gazeta.policja.pl/997/archiwum-1/2022/numer-23-112022-r/225150,Analiza-kryminalna-w-PG.html (dostęp: 15.06.2025).
16. Hanneman R.A., Riddle M., *Introduction to Social Network Methods*, University of California, Riverside 2005, [online] https://faculty.ucr.edu/~hanneman/nettext/ (dostęp: 15.06.2025).
17. Hołyst B., *Kryminalistyka*, Warszawa 2020, LexisNexis, s. 568–575.
18. Kadushin C., *Understanding Social Networks: Theories, Concepts, and Findings*, Oxford University Press, Oxford 2012.
19. Lebiedowicz A. (2023). Wykorzystanie analizy kryminalnej w działalności organów ścigania. *Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury*, Zeszyt 4 (52)/2023.
20. Łozińska-Piekarska A., Dąbrowski T., Profilowanie kryminalne jako nowoczesna i skuteczna technika zwalczania przestępczości i sposób poszerzenia kompetencji pracowników zatrudnionych w organach ścigania i w wymiarze sprawiedliwości, *Edukacja Ustawiczna Dorosłych* 2023, nr 3(122), s. 123–138.
21. Mazgaj G. (2025). *Operacyjna Analiza Kryminalna*, s. 18.
22. McKinney W. (2010). Data Structures for Statistical Computing in Python. W: *Proceedings of the 9th Python in Science Conference* (red. S. van der Walt, J. Millman), s. 51–56.
23. Morselli C., *Inside Criminal Networks*, New York 2009, Springer, s. 67–95.
24. Nawarecki E., Kisiel-Dorohinicki M., Dobrowolski G. (2012). *Doskonalsza analiza kryminalna dzięki aplikacji informatyków z AGH*. Akademia Górniczo-Hutnicza.
25. Perer A., Shneiderman B., "Balancing Systematic and Flexible Exploration of Social Networks", *IEEE Transactions on Visualization and Computer Graphics* 2006, vol. 12(5), s. 693–700.
26. Ratcliffe J.H. (2016). *Intelligence-led policing*, 2nd ed., London, Routledge, s. 101–123.
27. Scott J., *Social Network Analysis*, SAGE Publications, London 2017.
28. Skaliński Z. (2021). *Praktyczne wykorzystanie analizy sieci społecznej (SNA) w analizie śledczej*.
29. SNA – Social Network Analysis, [online] https://www.orgnet.com/sna.html (dostęp: 15.06.2025).
30. vTracer – narzędzie do konwersji rastrów na SVG, [online] https://github.com/visioncortex/vtracer (dostęp: 15.06.2025).
31. Wasserman S., Faust K. (1994). *Social Network Analysis: Methods and Applications*. Cambridge University Press.

32. Wójcik D., *Analiza kryminalna w praktyce: zastosowania wizualizacji relacji*, „Problemy Kryminalistyki" 2022, nr 23(112), s. 45–56.
33. yWorks GmbH, *yEd Graph Editor – Create high-quality diagrams quickly and easily*, [online] https://www.yworks.com/products/yed (dostęp: 14.06.2025).
34. yWorks GmbH, *yEd Graph Editor Manual*, [online] https://www.yworks.com/products/yed/documentation (dostęp: 14.06.2025).

Józef Druć[1]

Podsłuch i monitoring oraz prosty sprzęt do wykrywania ukrytych urządzeń

W czasach obecnych wszyscy jesteśmy świadkami szybkiego rozwoju technologii w każdym aspekcie życia. Szczególnie daje się to zauważyć w elektronice i telekomunikacji. Burzliwy rozwój telefonii komórkowej dla nikogo nie jest specjalnym zaskoczeniem. Każdy korzystający z urządzeń komunikacyjnych posiada jedno lub więcej takich urządzeń i niemal każdy, wybierając takie urządzenie, kuszony, jest przez sprzedawców możliwościami, jakie daje oferowany model. Sprzedawcy zachwalają możliwości multimediów w postaci wysokich parametrów aparatów fotograficznych oraz możliwości odsłuchu muzyki czy choćby ułatwień w korzystania z usług, oferowanych przez szereg dostawców w Internecie. Mało kto zwraca uwagę na ważne aspekty, takie jak prywatność, począwszy od możliwości lokalizacji a skończywszy na personalizacji po odwiedzinach na stronach internetowych lub serwisach społecznościowych. Sam, kilkukrotnie dokonując zakupu nowego telefonu, doświadczyłem praktyk stosowanych przez sprzedawców tych urządzeń. Po pytaniu o bezpieczeństwo, o wyłączenie określonych opcji spotykałem się z lekceważeniem tego typu pytań. Wielokrotnie też spotykając się z sugestiami sprzedawców, że sprzedawany telefon jest zabezpieczony przez producenta i nie należy zmieniać ustawień, ponieważ mogą one mieć wpływ na działanie różnych usług oferowanych użytkownikom, jeśli nie od razu, to na późniejszym etapie eksploatacji urządzenia. Mając „minimum" wiedzy w tym zakresie, nie drążę tematu, udając użytkownika masowego zainteresowanego zakupem telefonu określonego modelu. Przed wizytą w punkcie sprzedaży zapoznaję się z możliwościami aparatu oraz możliwościami dostępnych modeli aparatów telefonicznych. Pewnie dlatego używam telefonu dłużej niż przeciętny „Kowalski" pomimo tego, że na rynku pojawiły się nowsze modele oferujące lepsze parametry w zakresie czasu pracy, wyższej rozdzielczości zdjęć fotograficznych oraz nowych możliwości kamery znajdującej się w nowo oferowanych telefonach, ze szczególnym naciskiem na możliwości audio-wizualne i uzyskiwanie zawrotnych prędkości podczas korzystania z Internetu. Hasłowo niekiedy rzucane slogany o nowoczesnych systemach, które zapewniają większe bezpieczeństwo, nie do końca mnie przekonują, ponieważ stwierdzenia te nie są poparte żadnymi dowodami lub choćby porównaniami oferowanych urządzeń w stosunku do niższych modeli.

[1] Józef Druć – emerytowany funkcjonariusz państwowych służb fiskalnych. Kontakt z Autorem: jozef@druc.pl.

Działania takie nie są praktykowane z różnych powodów. Jednym z nich jest z pewnością niepodważanie autorytetu i jakości określonej marki. Nikt przecież nie przyzna się do tego, że coś, co wyprodukował, może zawierać gorsze lub słabsze rozwiązania. Te zweryfikują użytkownicy i czas. W przypadku wykrycia luk w systemie bezpieczeństwa urządzenia, naprawiane są one przez aktualizację systemu. Informacje o wykryciu luk w systemie nie są tym czymś, czym należy się chwalić. Niekiedy jednak takie informacje trafiają do wiadomości, jednak już po usunięciu wady. Trudno tu mówić o przejęciu telefonu i prowadzeniu podsłuchu, który można częściej skojarzyć z filmami o tematyce szpiegowskiej lub akcjami służb specjalnych. Nawet jeśli ten drugi przypadek ma miejsce, to z pewnością nikt tego nie rozgłasza, chociaż w ostatnich latach głośno jest o systemie Pegasus oraz możliwościach, jakie on stwarza.

Celem tego opracowania nie jest charakterystyka ani ocena tego typu działań, lecz sytuacji, która może przytrafić się potencjalnemu użytkownikowi urządzeń pracujących pod kontrolą systemów iOS oraz Android. Współczesne telefony bywają bowiem podsłuchiwane poprzez zainstalowane w nich złośliwe oprogramowanie. Zainstalowane przez użytkownika aplikacje, które w trakcie instalacji żądają dostępu do różnych zasobów znajdujących się w telefonie takich jak książka adresowa, galeria zdjęć, mikrofon lub kamera. Jak się potem okazuje, chwila nieuwagi może doprowadzić do braku poufności przekazywanych przez telefon informacji. Telefon na podsłuchu to urządzenie, które przesyła w nieuprawnione miejsce np. głos podczas rozmów lub dane. Strach pomyśleć o tym, że takie dane przesyłane są w trakcie dokonywania operacji bankowych lub prowadzenia rozmów w bardzo wrażliwych dla rozmówców sprawach. Nikomu nie trzeba tłumaczyć i udowadniać, jak daleko idące mogą być skutki takiego działania zwłaszcza w sytuacji, gdy obca osoba dysponuje informacjami znanym tylko dwóm rozmówcom. Informacjami, które mogą być związane z korespondencją MMS, SMS lub inną adresowaną tylko do określonego odbiorcy. Może się też zdarzyć, że na podstawie dziwnego działania telefonu użytkownik może dojść do wniosku, że jego telefon znalazł się na podsłuchu. Wiele objawów przemawiających za takim wnioskiem da się pewnie wyjaśnić bez większego problemu w inny sposób. Wbrew pozorom i przekonaniu o podsłuchu telefonu, może istnieć inne wyjaśnienie faktu wejścia w posiadanie informacji wrażliwych przez osoby inne. Choć jest to możliwe, to nie zdarza się często. Podsłuch może być dokonywany w różny sposób:

- Podsłuch programowy z wykorzystaniem aplikacji, wirusa lub złośliwego kodu szacuje się, że może być najczęściej występującą sytuacją.
- Aplikacje szpiegujące zdolne do przesyłania danych czy przekierowywania połączeń SMS i danych oraz keyloggery (oprogramowanie lub urządzenie, które rejestruje naciśnięcia klawiszy na klawiaturze, przechwytując wprowadzane przez

użytkownika dane) instalujące się często bez wiedzy użytkownika monitorujące jego zachowanie przesyłające dane na inne nieuprawnione numery.
- Podsłuchy założone przez uprawnione służby w przypadkach określonych prawem.

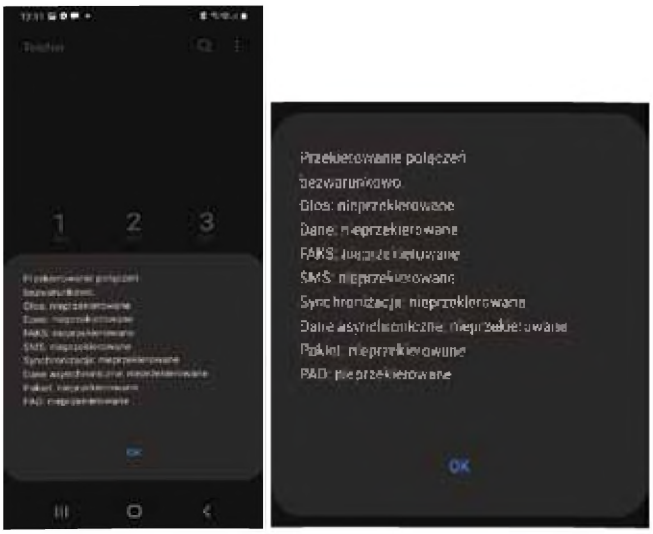
Telefon z zainstalowanym szpiegującym oprogramowaniem może bardzo nietypowo działać i choć zmiany w działaniu może zauważyć użytkownik często w sytuacji, gdy telefon się zawiesza, gdy spowalnia działanie, lub zauważa szybsze zużycie baterii niż dotychczas albo nagłe uruchamianie się nieuruchamianej przez użytkownika aplikacji. Często takich objawów można nawet nie zauważać. W przypadku stwierdzenia, że telefon nie działa tak, jak byśmy tego chcieli lub w obawie, że mamy założony podsłuch, samodzielnie możemy sprawdzić czy nasz telefon jest właściwie skonfigurowany oraz czy nie posiada przekierowań, o których nie ma wiedzy lub zapomniał o ich utworzeniu. Do tego służą kody MMI (Man-Machine Interface) służące do uruchamiania ukrytych funkcji i diagnostyki w telefonach komórkowych, a także zmiany niektórych parametrów sieci. Dla przykładu, na potrzeby niniejszego opracowania warto podać kilka kodów, które pozwalają zweryfikować ustawienia przekierowania:
Kod ***#21#** – informujący o bezwarunkowym przekazaniu połączeń,
Kod ***#61#** – informuje o przekierowaniu przy braku odpowiedzi,
Kod ***#62#** – przekierowanie poza zasięgiem,
Kod ***#67#** – przekierowanie przy zajętym numerze.

Sposób wprowadzenia kodu ***#21#** – informującego o bezwarunkowym przekazaniu połączeń:

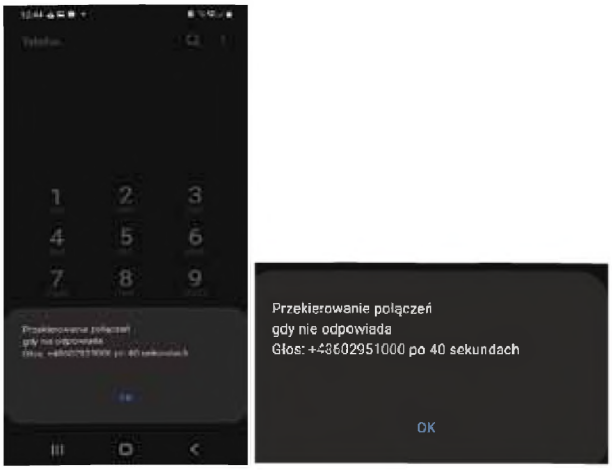


Wprowadzenie kodu i jego zatwierdzenie zielonym przyciskiem ze słuchawką potwierdzone jest komunikatem o uruchomieniu kodu MMI. Po czym dokonywane

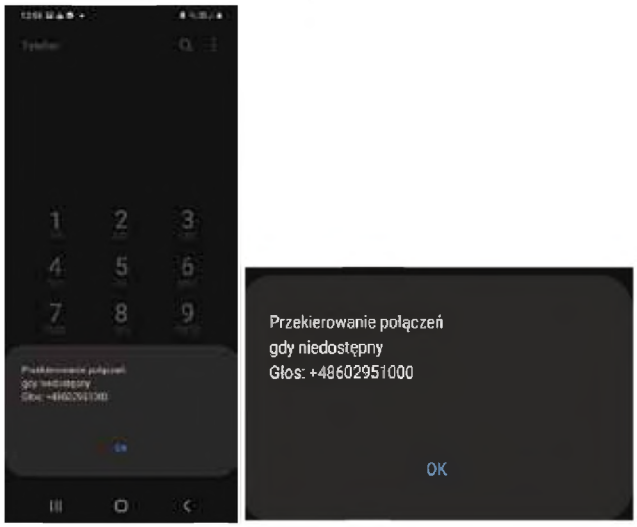
jest sprawdzenie ustawień smartfonu i generowana jest przez system odpowiedź, która przy braku przekierowań wygląda następująco:



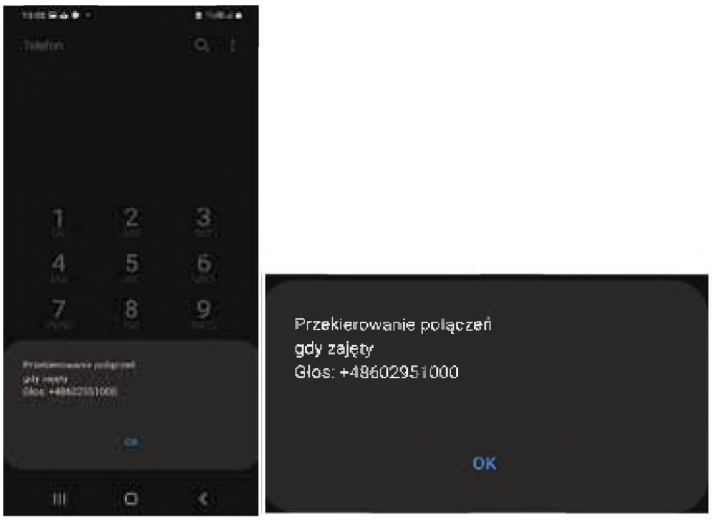
Kod ***#61#*** – informuje o przekierowaniu przy braku odpowiedzi, raport wygląda następująco:



Kod ***#62#*** – przekierowanie poza zasięgiem:



Kod ***#67#*** – przekierowanie przy zajętym numerze:



Nietrudno ustalić, że numer wygenerowany w raporcie to numer poczty głosowej.

Powyższe kody MMI nie wyczerpują możliwości diagnostycznych systemu Android, lecz pozwalają dokonać sprawdzenia niektórych parametrów związanych z działaniem smartfonu. Należy mieć świadomość, że niektóre z kodów mogą powodować zmiany w konfiguracji i działaniu urządzenia, dlatego też nie prezentowane są wszystkie, a jedynie wybrane, związane z weryfikacją możliwości

ustawień telefonu i czy nie jest on na podsłuchu. Istnieje możliwość odnalezienia pełnej listy kodów IMM oraz USSD (Unstructured Supplementary Service Data) – są to specjalne ciągi znaków wprowadzane na telefonie, które służą do bezpośredniej komunikacji z operatorem sieci komórkowej.

Znajomość kodów diagnostycznych oraz kodów do komunikacji z operatorem sieci może być bardzo przydatna, szczególnie w sytuacjach, gdy mamy podejrzenia o różnego rodzaju nieprawidłowości i każdy użytkownik może je stosować choćby po to, aby ustalić przyczyny lub wykluczyć podejrzenia, które same mogą nasuwać się przy nieprawidłowo działających urządzeniach. Nieprawidłowe działanie urządzeń typu telefon czy smartfon, które mogą stać się podejrzanymi, mogą być spowodowane poprzez uszkodzenia, którym uległo urządzenie, co w przypadku ich stwierdzenia zmienić może podejście do zauważonych nieprawidłowości. Inną rzeczą jest samo korzystanie z uszkodzonego w jakikolwiek sposób urządzenia, które nie powinno mieć miejsca i to nie tylko ze względu na nieprawidłowe działanie urządzenia, ale przede wszystkim ze względu na jego bezpieczeństwo. Aby uniknąć większości problemów, w tym związanych z możliwością ułatwienia dostępu niepowołanych osób do danych użytkownika, jest dbanie o regularne aktualizacje oprogramowania urządzenia, korzystanie z zaufanych aplikacji, niewyrażanie zgody na dostęp do danych zapisanych na telefonie, smartfonie, czy tablecie, korzystanie z programu antywirusowego, stosowanie weryfikacji dwuetapowej, niekorzystanie z otwartych nieszyfrowanych sieci Wi-Fi, wyłączanie łączności Bluetooth, gdy się z niej nie korzysta.

O ile poruszone wyżej aspekty dotyczą kwestii bezpiecznego i świadomego użytkowania urządzeń telekomunikacyjnych ogólnego przeznaczenia, to w dalszej części omówione zostaną inne urządzenia, dzięki którym możliwe jest szybkie wykrycie urządzeń służących do podsłuchiwania, podglądania lub komunikacji oraz ich lokalizacji. Zaprezentowany i omówiony zostanie prosty, łatwy i równie skuteczny sprzęt, co urządzenia laboratoryjne, które są skomplikowane w obsłudze. Sprzęt, który zostanie zaprezentowany jest bardzo prosty w obsłudze i nie wymaga posiadania szerokiej wiedzy rzeczoznawcy. Z całą pewnością dzięki prostocie w użytkowaniu i jednoznacznym wskazaniom, może przyczynić się do odnalezienia urządzeń ukrytych, zakamuflowanych lub najzwyczajniej w świecie zasygnalizować istnienie takiego typu urządzeń. Urządzenia ukrywane, najczęściej stosowane mogą być do podsłuchu, monitoringu a nawet sterowania. Choć każde z zastosowań wiąże się z innym przeznaczeniem i odmiennym działaniem, to ze względu na podstawowy czynnik wrażliwy dla tego rodzaju sprzętu diagnostycznego, jakim jest wykrywanie występowania natężenia pola elektromagnetycznego lub natężenia pola wysokiej częstotliwości przedstawione zostaną z krótką charakterystyką możliwości omawianych

urządzeń. Przytoczone zostaną regulacje prawne związane z naruszeniem przepisów Kodeksu Karnego, Rozporządzenia Ochrony Danych Osobowych oraz Kodeksu Pracy.

Być może nie zdajemy sobie sprawy z faktu, jak mocno elektronika użytkowa staje się dziś elektroniką „klockową". Jak w prosty sposób z wykorzystaniem gotowych modułów można realizować swoje techniczne projekty z niemal każdej dziedziny. Obecnie najwięcej modułów wytwarzanych jest w odległych Chinach i zakup nawet najnowszego modułu z oferty pochodzącej z tamtejszego rynku nie stanowi najmniejszego problemu. Z racji niskiej ceny i ciekawych możliwości wykorzystania wspomnianych modułów, kuszeni coraz młodsi „konstruktorzy" podejmują różnego rodzaju wyzwania związane ze stosowaniem modułów do przesyłania dźwięku i obrazu i to wszystko w związku z działaniami naukowymi, poznawczymi lub kolekcjonerskimi. Innym źródłem pomysłów związanych z udostępnianiem wiedzy potrzebnej do budowy takich urządzeń są tematyczne strony internetowe, które z racji swojej popularności mają ogromne zasoby projektów oraz olbrzymie zasięgi, przez co popularyzacja wszelakich propozycji jest bardzo duża.

Do rzeczy.

Podsłuch rozmów lub innych odmiennych form komunikowania się, wzbudzał i wzbudza szereg kontrowersji i emocji. W ostatnim czasie po głośnych i udostępnianych nagraniach rozmów w restauracji „Sowa i przyjaciele" można było dowiedzieć się nie tylko kto i o czym mówił, ale również o nielegalności tych nagrań. Przy okazji można było usłyszeć, kto dokonał nagrania i jaka go za to spotkała kara, bo przecież proceder ten jest uwzględniony w kodeksie karnym.

Ujęcie podsłuchu – bezprawne uzyskanie informacji znalazło odniesienie w Art. 267. K.K.

Art. 267. [Bezprawne uzyskanie informacji]

§ 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.

§ 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.

§ 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1–3 ujawnia innej osobie.

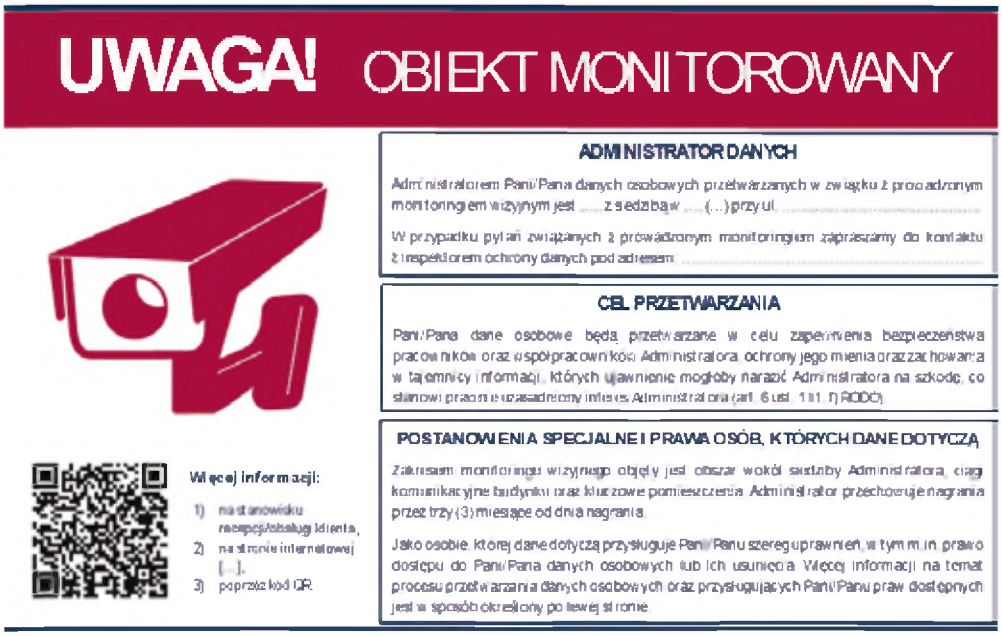
§ 5. Ściganie przestępstwa określonego w § 1–4 następuje na wniosek pokrzywdzonego.

Jak wynika z treści, sam proceder nie jest ścigany z urzędu. To osoba podsłuchiwana musi zwrócić się ze stosownym wnioskiem o wszczęcie postępowania karnego z wnioskiem o ściganie, ale tylko w sytuacji, w której osobiście padła ofiarą podsłuchu.

A co z monitoringiem wizyjnym?

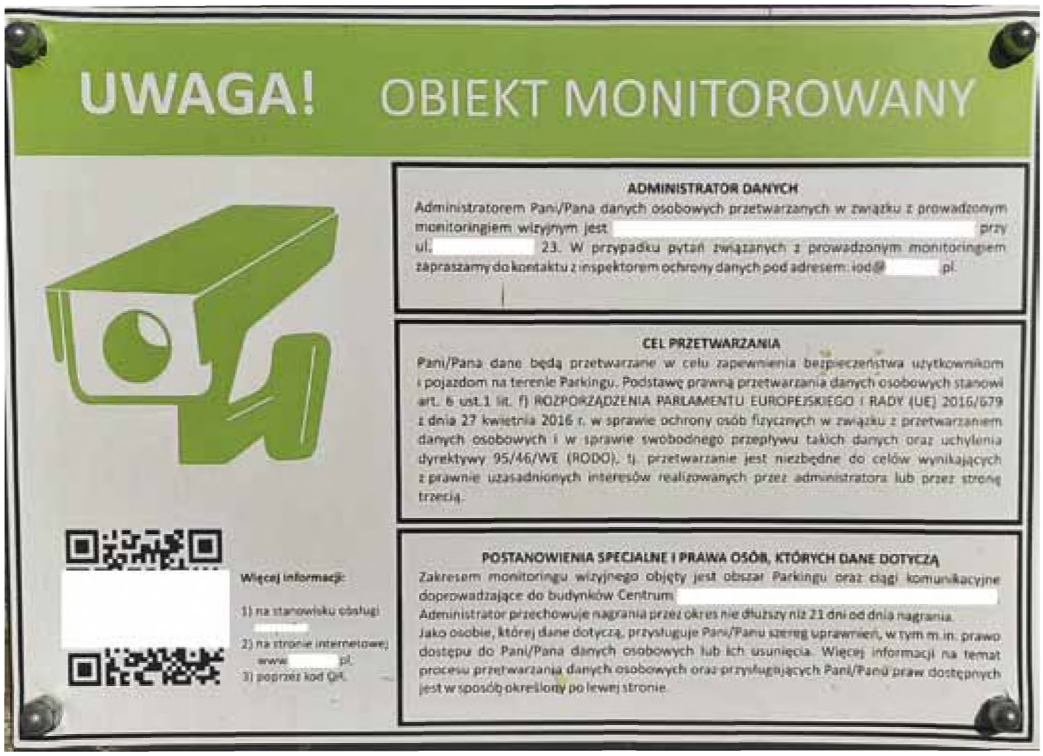
Rozwój technologii i powstanie nowoczesnych systemów bezpieczeństwa oraz stosunkowo niska cena sprawiły, że coraz więcej instalacji monitoringu wizyjnego zakładanych jest przez przedsiębiorców oraz osoby prywatne. Wiele tych instalacji powstaje w miejscach użyteczności publicznej również w przestrzeni miejskiej. O ile duże instalacje monitoringu miejskiego nie budzą emocji, dotyczących instalacji zdalnego nadzoru i nikt nie podejmuje kwestii zgodności z prawem, to w chwili montowania takich systemów w małych firmach lub w obszarze domów jednorodzinnych często podejmowana jest ta kwestia. Wszystko to wynika z braku wiedzy lub niezrozumienia przepisów prawnych dotyczących monitoringu przez przeciętnego użytkownika takiego systemu. Choć monitoring jest legalnie instalowany, to w wielu sytuacjach wzbudza wiele niepotrzebnych emocji. Co ciekawe, to, co związane jest często z protestami dotyczy głownie sytuacji objęcia prywatnej posesji rejestracją przez taki system. Może to być usprawiedliwione, bo w pewnym sensie narusza prawo. Reakcja instalującego taki system powinna być jedna możliwa, polegająca na dostosowaniu systemu monitoringu do braku zgody lub protestu sąsiadujących z obszarem monitorowanym. Możliwości techniczne podczas konfiguracji takiego systemu pozwalają na takie ustawianie kamer lub programowe ograniczenie obszaru objętego rejestracją, aby obszar ten nie był rejestrowany. Od dłuższego czasu staram się śledzić regulacje prawne dotyczące obszaru związanego z monitoringiem wizyjnym. Czasem zadziwić może pomysłowość oraz interpretacje prawników, dotyczące uzasadnienia instalacji monitoringu w pobliżu swoich posesji w ramach realizacji obowiązku prawnego związanego z oznaczeniem obiektu objętego monitoringiem oraz uzasadnieniem instalacji oraz wskazaniem administratora danych gromadzonych w postaci zapisu monitoringu jak na ilustracjach:





Informacje dotyczące monitorowanego obiektu są bardzo przydatne szczególnie, gdy zachodzi potrzeba szybkiego ustalenia administratora monitoringu w sytuacji, gdy na monitorowanym obszarze doszło do zdarzenia, którego przebieg mógł zostać zarejestrowany.

Przykład tablicy informacyjnej posiadającej niezbędne informacje wymagane przez prawo. Tablica sfotografowana została w miejscu ogólnie dostępnym na wejściu (wjeździe) na obiekt monitorowany.



Co mówią na temat monitoringu przepisy prawne?

Zainstalowanie na budynku mieszkalnym kamer podlega wielu regulacjom wynikającym z rozporządzenia o ochronie danych osobowych (RODO) oraz art. 140 kodeks cywilnego:

Art. 140. KC. W granicach określonych przez ustawy i zasady współżycia społecznego właściciel może, z wyłączeniem innych osób, korzystać z rzeczy zgodnie ze społeczno-gospodarczym przeznaczeniem swego prawa, w szczególności może pobierać pożytki i inne dochody z rzeczy. W tych samych granicach może rozporządzać rzeczą.

Najważniejszą informacją jest to, że cele przetwarzania informacji z monitoringu wizyjnego są ograniczone, a sam montaż kamer nie wszędzie jest dopuszczalny. Zakres obszaru, jaki może obejmować monitoring prywatny jest ograniczony do granic danej posesji, ale jak już wspomniano wcześniej, prawnicy znaleźli sposób na to, by uzasadnić ewentualne rozszerzenie obszaru monitorowanego, uzasadniając poszerzenie tego obszaru skądinąd w bardzo logiczny sposób trudny do podważenia. Zdarzają się bowiem sytuacje związane ze specyfiką miejsca, w którym montowany jest taki system monitoringu np.: wspólny chodnik – obszar, po którym można przemieszczać się po dowolnej stronie tego chodnika. W związku z wieloma

wątpliwościami, dotyczącymi spraw związanych z monitoringiem, Urząd Ochrony Danych Osobowych wydał instrukcje formułując 10 wskazówek dla prywatnego monitoringu.



NA TEMAT MONITORINGU WIZYJNEGO PRYWATNYCH POSESJI

URZĄD OCHRONY DANYCH OSOBOWYCH

Jeśli masz kamerę w domu...

Czy wiesz, że obserwując teren przy pomocy kamer, przetwarzasz dane osób obserwowanych, które wchodzą w zasięg działania Twojej kamery?

Czy wiesz, że jako właściciel kamery jesteś uznawany za administratora danych i spoczywa na Tobie szereg obowiązków? Osoby obserwowane mogą korzystać z wielu praw dających im kontrolę nad swoimi danymi osobowymi.

Czy wiesz, że Prezes Urzędu Ochrony Danych Osobowych może przeprowadzić kontrolę Twojego systemu kamer lub wszcząć postępowanie na podstawie skargi osoby obserwowanej? Jeżeli stwierdzi naruszenie zasad, może nakazać Ci wprowadzenie zmian, zaprzestanie obserwowania terenu przy pomocy kamer, a nawet nałożyć karę finansową.

Jeżeli kamery nie obserwują terenu poza Twoją posesją oraz nie obserwują osób spoza kręgu rodziny i znajomych, to poniższe obowiązki nie mają zastosowania. Takie sytuacje są objęte wyjątkiem domowym i osobistym, a przepisy o ochronie danych nie mają wtedy zastosowania.

Jeśli kamery obserwują zarówno teren poza Twoją posesją, jak i osoby postronne przeczytaj uważnie poniższe wskazówki.

Po co wykorzystujesz kamerę?

Zacznijmy od prostego pytania: po co wykorzystujesz kamerę? Do jakich celów? Dopuszczalna jest ochrona osób i mienia przy pomocy kamer, jeżeli w przeszłości na Twojej posesji lub w sąsiedztwie dochodziło do takich incydentów, jak włamania, kradzieże, dewastacje, a nie możesz innymi sposobami (np. alarm, ogrodzenie, pies wartownik) zapewnić sobie bezpieczeństwa.

Dopuszczalne jest obserwowanie ludzi wykonujących prace na Twojej posesji (opiekunka, osoba sprzątająca, hydraulik itd.) w związku z wykonaniem umówionych prac. Ale, jeżeli zatrudniasz ich na podstawie umowy o pracę, to musisz uwzględnić przepisy o monitorowaniu pracowników. Stosuj tylko te funkcje kamer, które są zgodne z przyjętymi przez Ciebie celami, np. nie nagrywaj dźwięku, bo nie jest on potrzebny do celu ochrony osób i mienia.

Jaki teren obserwujesz?

Kamerami możesz obejmować przede wszystkim swój teren. Możesz też obserwować bezpośredni teren wokół Twojej posesji, np. część chodnika, drogi i łąki. Nie powinieneś jednak monitorować posesji sąsiadów. Istnieje ryzyko, że naruszysz ich prywatność.

Gdzie i kiedy nie możesz stosować kamer?
Nie możesz wykorzystywać kamer do obserwowania ludzi w sytuacjach naruszających ich godność, prywatność i intymność. Nie możesz podglądać innych osób np. sąsiadów na ich terenie (z wyłączeniem osób wykonujących pracę na Twojej posesji), obserwować pomieszczeń takich jak łazienki i toalety i nagrywać dalszej okolicy (np. kamerą na szczycie dachu).

Jak długo obserwujesz teren?
Odpowiedz sobie na pytanie: czy obserwujesz teren stale czy tylko okresowo? Dostępne dzisiaj kamery mogą monitorować teren 24 godz. na dobę, zostać uruchomione przez użytkownika albo automatycznie, np. przez fotokomórkę. Powinieneś wybrać formę działania niezbędną dla Twoich celów. Dobrym przykładem jest wideodomofon, który może być włączany przez użytkownika, zamiast nieprzerwanie obserwować teren przed drzwiami lub furtką.

Jak długo przechowujesz nagrania?
Jeżeli Twój system zapisuje nagrania, musisz zdecydować, jaki jest niezbędny czas ich przechowywania. Przy ciągłym monitoringu, czas przechowywania nagrania powinien być krótki np. 24 godz. Gdy udajesz się na urlop, możesz wydłużyć ten czas do powrotu z urlopu i zapoznania się z monitoringiem o np. 2 tygodnie. Jeżeli nie nagrałeś żadnych incydentów, to po tym okresie musisz usunąć nagrania. Zauważ, że Ty, jako administrator danych, odpowiadasz za czas przechowywania nagrania. Im krótszy jest ten okres, tym masz mniej danych, które musisz zabezpieczać.

Jakich zabezpieczeń kamer i rejestratora używasz?
Każdemu zależy na tym, aby jego dane były chronione. Dlatego system kamer musi być zabezpieczony przed dostępem osób nieupoważnionych. Jako administrator musisz przeciwdziałać próbom podłączenia z zewnątrz do sygnału z kamer (kablowych i bezprzewodowych) i nagrań. Oznacza to np. ograniczenie fizycznego dostępu do kamer, źródeł zasilania, monitora i rejestratora. Konieczne jest też zabezpieczenie systemu operacyjnego, np. hasłem dostępowym. Pamiętaj, by nie korzystać z fabrycznego hasła i okresowo je zmieniać. Przy zdalnym dostępie do obrazu z kamer (np. aplikacją na telefon), urządzenia te także muszą być zabezpieczone.

Kto może mieć dostęp do nagrań?
Osoby obserwowane mają prawo dostępu do swoich danych na nagraniach. Przy tym nie możesz udostępniać danych innych osób - powinieneś je zamazać, np. przy pomocy oprogramowania. Nagrane przez Ciebie sytuacje mogą być udostępnione np. Policji lub ubezpieczycielowi w związku z napaścią, włamaniem albo zniszczeniem mienia w celu przeprowadzenia odpowiednich postępowań. Także osoby prywatne, które mają usprawiedliwiony interes mogą domagać się dostępu do nagrań, np. gdy uszkodzono ich samochód stojący w zasięgu Twojej kamery. Musisz ocenić, czy udostępnienie nagrania jest zasadne. W obu przypadkach możesz udostępnić całe nagranie bez zamazywania wizerunku uczestników.

Kiedy nie możesz udostępniać nagrań?
Jeżeli wykorzystujesz kamery do ochrony osób i mienia lub nadzoru nad osobami pracującymi na posesji, to nie wolno Ci publicznie udostępniać ich wizerunków, np. w Internecie. Robiąc to narażasz się na odpowiedzialność przed sądami i Prezesem Urzędu Ochrony Danych Osobowych.

Czy możesz podłączyć Twoje kamery do agencji ochrony?
Tak, ale powinieneś w umowie z agencją ustalić zasady powierzenia danych. Musisz określić cel, zakres i czas trwania monitorowania oraz obowiązki agencji w związku z bezpieczeństwem danych. Pamiętaj, agencja nie może wykorzystywać uzyskanych nagrań do swoich celów niezwiązanych z umową.

Jak informujesz o kamerach na swojej posesji?
Osoby obserwowane muszą być poinformowane o przetwarzaniu ich danych przy pomocy kamer. Przy wejściu na teren monitorowany musisz umieścić informację co najmniej wskazującą: Ciebie jako administratora (podać dane kontaktowe), cele przetwarzania, obserwowany obszar i okres przechowywania nagrań. Powinieneś także wskazać, gdzie można uzyskać pozostałe informacje (podstawa prawna przetwarzania, informacje o odbiorcach, wykaz praw osoby obserwowanej, możliwości złożenia skargi do Prezesa Urzędu).

Jeżeli chciałbyś wiedzieć więcej, zachęcamy do zapoznania się ze wskazówkami dot. wykorzystywania monitoringu wizyjnego (https://uodo.gov.pl/pl/138/354).

Jeżeli nadal masz wątpliwości, skontaktuj się z naszą infolinią pod numerem telefonu: 606-950-000

Urząd Ochrony Danych Osobowych ul. Stawki 2 00-193 Warszawa
e-mail: kancelaria@uodo.gov.pl; e-PUAP: /UODO/SkrytkaESP

UODO
URZĄD OCHRONY DANYCH OSOBOWYCH

Odmienne podejście jest do monitoringu, zostało szczegółowo uregulowane w Kodeksie Pracy w Art. 22 2. – [Monitoring w zakładzie pracy] – Kodeks pracy, który ma brzmienie:

§ 1. Jeżeli jest to niezbędne do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, pracodawca może wprowadzić szczególny nadzór nad terenem zakładu pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring).

§ 11. Monitoring nie obejmuje pomieszczeń udostępnianych zakładowej organizacji związkowej.

§ 2. Monitoring nie obejmuje pomieszczeń sanitarnych, szatni, stołówek oraz palarni, chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji celu określonego w § 1 i nie naruszy to godności oraz innych dóbr osobistych pracownika, w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób. Monitoring pomieszczeń sanitarnych wymaga uzyskania uprzedniej zgody zakładowej organizacji związkowej, a jeżeli u pracodawcy nie działa zakładowa organizacja związkowa – uprzedniej zgody przedstawicieli pracowników wybranych w trybie przyjętym u danego pracodawcy.

§ 3. Nagrania obrazu pracodawca przetwarza wyłącznie do celów, dla których zostały zebrane i przechowuje przez okres nieprzekraczający 3 miesięcy od dnia nagrania.

§ 4. W przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub pracodawca powziął wiadomość, iż mogą one stanowić dowód w postępowaniu, termin określony w § 3 ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.

§ 5. Po upływie okresów, o których mowa w § 3 lub 4, uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe podlegają zniszczeniu, o ile przepisy odrębne nie stanowią inaczej.

§ 6. Cele, zakres oraz sposób zastosowania monitoringu ustala się w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu, jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy.

§ 7. Pracodawca informuje pracowników o wprowadzeniu monitoringu, w sposób przyjęty u danego pracodawcy, nie później niż 2 tygodnie przed jego uruchomieniem.

§ 8. Pracodawca przed dopuszczeniem pracownika do pracy przekazuje mu na piśmie informacje, o których mowa w § 6.

§ 9. W przypadku wprowadzenia monitoringu pracodawca oznacza pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż jeden dzień przed jego uruchomieniem.

§ 10. Przepis § 9 nie narusza przepisów art. 12 i art. 13 rozporządzenia 2016/679.

Jak wynika z treści zapisów kodeksu pracy monitoring wizyjny może służyć zapewnieniu bezpieczeństwa i nie może być stosowany do zarządzania w przedsiębiorstwie lub nadzoru nad pracownikami.

Jak wiadomo, regulacje poprzez system prawny, zawsze są wynikiem powstania możliwego zagrożenia (w przypadku monitoringu – np. ograniczenie swobody .....). Wszyscy którzy zajmują się monitoringiem wizyjnym mają wiedzę i świadomość funkcjonowania tych systemów ich zdolności do rozpoznawania sylwetek, twarzy, numerów rejestracyjnych pojazdów i ich kolorów. Swoją drogą ciekawe, kiedy ta funkcjonalność znajdzie swoje miejsce w regulacjach dotyczących monitoringu szczególnie w odniesieniu do przechowywania zapisów. Czym będzie zapisany wzorzec w postaci sylwetki, twarzy czy innych danych, mających być punktem odniesienia do analizy już na etapie zapisu obrazu i reakcji systemu w przypadku stwierdzenia zgodności ze zdefiniowanym wzorcem? A czym sam proces analizy tego zapisu. Choć dokonywany przez system w urządzeniu do rejestracji to jednak mamy do czynienia z analizą obrazu. Idąc dalej należy zauważyć, iż obecnie kamera z możliwością transmisji lub zapisu dźwięku, śledzenia obiektu, który sam z siebie jest poruszającym się obiektem, nie jest żadną nowinką, a staje się standardem, który daje szereg możliwości związanych z analizowaniem sparametryzowanego obrazu oraz zapisu uzyskanych w wyniku przetwarzania „widzianych" przez kamerę obrazów oraz danych pochodzących z analizy tego obrazu.

Poruszone wyżej kwestie związane z podsłuchem oraz z monitoringiem nie wyczerpują wszystkich możliwości związanych ze sposobami nielegalnego pozyskiwania różnych informacji. Do tej pory nie poruszono jeszcze jednej istotnej kwestii mianowicie podsłuchu z wykorzystaniem technik radiowych. I nie starano się, by dochodzić powodów stosowania podsłuchów niezależnie od techniki, jaka by nie była zastosowana. Nadszedł wiec czas, aby spróbować dociec, dlaczego ludzie się podsłuchują?

Zapewne dla nikogo nie będzie zaskoczeniem stwierdzenie, że powody tego są różne. Jedni ze zwyklej ciekawości, inni z chęci zdobycia informacji czy przejęcia kontroli nad podsłuchiwanymi, w celach przestępczych lub przez służy w celu inwigilacji. Czasy podsłuchu za pomocą szklanki, prezentowane w niektórych filmach niskich lotów lub przez drzwi, to już jest historia. Z zasady te bardziej wyrafinowane sposoby podsłuchu nie były i nie są udostępniane i na ogół trudno wydobyć na światło dzienne, szczególnie w szpiegostwie przemysłowym lub polityce. Wiele

osób mających tajemnice przemysłowe, technologiczne, handlowe lub inne stara się je chronić, w każdy możliwy sposób, tworząc tajemne pomieszczenia, wymyślne sejfy czy wprowadzając uzbrojoną ochronę wspieraną, wymyślnym monitoringiem. Czasy, gdy podsłuch na polu walki realizowano za pomocą tub zakładanych na uszy by zbierać dźwięki z określonego kierunku za pomocą bardzo czułych mikrofonów szczelinowych lub stosowanie technik czasem bardzo dziwnych, których przytaczanie w tym opracowania nie jest teraz potrzebne – dawno minęły. Ważne natomiast jest pokazanie trendów i sposobów na wykrywanie ew. podsłuchów lub innych poznanych sposobów nielegalnego pozyskiwania informacji, w tym również inwigilacji.

Zapewne wielu z nas spotkało się z reklamą urządzeń do inwigilacji i podsłuchu za pomocą sieci GSM i to głównie za sprawą systemu Facebook. Może nie byłoby w tym nic dziwnego, gdyby nie fakt, że reklamowano urządzenia jako pozwalające na sprawdzenie wierności kochanków lub monitorowania sytuacji w domu, gdy dzieci lub osoby starsze pozostawiano pod nadzorem opiekunów. Powstały różnego rodzaju urządzenia ułatwiające takie monitorowanie sytuacji we własnym domu. Urządzenia bezprzewodowe typu „Baby niania", które to od pierwszych wersji jeszcze jako przewodowe, służyły do nasłuchu tego, co dzieje się w dziecięcym pokoju. Aktualnie tego typu urządzenia pozwalają na bieżąco znać sytuację w takim pokoju z dowolnego miejsca na świecie. Po zalogowaniu się do urządzenia podłączonego do sieci Wi-Fi można nie tylko słyszeć, ale widzieć to, co dzieje się w pomieszczeniu, w którym zainstalowano urządzenie. Aktualnie na rynku jest duża ilość sprzętu o podobnej funkcjonalności o bardzo rozbudowanych układach i możliwościach związanych wykorzystaniem sieci Wi-Fi oraz GSM, do których możliwe jest logowanie się za pomocą własnego telefonu komórkowego. Nie sposób nie wspomnieć o takich urządzeniach, ponieważ są one w naszej przestrzeni możliwe do zakupu i zapoznania się z ich działaniem, przeznaczeniem do jakiego zostały one wyprodukowane. Warto jednak wskazać na inny bardzo niszowy rodzaj urządzeń z obszaru podsłuchowego szczególnie tego, który wykorzystuje techniki radiowe do transmisji treści podsłuchu. Urządzenia, które łatwo można zakupić poprzez portale handlowe oferujące szereg innych produktów a między nimi nadajniki radiowe z podaniem parametrów istotnych dla tego urządzenia.

www.[illegible].pl

Dziękuję za zakup.

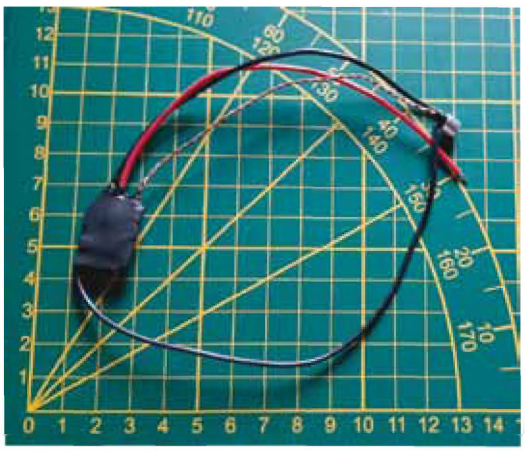
Nadajnik radiowy pracujący na paśmie 70cm około 433Mhz(dokładna częstotliwść poniżej).
Można zasilić i schować według swojego upodobania.
Idealne pod jedno ogniwwo Li-ion. 3.7v 1S np. 18650 itp.
Czerwony przewód + , czarny przewód -

Częstotliwość pracy ....434,0125 Mhz....
Modulacja NFM (wąski fm)
Zasięg w terenie zabudowanym ....do 300 m....
Zasięg w terenie otwartym ....do 3km....
Zasilanie ....2,7V ÷ 5,5V....

Gwarancja obowiązyje 12 miesięcy od dnia ...31.10.2024r....

Pozdrawiam
www.[illegible]

To, co istotnym jest dla tego typu ofert, to cecha która laikowi nic nie powie. Dla choć trochę znającego realia dotyczące pasm i fal radiowych, jasnym jest, że urządzenie to, choć łatwe do pozyskania, może okazać się problemem związanym z odbiorem sygnału nadawanego przez ten nadajnik, ponieważ częstotliwość pracy tego urządzenia 434,0125 MHz nie mieści się w zakresie odbiorników ogólnodostępnych w sieci sprzedaży i do odbioru niezbędny jest w tym przypadku skaner, posiadający zakres do odbioru pasma 70 cm lub radiotelefon radioamatorski pozwalający ustawić szerokość kanału 12,5 KHz. Samo urządzenie wygląda bardzo niewinnie.



Deklarowany zasięg w terenie zabudowanym oraz otwartym to tylko chwyt marketingowy, w rzeczywistości zasięg ten zależy od wielu czynników takich jak teren, na którym takie urządzenie jest użytkowane. W przypadku terenu zabudowanego, jaki materiał wykorzystany został do budowy obiektu, w którym się znajduje zaprezentowany nadajnik. Z racji posiadanych uprawnień radiowych możliwe było zbadanie tego urządzenia (zakupionego w celach poglądowych) zasięg w terenie otwartym w „fabrycznej" konfiguracji był bardzo zbliżony. Po załączeniu anteny ¾ lambda wystrojonej bardzo ostro do częstotliwości pracy nadajnika, odległość, z której był słyszany sygnał z tego nadajnika przekroczył 18 km w linii prostej. Urządzenia nadawcze wykorzystujące częstotliwości 433 MHz i 868 MHz mieszczące się w paśmie ISM (Industrial, Scientice, Medical) – „przemysłowe, naukowe, medyczne" są legalne w Europie pod warunkiem, że moc nadawania sygnału nie przekracza 100 mW. Zaprezentowane urządzenie mieści się w zakresie częstotliwości akceptowanych na terenie RP, lecz ze względu na podany zasięg może być problem ze zmieszczeniem się w limicie mocy. Może być problem szczególnie w górnych granicach napięcia zasilania podanego przez „producenta". Poniżej, przedziały częstotliwości ISM akceptowane na terenie RP.

Przedziały częstotliwości ISM akceptowanych na terenie Polski

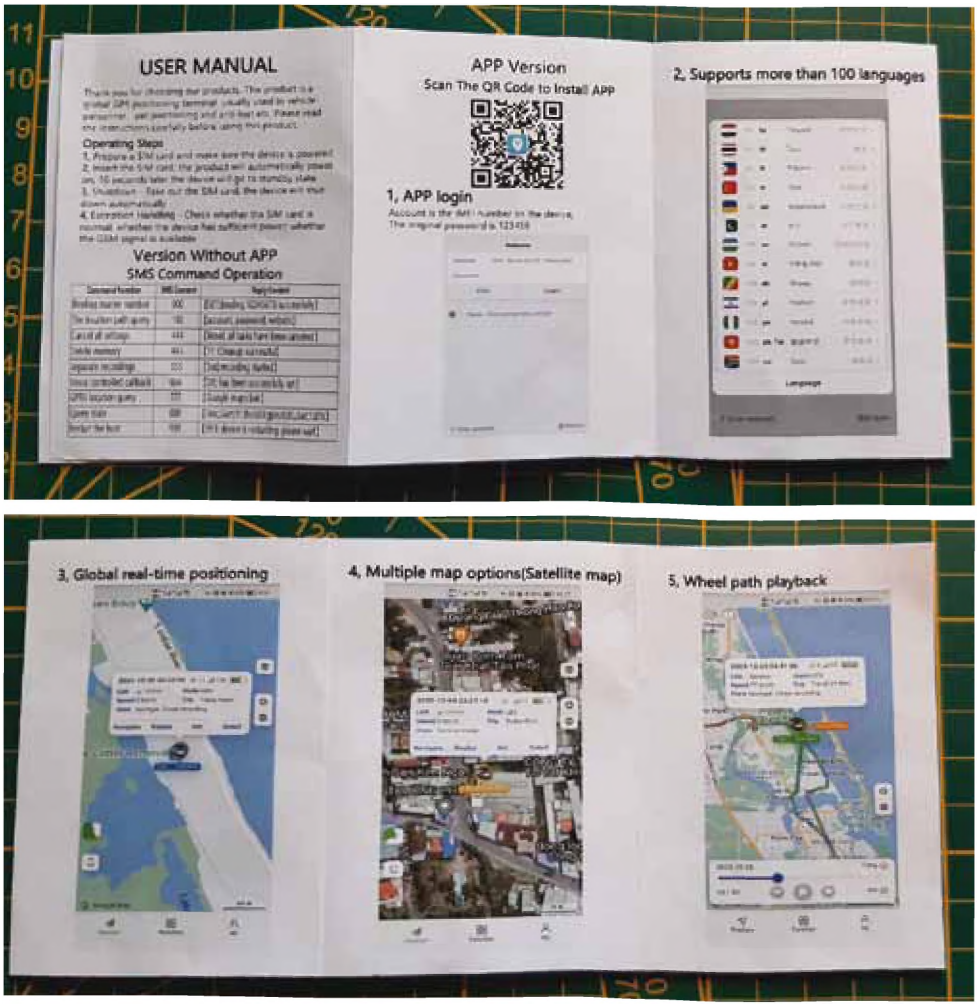
Od	Do
6,765 MHz	6,795 MHz
13,553 MHz	13,567 MHz
26,957 MHz	27,283 MHz
40,660 MHz	40,700 MHz
433,050 MHz	434,790 MHz
868,000 MHz	870,000 MHz
2400 MHz	2483 MHz
5725 MHz	5875 MHz
24,00 GHz	24,25 GHz
61,00 GHz	61,50 GHz
122,00 GHz	123,00 GHz
244,00 GHz	246,00 GHz

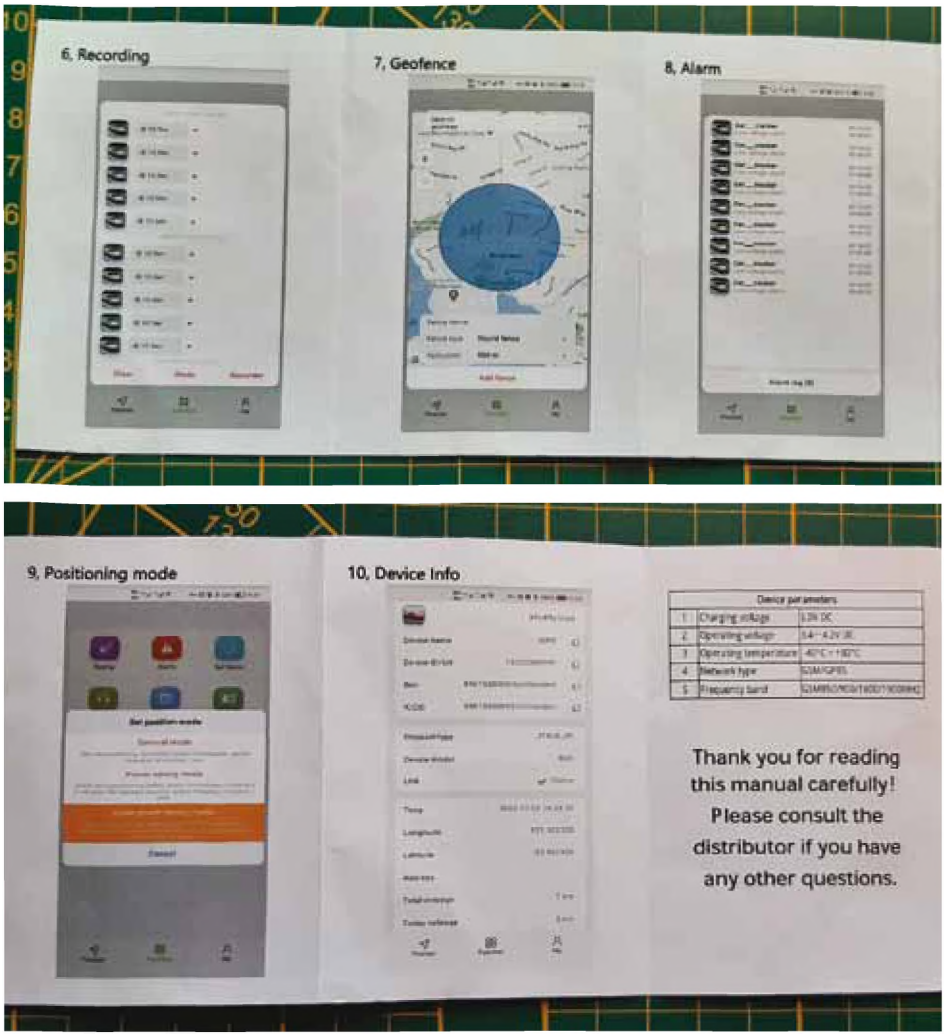
Trudno jest ocenić na oko czy urządzenie mieści się w zakresie podanych częstotliwości, tym bardziej czy limit mocy jest odpowiedni. Stosunkowo łatwo jest określić przeznaczenie takiego urządzenia z zamontowanym mikrofonem. I choć znalezienie takiego urządzenia jest nie tak wcale trudne, to już znalezienie odbiorcy nadawanego sygnału, może stać się niemożliwe. Dodatkowo pomimo tego, że jest to urządzenie pracujące w zakresie częstotliwości legalnych, to cel, w jakim to urządzenie jest stosowane, budzi szereg obaw.

Innym urządzeniem bardzo popularnym stał się GF-07 GPS. Jest to niedrogie urządzenie pozwalające śledzić „obiekt" wyposażony w to urządzenie, który wymaga do swojego działania karty SIM. Dodatkowo posiada gniazdo na zainstalowanie karty microSD, na którą możliwy jest zapis dźwięków z najbliższego otoczenia.



Urządzenie choć niepozorne, to dające duże możliwości, a w rękach świadomego użytkownika dające wiele możliwości nie tylko związanych z podsłuchem tego co dzieje się w otoczeniu urządzenia, ale również zapisu. Ponadto urządzenie pozwala na zlokalizowanie go i wskazanie położenia na mapie. Do urządzenia dołączona jest krótka, ale bardzo treściwa instrukcja:





Urządzenie GPS GF-07 zakupiono w celach poznawczych, aby wypracować metodykę pozwalającą na szybkie i sprawne wykrywanie tego i temu podobnych urządzeń, co mogłoby się wydawać zbyt dużym wyzwaniem, nawet dla biegłego z zakresu informatyki śledczej. Z jednej strony dla dopuszczających się procederu podsłuchu posiadanie i użytkowanie takich urządzeń może wydawać się niewykrywalnym. Dla osób znających specyfikę działania takich urządzeń, posiadających minimum wiedzy o sposobach konstruowania takich urządzeń, wystarczy najprostszy miernik natężenia pola wysokich częstotliwości oraz występowania obszarów z silnym polem elektromagnetycznym, by zorientować się, że takie urządzenia są eksploatowane w miejscu, w którym się przebywa. Nie jest też tajemnicą, że większość urządzeń podsłuchowych wykorzystujących techniki radiowe konstruowanych jest

w zakresie VHF lub UHF. Jest też grupa urządzeń, których działanie związane jest z wykorzystaniem górnej części pasma UKF pomiędzy 88 MHz a 108 MHz. Wszystko tylko spowodowane jest posiadanym sprzętem odbiorczym do odbioru sygnału z tego zakresu częstotliwości. Innym argumentem przemawiającym za wyborem tego pasma przez konstruktorów urządzeń podsłuchowych są prostota konstrukcji i czynnik psychologiczny. Pierwszy, związany z prostotą konstrukcji wynika z łatwości w dostępie do półprzewodników i innych elementów działających w tym zakresie częstotliwości. Psychologiczny związany jest z podejściem odbiorcy radiowego, który w 99,9 % jest słuchaczem jednej lub kilku określonych stacji nadawczych, które są dla niego opiniotwórcze lub nadające ulubiony rodzaj muzyki. Wszystkie inne sygnały pojawiające się w pasmie traktowane są jako zakłócenia. Rozpowszechnienie standardu odbiorników do odbioru transmisji w modulacji FM bardzo ułatwiło stosowanie podsłuchu w tej modulacji, ponieważ najważniejszą właściwością tej modulacji jest to, że słyszymy tylko najsilniejszą stację. Zatem ci, którzy wiedzą o tych właściwościach, mogą stosować urządzenia z zakresu UKF stacji nadających we wskazanym zakresie, mają niemal pewność, że nikt tego nie odkryje, a jeśli już, to potraktuje słyszane sygnały jako nieprzydatne zakłócenia, produkty spamowe od innych urządzeń.

Tak więc w pewnym sensie każdy z nas, posiadających urządzenie do odbioru zakresu fal UKF w przedziale 88–108 MHz (samochodowe odbiornik radiowe, smartfony wyposażone w odbiornik radiowy) jest posiadaczem wysokiej klasy przyrządu pomiarowego działającego we wskazanym zakresie i może posłużyć do wykrywania urządzeń nadawczych pracujących w zakresie UKF. Choć odbiornik taki może zapewnić przeskanowanie określonego wycinka pasma, to nie jest on w stanie wykryć pól elektromagnetycznych, które mogą być wytwarzane poprzez agregaty prądotwórcze w nielegalnych, zakamuflowanych fabrykach wyrobów tytoniowych lub lampy kwarcowe dużej mocy, służące do podgrzewania i oświetlania upraw nielegalnie uprawianych roślin. Z pomocą przychodzą sprzedawcy urządzeń podsłuchowych, którzy oferują urządzenia do wykrywania źródeł promieniowania elektromagnetycznego w postaci detektorów takiego pola obu stronom. Urządzenia o różnym stopniu specjalizacji i naturalnie w różnej cenie. Chociaż po seansie na serwisie YouTube można odnieść wrażenie, że prezentujący wyszukiwanie urządzeń podsłuchowych za pomocą bardzo skomplikowanych urządzeń, że jest to bardzo skomplikowany proces wymagający takich jak prezentowany przez nich sprzęt. Prezentacja dokonywana w pomieszczeniu, w którym znajduje się jedna osoba – ta prezentująca – umieszcza szerokopasmowy odbiornik SDR w różnych miejscach tego pomieszczenia i na podstawie wskazań wyświetlacza tego odbiornika może określić częstotliwość i siłę sygnału, lecz nie miejsce ukrycia poszukiwanego urządzenia

nadawczego. Do szybkiego wyszukiwania i detekcji występowania wspomnianych pól służą proste detektory, które choć nie wyświetlają częstotliwości pracy urządzeń promieniujących, to bardzo dobrze określają siłę sygnału. Po pewnym czasie eksploatujący takie urządzenie nauczy się określać odległość i kierunek z jakiego pochodzi sygnał nadawany.

Najprostszym z najprostszych urządzeń, które sprawdziło się kilkukrotnie w wyszukiwaniu urządzeń jest laserowy wykrywacz podsłuchów **CC308+**.



To urządzenie, które z łatwością pozwala na wykrycie oraz zlokalizowanie prawie wszystkich dostępnych na rynku urządzeń szpiegujących: podsłuchów (pluskiew), podsłuchów GSM, lokalizatorów GPS, kamer. Optyczny system wykrywania światła odbitego od krzywizny obiektywu pozwala na wykrycie kamery każdego typu – nawet wyłączonej. Posiada regulację ustawienia czułości odbieranego sygnału, dzięki czemu można wyeliminować niepożądane promieniowanie elektromagnetyczne. Wykrywacz nie reaguje na fałszywe alarmy typu pola elektromagnetyczne wytwarzane przez urządzenia elektryczne takie jak fax, telewizory, monitory, komputery. Częstotliwość pracy do 6500 MHz.

Urządzenie # **M128**.



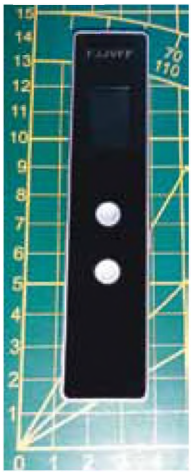
Przy pomocy tego prostego urządzenia można zlokalizować aktywne nadajniki podsłuchowe zainstalowane w pomieszczeniu, komputerze lub telefonie stacjonarnym. Detektor ten reaguje na wszystkie urządzenia pracujące o częstotliwości w zakresie 30 MHz–3,6 GHz. Wskaźnik w postaci diody LED światłem pulsującym sygnalizuje obecność od nadajnika (im bliżej nadajnika tym szybsze pulsowanie światła).

Wykrywacz ukrytych urządzeń – **X13**.



Urządzenie to pozwala wykryć fale radiowe (kamer bezprzewodowych/podsłuchów itp.), wykryć ukryte kamery (przy wyłączonym świetle w pomieszczeniu), detekcję pola magnetycznego GPS, oraz wykryć laser w odległości 0,1 do 6 m. Urządzenie pracuje do częstotliwości 5.8 GHz.

Wykrywacz ukrytych kamer szpiegowskich **FJJVFF**



Urządzenie proste w obsłudze i praktyczne. Umożliwia wykrywanie sygnałów wysokiej częstotliwości pochodzących z ukrytych kamer Wi-Fi, lokalizatorów GPS, bezprzewodowych podsłuchów audio. Posiada wbudowany detektor ukrytej kamery do wykrywania kamery z ukrytym otworem poprzez prostą kontrolę wizualną za pomocą skanowania laserowego w podczerwieni. Urządzenie wykrywa pola magnetyczne oraz lokalizatory GPS. W urządzeniu znajduje się oświetlacz UV. Wielofunkcyjny detektor może wykryć ukryte kamery urządzenia GSM / 3G / 4G oraz trackery (urządzenia pozwalające na śledzenie lokalizacji) i silne sygnały magnetyczne. Częstotliwość pracy do 3800 MHz.

Wykrywacz GPS, kamer i podsłuchów **K600**.



K600 – urządzenie wojskowej jakości umożliwia wykrywanie fal radiowych (w tym kamer bezprzewodowych, urządzeń Wi-Fi, podsłuchów radiowych trackerów). Wizjer ze specjalnym filtrem optycznym do wykrywania kamer. Urządzenie zaopatrzone w optyczny sygnalizator siły sygnału – detekcji z 10 segmentową skalą oraz detektor pola magnetycznego GPS. Zakres wykrywanych częstotliwości: 1 MHz–8 GHz (większość lokalizatorów GPS).

Wykrywacz podsłuchów i kamer **G318**.



Wykrywacz podsłuchów G318 to niewielkich rozmiarów urządzenie służące do lokalizowania urządzeń szpiegowskich pracujących w oparciu o transmisje cyfrowe GSM, GPS oraz podsłuchy analogowe. Urządzenie pozwala na wykrycie podsłuchów, aktywnych telefonów komórkowych (2G, 3G, 4G LTE, HSDPA), lokalizatorów GPS a także kamer bezprzewodowych np. 1.2 GHz, 2.4 GHz, 5.8 GHz. Daje możliwość zlokalizowania rzadziej spotykanych nadajników, działających w technologii Bluetooth oraz Wi-Fi. G318 wspomaga wykrycie bezprzewodowych kamer lub podsłuchów, które emitują fale radiowe, a także ukrytych kamer bezprzewodowych, które mogą emitować fale radiowe. Detektor jest w stanie także wykryć nadajniki GSM oraz lokalizatory GPS. Stopniowanie czułości umożliwia regulator (potencjometr), Siłę nadawanego przez urządzenia szpiegowskie sygnału można odczytać na detektorze za pomocą linijki siły sygnału. Zakres częstotliwości 1–8000 MHz.

Wykrywacz podsłuchów i GPS **DM-K18**.



Urządzenie wykrywa podsłuchy HF i GSM, telefony z aktywnym LTE, kamery. Wykrywa sygnały: AM, FM, WFM nadawane w pasmach GSM, VHF, UHF oraz Wi-Fi i Bluetooth. Wykrywacz DM-K18 to podstawowe urządzenie, które umożliwia identyfikację oraz lokalizację większości dostępnych na rynku aktywnych urządzeń szpiegujących, takich jak trackery GPS, podsłuchy GSM czy kamery bezprzewodowe. Sprzęt wyposażony jest w dodatkowy czujnik magnetyczny do wykrywania magnesów urządzeń GPS. Rozpoznaje urządzenia pracujące w zakresie częstotliwości 1 MHz–6,5 GHz.

Zaprezentowane urządzenia nie są jedynymi urządzeniami na rynku. Mnogość dostępnych urządzeń, również na rynku wtórnym, świadczy o wielkości rynku tych produktów, co pozwala na stwierdzenie olbrzymiego zapotrzebowaniu na tego typu urządzenia. Może jest to związane ze strachem przed możliwością ujawnienia rzeczy, które są ważne lub stanowią tajemnice różnego rodzaju począwszy od najzwyklejszych wstydliwych po tajemnice handlowe czy technologiczne. Biorąc pod uwagę możliwości dzisiejszej elektroniki oraz informatyki, należy spodziewać się innych ciekawszych rozwiązań pozwalających nie tylko wykrywać zastawiane pułapki, ale również urządzenia, które pozwolą na ochronę tajemnic o wiele skuteczniej niż obecnie. Choć nigdy pewności na 100% zabezpieczenie i ochronę prywatności przez tych którzy chcą takiej ochrony nie będzie, ponieważ postęp działa też na korzyść

tych, którzy wymyślają różne sposoby na wykradanie tajemnic, podsłuchiwanie czy śledzenie jakimi ścieżkami przemieszcza się interesująca ich osoba. Obserwując trendy można być niemal pewnym, że urządzenia, które służą wykrywaniu i odnajdowaniu będą w przyszłości dużo bardziej precyzyjne i bardziej skuteczne w swoim działaniu. Z całą pewnością staną się również łatwiejsze w obsłudze przez ludzi, którzy nie będą musieli obcować z branżą elektroniki czy też informatyki. Wystarczy, że będą umieli włączyć takie urządzenie a interpretacji tego, co zostanie wykryte, dokona posiadane urządzenie, wskazując, co w najbliższym otoczeniu tego urządzenia się znajduje.

Jacek Garbaczewski[1]

Nie ma portu? I co z tego! Jak dojść do użytkownika końcowego, kiedy wszyscy mówią, że się nie da

1. Wprowadzenie

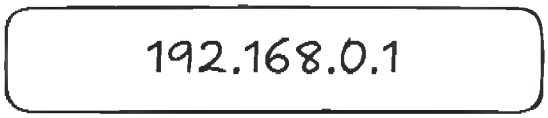
Wielu z nas zna to zdanie: „Nie da się ustalić sprawcy, bo nie ma portu". I na tym się kończy. A ja powiem tak – da się. Trzeba tylko pogrzebać głębiej. Pokażę Wam, jak to zrobić, z jakich narzędzi korzystać, i jak zmusić dane, żeby zaczęły mówić. Nie znajdziesz tu rozbudowanej teorii – skupiam się na praktyce, pokazanej możliwie najprościej w wersji „dla każdego".

Inspiracją do podjęcia tego tematu stał się mój udział w szkoleniu, gdzie prowadzący przeprowadził wprowadzającą ankietę zadając pytanie „Jakie są dla Ciebie największe utrudnienia w zwalczaniu cyberprzestępczości?". Znakomita większość ankietowanych pomijając wskazywane czynniki ściśle związane z finansowaniem organów ścigania, wskazała właśnie poruszaną w tej publikacji kwestie.

Często słyszę od innych, że skoro nie ma portu źródłowego w logach np. od banków czy sklepów online, to nie ma sensu drążyć. Tyle że te usługi – świadczone drogą elektroniczną – to dla nas źródło, z którego da się bardzo często jeszcze coś wyciągnąć. Trzeba tylko wiedzieć, jak. Ale, przejdźmy do podstaw.

Bardzo upraszczając, każde urządzenie pracujące w sieci ma swój adres przy pomocy którego „rozmawia" z innymi urządzeniami. Tym adresem jest adres IP właśnie.

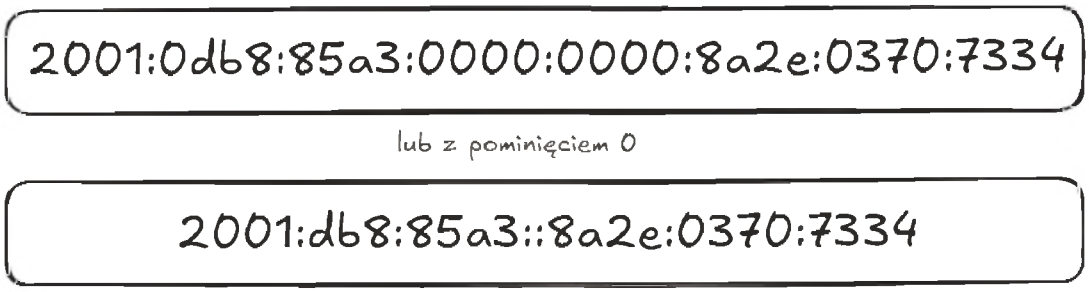
Protokół IPv4 przewiduje adresację 32 bitową, co pozwala na istnienie ok. 4,3 mld unikalnych adresów IP. Tak ograniczona ilość na etapie rozwoju sieci, wymusiła na dostawcach stosowanie translacji (NAT), która pozwala na „wypuszczanie na świat" wielu użytkowników na tym samym adresie IP, segregując ich i pozwalając na ich identyfikację na podstawie przydzielonych im portów źródłowych. Adres IPv4, to cztery liczby w zakresie od 0..255 oddzielone kropkami.



Rysunek 1 – Przykładowy adres IPv4

[1] Jacek Garbaczewski – oficer Policji, biegły sądowy Sądu Okręgowego w Krośnie z zakresu informatyki śledczej.

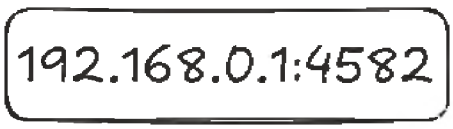
Protokół IPv6 natomiast przewiduje adresację 128 bitową, co zapewnia praktycznie nieograniczoną liczbę unikalnych adresów IP w ilości 340 sekstylionów. Adres IPv6, to 8 grup znaków (liczb szesnastkowych) oddzielonych dwukropkiem.



Rysunek 2 – Przykładowy adres IPv6

2. Problem NAT-a i braków w logach – jak to wygląda w praktyce

Czym jest NAT? Wyobraź sobie blok z dużą ilością mieszkań. Każde mieszkanie to inny użytkownik Internetu (lokator). Na dole siedzi odźwierny, który znając lokatorów i numer ich mieszkania, wypuszcza ich „na świat" bądź wpuszcza ich do wnętrza przez jedną klatkę. Owa klatka, to jeden zewnętrzny adres IPv4. Numer mieszkania, to port źródłowy użytkownika. Przyjmijmy więc, że klatka jest oznaczona adresem IPv4 192.168.0.1, a poszczególne mieszkania to numery portów źródłowych. Portów źródłowych dla usługi NAT jest ponad 60 tysięcy. Właśnie dlatego i z racji oszczędności adresów, powstała taka usługa jak NAT. Dzięki temu działalność w Internecie każdego z lokatorów widoczna jest jednym adresem IP „klatki", działającym na innym porcie.



Rysunek 3 – Przykładowy zapis adresu IPv4 z portem

W przypadku adresów IPv6 problem ograniczenia ilościowego adresacji został rozwiązany. Opierając to na przytoczonej wcześniej metaforze, każdy z lokatorów ma swoje indywidualne i własne wyjście „na świat". Co więcej, wielu operatorów czy dostawców internetowych przydziela nam całe bloki adresowe IPv6 na czas trwania sesji.

Dlaczego więc posiadanie danych tych portów w przypadku adresów IPv4 jest ważne? Właśnie dlatego, aby móc wskazać konkretnego lokatora, który z tych usług

korzystał. Jeśli mamy tylko adres IP – czyli numer klatki – nasz odźwierny nie wskaże konkretnego lokatora. Może co najwyżej udostępnić dane wszystkich mieszkańców i... wrócimy do tego za chwilę.

Do tej pory mówiłem lekko i obrazowo – ale żeby zrozumieć, jak to wszystko działa w realiach sprawy, musimy na chwilę wejść w przepisy i obowiązki podmiotów, od których pozyskujemy dane.

Zazwyczaj zbierając cyfrowy materiał dowodowy w sprawie, zwracamy się do wszelkich podmiotów dostarczających swoje usługi za pośrednictwem sieci Internet o tzw. logi. Mowa tu o bankach, serwisach sprzedażowych, portalach społecznościowych czy ogłoszeniowych, bądź wszelkich innych o które dana sprawa się opiera.

W praktyce – i co ważne – nie ma przepisu, który kazałby tym firmom trzymać logi z pełnymi danymi użytkownika. Często mają tylko to, co przydaje się im samym – a niekoniecznie nam.

W przypadku banków i sektora finansowego istnieją przepisy obligujące je do monitoringu transakcji, rozliczalności operacji, monitoringu bezpieczeństwa czy też zachowania procedur AML zgodnie z ustawą o przeciwdziałaniu prania pieniędzy i finansowania terroryzmu, ustawy o usługach płatniczych czy też rekomendacji Komisji Nadzoru Finansowego. Wytyczne te powodują, że banki czy instytucje finansowe, rejestrują tylko te dane, które pozwolą zabezpieczyć się przed oszustwami i reklamacjami klientów oraz wypełnić rekomendacje organu nadzorczego jakim jest KNF.

Pozostałe podmioty (sklepy internetowe, serwisy sprzedażowe, itp.) przechowują tego typu dane dobrowolnie, choć głównie z przyczyn bezpieczeństwa, wymagań wewnętrznych, reputacyjnych czy też zgodności z RODO.

Należy pamiętać, że jednym z priorytetów podmiotów świadczących usługi drogą elektroniczną są m. in. względy ekonomiczne prowadzonej przez nie działalności. Niewątpliwie na ich stan mogą mieć wpływ koszty ponoszone w związku z przechowywaniem danych przydatnych dla organów ścigania, a niekoniecznie przydatnych dla nich samych. Biorąc jednak pod uwagę zakres udostępnianych przez takie podmioty aktualnie danych w zakresie logowań użytkowników (data, godzina, minuta, sekunda, adres IP, czasami nagłówek przeglądarki), dodatkowe zobowiązanie w postaci przechowywania portów źródłowych zajmujących dla jednego logowania kilka bajtów, zdaje się nie wpływać znacząco na ponoszone w związku z tym koszty. Ponadto wybiórczość i niekonsekwencja podmiotów w tym zakresie, także nie ułatwia pracy organom procesowym.

Zanim jednak zarzucimy coś firmom, warto zobaczyć, co faktycznie nakładają na nie przepisy – bo nie każda firma działa według tych samych zasad, a prawo rozróżnia

choćby przedsiębiorców komunikacji elektronicznej i podmioty świadczące usługi drogą elektroniczną.

Spójrzmy na to okiem przedsiębiorcy komunikacji elektronicznej z którego łącza korzystamy. *Ustawa z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej*[2], w szczególności *Art. 43 ust. 1 pkt 1 lit. a tiret drugie PKE*, zobowiązuje przedsiębiorców do zapewnienia warunków technicznych i organizacyjnych dostępu i utrwalania m.in. danych abonentów związanych z komunikatami elektronicznymi przesyłanymi w ramach świadczonej publicznie dostępnej usługi telekomunikacyjnej. Na moment pisania tej publikacji, nie opublikowano jeszcze aktu wykonawczego (rozporządzenia) do nowej ustawy. Wcześniejsze przepisy – oparte o prawo telekomunikacyjne – wskazywały wprost na konieczność przechowywania także portów sieciowych.

Dobrą wiadomością jest to, że regulacjami wynikającymi z *ustawy z dnia 12 lipca 2024 r. – Prawo komunikacji elektronicznej*, objęto również „komunikację interpersonalną niewykorzystującą numerów". To nowa definicja w polskim prawie, bazująca na Europejskim Kodeksie Łączności Elektronicznej, mówiąca o tzw. usługach over-the-top, w tym komunikatorach internetowych. Ukłony więc wobec WhatsApp, Messenger i innych podlegających lub stosujących się do regulacji unijnych.

3. ISP ≠ dostawca usługi – różne światy, inne przepisy

Na potrzeby niniejszej publikacji, wspomnę tylko kim nazywam ISP, a kim dostawcę usług świadczonych drogą elektroniczną.

ISP (z ang. Internet Service Provider), to nikt inny jak podmiot dający nam dostęp do „świata" za pośrednictwem sieci Internet. To każdy dostawca usług internetowych bez rozróżnienia na wielkich graczy tj. kluczowych operatorów czy drobnych lokalnych dostawców.

Dostawcą usług świadczonych drogą elektroniczną, będą wszelkie podmioty, które świadczą swoje usługi również w Internecie, tj. sklepy internetowe, banki, portale ogłoszeniowe/aukcyjne/ społecznościowe.

ISP w Polsce działają w oparciu o wspomnianą już *ustawę z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej*, natomiast dostawcy usług świadczonych drogą elektroniczną w oparciu o *ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną*[3].

Zapytanie do ISP musi być podparte w postępowaniu karnym postanowieniem prokuratora bądź Sądu. ISP oczekuje od organu procesowego wskazania dokładnego

[2] Portal Gov.pl, online: https://www.gov.pl/attachment/a76fef62-3934-401d-b876-d8d7b5add8c3, dostęp: 27.07.2025.

[3] Internetowy System Aktów Prawnych, online: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20021441204/ U/D20021204Lj.pdf, dostęp: 27.07.2025.

punktu w czasie (data, godzina, minuta, sekunda), adresu IP i zazwyczaj w przypadku adresu IPv4 portu źródłowego użytkownika. Pewnym kluczem jest tutaj trafienie w zakres interpretacyjny operatora przepisów dotyczących zwolnienia z tajemnicy komunikacji elektronicznej. Okazuje się bowiem, że część z nich odpowiada na pytania niestandardowe, a część zasłania się brakiem możliwości udzielenia informacji z uwagi na fakt, że niezbędne w celu wskazania użytkownika końcowego jest wskazanie portu źródłowego przydzielonego mu w danej jednostce czasu.

4. Jak pytać, by dostać odpowiedź?

Pomijając kwestie proceduralne i formalne wynikające z organizacji współpracy z jednostką prokuratury nadzorującą postępowanie, co do zasady głównym przepisem pozwalającym na uzyskanie żądanych od ISP danych jest *art. 386 ust. 1 i 4 ustawy z dnia 12 lipca 2024 r. Prawo Komunikacji Elektronicznej*. W naszym przypadku (czyt. mamy adres IPv4 bez portu źródłowego), niezbędne będzie zwrócenie się do ISP o wskazanie **wszystkich osób – nie tej jedynej**, które w danej jednostce czasu (data, godzina, minuta, sekunda) korzystały ze wskazanego przez nas adresu IP. Warto już tutaj zaznaczyć, że takich użytkowników może być bardzo wielu (patrz pkt 2). W praktyce, w przypadku posiadania kompletu danych (czas, IPv4, port), organy ścigania skupiają się na jednostce czasu zbieżnej z czasem zdarzenia lub kluczowymi czynnościami, które mogłyby wskazywać na sprawcę. W przypadku braku portu, powinno następować odstępstwo od tej reguły, ponieważ im więcej danych zbierzemy, tym mniejsze będzie prawdopodobieństwo uznania dowodów jako poszlaki. Szykuj się więc, na potężną dawkę danych.

5. Korelacja danych – czyli jak z chaosu zrobić wskazanie osoby

Na etapie postępowania przygotowawczego ocierającego się o sieć internetową, istnieją spore możliwości uzyskiwania danych od przedsiębiorców świadczących usługi drogą elektroniczną. Mamy przecież bankowość elektroniczną, pośredników i sprzedawców internetowych, aplikacje związane z kurierami na żądanie, aplikacje lojalnościowe, czy choćby aplikacje mobilne przeznaczone do pośrednictwa w organizowaniu transportu osobowego. To ogrom możliwości ograniczany jedynie inwencją i czasem prowadzącego postępowanie. Często te możliwości są pomijane z powodu wcześniejszych doświadczeń, z których wynika, że dany podmiot zwykle nie rejestruje portów źródłowych. Wtedy też kierunek ten może zostać pominięty, stąd też ta publikacja, która ma dowieść, że czasami jednak warto.

Przyjmijmy, że w danym zdarzeniu możemy pozyskać logi z banku, historia transakcji banku wskazuje np. na Uber i zakupy za pośrednictwem sklepów internetowych. Przyjmijmy również, że żaden z tych podmiotów nie będzie rejestrował

portów źródłowych użytkownika – bo przecież nie musi. Analizując logi przekazane przez te podmioty zauważamy jednak, że adresy IP powielają się w różnych źródłach w danym czasie, albo co najmniej powiela się operator, w którego puli adresowej dany adres IP się znajduje. To może być dla nas pierwsze światełko w tunelu.

W zależności od występujących korelacji w adresach IP pochodzących z logów z różnych źródeł, zwracamy się do ISP o wskazanie danych wszystkich osób, którym we wskazanych jednostkach czasu, przydzielony został dany adres IP. Słowem kluczem jest „korelacja", wobec czego liczba mnoga jednostek czasu jest niezbędna, by korelacja była możliwa bądź z punktu widzenia postępowania efektywna.

6. Narzędzia – prosto, tanio i skutecznie

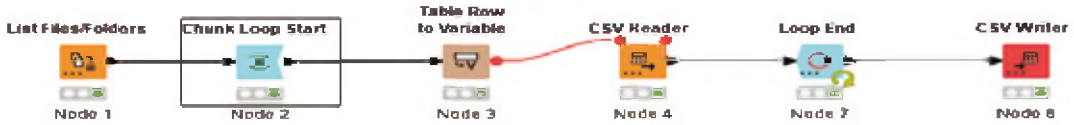
Przyjmijmy, że po wytężonej pracy z punktu 5, mamy 40 jednostek czasu z różnymi adresami IP od tego samego ISP. ISP, dzięki swojej uprzejmości wskazuje nam, że tylko w jednej jednostce czasu, ze wskazanego adresu IP, korzystało ok. 1000 użytkowników. Pomijając duplikaty, których właśnie szukamy, to ok. 40 tys. osób dla wszystkich uzyskanych odpowiedzi.

Jak ogarnąć taką ilość danych? Z pomocą przychodzi wiele narzędzi do analizy danych, które potrafią proces ten zautomatyzować czy też usprawnić. Już sam arkusz kalkulacyjny daje nam spore możliwości wykazania powiązań, w przypadku Microsoft Excel narzędzia Power Query czy same Power BI, będą nam jednak bardzo przydatne. Dla osób „umiejących w komputery" z pomocą przychodzą proste skrypty Python z pakietem Pandas, które w mgnieniu oka są w stanie wyłuskać interesujące nas powiązania.

Nie sposób pominąć obowiązujących obostrzeń w zakresie bezpieczeństwa teleinformatycznego, które stanowią istotne wyzwanie dla prowadzących postępowania. Tutaj z pomocą przychodzi darmowe narzędzie działające również w wersji bez instalacji, tj. KNIME.

KNIME jest darmowym i otwartym narzędziem do analizy danych, integracji danych i automatyzacji procesów przetwarzania informacji. Z racji tego, że KNIME (czyt. najm) powstał na Uniwersytecie w Konstancji w Niemczech, nazwa jego to skrót od Konstanz Information Miner.

To oprogramowanie posiadające ogromne możliwości i warto się nim zainteresować chcąc rozwijać się w kierunku analitycznym. Z opisywanymi w niniejszej publikacji danymi, radzi sobie wyśmienicie przy niewielkim nakładzie pracy użytkownika. W sieci Internet jest mnóstwo publikacji, w których podejrzeć można w jaki sposób skonfigurować swój „workflow" aby wykonywał on oczekiwane zadania.



Rysunek 4 – Przykładowy "workflow" aplikacji KNIME

Czym jest ten „workflow"? To nic innego jak określony poszczególnymi węzłami „nodami" schemat działań (przebieg), przetwarzający wskazane mu dane. Celem użytkownika jest takie ułożenie tych klocków (nodów), aby każdy kolejny krok przebiegu oznaczony był kolorem zielonym. Najprościej będzie wskazać taką przykładową konfigurację w oparciu o rzeczywisty case.

7. Przykład sprawy – jak to wygląda w realu

Jedna z jednostek prokuratury prowadziła postępowanie w sprawie o przestępstwo z art. 202 § 3 k.k. Zawiadomienie złożył pracownik Miejskiego Ośrodka Pomocy Społecznej, sprawujący opiekę nad rodziną. Wynikało z niego, że kobieta (dla celów publikacji nazwijmy ją Janina Kowalska) otrzymała za pośrednictwem komunikatora Messenger wiadomość od osoby przedstawiającej się jako Martyna Kanik. Nadawczyni twierdziła, że jest studentką pielęgniarstwa odbywającą praktyki w szkole podstawowej, do której uczęszczają dzieci Pani Kowalskiej. W ramach prowadzonej korespondencji, poprosiła o przesłanie zdjęć różnych części ciała dziewczynek, powołując się na konieczność przeprowadzenia bilansu zdrowotnego. Zapis rozmowy z komunikatora Messenger został zabezpieczony w formie screenshotów, a rozmowa w wersji cyfrowej z komunikatora usunięta przez pokrzywdzoną. W toku postępowania udało się ustalić jedynie identyfikator Facebook ID, wskazujący na profil Martyny Kanik na tym portalu: 1000869XXXXXXXX, który umożliwił jednak na pozyskanie danych od administratora portalu Facebook, tj. Meta Platforms.

Zakres przekazanych przez Meta logowań do profilu obejmował okres od 16 września 2023 r. od godziny 22:23:39 UTC do 20 września 2023 r. do godziny 16:15:21 UTC. Zestawienie zawierało łącznie 60 punktów w czasie, zawierających 48 adresów IP będących w puli adresowej operatora sieci PLAY i 12 adresów IP innego dostawcy, który jak ustalono z uwagi na konfigurację systemów retencyjnych, nie był w stanie wyodrębnić użytkowników bez wskazania adresu IP docelowego z jakim użytkownik łączył się. Wszystkie logi przekazane przez Meta, nie zawierały portów źródłowych użytkownika.

To właśnie w takim momencie często pojawia się zwątpienie... Czy jest sens pytać, skoro nic to nie da? W dalszej części przekonasz się, że owszem.

Z zestawienia wyodrębniono 48 logowań pochodzących od operatora sieci PLAY. Przyjrzyjmy się krótko statystykom. Operator sieci PLAY w swojej odpowiedzi przekazał zestawienie łącznie **59153** sesji transmisji danych odpowiadającym zadanym kryteriom oraz przypisanym numerem telefonu, co daje średnio **1232** sesji dla każdej z 48 odpytanych jednostek czasu. Wszystkie sesje przydzielone zostały łącznie **6245 indywidualnym numerom telefonów**. Jak widać jest tego sporo. Pomijając jedno zapytanie z błędnym adresem IP z trzech jednostek czasu, pozostało 45 skutecznych, poprawnych i przydatnych dla postępowania odpowiedzi.

Jaki był tego wynik? Tylko jeden z numerów telefonów powtórzył się w **44 na 45** zapytań. To też przyczyniło się do ustalenia użytkownika końcowego, który jak się okazało zajmował się tego typu działalnością w przeszłości. W tym przypadku dane te uzasadniły dostatecznie podejrzenie, że czyn ten popełniła ustalona osoba – czyt. była podstawa do wydania postanowienia o przedstawieniu zarzutów.

Ale... dlaczego w 44 na 45 przypadkach ten jedyny numer telefonu się pojawił? A gdzie podział się ten jeden? Taka sytuacja może się pojawić i pewnie zdarzyło Ci się z nią spotkać. Pytamy operatora z dokładnością do jednej sekundy. To w cyfrowym świecie może okazać się całkiem sporo i nie jest powiedziane, że to co odnotował w swoich logach dostawca usług świadczonych drogą elektroniczną, będzie zbieżne w czasie z tym co odnotował ISP.

Przejdź dalej, aby sprawdzić jak to zrobić w KNIME.

8. KNIME w praktyce – jak zbudować skuteczny workflow

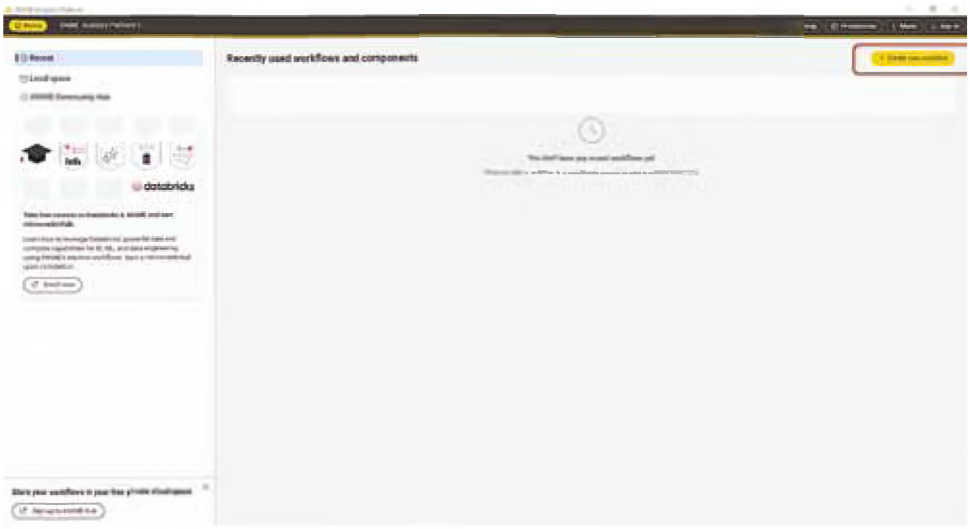
Na dzień pisania tej publikacji używam aktualnej wersji oprogramowania KNIME – 5.5.0.

Standardowym i pierwszym krokiem w pracy z KNIME jest wskazanie lokalizacji, w której program będzie przechowywał pliki związane z naszym projektem.W jednej lokalizacji (tzw. workspace) możemy tworzyć wiele przebiegów (workflow), które wykorzystujemy w danej sprawie.

Głównym celem tej publikacji nie jest stworzenie pełnej instrukcji obsługi KNIME – byłoby to niemożliwe w tak krótkiej formie. Chodzi raczej o to, by pokazać praktyczne zastosowanie tego narzędzia w konkretnym scenariuszu analizy danych.

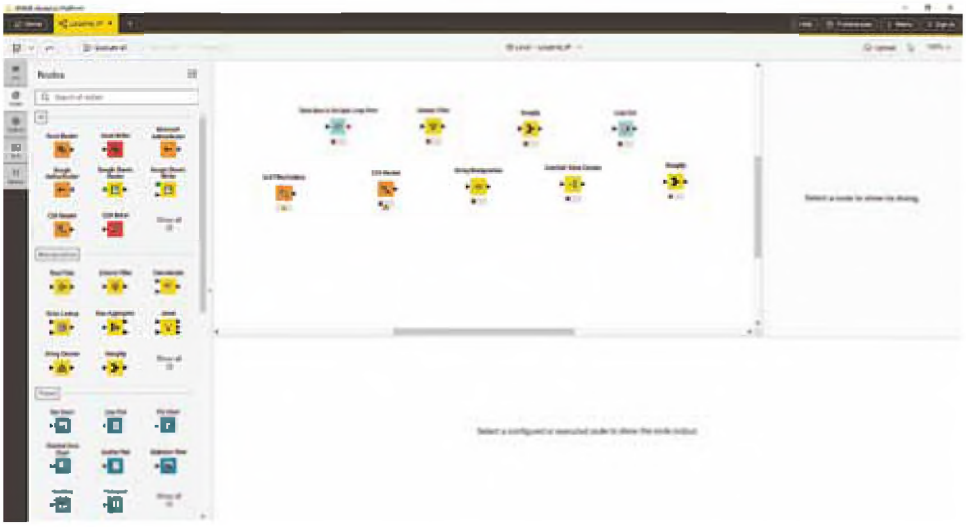
Mam nadzieję, że przykład ten zainspiruje Cię do sięgnięcia po KNIME także w innych typach spraw.

Utwórzmy więc nowy przebieg (workflow) o nazwie roboczej Liczenie_IP.



Rysunek 5 – Okno główne KNIME

Po lewej stronie okna głównego, znajduje się sekcja Nodów – klocków, z których układamy nasz przebieg.



Rysunek 6 – Okno workflow z wykorzystywanymi nodami

Umieszczanie nodów w workflow, to nic innego jak przeciąganie ich ze zbioru do okna głównego aplikacji, a następnie odpowiednie łączenie ich ze sobą.



Rysunek 7 – Połączenie nodów w workflow

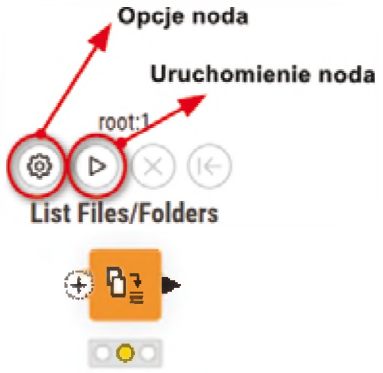
Przedstawione powyżej nody celowo zostały rozłożone w ten sposób, aby jasno było widać, co dzieje się po kolei. W czerwonej ramce oznaczone zostały nody pracujące w pętli rozpoczętej przez Loop Start i kończącej Loop End. Ta część odpowiada za to, w jaki sposób przetwarzany jest każdy z plików w tym przykładzie operatora sieci PLAY.

Za dane wejściowe, posłużyło 48 plików CSV przekazanych przez operatora, zawierających wynik zapytania po podaniu adresu IP (bez portu) w danej jednostce czasu.

DATA_I_GODZ_POLACZ	CZAS_TRWANIA	RODZAJ_USLUGI	UI_MSISDN	UI_IMEI	UI_IMSI	UI_LAC	UI_CID
2023-09-17 00:00:00	36109	połączenie z internetem	488 2	3 3	26 4	5	1
2023-09-17 00:00:00	37716	połączenie z internetem	485 4	3 0	26 9	4	12
2023-09-17 00:00:00	39224	połączenie z internetem	486 7	3 5	26 9	4	12
2023-09-17 00:00:00	41485	połączenie z internetem	487 2	3 1	26 0	2	13
2023-09-17 00:00:00	41660	połączenie z internetem	485 3	8 8	26 7	4	
2023-09-17 00:00:00	43497	połączenie z internetem	488 0	3 8	26 1	4	12
2023-09-17 00:00:00	45381	połączenie z internetem	487 6	3 7	26 1	9	10
2023-09-17 00:00:00	46667	połączenie z internetem	487 6	3 5	26 3	4	
2023-09-17 00:00:00	47635	połączenie z internetem	487 8	3 0	26 5	1	13
2023-09-17 00:00:00	47661	połączenie z internetem	485 7	8 2	26 3	1	10
2023-09-17 00:00:00	47808	połączenie z internetem	486 5	8 0	26 2	1	10
2023-09-17 00:00:00	48242	połączenie z internetem	486 9	8 3	26 4	6	13

Rysunek 8 – Fragment danych wejściowych – wykaz połączeń operatora sieci PLAY

Każdy z nodów, po najechaniu na niego myszą ma możliwość jego niezależnego od reszty przebiegów uruchomienia, bądź w przypadku posiadania takiej funkcjonalności, zmiany jego opcji. Możliwość niezależnego uruchomienia jest szczególnie przydatna do testowania sposobu jego działania, jak i weryfikowania poprawności wyników.

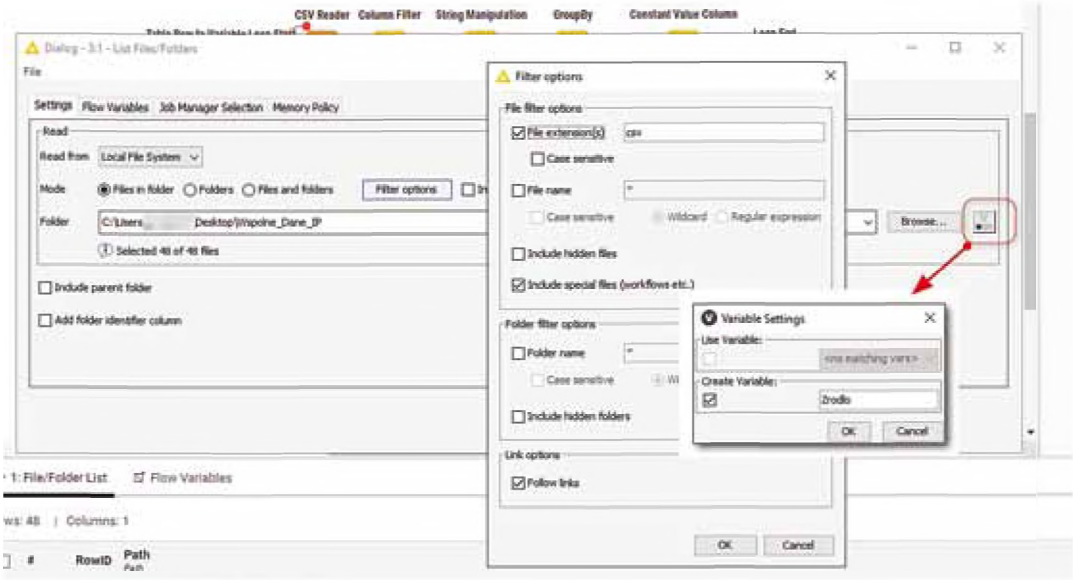


Rysunek 9 – Opcje przykładowego noda

W dolnej części noda, widoczne są zmiany statusu poszczególnych „klocków", które wskazują na poprawną pracę, bądź ewentualne błędy w danych wejściowych bądź konfiguracji. Poszczególne klocki łączymy przeciągając z wyjścia do wejścia kolejnego linię połączenia myszą.

Przyjrzyjmy się teraz poszczególnym nodom i funkcjom jakie one pełnią w tym przykładzie.

List Files/Folders – w naszym przypadku wskazuje folder w którym znajdują się pliki poddawane analizie (48 plików). Oczywiście mamy ponadto możliwość wskazania tylko jednego pliku, lub zestawu folderów i plików. Tutaj warto skorzystać z opcji „Filter options", aby zapobiec poddawaniu analizie innych plików ewentualnie znajdujących się w wybranym folderze.

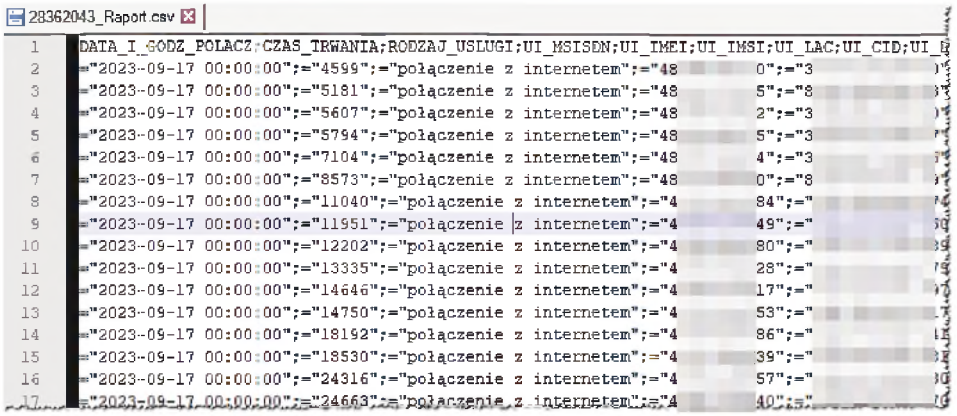


Rysunek 10 – Wybór opcji dla noda List Files/Folders

Teraz bardzo istotna rzecz w powodzeniu dalszych działań. Działanie noda List Files/ Folders to również utworzenie tabeli, gdzie każdy wiersz to nazwa pliku znajdującego się we wskazanym folderze. Lista ta będzie potrzebna do dalszego ich przetwarzania we wspomnianej wcześniej pętli. Aby kolejne klocki wiedziały, jaki następny plik wziąć na warsztat, musimy je o tym poinformować. Stąd też nazwę pliku przekazujemy jako zdefiniowaną zmienną o nazwie „Zrodlo".

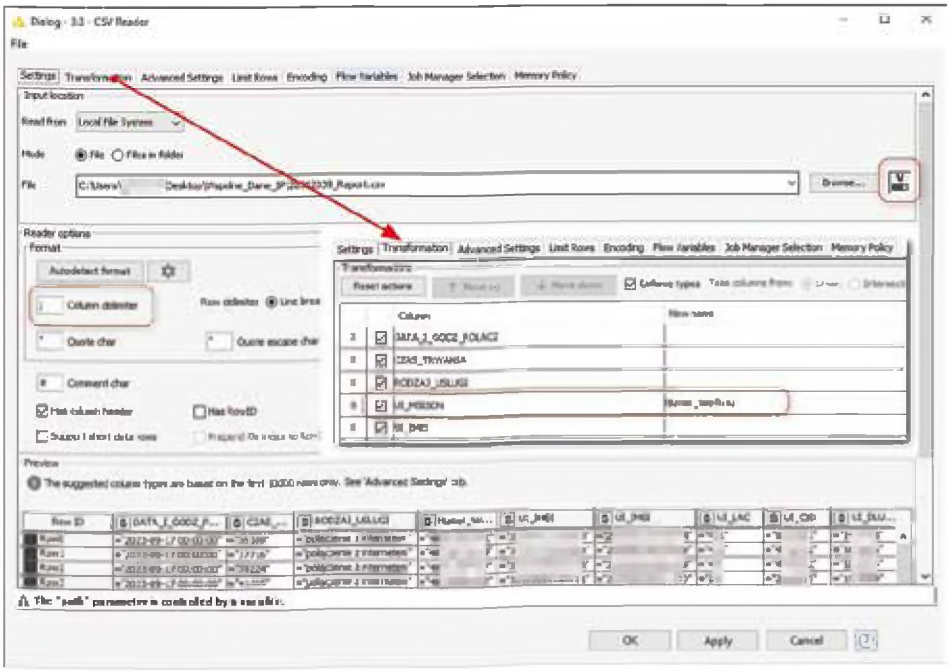
Table Row to Variable Loop Start – nod ten otrzymuje w zmiennej „Zrodlo" nazwę pliku i rozpoczyna przebieg jednej pętli dla jednej otrzymanej zmiennej. W jego przypadku modyfikacja żadnych opcji nie jest potrzebna.

CSV Reader – to nod, który po prostu odczytuje wskazany w zmiennej „Zrodlo" plik CSV. Oczywiście w przypadku innych operatorów udostępniających dane w formie arkuszy kalkulacyjnych, istnieje możliwość uruchomienia innych czytników w tym „XLS Reader". Tutaj możemy zatrzymać się na chwilę i przyjrzeć się opcjom tego pierwszego, ponieważ w zależności od otrzymanego do analizy pliku może wystąpić potrzeba ich dostosowania, szczególnie w zakresie znaku oddzielającego poszczególne wartości. Otwierając plik CSV otrzymany od operatora sieci PLAY jako plik tekstowy widzimy, że poszczególne wartości rozdzielone są znakiem średnika **;**.



Rysunek 11 – Fragment pliku CSV otwartego w Notepad++

Ten znak musimy więc wskazać jako znak oddzielający w KNIME. Przy nazwie pliku należy wcisnąć opcję „Flow variable", czyli w wolnym tłumaczeniu „nazwę pliku pobierz sobie ze zmiennej Zrodlo". Dla ułatwienia późniejszej analizy, można również zmienić nazwę kolumny tabeli, która będzie dla nas kluczowa z „UI_ MSISDN" na „Numer_telefonu". Nie jest to niezbędne, jednak w gąszczu znaków i ew. szukaniu przyczyn niepoprawnego działania przebiegu, potrafi skutecznie ułatwić poszukiwania.



Rysunek 12 – Konfiguracja noda CSV Reader

Column Filter – na obecnym etapie analizy skupiamy się na kluczowej dla nas wartości czyli numerze telefonu, któremu przydzielony był nasz adres IP. Pozostałe dane możemy więc odrzucić, ponieważ nie są nam potrzebne. Column Filter spowoduje, że nasza tabela wyjściowa zawierać będzie tylko numery telefonu bez pozostałych danych udostępnionych przez operatora. Konfiguracja noda Column Filter, możliwa jest z okna w KNIME, które widoczne jest po jego wybraniu w oknie przebiegu.



Rysunek 13 – Konfiguracja noda Column Filter

W Column Filter wskazujemy aby nasza tabela zawierała (include) tylko kolumnę z numerem telefonu, czyli tak naprawdę „UI_MSISDN" po zmienionej w CSV Reader nazwie na „Numer_telefonu". Po próbnym uruchomieniu przebiegu przyciskiem (Execute all), w dolnej części KNIME widzimy aktualny stan wyniku przetwarzania czyli kolumnę „Numer_telefonu".



Rysunek 14 – Wynik przetwarzania po Column Filter

Jak widać wynik działania dotychczasowego przebiegu na etapie jego tworzenia nie jest spektakularny. Pamiętaj, że finalnie nie będzie istotne ile plików wejściowych

wstawisz do przetwarzania, KNIME zrobi to za Ciebie, zgodnie z utworzonym przebiegiem.

W wyniku widzimy jednak znaki, które mogą przeszkodzić nam w późniejszych poszukiwaniach tego jedynego numeru telefonu, który powtórzy się w 44/45 przypadków. W późniejszym etapie przebiegu KNIME, będzie musiał pozbyć się występujących duplikatów numerów telefonów przy zliczaniu ich ilości. Nie chodzi w końcu o to ile razy dany numer telefonu wystąpił łącznie w każdym ze wskazanych plików odpowiedzi operatora, tylko który z nich wystąpił w każdym z tych plików.

Na marginesie warto w tym miejscu wyjaśnić skąd w jednym pliku odpowiedzi operatora, może się pojawić kilkukrotnie ten sam numer telefonu? Przecież jeden plik z odpowiedzi operatora to dany adres IP w czasie jednej sekundy! Otóż operator rezerwuje aktywne sesje dla danego użytkownika na określony czas i w określonym zakresie portów. Dlatego odpytana jednostka czasu może wskazywać na kilkukrotne wystąpienie odbiorcy usługi.

DATA_I_GODZ_POLACZ	CZAS_TRWANIA	RODZAJ_USLUGI	UI_MSISDN	INTERNET_IP_PORT
2023-09-17 00:00:00	60389	połączenie z internetem	488 88	5.173.176.20 (25120:25151) 2023-09-16 22:44:21
2023-09-17 00:00:00	35250	połączenie z internetem	488 88	5.173.176.20 (18336:18367) 2023-09-16 22:44:21

Rysunek 15 – Fragment odpowiedzi operatora sieci PLAY

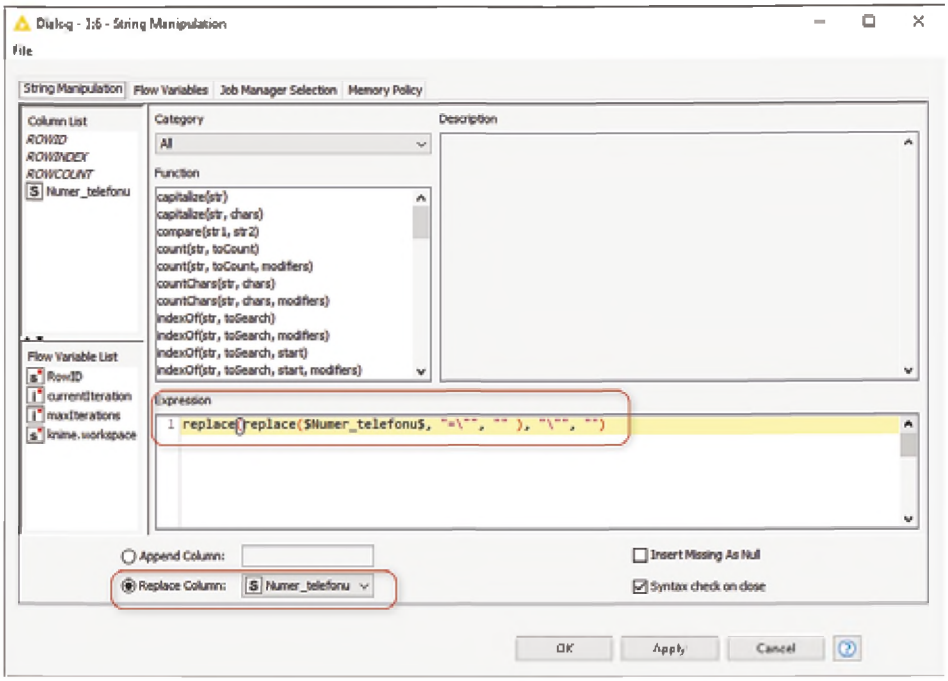
Fragment powyższej odpowiedzi wskazuje jak widać, że od godziny 00:00:00 w dniu 17 września 2023 r. wskazany numer telefonu miał przydzielone dwie sesje w czasie trwania określonym w sekundach, czyli w pierwszym wierszu do godziny 16:46:28, a w drugim do 09:47:30. Warto zaznaczyć, że odpowiedź ta była wynikiem zapytania o wszystkich użytkowników (numerów telefonów), którzy w dniu 17 września 2023 r. o godzinie 09:44:47 przydzielony mieli adres IP 5.173.176.20. Oba wiersze wskazane powyżej zawierają odpytaną jednostkę czasu w swoim zakresie. Łącznie jest to 1367 rekordów.

Wróćmy do KNIME. Aby potrafił on odróżnić numery telefonów musimy pozbyć się znaków specjalnych zawartych w kolumnie „Numer_telefonu". Osiągnąć ten cel można w wieloraki sposób, jednak z uwagi na to, że tekst ten jest przeznaczony dla osób mniej technicznych, wybrałem opcję najprostszą.

String Manipulation – bo o tym nodzie mowa, przeszukuje podaną na wejściu tabelę i zamienia napotkane w wierszach znaki „=" „ i „ " " na pusty znak. W tym celu musimy skonfigurować nod wpisując funkcję, która wykona za nas tą pracę, tj.:

```
replace(replace($Numer_telefonu$, „=\"", „" ), „\"", „")
```

Funkcja ta wskazuje, w przypadku gdy „Numer_telefonu" zawiera znak „ = " zamień go na znak pusty „" a gdy napotkasz „ " ", również zamień go na znak pusty. To najtrudniejszy etap konfiguracji naszego workflow.



Rysunek 16 – Konfiguracja noda String Manipulation

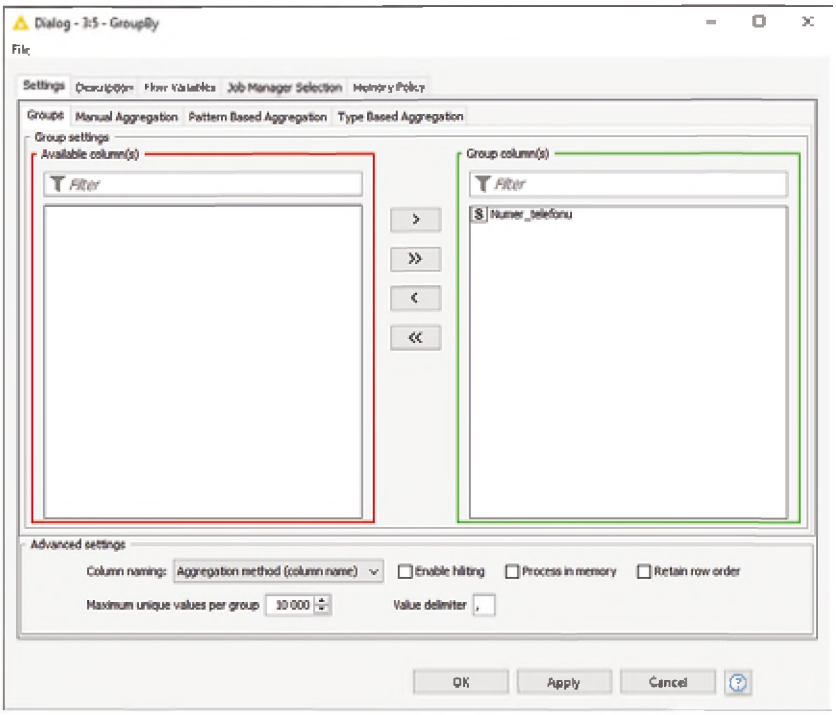
Warto również zaznaczyć, że przetworzony tekst powinien zostać zapisany w tej samej kolumnie, czyli zamienić napotkaną wartość (replace), bez utworzenia nowej kolumny.



Rysunek 17 – Wynik działania noda String Manipulation

Teraz pozbądźmy się kilkukrotnych wystąpień numeru telefonu w jednej jednostce czasu, czyli w pojedynczym przetwarzanym na chwilę obecną pliku stanowiącym odpowiedź operatora.

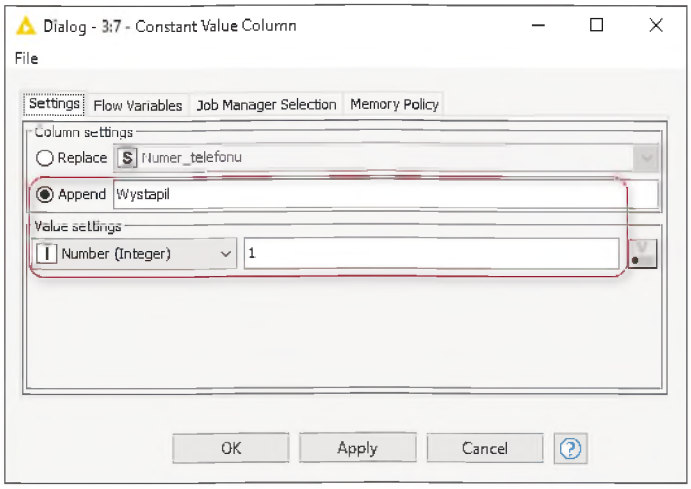
GroupBy – nod, który wyeliminuje duplikaty numerów telefonów występujące w każdym z pojedynczo przetwarzanych plików.



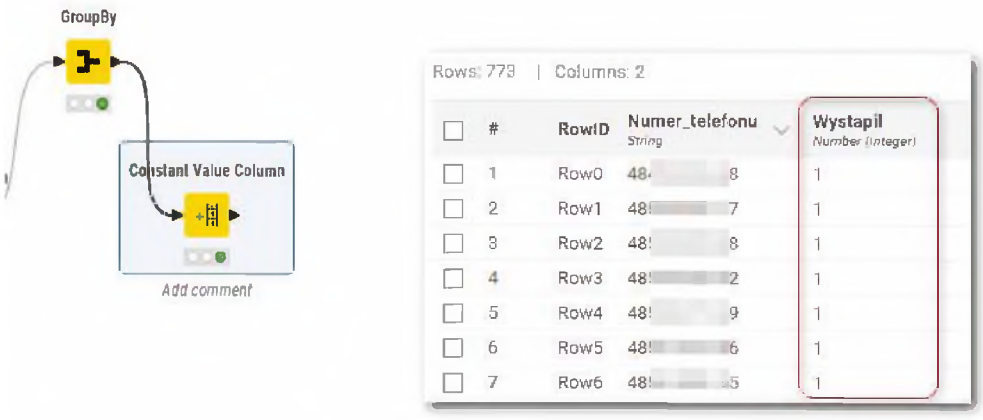
Rysunek 18 – Konfiguracja noda GroupBy

Konfiguracja tego noda jest prosta. Jako że otrzymuje on na wejściu tabelę z tylko jedną kolumną „Numer_telefonu", to jej nazwę przenosimy z pola czerwonego do pola zielonego. W wyniku działania GroupBy nasza lista skurczyła się już z 1367 na 773 indywidualnych numerów telefonów. Naszym celem jest jednak policzenie w ilu podstawionych do analizy plikach, dany numer telefonu się pojawił. Musimy gdzieś więc notować aktualny stan. Na obecnym etapie wiemy już że 773 numery telefonów wystąpiły w pierwszym analizowanym pliku. Musimy więc wstawić nod, który odnotuje wartość „1" dla każdego z 773 numerów telefonów.

Constant Value Column – utworzy nową kolumnę (append), gdzie każdemu z wystąpień indywidualnych numerów telefonów przypisze wartość 1.



Rysunek 19 – Konfiguracja noda Constant Value Column



Rysunek 20 – Wynik działania noda Constant Value Column

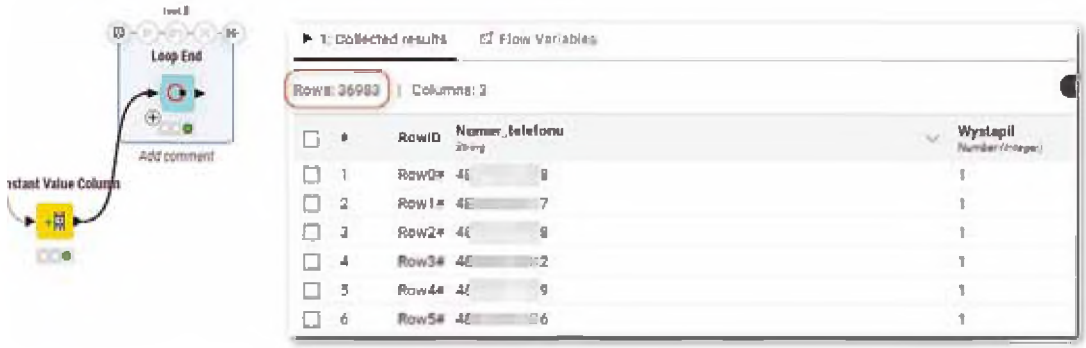
Ten etap kończy przetwarzanie jednego z podstawionych plików w pierwszym kroku pętli. Dlatego też w tym miejscu wstawiamy nod **Loop End**, który jej działanie zakończy i przejdzie do Table Row to Variable Loop Start, aby przetwarzać kolejny z plików.

Ok, ale co z naszym liczeniem wystąpień numerów telefonów? Constant Value Column po raz kolejny przypisze wartość 1 kolejnym indywidualnym numerom telefonów występujących w kolejnym przetwarzanym pliku. Musimy więc te wartości odkładać i sumować poza przebiegiem samej pętli.

Ponownie użyjemy noda **GroupBy** z trochę bardziej skomplikowaną konfiguracją. Ostatni nod GroupBy otrzymuje od poprzedzającego go Loop End tabelę wszystkich wystąpień indywidualnych numerów telefonu we wszystkich przebiegach pętli z kolumną „Wystapil" i o wartości „1" dla każdego wiersza i kolumną „Iteration", zapisującą krok przebiegu pętli, która dla nas jest pomijalna.

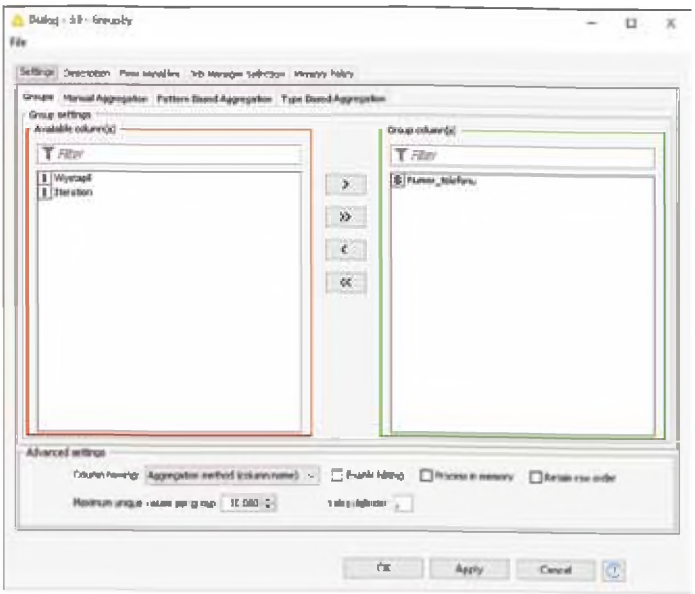
Postaram się to zobrazować. Jeśli w pierwszym przetwarzanym w pętli pliku – odpowiedzi operatora, dotyczącej jednej jednostki czasu i adresu IP, pojawi się trzykrotnie numer telefonu 500100200, to w wyniku działania pierwszego noda GroupBy i Constant Value Column przypisana mu zostanie wartość „Wystapil" = 1 i taka też odłoży się w wyniku noda kończącego pętlę Loop End. Jeśli w kolejnym przetwarzanym pliku ponownie wystąpi numer telefonu 500100200 przyjmijmy dwukrotnie, to również w wyniku działania pierwszego noda GroupBy i Constant Value Column przypisana mu zostanie wartość „Wystapil" = 1. W wyniku końcowym noda Loop By, znajdą się dwa wiersze z numerem telefonu 500100200 i oba z wartością „Wystapil" = 1.

Te duplikaty również należy wyeliminować, ale przede wszystkim zsumować kolumnę „Wystapil" z każdego przebiegu pętli dla indywidualnego numeru telefony, aby osiągnąć oczekiwany wynik. Na tym etapie, po przetworzeniu 48 przetwarzanych plików CSV, mamy 36983 wystąpień numerów telefonów w tym ich duplikatów.



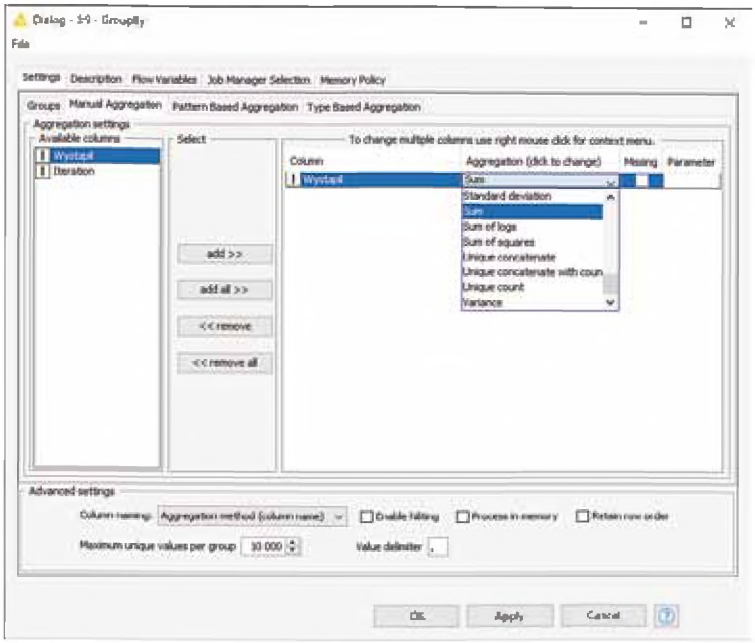
Rysunek 21 – Wynik przetwarzania 48 plików CSV

Ostatni nod **Group By** ma za zadanie wyeliminować duplikaty i zsumować wszystkie „jedynki" z kolumny „Wystapil" przypisane dla indywidualnych numerów telefonów. Przyjrzyjmy się jego konfiguracji. W sekcji Groups ponownie przesuwamy na pole zielone kolumnę „Numer_telefonu", bo to on będzie dla nas wartością indywidualna. Na polu czerwonym pozostawiamy nadal kolumny dodane w przebiegu, tj. „Wystapil" i „Iteration".



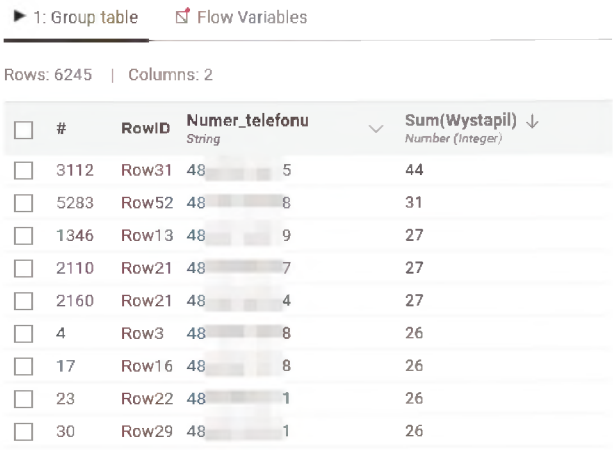
Rysunek 22 – Konfiguracja ostatniego noda GroupBy

Duplikaty mamy już wyeliminowane. Teraz pora zsumować wartości kolumny „Wystapil" w zakładce Manual Aggregation.



Rysunek 23 – Konfiguracja zliczania wystąpień w GroupBy

W tym celu przenosimy nazwę kolumny „Wystapil" i z listy rozwijanej wybieramy wartość Sum, aby finalnie tabela końcowa posiadała tylko wiersze z indywidualnymi numerami telefonów ze wszystkich przetwarzanych plików z wartością w kolumnie „Wystapil" będącą sumą przetwarzanych plików, w których numer ten wystąpił.



Rysunek 24 – Wynik końcowy działania przebiegu KNIME

Po ustawieniu sortowania od największej wartości kolumny „Wystapil" widać, że tylko jeden z numerów wystąpił w 44 z 45 odpytanych przypadkach.

Czy przy każdej tego typu sprawie, poświecenie takiej ilości czasu na konfigurację jest potrzebne? Oczywiście, że nie. Zapisanie takiego przebiegu z powodzeniem może posłużyć Ci przy wszystkich case'ach, gdzie będziesz miał zestawienia od operatora sieci PLAY. Przy drobnych modyfikacjach, dostosujesz również szablon do innych danych wejściowych.

9. To wciąż poszlaki – logi IP jako dowód pośredni

Pamiętaj, że uzyskane jak w powyższym przykładzie dane to dla Ciebie trop. To tylko poszlaka, ale w myśl zasady, że poszlaki się sumują, ważne jest aby poszukać przynamniej jednego dowodu z drugiej strony. Powyższe ustalenia nie znaczą przecież, że użytkownik na którego zarejestrowany został uzyskany w wyniku analizy numer telefonu, był tym, który faktycznie korzystał z komunikatora Messenger w opisywanej sprawie.

Dowód pośredni (inaczej poszlakowy) to taki, który nie wskazuje bezpośrednio na sprawcę, lecz pozwala wnioskować o nim na podstawie faktów ubocznych, które z dużym prawdopodobieństwem prowadzą do określonego wniosku.

W przeciwieństwie do dowodu bezpośredniego, poszlaki wymagają korelacji i dodatkowego wsparcia, aby zbudować pełen obraz sytuacji.

Adres IP, port źródłowy i czas logowania czy informacja odnotowująca u operatora fakt przeprowadzenia rozmowy głosowej, to tylko informacje techniczne oznaczająca, że dany ruch w komunikacji elektronicznej miał miejsce. IP to nie człowiek, to tylko identyfikator użyty przez urządzenie, do którego ktoś miał dostęp[4].

Wszelkie użyte narzędzia do tego typu ustaleń, to suche działanie na zebranych danych. Pamiętaj, analiza danych to tylko jeden z elementów układanki. Korelacja logów może być silną poszlaką, ale ostateczne przypisanie sprawstwa wymaga wsparcia z innych źródeł – technicznych (jak metadane z urządzeń), dowodowych (np. zeznania świadków), bądź fizycznych (np. zabezpieczenie sprzętu). Traktuj więc takie ustalenia jako narzędzie wspierające – nie cel sam w sobie.

Powodzenia.

[4] Piotr Słowiński, *Internet rzeczy. Kryminalistyczna analiza aspektów dowodowych oraz studia przypadków*, Polskie Towarzystwo Kryminalistyczne, online: https://kryminalistyka.pl/wp-content/uploads/2021/02/Internet_Rzeczy_do-druku.pdf, dostęp: 27.07.2025.

Artur Kubiak[1]

Kryptowaluty a ich wykorzystanie w procederze oszustw inwestycyjnych

Streszczenie

W ostatnim czasie obserwujemy rosnące zainteresowanie kryptowalutami, które traktowane są nie tylko jako alternatywa inwestycyjna umożliwiająca dywersyfikację aktywów, lecz także jako nowatorskie rozwiązanie technologiczne, wyraźnie odbiegające od klasycznych rynku kapitałowego. Popularność walut wirtualnych z zasady przyjaznych inwestorom przyciąga jednak nie tylko ich uwagę, ale również cyberprzestępców, dostrzegających w nich nowe możliwości działania. Nie bez znaczenia jest tu teoria o anonimowości transakcji kryptowalutowych. Zaangażowanie cyberprzestępców w kryptowaluty jest elementem złożonych operacji finansowych mających cechy prania pieniędzy. Wraz z rozwojem rynku kryptowalut globalnym problemem stały się oszustwa inwestycyjne, coraz częściej przybierające złożone i trudne do wykrycia formy, które prowadzą do poważnych strat finansowych wśród użytkowników. Niniejsze opracowanie ma na celu zarówno przybliżenie zjawiska oszustw inwestycyjnych gdzie kryptowaluty wykorzystywane są jako nośnik wartości, jak i przedstawienie praktycznych sposobów ochrony przed tego rodzaju zagrożeniami. Zawarte w artykule przykłady pełnią funkcję edukacyjną i prewencyjną, mając na celu zwiększenie świadomości na temat ryzyka i poprawę bezpieczeństwa finansowego uczestników rynku. Autor artykułu do niedawna pracował w Dziale Bezpieczeństwa jednej z giełd kryptowalutowych i aktywnie uczestniczył w procesie przeciwdziałania cyberprzestępczości w tym oszustw inwestycyjnych.

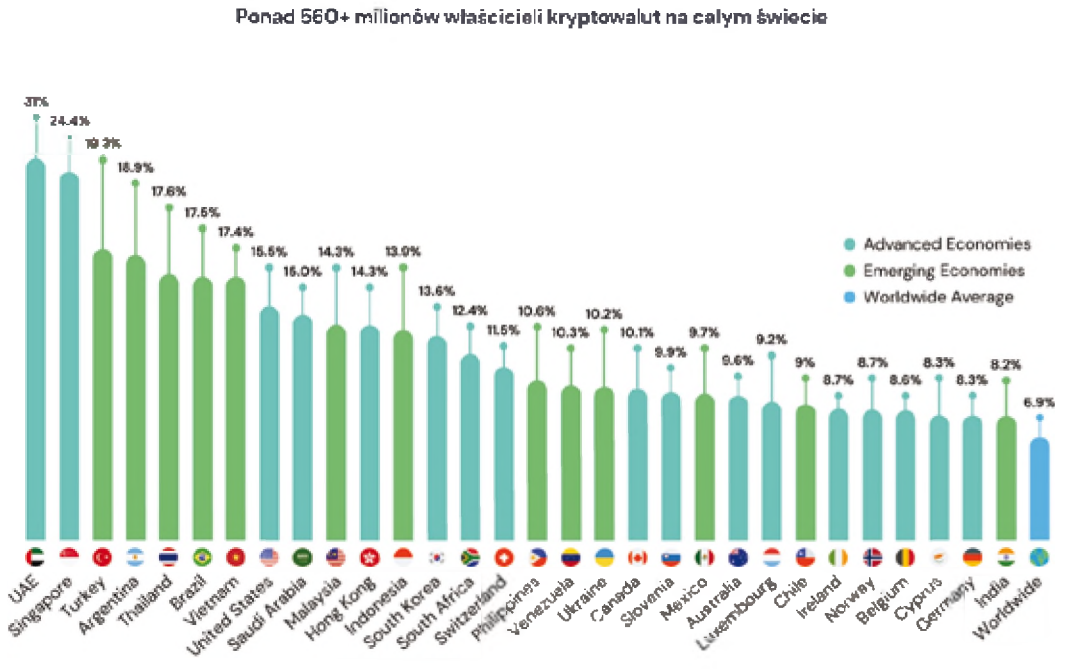
Słowa kluczowe: cyberprzestępczość, oszustwo inwestycyjne, socjotechnika, kryptowaluty, platformy inwestycyjne

Wprowadzenie

Rozwój nowoczesnych technologii cyfrowych nieodwracalnie zmienił krajobraz globalnych rynków finansowych. Jednym z najbardziej przełomowych zjawisk ostatnich lat stało się upowszechnienie kryptowalut – zdecentralizowanych aktywów cyfrowych opartych na technologii blockchain. Początkowo traktowane jako eksperyment technologiczny lub niszowa alternatywa dla tradycyjnych instrumentów finansowych, z czasem kryptowaluty zyskały ogromną popularność wśród inwestorów

[1] Artur Kubiak – emerytowany oficer Policji, b. naczelnik Wydziału dw z Cyberprzestępczością KWP w Katowicach, b. Dyrektor Działu Bezpieczeństwa Zondacypto. Kontakt z Autorem: artur.kubiak.kontakt@gmail.com.

indywidualnych i instytucjonalnych na całym świecie. Ich atrakcyjność wynika m.in. z potencjału wysokiego zysku, braku pośredników, globalnego zasięgu oraz idei wolności finansowej, jaką promują ich twórcy i zwolennicy.



1. Procentowe rozłożenie posiadaczy kryptowalut na świecie – źródło https://www.triple-a.io/cryptocurrency-ownership-data (dostęp 14.06.2025)

Według danych zawartych w raporcie Triple-A jest ponad 560 milionów posiadaczy kryptowalut. Wynika z tego ze 6,8 procent światowej populacji posiada i korzysta z walut cyfrowych. Szacunkowo w Europie ok. 49 milionów mieszkańców posiada kryptowaluty. W Polsce posiadaniem kryptowalut może pochwalić się ok. 2,5 mln. osób.[2]

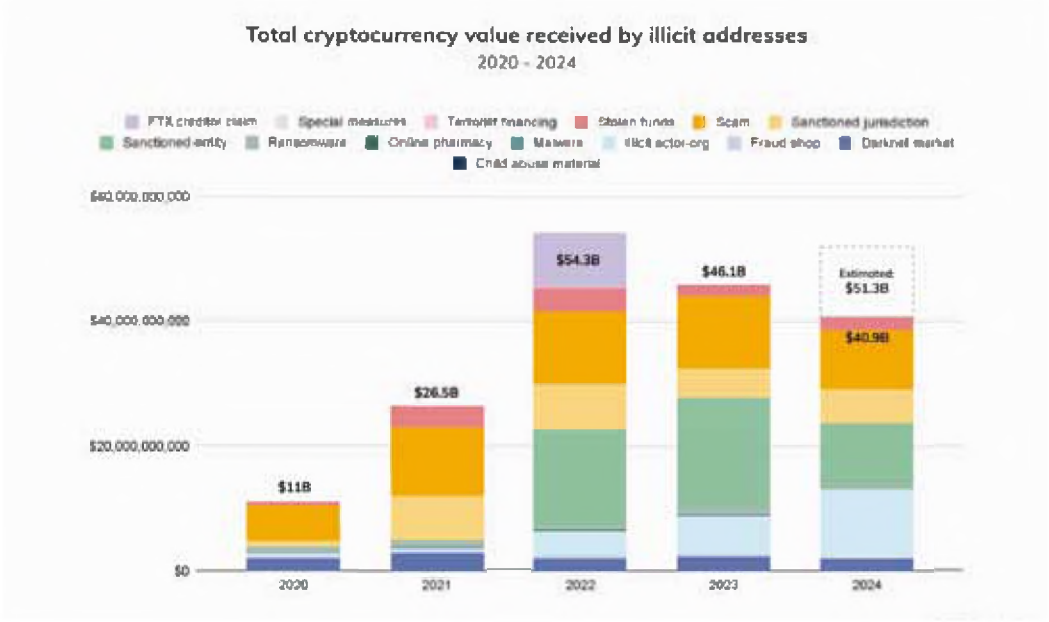
Podobne dane prezentują badania przeprowadzone przez giełdę kryptowalutową crypto.com gdzie ilość użytkowników kryptowalut szacuje się na 575 milionów.[3]

Dynamiczny wzrost wartości rynkowej kryptowalut oraz ich coraz powszechniejsze zastosowanie w obrocie cyfrowym przyciągnęły nie tylko uczciwych inwestorów, ale również osoby i grupy przestępcze, które dostrzegły w tym obszarze możliwość łatwego wzbogacenia się przy ograniczonym ryzyku wykrycia. Z uwagi na swoją specyfikę – m.in. pseudonimowość transakcji, brak centralnego nadzoru, trudności

[2] https://www.triple-a.io/cryptocurrency-ownership-data (dostęp 14.06.2025).
[3] https://crypto.com/en/research/2023-review-2024-ahead.

w odzyskaniu środków po ich przesłaniu – kryptowaluty stały się dogodnym narzędziem wykorzystywanym w różnego rodzaju oszustwach finansowych.

Według raportu Chainalysis w 2024 roku wolumen przestępczych transakcji wynosił 40,9 mld. USD. Jest to wartość określona na podstawie analizy przepływu środków na zidentyfikowanych nielegalnych adresach kryptowalutpwych. Jest to spadek w stosunku do roku 2023 gdzie wolumen nielegalnych transakcji był określony na kwotę 46,1 mld USD jednakże sami badacze wskazują, że prognozują wzrost wolumenu transakcji z 2024 r. do kwoty 51,3 mld. USD gdyż w miarę analizy kolejnych spraw wzrasta liczba nielegalnych adresów i coroczne analizy wskazują, że początkowe wartości są niedoszacowane.[4]



2. Całkowita wartość kryptowalut otrzymana przez nielegalne adresy – źródło Chainalysis, The 2024 Crypto Crime Report s. 2

Jednym z najpoważniejszych i najczęściej spotykanych zagrożeń w tym obszarze są oszustwa inwestycyjne, które zyskały nowe oblicze dzięki wykorzystaniu technologii blockchain.

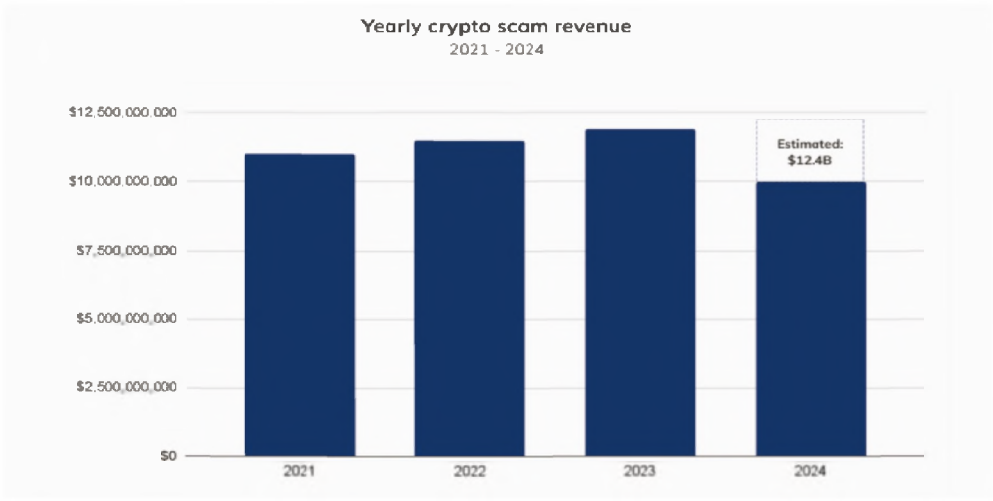
Oszustwa te mogą przybierać różnorodne formy – od fałszywych ofert inwestycyjnych, przez piramidy finansowe i tzw. „rug pull'e" w projektach kryptowalutowych, po działalność nielegalnych platform tradingowych imitujących legalne giełdy. Ofiarami takich działań padają często osoby, które nie posiadają

[4] Chainalysis, The 2024 Crypto Crime Report s. 3.

wystarczającej wiedzy na temat działania kryptowalut ani świadomości ryzyk związanych z inwestowaniem w tego typu aktywa. Zjawisko to ma charakter międzynarodowy i stanowi coraz większe wyzwanie zarówno dla organów ścigania, jak i dla instytucji odpowiedzialnych za regulacje rynku finansowego. Przestępczość ta trafia na podatny grunt podbudowywany w świadomości społeczeństwa informacjami o niezwykłych zyskach z kryptowalut poniekąd mających uzasadnienie w notowanych zwyżkach kursów kryptoaktywów.

Niniejszy artykuł ma na celu przybliżenie problematyki oszustw inwestycyjnych z uwzględnieniem wykorzystywania kryptowalut w tym procederze, a także ukazanie mechanizmów działania sprawców oraz metod wykorzystywanych do pozyskiwania środków od ofiar.

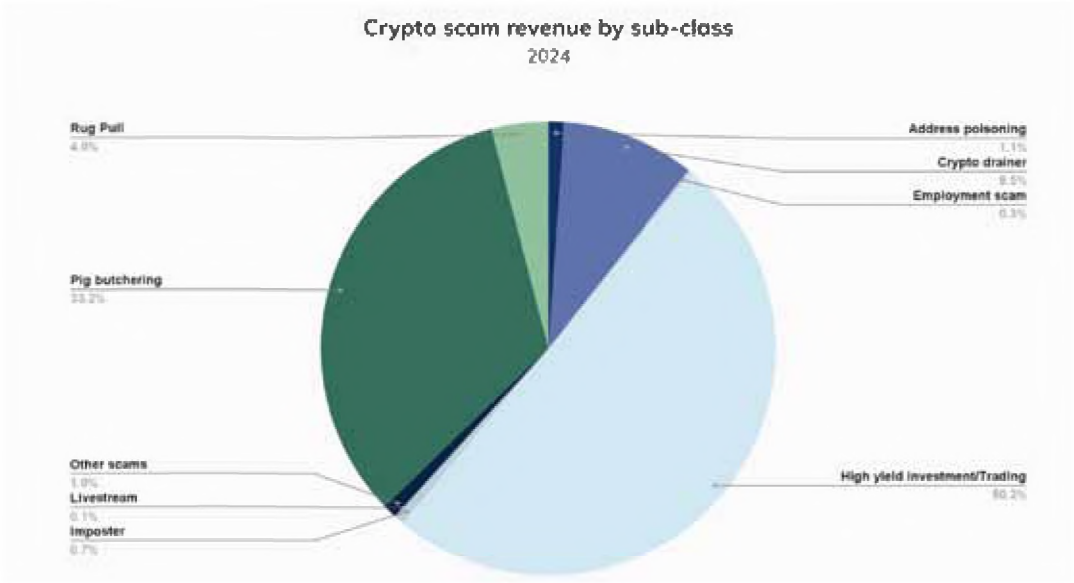
Zrozumienie i identyfikacja zagrożeń wynikających z funkcjonowania kryptowalut na styku z przestępczością finansową staje się dziś koniecznością w kontekście ochrony interesów publicznych, stabilności rynków finansowych oraz bezpieczeństwa użytkowników cyfrowych środków płatniczych.



3. Całkowita wartość kryptowalut otrzymana przez nielegalne adresy – źródło Chainalysis, The 2024 Crypto Crime Report

Analizując dostępne dane na temat oszustw inwestycyjnych można stwierdzić, że notują one dynamiczne wzrosty. Wspomniany wcześniej Raport Chainalysis, określa wzrost przypadków oszustw na 40 procent w skali roku do roku. Analizy wskazują, że 9,9 mld. USD przeszło przez adresy kryptowalutowe zidentyfikowane jako te mające związek z oszustwami. Oczywiście tu również występuje zjawisko niedoszacowania

i prognozuje się, że całkowita wartość wolumenu środków związanych z oszustwami dobije do 12,4 mld. USD.[5]



4. Przychody z oszustw kryptowalutowych według podklasy – źródło Chainalysis, The 2024 Crypto Crime Report

Ponad połowa „przychodów" z oszustw zasila portfele cyberprzestępców zajmujących się oszustwami inwestycyjnymi (50,2%). Powiązane oszustwo określane jako „pig butchering" zasiliło portfele cyberprzestępców o kolejne 33,3 %.[6] Liczby te muszą niepokoić.

W ciągu siedemnastu lat od pojawienia się na rynku, kryptowaluty przekształciły się z marginalnego rozwiązania technologicznego, rozwijanego głównie przez entuzjastów zdecentralizowanych rejestrów, w zjawisko o charakterze globalnym. Ich dynamiczny rozwój wywołuje silnie spolaryzowane reakcje – od entuzjazmu środowisk zaangażowanych w projekty kryptowalutowe po głęboką rezerwę ze strony przedstawicieli tradycyjnego sektora finansowego oraz instytucji regulacyjnych. Zwolennicy kryptowalut wskazują na ich potencjał w zakresie zwiększania wolności finansowej, demokratyzacji dostępu do usług finansowych, redukcji kosztów transakcyjnych oraz ochrony przed inflacją. Z kolei krytycy postrzegają aktywa cyfrowe jako elementy spekulacyjnych baniek inwestycyjnych, nierzadko utożsamiane z mechanizmami charakterystycznymi dla piramid finansowych,

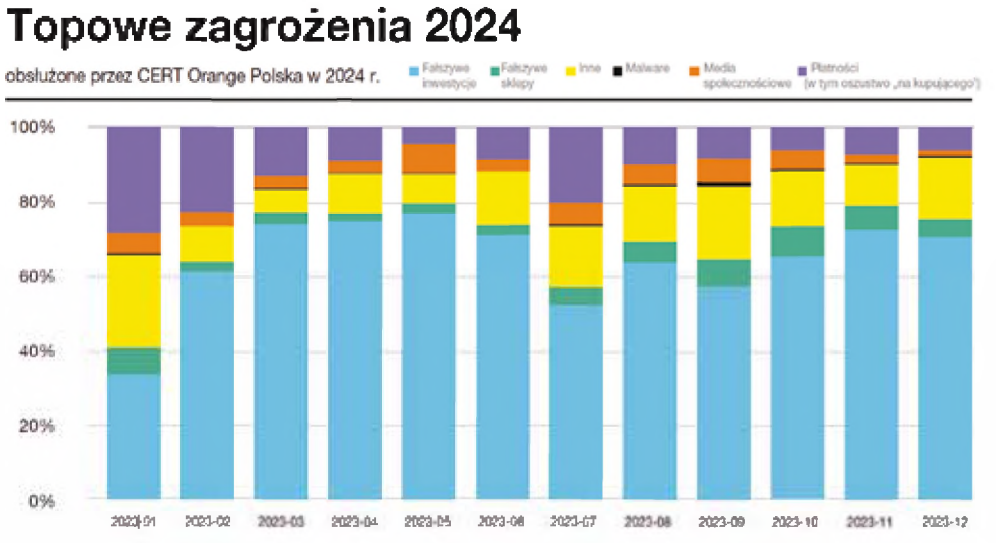
[5] Chainalysis, The 2024 Crypto Crime Report s. 54.
[6] Chainalysis, The 2024 Crypto Crime Report s. 56.

których funkcjonowanie może sprzyjać działalności przestępczej i stwarzać ryzyko dla nieświadomych uczestników rynku.

Niestety polskie organy ścigania nie publikują raportów, z których można by wnioskować jakie jest zagrożenie cyberprzestępczością związaną z oszustwami inwestycyjnymi czy kryptowalutami. Można jedynie wnioskować po komunikatach zarówno Policji jak też Związku Banków Polskich i Departamentów Bezpieczeństwa poszczególnych banków, że zagrożenie i skala tego typu przestępczości jest duża.

O skali zjawiska na terenie Polski mogą świadczyć dane publikowane przez CSIRT KNF, gdzie w 2024 roku instytucja ta zgłosiła do blokady 45 985 domen związanych z fałszywymi inwestycjami, jest to 89,4 % wszystkich zgłoszonych domen.[7] CSIRT KNF zwraca tez uwagę na oszukańcze reklamy w mediach społecznościowych.

W Raporcie CERT Orange Polska za rok 2024 autorzy również zauważają, że problem oszustw inwestycyjnych jest jednym z najpoważniejszych zagrożeń. W scenariuszach dominujących oszustw w 2024 roku – fałszywe inwestycje to 60 % – gdzie w 2023 roku było to „tylko" 28,2%.[8]



5. Topowe zagrożenia według podklasy – źródło Raport CERT Orange Polska za 2024 rok.

Specjaliści z CERT Orange Polska zwracają też uwagę na fałszywe reklamy na portalach społecznościowych i trudności z ich blokowaniem. Formułowane przez nich wnioski, że „obecny sposób, w jaki Facebook (nie) radzi sobie z oszustwami na

[7] Raport Roczny CSIRT KNF 2024 s. 16.
[8] Raport CERT Orange Polska za rok 2024 s. 15.

swojej platformie, nie pozwala na bezpieczne korzystanie z tej platformy przez osoby nieświadome cyberzagrożeń".[9]

Raport Roczny 2024 z działalności CERT Polska również wykazuje, że najwięcej domen wpisywanych na listę ostrzeżeń jest z zakresu oszustw inwestycyjnych – w 2024 roku były to 42 172 domeny, niepokojące jest to, że w 2023 roku takich domen było 20 609.[10] Wzrost o ponad 100 procent musi niepokoić. Niestety prezentowane dane wykazują jedynie obciążenie dla instytucji związanych z cyberbezpieczeństwem i chwała im, że z roku na rok coraz więcej oszukańczych domen podlega blokadzie. Nie dysponujemy jednak danymi mówiącymi o wielkości strat jakie ponoszą w wyniku oszustw inwestycyjnych polscy internauci. Nie udostępniają tych danych ani organy ścigania ani banki, których to klienci najczęściej są pokrzywdzeni. Z jednostkowych informacji medialnych można przypuszczać, że są one duże, i że też mają tendencję wzrostową.

Cel phishingu	Liczba domen 2024 r.	Liczba domen 2023 r.
Oszustwa inwestycyjne	42 172	20 609
OLX	9714	4564
Allegro	4074	11 015
Facebook	3862	6638
InPost	2908	2770
Baltic Pipe	2795	6971
Netflix	2470	1495
Gazeta.pl	2057	658
Meta	1142	660
Booking	1064	94

6. Najczęściej występujące cele phishingu, które znalazły się na Liście Ostrzeżeń CERT Polska – źródło Raport Roczny 2024 z działalności CERT Polska

Bazując tylko na danych z tych trzech instytucji zajmujących się cyberbezpieczeństwem można śmiało formułować wnioski, że zjawisko oszustw inwestycyjnych niestety jest w fazie dynamicznego rozwoju.

Oszustwa inwestycyjne to dynamicznie rozwijająca się forma cyberprzestępczości, która wykorzystuje brak wiedzy finansowej, łatwowierność i zaufanie ofiar. Oszuści

[9] Raport CERT Orange Polska za rok 2024 s. 71.
[10] Raport Roczny 2024 z działalności CERT Polska s. 98.

stosują coraz bardziej wyrafinowane metody – od fałszywych platform inwestycyjnych po manipulacje psychologiczne, jak w przypadku „pig butchering".

Brak danych statystycznych w tym zakresie – publikowanych przez polskie organy ścigania nie musi świadczyć o braku zainteresowania tego typu przestępczością, bo przecież pokrzywdzeni składają zawiadomienia o popełnionych przestępstwach i muszą one być prowadzone. Mam nadzieję, że wewnętrznie takie statystyki istnieją, gdyż na ich podstawie można by prognozować dynamiczny rozwój tego typu przestępczości. W konsekwencji zaplanować przedsięwzięcia zarówno organizacyjne, kadrowe jak i legislacyjne, które byłyby w stanie mitygować zagrożenia związane z dynamicznym wzrostem oszustw inwestycyjnych. W dużym uproszczeniu można stwierdzić, że potrzeba dużych zasobów ludzkich ze strony Policji i Prokuratury do prowadzenia tych postepowań. Co więcej muszą to być funkcjonariusze i prokuratorzy którzy posiadają wiedzę zarówno z zakresu Internetu jak i kryptowalut.

A jak to wygląda na świecie?

Federalne Biuro Śledcze USA w corocznym raporcie publikowanym przez komórkę do zwalczania cyberprzestępczości IC3 – Internet Crime Report 2024 przedstawiło stan zagrożenia cyberprzestępczością w 2024 roku ale należy pamiętać, że dotyczy to cyberprzestępstw związanych z jurysdykcją FBI. Z raportu wynika, że cyberprzestępstw związanych z użyciem kryptowalut zostało zgłoszonych 149 686 przy ujawnionych stratach 9 322 335 911 USD. Przy czym samych oszustw inwestycyjnych 47 919 na kwotę 6 570 639 864 USD.[11]

Porównując liczbę skarg widać dynamiczny wzrost oszustw inwestycyjnych w 2024 było 47 919 skarg przy stratach 6 570 639864 USD, w 2023 roku 39 570 skarg przy stratach 4 570 275 683 USD a w 2022 roku 30 529 skarg przy stratach 3 311 742 206 USD.[12] Jak widać tendencje narastające są również w USA.

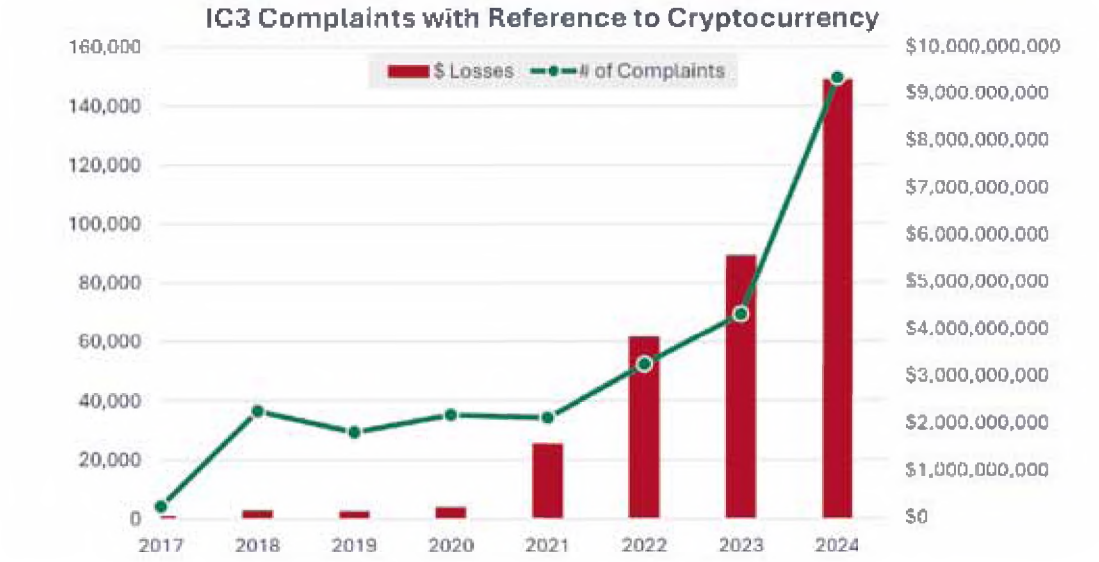
Rok	Liczba skarg	Straty
2024	47 919	6 570 639864
2023	39 570	4 570 275 683
2022	30 529	3 311 742 206

1. Tabela – opracowanie własne – skargi IC3 odnoszące się do kryptowalut w okresie 2022–2024 – źródło FBI Internet Crime Report 2024

[11] IC3 – Internet Crime Report 2024 s. 10.
[12] IC3 – Internet Crime Report 2024 s. 18.

Trendy wzrostowe związane z oszustwami inwestycyjnymi są globalne, sprzyja temu rosnąca skala zjawiska i globalny zasięg, użycie kryptowalut i metod anonimizacji i maskowania się w sieci, użycie zaawansowanej socjotechniki, charakter transgraniczny, a w ostatnim okresie wsparcie sztucznej inteligencji praktycznie na każdym etapie oszustw.

FBI zwraca również uwagę na wysoką profesjonalizację działań cyberprzestępczych wspartych zaawansowaną technologią pozwalającą na każdym etapie działań podejmować skuteczne próby przełamania zabezpieczeń pokrzywdzonych i instytucji finansowych biorących udział w procesie oszukańczej inwestycji.



7. Skargi IC3 odnoszące się do kryptowalut – źródło FBI Internet Crime Report 2024

Na załączonym wykresie widać dynamiczny wzrost całkowitej przestępczości związanej z kryptowalutami. Całkowita skala strat w 2024 roku wynosi 9 322 335 911 USD z czego na oszustwa inwestycyjne przypada 6 570 639864 USD[13] co również pokazuje o jaki kawałek „tortu" toczy się gra. Gra którą, jak wskazują przytoczone statystyki, społeczeństwo i organy ścigania niekoniecznie wygrywa.

Oszustwa Inwestycyjne

Oszustwa inwestycyjne oparte na wykorzystaniu technologii zdalnego pulpitu stanowią rosnące zagrożenie w krajobrazie cyberprzestępczości ostatniej dekady. Pomimo trudności w jednoznacznym określeniu momentu ich pojawienia się, obserwacje wskazują, iż istotny wzrost liczby tego typu incydentów nastąpił w okresie

[13] IC3 – Internet Crime Report 2024 s. 19.

pandemii COVID-19. Sytuacja ta była związana z gwałtownym upowszechnieniem pracy zdalnej oraz powszechnym wykorzystaniem narzędzi umożliwiających zdalny dostęp do zasobów komputerowych. Zjawisko to zostało szybko zaadaptowane przez cyberprzestępców, którzy wdrożyli zaawansowane strategie socjotechniczne w celu nakłonienia użytkowników do instalacji zdalnego oprogramowania, umożliwiającego przejęcie kontroli nad urządzeniami ofiar.

Kluczowym mechanizmem umożliwiającym realizację tego typu ataków jest inżynieria społeczna (ang. social engineering), rozumiana jako zestaw technik manipulacyjnych, których celem jest skłonienie jednostek do podejmowania działań nieleżących w ich interesie, np. ujawnienia danych uwierzytelniających, instalacji szkodliwego oprogramowania, czy też udostępnienia zasobów cyfrowych. W odróżnieniu od klasycznych metod ataków informatycznych, socjotechnika bazuje nie na podatnościach technologicznych, lecz na błędach poznawczych, emocjach i mechanizmach psychologicznych charakterystycznych dla ludzkiego zachowania.

Ofiary tego typu oszustw najczęściej są nakłaniane do przekazania poufnych informacji, takich jak dane logowania do bankowości elektronicznej, skrzynek e-mailowych, czy portfeli kryptowalutowych. W przypadkach, gdy napastnik uzyska pełny dostęp do urządzenia użytkownika za pośrednictwem aplikacji zdalnego pulpitu (np. AnyDesk, TeamViewer), możliwe jest również przeprowadzenie kradzieży tożsamości, usunięcie lub modyfikacja danych, a także transfer środków finansowych bez wiedzy ofiary.

Typowe schematy wykorzystywane w omawianych atakach opierają się na wzbudzaniu określonych stanów emocjonalnych u użytkownika – przede wszystkim strachu, ciekawości, poczucia presji czasowej lub chciwości. Są to techniki dobrze opisane w literaturze z zakresu psychologii społecznej i stanowią skuteczne narzędzia w arsenale działań przestępczych.

Praktyczna analiza oszustw inwestycyjnych, a także wymiana doświadczeń i wiedzy z zakresu przeciwdziałania cyberprzestępczości przez wielu specjalistów i instytucji wykazała, że przygotowanie tego typu ataku składa się z wielu etapów działań cyberprzestępców. Działania te wymagają od nich dużej koordynacji i zaangażowania w przestępczy proceder. Muszą być podzielone na poszczególne role. Role te, aby przestępstwo było skuteczne muszą być ściśle skoordynowane i od siebie zależne. Często przeciwdziałając cyberprzestępczości, a w szczególności oszustwom inwestycyjnym odnosiłem wrażenie, że przeciwnikiem jest prężnie działająca korporacja. Zatrzymania przez Policję niektórych działających grup przestępczych trudniących się oszustwami inwestycyjnymi potwierdzają te spostrzeżenia.

W kolejnej części artykułu postaram się przybliżyć etapy przestępczej działalności, która co do zasady jest stała, jednakże cyberprzestępcy stale modyfikują swoje

działanie co jest skutkiem analizy zachowania pokrzywdzonych, banków, operatorów płatności i organów ścigania.



8. Fazy ataku przy oszustwie inwestycyjnym – opracowanie własne

Oszukańcze reklamy

Faza ta charakteryzuje się wywołaniem zainteresowania potencjalnej ofiary jakimś zdarzeniem, najczęściej gospodarczym, które oferuje możliwość dużego zysku w krótkim czasie. Do uwiarygodnienia historii wykorzystywane są wizerunki znanych ludzi – sportowców, polityków, aktorów czy tez realnych wydarzeń gospodarczych. Według Raportu Rocznego CSIRT KNF 2024 analiza kampanii wykazała zróżnicowane strategie działania. Procentowo sprawcy wykorzystywali wizerunki polityków w 26 %, celebryci i influenserzy – 14 %, spółki Skarbu Państwa – 11 %, Baltic Pipe – 7 %, przedsiębiorcy – 6 %.[14]

Najczęstsze sposoby przyciągania potencjalnych ofiar:

- reklamy internetowe, m.in. na Facebooku;
- grupy w mediach społecznościowych czy komunikatorach, np. na Telegramie, Facebooku;

[14] Raport Roczny CSIRT KNF 2024 str. 16.

- inwestycje reklamowane przez popularne osoby, np. oszustwo „na Hołownię";
- podszywanie się pod znane w branży kryptowalut osoby, m.in. Rafała Zaorskiego;
- podszywanie się pod pracowników giełd kryptowalutowych;
- aplikacje randkowe, np. Tinder;
- próby nawiązania kontaktu poprzez odpowiedzi na komentarze, które umieszczane są przez potencjalne ofiary pod filmikami dotyczącymi tematyki kryptowalut, publikowanymi w serwisie YouTube.

Najczęstszym sposobem „pozyskiwania klienta" czytaj osoby która stanie się pokrzywdzonym są targetowane reklamy w mediach społecznościowych, wykorzystują one algorytmy do precyzyjnego docierania do potencjalnych ofiar.



9. Grafiki przykładowych ogłoszeń z fałszywymi inwestycjami – źródło Raport Roczny CSIRT KNF 2024



10. Grafiki przykładowych ogłoszeń z fałszywymi inwestycjami – źródło Raport Roczny CSIRT KNF 2024

Należy zwrócić uwagę, że cyberprzestępcy reagują szybko na zmieniającą się rzeczywistość polityczną i tuż po wyborze nowego prezydenta RP, a jeszcze przed zaprzysiężeniem stał się on obiektem oszukańczej reklamy.

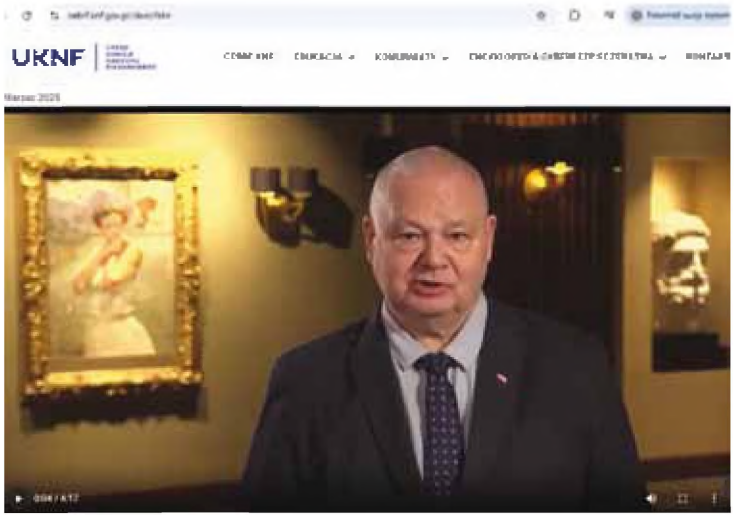


11. Grafika ogłoszenia z fałszywymi inwestycjami – źródło Facebook – opracowanie własne

Do tworzenia oszukańczych ogłoszeń służy bardzo często sztuczna inteligencja tworząc tzw. deepfake – materiały video, gdzie tworzony jest fałszywy obraz i dźwięk z udziałem znanych osób. Bardzo profesjonalnie przykłady takich deepfake zostały zaprezentowane na stronie KNF – https://cebrf.knf.gov.pl/deepfake

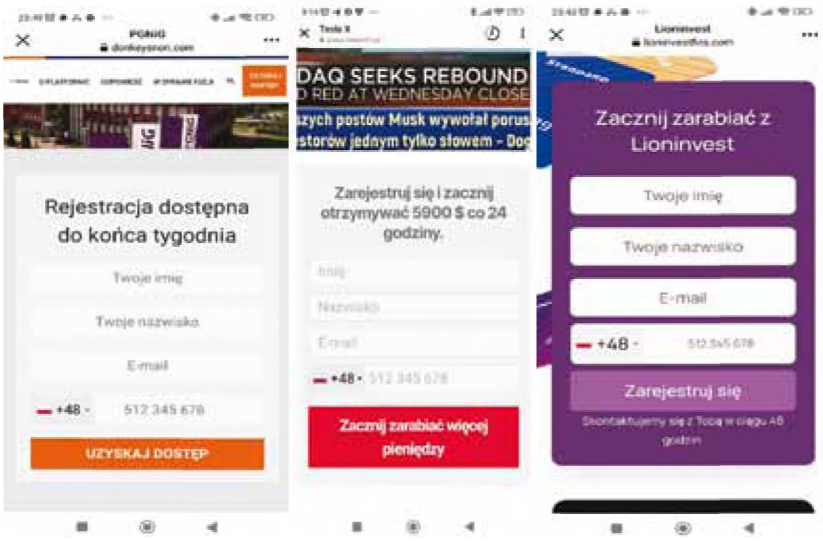


12. Grafika filmu w serwisie YT z deepfake z fałszywymi inwestycjami – źródło https://cebrf.knf.gov.pl/deepfake



13. Grafika filmu w serwisie YT z deepfake z fałszywymi inwestycjami – źródło https://cebrf.knf.gov.pl/deepfake

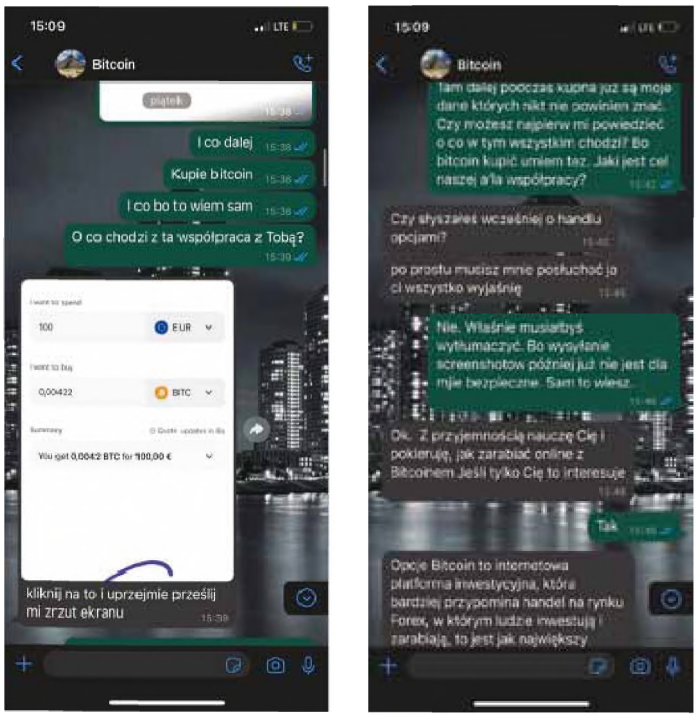
Wszystkie te zabiegi służą jednemu, aby potencjalny pokrzywdzony uzupełnił pola w formatkach do kontaktu. Chodzi o pozyskanie jego danych osobowych takich jak imię i nazwisko, email, numer telefonu.



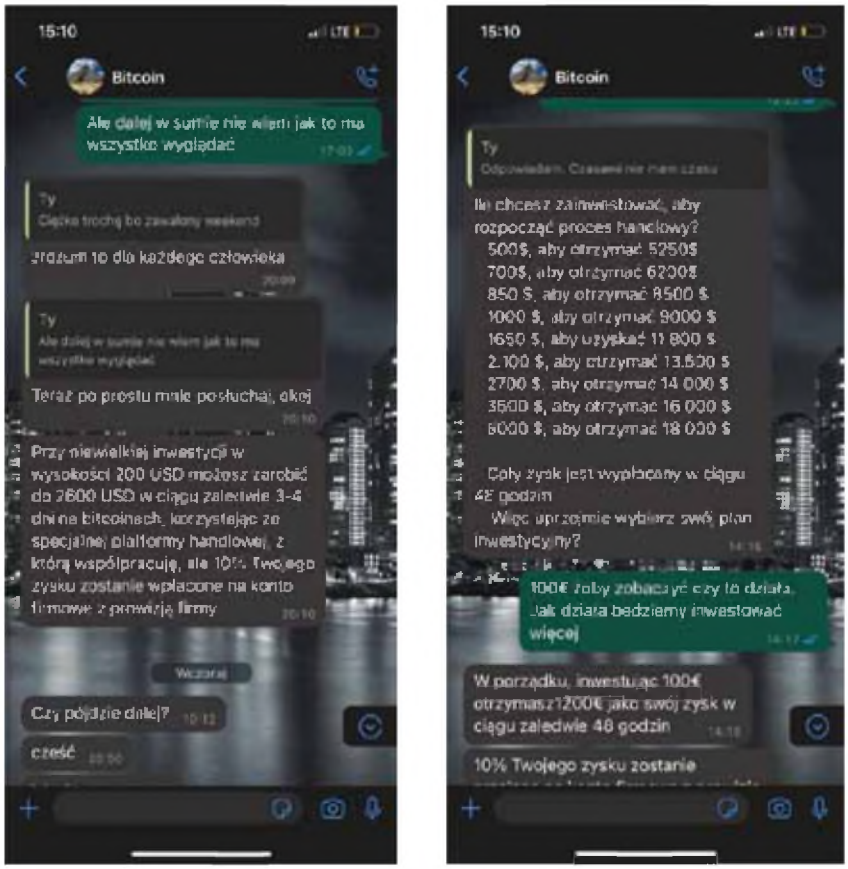
14. Grafika ogłoszenia z fałszywymi inwestycjami – rejestracja – źródło Facebook – opracowanie własne

Po pozyskaniu tych danych przed cyberprzestępcami otwierają się całkiem nowe możliwości.

Jak wspominałem wcześniej metody te ewoluują albo przybierają inne formy. Inną metodą przyciągania potencjalnych ofiar jest ich rekrutacja na grupach w social mediach min. na Facebooku czy Instagramie. Oszustwa inwestycyjne w grupach na Facebooku, Instagramie i innych social mediach to coraz bardziej wyrafinowana metoda „łowienia" ofiar – często pod przykrywką społeczności, które wydają się przyjazne i pomocne. Przestępcy wykorzystują zaufanie budowane w grupach tematycznych, by wciągnąć użytkowników w fałszywe inwestycje, najczęściej w kryptowaluty lub „nowe technologie". Oszuści zakładają grupy o tematyce finansowej, rozwoju osobistego, inwestowania, a nawet lifestyle'u. Czasem w miarę możliwości przejmują istniejące grupy z dużą liczbą członków. W ten sposób uzyskują dotarcie do dużych grup osób. Pojawiają się wpisy typu „Zainwestowałem 600 złotych i po tygodniu mam 6000 zł" – komentarze te często wspomagane są fałszywymi screenami wypłat środków. Konta należące do cyberprzestępców komentują zamieszczane posty, nakręcając atmosferę, chwaląc skuteczność inwestycji i polecając „inwestora". Po wykazaniu zainteresowania przez przyszłego pokrzywdzonego korespondencja przechodzi na poziom wiadomości prywatnych. Tym kanałem przesyłane są instrukcje jak „inwestować". Najczęściej jest to oszukańcza platforma inwestycyjna – ale o tym za chwilę.

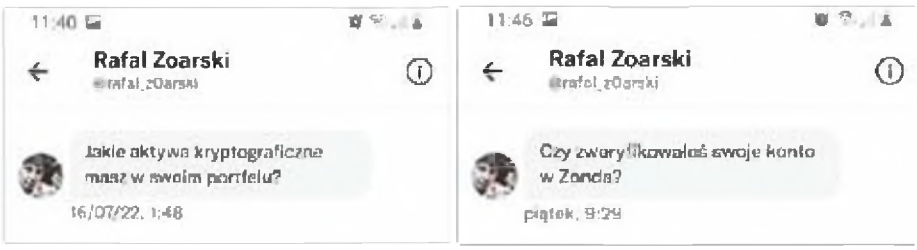


15. Grafika konwersacji na grupie w socjal mediach – źródło Facebook – opracowanie własne

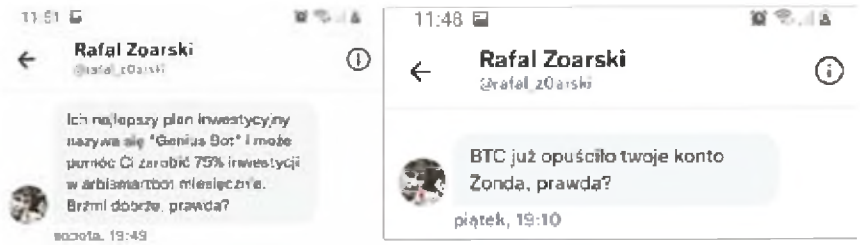


16. Grafika konwersacji na grupie w socjal mediach cd. – źródło Facebook – opracowanie własne

Kolejnym przykładem przyciągania osób do fałszywych inwestycji jest podszywanie się pod osoby znane z branży kryptowalut – na potrzeby artykułu przedstawimy przykład rozmowy ze znanym inwestorem Rafałem Zaorskim.



17. Grafika konwersacji w socjal mediach cd.
– źródło materiały pokonferencyjne 19–21 października 2022 Białowieża



18. Grafika konwersacji w socjal mediach cd. – źródło materiały pokonferencyjne 19–21 października 2022 Białowieża



19. Grafika konwersacji w socjal mediach cd. – źródło materiały pokonferencyjne 19–21 października 2022 Białowieża

Oczywiście w tym przypadku konto Rafał Zoarski (@rafal z0arski) jest kontem oszukańczym, nie należy do Rafała Zaorskiego i służy tylko i wyłącznie do nakłaniania do wejścia w oszukańcze inwestycję – wykorzystując autorytet znanej osoby.

Jedną z metod przyciągania potencjalnych ofiar jest też rekrutacja na znanym portalu randkowym Tinder

Można wyróżnić 5 etapów oszustwa na Tinderze:

- nawiązanie kontaktu, przeniesienie rozmowy na WhatsApp,
- budowanie więzi i zaufania, bardzo często jest to połączone w przesyłaniem intymnych zdjęć, które później służą do wywierania presji czy wręcz szantażu,
- wzmianka o inwestycjach,

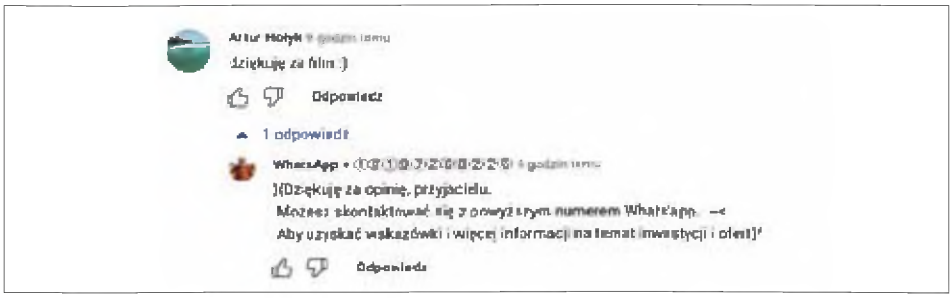
- namówienie do wpłaty na fałszywą platformę inwestycyjną,
- po zerwanie kontaktu.

Oszustwa inwestycyjne na Tinderze to coraz częstsza forma tzw. „romance scam", czyli oszustwa opartego na budowaniu relacji emocjonalnej w celu wyłudzenia pieniędzy. Przestępcy wykorzystują aplikacje randkowe, by zdobyć zaufanie ofiary, a następnie wciągnąć ją w fałszywe inwestycje – najczęściej w kryptowaluty.[15]

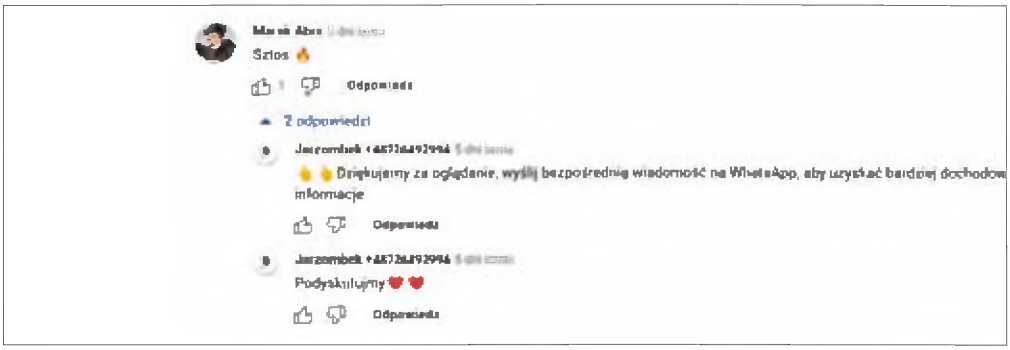
Problem ten został dostrzeżony przez belgijskiego regulatora FSMA który wydał ostrzeżenie przed oszustwami w mediach społecznościowych. Nawet na portalach randkowych takich jak Tinder można napotkać fałszywe oferty inwestycyjne.[16]

Kolejną metodą pozyskiwania przyszłych pokrzywdzonych są próby nawiązania kontaktu poprzez odpowiedzi na komentarze, które umieszczane są przez potencjalne ofiary pod filmikami dotyczącymi tematyki kryptowalut, publikowanymi w serwisie YouTube. Osoba komentuje legalne wystąpienie/nagranie odnoszące się do tematyki kryptowalut, które opublikowane zostało przez np. znanego krypto-infulencera na jego kanale prowadzonym w serwisie YouTube. Reakcja oszusta jest dość szybka – odpowiada on na umieszczony komentarz i informuje, że jest w stanie pomóc w inwestowaniu, udzieli niezbędnych porad i instrukcji, tym samym zachęca osobę komentującą do bezpośredniego kontaktu. Oszust, aby wzbudzić zaufanie, często wykorzystuje wizerunek znanej osoby (najczęściej tej, która opublikowała konkretny film). W trakcie rozmowy nakłania potencjalną ofiarę do inwestycji – zwykle poprzez założenie konta na giełdzie kryptowalut i dokonanie wpłaty środków, a następnie zakupienie konkretnej kryptowaluty. Gdy kryptowaluty znajdują się już na saldzie poszkodowanego na koncie giełdowym, oszust dostarcza mu adres portfela (do którego rzekomo ofiara będzie miała swobodny dostęp), a następnie instruuje w jaki sposób dokonać wypłaty środków. Instrukcje udzielane są poprzez przesyłane za pomocą komunikatora zrzuty ekranu ze wskazówkami dotyczącymi tego, jak należy postępować (bez wykorzystania zdalnych pulpitów, jak AnyDesk czy TeamViewer). W toku rozmowy, dla uwiarygodnienia, oszust może również dostarczyć dane do logowania do wspomnianego portfela kryptowalutowego (są to fałszywe dane). W konsekwencji tych działań, osoba poszkodowana całkowicie traci dostęp do swoich środków.

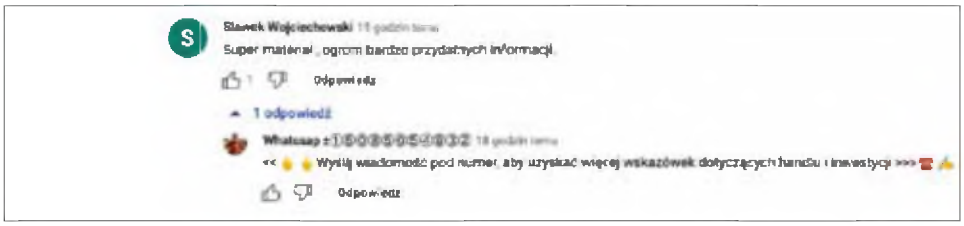
[15] https://cryps.pl/ostrzezenie/uwaga-na-kryptowalutowe-oszustwa-na-tinderze/
[16] https://forexrev.pl/belgijskie-fsma-uwaga-na-oszustwa-na-tinderze/



20. Grafika konwersacji w serwisie You Tube pod filmem zamieszczonym przez Phila Koniecznego – źródło materiały pokonferencyjne 06.06.2023 r. PT XXI Gdynia

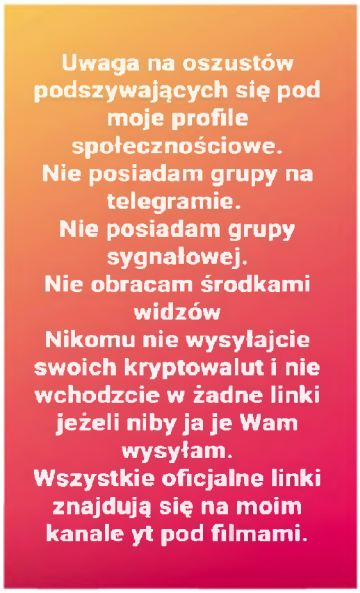


21. Grafika konwersacji w serwisie You Tube. – źródło materiały pokonferencyjne 06.06.2023 r. PT XXI Gdynia



22. Grafika konwersacji w serwisie You Tube. pod filmem zamieszczonym przez Phila Koniecznego – źródło materiały pokonferencyjne 06.06.2023 r. PT XXI Gdynia

Warto zwrócić uwagę, że sprawca wykorzystuje zdjęcia lub nazwiska znanych influencerów, którzy opublikowali materiały w serwisie You Tube odpowiadają w ich imieniu pod komentarzami osób, które obejrzały zamieszczony materiał. Można zauważyć, że numer telefonu do kontaktu podany jest w kółeczkach – utrudnia to wykrycie nieprawidłowości przez algorytmy serwisu. Na profilach influencerów w mediach społecznościowych zaczęły pojawiać się też ostrzeżenia o oszustwach.



23. Grafika ostrzeżenia jakie pojawiło się na profilu Phila Koniecznego w serwisie You Tube – źródło materiały pokonferencyjne 14.12.2022 r. ZBP Warszawa

Kontakt telefoniczny

Kolejny etap – jak już sprawcy mają numer telefonu potencjalnego pokrzywdzonego to dzwonią. Tu rozmowę też można podzielić na kilka etapów. Na początku jest to etap budowania zaufania. Oszust przedstawia się jako broker, doradca inwestycyjny lub analityk finansowy współpracujący z renomowaną firmą. Mówi płynnie ale z akcentem wschodnim, używa specjalistycznego języka i odnosi się do znanych instytucji (np. KNF, GPW, Bloomberg), by nadać sobie wiarygodność. Rozmówca słyszy o „niskim ryzyku" i „gwarantowanych zyskach". Oszust może powoływać się na fałszywe wyniki innych klientów lub opowiedzieć o „spektakularnych sukcesach". Bardzo często opowieść dotyczy stosowanych metod sztucznej inteligencji i specjalnie dopasowanych algorytmów co ma gwarantować duże zyski bez żadnego ryzyka inwestycyjnego. Bardzo często są to obietnice inwestycji w kryptowaluty, ale jak wiemy z wcześniej opisywanych kampanii reklamowych mogą to być metale szlachetne czy udziały w inwestycjach. Niestety królują tu jednak kryptowaluty. Gdy ofiara się waha oszust stosuje presję czasu, pochlebstwa lub strach przed utratą okazji. Padają argumenty „to oferta tylko dla wybranych, jeśli się pan/pani dzisiaj nie zdecyduje najkorzystniejsze opcje mogą być już niedostępne, szkoda było by stracić taką szansę". Przerażające jest to, że rozmowy takie można już zlecać sztucznej inteligencji, gdzie modele językowe są coraz lepsze. Eksperyment przepro-

wadzony przez użytkownika portalu YouTube o nicku „Ag_t" pokazuje, że jest to już możliwe.[17] I tu płynnie przechodzimy do etapu trzeciego.

Instalacja oprogramowania typu zdalny pulpit, przejęcie komputera pokrzywdzonego

Po przekonaniu pokrzywdzonego do inwestowania oszust instruuje, jak zainstalować aplikację do zdalnego pulpitu (np. AnyDesk, TeamViewer, QuickSupport czy Alpemix)[18], by „pomóc w inwestycji". Tutaj legendy też bywały różne – raz była to pomoc w inwestycjach, raz konieczność nadzoru czynności przez regulatora – w przypadku Polski był to KNF, w przypadku innych jurysdykcji powoływano się na regulatorów lokalnych. W rzeczywistości sprawca przejmuje kontrolę nad komputerem. Skutkuje to przejęciem praktycznie całego cyfrowego ja i nie tylko życia ofiary. Przejmowane są konta email, konta w social mediach i dostępy do kont bankowych. Oszukańczy doradca inwestycyjny, jak już ofiara znajduje się pod jego kontrolą, przechodzi do kolejnego etapu.

Rejestracja ofiary na oszukańczej stronie inwestycyjnej

Oszukańcze strony inwestycyjne to fałszywe platformy internetowe stworzone przez cyberprzestępców w celu wyłudzenia pieniędzy od osób zainteresowanych inwestowaniem. Z zewnątrz wyglądają bardzo profesjonalnie – często przypominają legalne serwisy finansowe, używają logo znanych firm, a nawet wizerunków celebrytów lub ekspertów finansowych.

https://celineinvest.pro/	http://www.cashfxgroup.com
http://enduringmarkets.com	http://trade7fx.com
http://solidinvest.co/	http://newtradersholdings-fx.com
http://fxactivetrading.com	http://binvesting.com
https://www.bitroex.com/	Livescalpers.com
https://www.cupiro.io/.	https://bnbtgroup.com/
https://sevenfinancialgroup.com/pl/	http://opeory.com
https://cryptotradecorp.co/	https://www.danskery.com/pl/
https://litegap.com/pl/	ecofxtrade.com

Przykłady oszukańczych platform inwestycyjnych – opracowanie własne

[17] https://www.youtube.com/watch?v=QMdnfJveOaU

[18] https://www.knf.gov.pl/dla_konsumenta/kampanie_informacyjne/cyberoszustwa_inwestycyjne/schematy_oszu stw/oszustwa_inwestycyjne

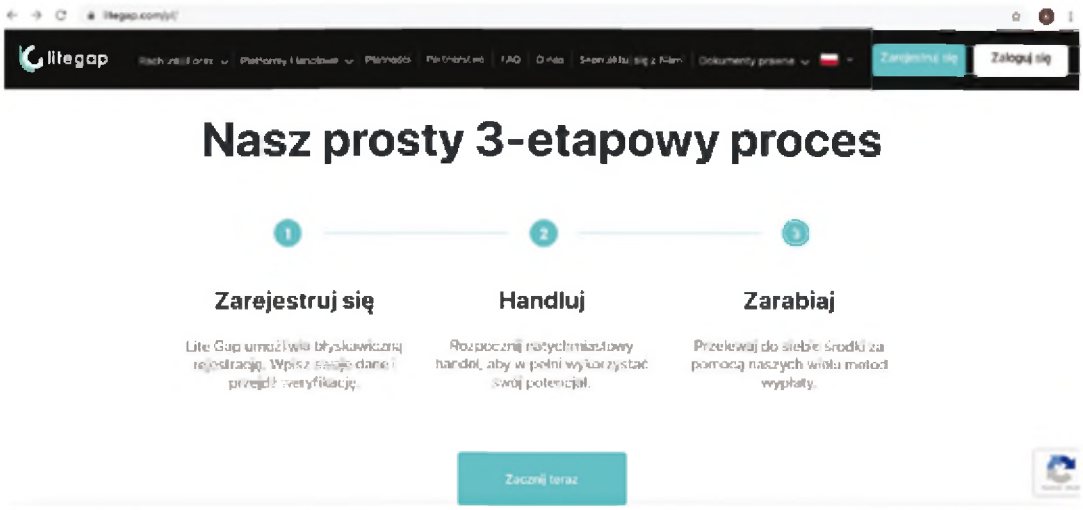
Większość z tych podmiotów została wpisana na listę ostrzeżeń KNF, wobec tych podmiotów zostały wszczęte postepowania przygotowawcze. Pamiętajmy, że rejestrując się na oszukańczej platformie inwestycyjnej osoba oszukana jest poddawana pozorom pełnego rygoru AML, a co się z tym wiąże musi wykonać pełną weryfikację. Wiąże się to z udostepnieniem pełnych danych osobowych i skanów dokumentów tożsamości. Jest to dodatkowe ryzyko późniejszego ich wykorzystania przez cyberprzestępców.

Na potrzeby niniejszego artykułu posłużymy się przykładem platformy inwestycyjnej https://litegap.com/pl/. W chwili obecnej platforma już nie działa – znalazła się też na liście ostrzeżeń KNF.[19] W dalszej części artykułu przedstawię kilka zrzutów ekranu strony litegap.com. Należy zwrócić uwagę na szatę graficzną samej strony, ale też na szczegóły przedstawiające dane dotyczące inwestowania. Materiały te zostały uzyskane bezpośrednio od pokrzywdzonego. Z całym przekonaniem można twierdzić, że budowa tej strony gdzie na każdym kroku w prawym górnym rogu są wyszczególnione środki z inwestycji, gdzie pokrzywdzony może sobie co chwila sprawdzić jakie zyski stały się jego udziałem, niestety to tylko iluzja.

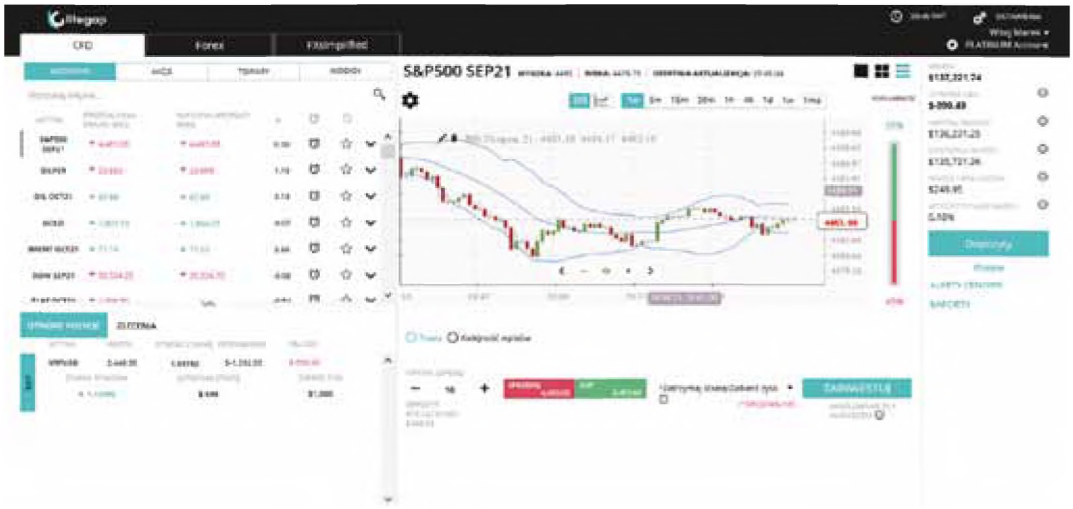


24. Grafika – strona startowa LiteGap – źródło materiały pokonferencyjne 21–23.09.2021 r. Gdynia

[19] https://www.knf.gov.pl/dla_konsumenta/ostrzezenia_publiczne?warningName=litegap.com&warningTypeId=all (dostęp 10.06.2025 r.)



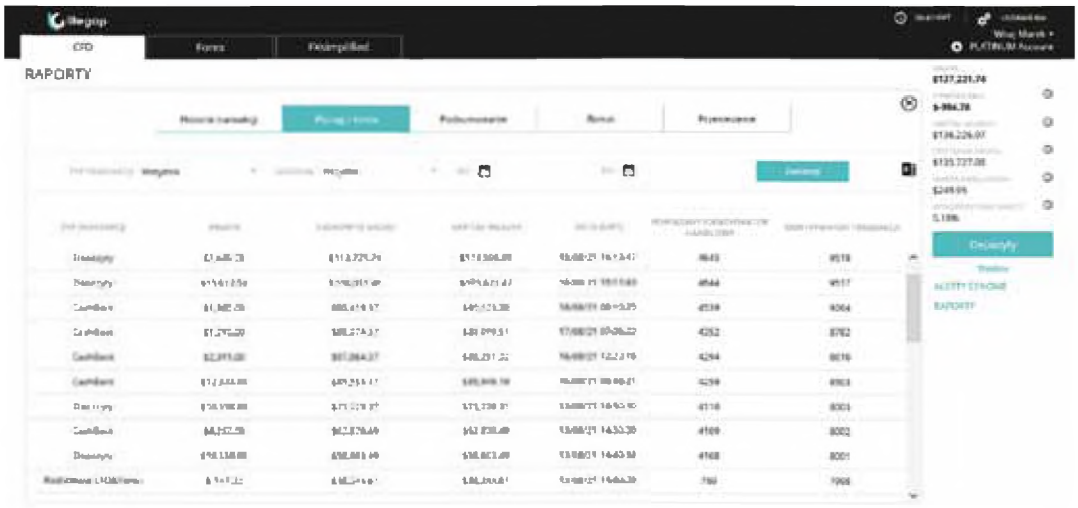
25. Grafika – strona startowa LiteGap – źródło materiały pokonferencyjne 21–23.09.2021 r. Gdynia



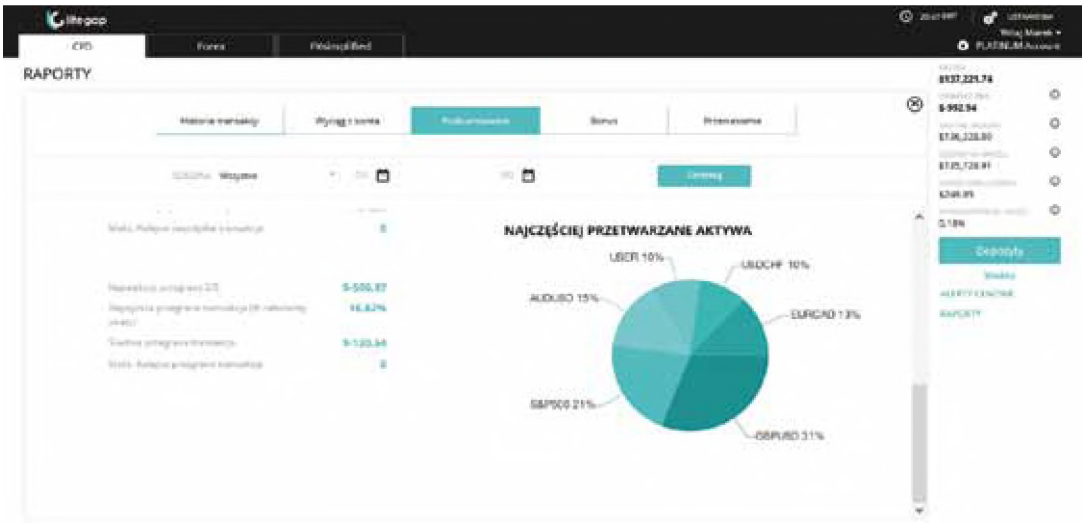
26. Grafika – platforma LiteGap z zalogowanym panelem klienta – zakładka z wykresami – źródło materiały pokonferencyjne 21–23.09.2021 r. Gdynia



27. Grafika – platforma LiteGap z zalogowanym panelem klienta – zakładka z ustawieniami – źródło materiały pokonferencyjne 21–23.09.2021 r. Gdynia

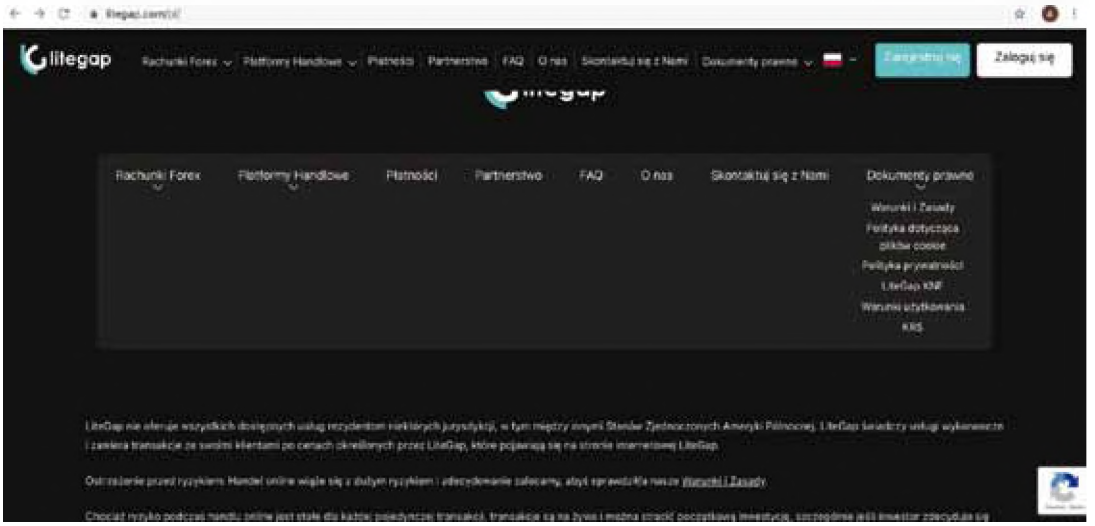


28. Grafika – platforma LiteGap z zalogowanym panelem klienta – zakładka z wyciągiem z konta – źródło materiały pokonferencyjne 21–23.09.2021 r. Gdynia



29. Grafika – platforma LiteGap z zalogowanym panelem klienta – zakładka z podsumowaniem – źródło materiały pokonferencyjne 21-23.09.2021 r. Gdynia

Podjęta analiza strony wykazała, że prawdopodobnie w celu uwiarygodnienia platformy w zakładce „dokumenty prawne" załączone było zezwolenie na prowadzenie działalności wydane przez KNF. Dokument był słabej jakości, na tyle jednak, że dawało się odczytać treść, numery i pieczęć.



30. Grafika – platforma LiteGap – zakładka z „ dokumenty prawne" – źródło materiały pokonferencyjne 21–23.09.2021 r. Gdynia

Firma Polish General Traiding Spółka z o.o., zwana dalej Internetową platformą handlową „LITEGAP" oferuje inwestycje w krypto – Firma przedstawia się jako doradcy, którzy będą dokonywać inwestycji w imieniu klienta na giełdzie kryptowalut.

Sama strona robiła dobre wrażenie pod kątem grafiki jak i udostępnianych klientowi narzędzi i możliwości.

LiteGap na swojej stronie www.litegap.com/pl/ posługiwał się zezwoleniem KNF Nr 1966/13 z dnia 17 lipca 2013 r.

Dokonano sprawdzenia na stronach KNF w dostępnych wyszukiwarkach podmiotów nadzorowanych w celu potwierdzenia informacji czy faktycznie taki podmiot jak Firma Polish General Traiding Spółka z o.o, zwana dalej Internetową platformą handlową „LITEGAP" posiada zezwolenie na prowadzenie działalności.

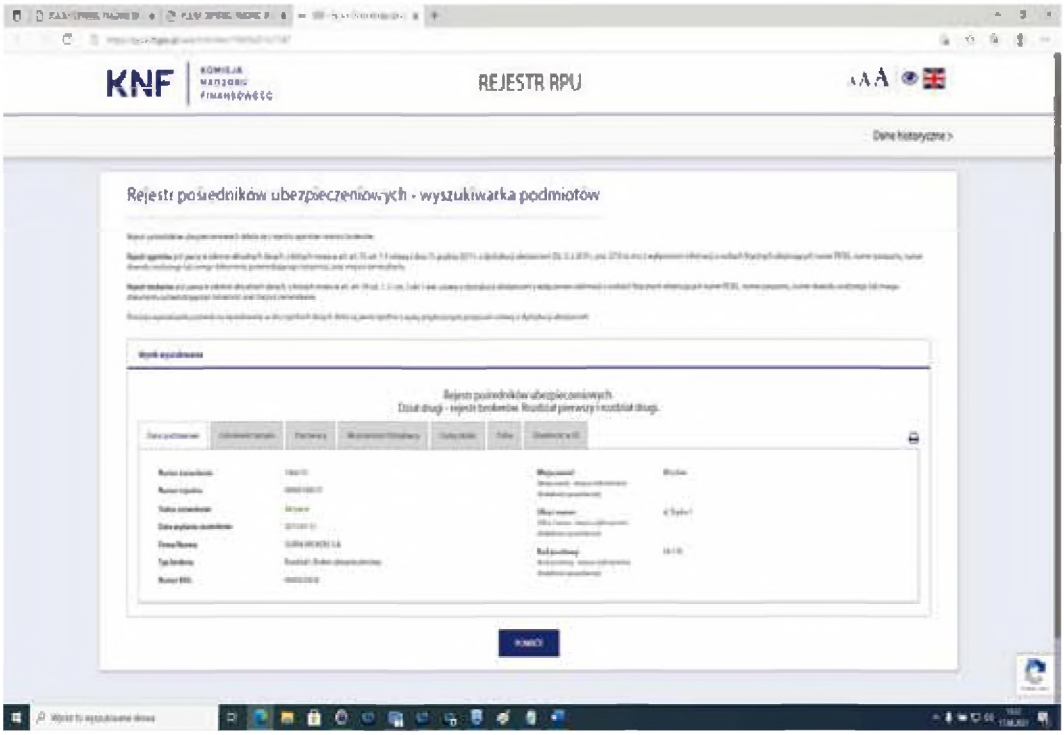


KOMISJA NADZORU FINANSOWEGO

ZEZWOLENIE NR 1966/13

POUCZENIE

31. Grafika – platforma LiteGap – zakładka z „dokumenty prawne" – zezwolenie KNF – źródło materiały pokonferencyjne 21–23.09.2021 r. Gdynia



32. Grafika – sprawdzenie na stronie KNF numeru zezwolenia – źródło materiały pokonferencyjne 21–23.09.2021 r. Gdynia

Po sprawdzeniu można było stwierdzić, że KNF pod Nr 1966/13 z dnia 17 lipca 2013 r. wydało zezwolenie dla legalnie działającej firmy: SUPRABROKERS SPÓŁKA AKCYJNA, KRS: 0000425834, NIP: 8943041146, siedziba: 54-118 Wrocław, Aleja Śląska 1. Data wydania zezwolenia: 17 lipca 2013 r., numer zezwolenia: 1966/13 oraz znak sprawy w KNF: DLU/WB/ 6320/950/2/2013/AP są zgodne dla oryginalnego zezwolenia dla SUPRA BROKERS SA, która widnieje w rejestrze i sfałszowanego zezwolenia dla LITEGAP.

Jak dalej ustalono LITEGAP jako siedzibę spółki wskazało: 00-382 Warszawa, ul. Solec 81 B, nr lokalu A-51, w którym miała siedzibę firma, zajmująca się „hodowaniem spółek" – farma spółek w celu późniejszej ich odsprzedaży. W podrobionym zezwoleniu brak jest informacji jakiej działalności i w jakim zakresie ono dotyczy firmy LITEGAP. Podczas prowadzonych sprawdzeń w dniu 19 sierpnia 2021 r. LITEGAP na swojej stronie usunął sfałszowane zezwolenie KNF Nr 1966/13 z dnia 17 lipca 2013 r., w zamian wystawiono Regulamin świadczenia usług maklerskich – Regulamin świadczenia usług wykonywania zleceń nabycia lub zbycia praw majątkowych i papierów wartościowych, prowadzenia rachunków

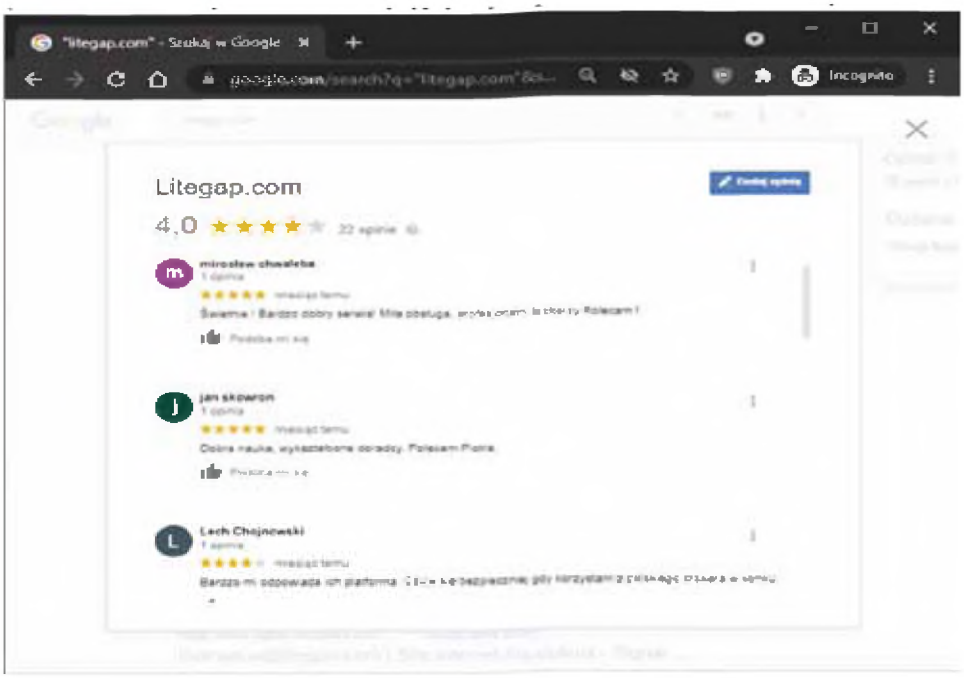
papierów wartościowych i praw majątkowych i rachunków pieniężnych przez LiteGap („Warunki Ogólne") – z dnia 5 sierpnia 2019 r. Może to świadczyć o tym, że strona była stale monitorowana i nagłe wejście w zakładkę „dokumenty prawne" i pobranie sfałszowanego zezwolenia zostało zauważone. Ponadto podrobione zezwolenie dla LITEGAP dotyczy działalności brokerskiej związanej z ubezpieczeniami i reasekuracją a nie działalności brokerskiej/ maklerskiej na rynku inwestycyjnym.



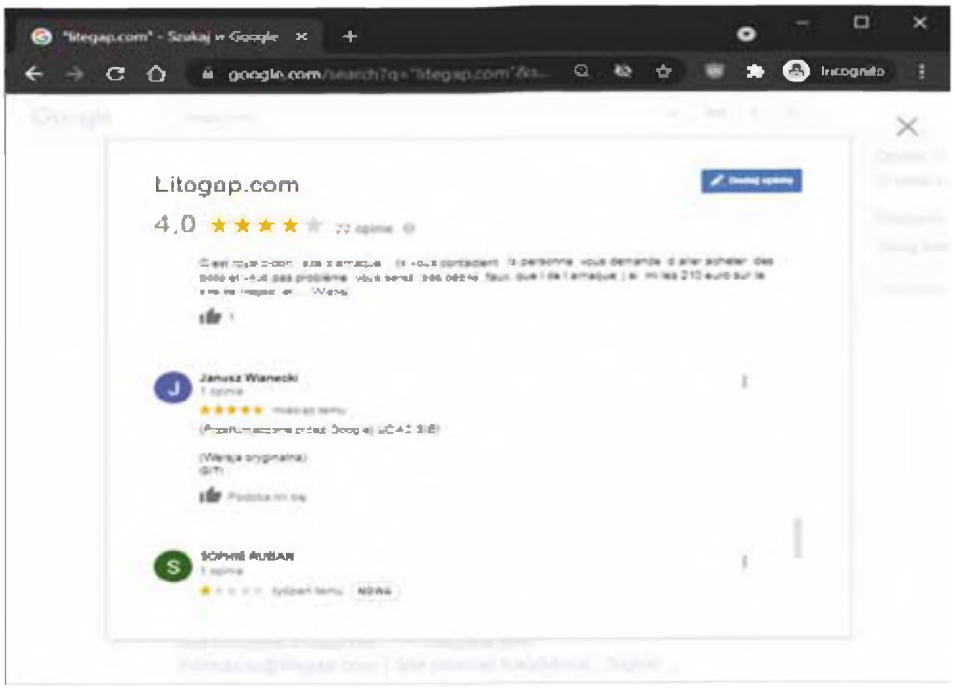
33. Grafika – sprawdzenie na stronie rejestr.io – źródło materiały pokonferencyjne 21–23.09.2021 r. Gdynia

Z dalszych sprawdzeń wynika, że LITEGAP podszywała się pod legalnie działającą firmę: POLISH GENERAL TRADING SPÓŁKA Z OGRANICZONĄ ODPOWIEDZIALNOŚCIĄ, KRS: 0000401586, NIP: 7010322588, siedziba: 02-699 Warszawa, ul. Kłobucka 8B/255.

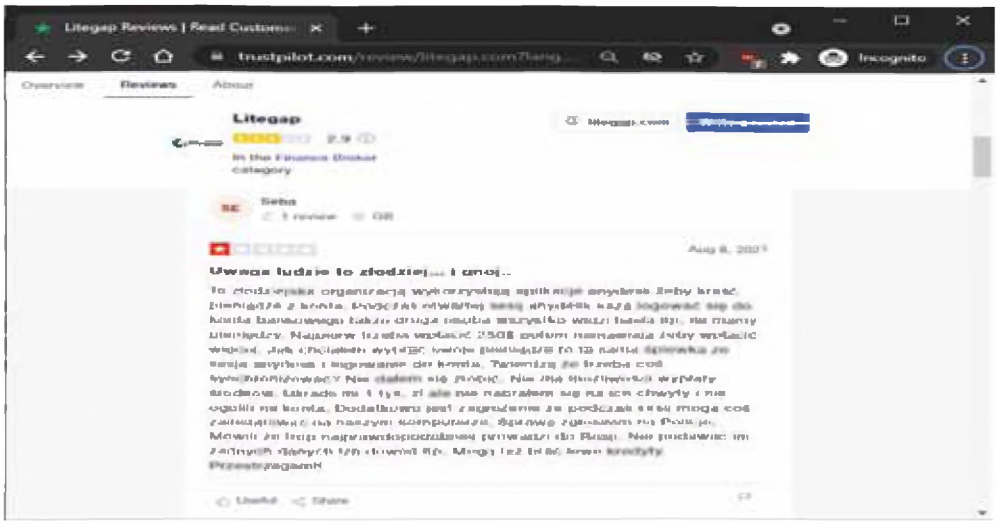
W dalszej kolejności sprawdzono komentarze na temat tej strony internetowej. Początkowo otrzymywała doskonałe opinie – widać jak było budowane zaufanie do strony a właściwie iluzja zaufania. Wśród komentarzy pojawiły się też komentarze w języku francuskim. Świadczyło by to o tym, że kampanie reklamowe najprawdopodobniej były prowadzone również na tym rynku. Jak widać już analiza danych na stronie mogła dostarczyć wiarygodnych i sprawdzalnych informacji, że strona jest niewiarygodna i nie należy powierzać jej żadnych środków. Strona postawiona jest w WordPress na bardzo oklepanym szablonie gdzie dla większości oszukańczych stron inwestycyjnych jest prawie taki sam układ strony.



34. Grafika – komentarze w Google – źródło materiały pokonferencyjne 21–23.09.2021 r. Gdynia

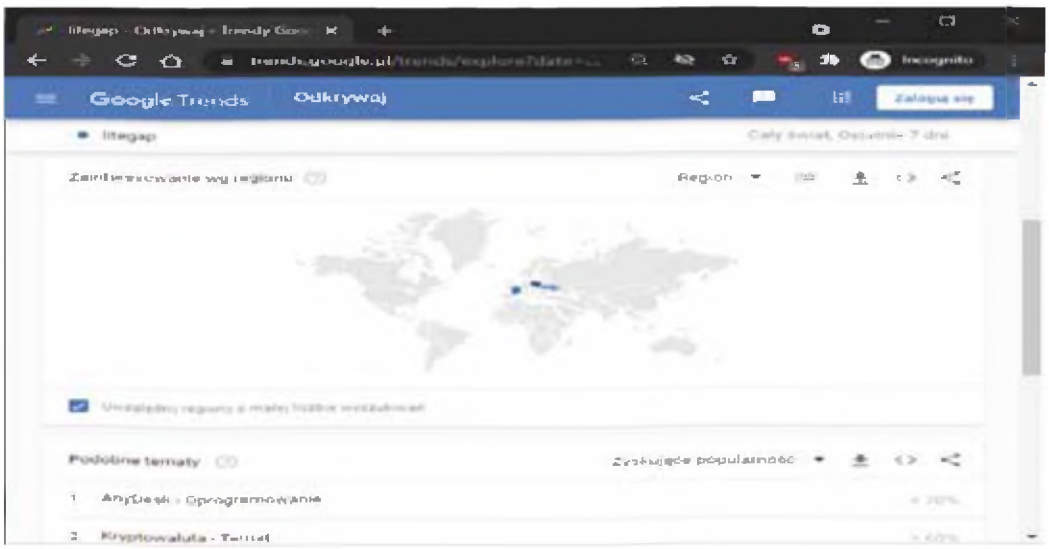


35. Grafika – komentarze w Google – źródło materiały pokonferencyjne 21–23.09.2021 r. Gdynia



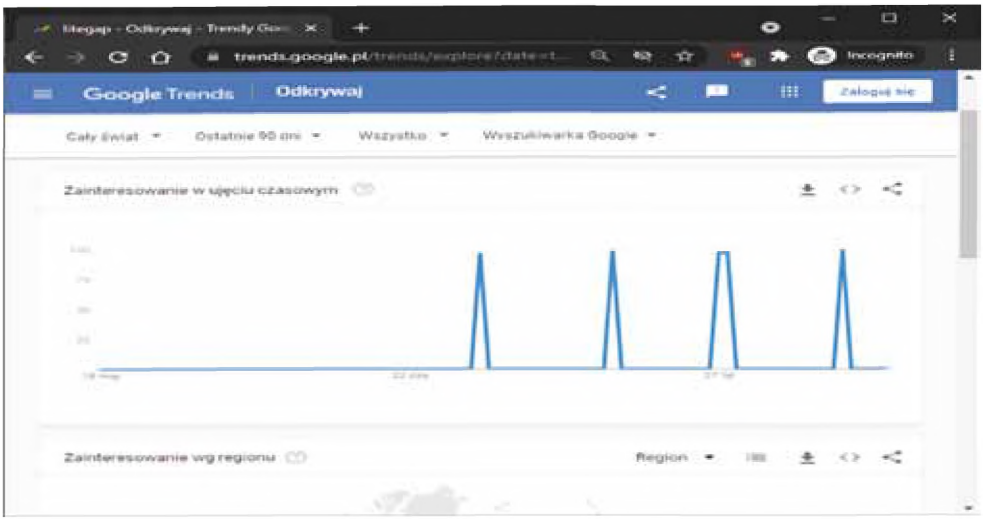
36. Trustpilot – opis metody oszustwa wpisany przez oszukanego klienta https://www.trustpilot.com/review/litegap.com?languages=pl (dostęp 10.06.2025 r.)

Jak widać LiteGap wyszukiwany był za pomocą Google we Francji, Polsce oraz na Ukrainie. Na tej podstawie można ustalić, gdzie były prowadzone prawdopodobne kampanie reklamowe, a co za tym idzie w obrębie jakiego kraju możemy mieć pokrzywdzonych.



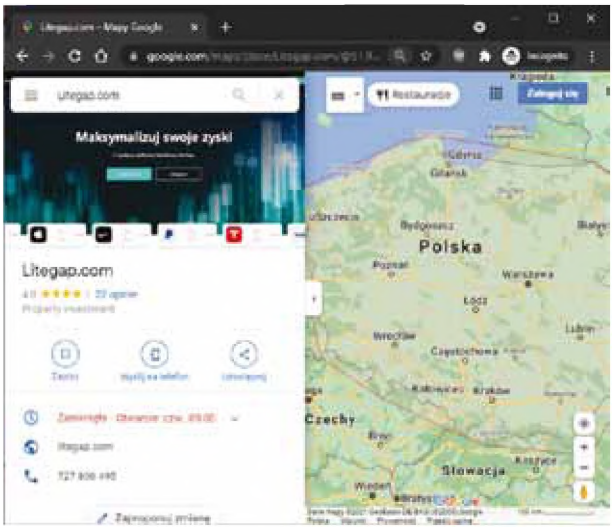
37. Grafika – wyszukiwania w Google Trends
– źródło materiały pokonferencyjne 21–23.09.2021 r. Gdynia

Na podstawie zainteresowania można zauważyć przeprowadzane kampanie marketingowe.



38. Grafika – wyszukiwania w Google Trends
– źródło materiały pokonferencyjne 21–23.09.2021 r. Gdynia

W wyniku prostego wyszukiwania można też było ustalić numer telefonu 727 806 495, który był podpięty pod LiteGap.com w Google.



39. Grafika – wyszukiwania w Google – telefon
– źródło materiały pokonferencyjne 21-23.09.2021 r. Gdynia

Analizując oszukańczą stronę inwestycyjną można zebrać sporo danych z pułapu zwykłego użytkownika. Analiza organów ścigania zapewne była głębsza i bardziej efektywna bo wsparta o ustalenia telekomunikacyjne i internetowe, jakie są dostępne dla służb. Jak nasz pokrzywdzony zarejestrował się na oszukańczej stronie to czas przejść do kolejnych etapów.

Rejestracja konta na giełdzie kryptowalut

Skoro inwestycje mają być w kryptowaluty to jakoś trzeba je zdobyć. Po przejęciu konta w banku środki klienta czekają na przelew. Do tego potrzebny jest podmiot świadczący usługi w wymianie walut fiducjarnych na krypto. Może to być giełda kryptowalut lub kantor, ewentualnie operator płatności obsługujący takie podmioty. Klient dostaje zlecenie na założenie konta na swoje dane w podmiocie świadczącym usługi kryptowalutowe. Z uwagi na fakt, że wszystkie podmioty krypto działają w reżimie AML weryfikacji nie można zrobić łatwo za klienta. Przy procedurze poznaj swojego klienta (KYC) podmioty mają obowiązek korzystać z narzędzi, które podczas robienia zdjęcia lub filmiku podczas procesu KYC stosują tzw. próbę żywotności. Uniemożliwia to w praktyce zrobienie weryfikacji ze zdjęcia. Klient sam musi pokazać się do kamery. W praktyce najczęściej odbywa się to tak, że klient po przeprowadzonej weryfikacji oddaje dane do logowania swoim „doradcom inwestycyjnym". Ci mając pełen dostęp do konta mogą swobodnie realizować każdą operację. Używając popularnego określenia „system został domknięty" czas na przejście do kolejnego etapu.

Wypłata środków na oszukańczą stronę inwestycyjną

Na początku proces „inwestycji" rozpoczyna się od uiszczenia przez ofiarę tzw. opłaty wstępnej lub rejestracyjnej, która zwykle wynosi około 250 dolarów bądź euro. Pieniądze te trafiają bezpośrednio na rachunek wskazany przez oszustów albo są wpłacane poprzez proces rejestracyjny prowadzony na pozornie legalnej, regulowanej giełdzie – z której rzekomo będzie można później wypłacić środki w kryptowalucie.

Pomimo że banki i giełdy kryptowalut wdrażają różne procedury zabezpieczające przed tego rodzaju oszustwami, osoby zmanipulowane wizją łatwego i dużego zysku stają się odporne na ostrzeżenia i nie dostrzegają zagrożenia.

Dzięki zainstalowanemu oprogramowaniu zdalnego dostępu, przestępcy mogą obserwować aktywność na komputerze i znają dokładnie sytuację finansową ofiary. Co gorsza, dostęp ten bywa ciągły i nieograniczony, co daje im pełną kontrolę. Mając dostęp do konta bankowego i konta założonego na giełdzie kryptowalut lub kantorze sprawcy wykonują przelew z bankowości elektronicznej samodzielnie albo zlecają ten przelew pokrzywdzonemu. Na pierwszym etapie „inwestycji" jest on podatny na

perswazję i wykonuje przelewy sam. Ewentualnie autoryzuje je za pomocą kodów czy smsów. Znane mi są też przypadki, że po dostaniu się do bankowości elektronicznej i po stwierdzeniu, że ofiara nie ma na koncie dużo środków, cyberprzestępcy uruchamiali (często bez wiedzy ofiary) kredyt w koncie i ten był przelewany do podmiotu świadczącego usługi kryptowalutowe. Pokrzywdzony dostawał informację, że wypłacone przez niego środki po zamienieniu na kryptowalutę trafiały na konta oszukańczej strony inwestycyjnej. I co do zasady po uruchomieniu przelewu kwota odpowiadająca przelewowi „księgowała" się na koncie pokrzywdzonego na oszukańczej stronie inwestycyjnej. Było to jednak tylko elektroniczne odwzorowanie wartości nieodpowiadające rzeczywistości. Śledząc wykonywane w kryptowalutach transakcje widać, że przelewy środków są kierowane na inne giełdy kryptowalut niemające nic wspólnego z oszukańczą stroną inwestycyjną. Przesłane tam środki poddawane są procesowi prania pieniędzy i w konsekwencji wyprowadzeniem kryptowalut z systemu tak, aby uniemożliwić ich zatrzymanie. Natomiast „elektroniczne odwzorowanie wartości" na oszukańczej stronie inwestycyjnej żyje swoim życiem, generuje „zyski", które w tabelkach i na wykresach objawiają się pokrzywdzonemu.

Kontynuowanie „inwestycji"

Przez cały czas „doradca inwestycyjny" w sposób bardzo profesjonalny utrzymuje kontakt z pokrzywdzonym, przedstawiając mu wizje coraz większych zysków. Po wpłacie początkowej następuje intensyfikacja kontaktów z oszustami – przez tygodnie, a czasem nawet miesiące, nakłaniają oni swoje ofiary do coraz większych wpłat, aż w końcu zachęcają do zaciągania kredytów. Kiedy sprawcy oceniają, że nie są w stanie już wyciągnąć więcej pieniędzy od pokrzywdzonego albo domaga się on wypłaty środków przestają być mili i uprzejmi. W sytuacji kiedy klient chce wypłacić środki, pojawia się żądanie wpłaty „podatku". Sprawcy powołując się na wyimaginowane przepisy podatkowe uzależniają wypłatę od zapłacenia wspomnianego podatku. Ukierunkowane to jest na wyłudzenie kolejnych sum od pokrzywdzonego. Stwarzając takie sytuacje zdają sobie sprawę, że ofiara nie rokuje już na dalsze wpłaty i dlatego jest to niejako ostatnia próba wyłudzenia środków. W zależności od reakcji pokrzywdzonego kontakt albo jest utrzymywany albo oszuści zrywają kontakt z wyłączeniem dostępu do oszukańczej strony inwestycyjnej. Bywa tak, że strona jest wyłączana w wyniku działania służb – Policji, Prokuratury albo właściwego regulatora – w polskim przypadku KNF. I na tym historia inwestycji w zasadzie powinna się zakończyć.

Odzyskiwanie mienia – ostatni etap

W ostatnich latach pojawiło się wiele kancelarii prawnych i firm specjalizujących się w pomocy osobom, które padły ofiarą oszustw inwestycyjnych – zwłaszcza tych związanych z fałszywymi platformami inwestycyjnymi, brokerami czy kryptowalutami.

Niestety, przestępcy często podszywają się pod kancelarie lub firmy odzyskujące środki, oferując „pomoc" za opłatą z góry. To tzw. recovery scam.

„Recovery scam" (czyli oszustwo związane z odzyskiwaniem środków) to wyjątkowo perfidna forma oszustwa, która żeruje na osobach, które już wcześniej padły ofiarą oszustwa finansowego. Przestępcy kontaktują się z takimi osobami, oferując pomoc w odzyskaniu utraconych pieniędzy – oczywiście za opłatą z góry. W rzeczywistości to kolejna próba wyłudzenia pieniędzy.

Jak działa recovery scam?

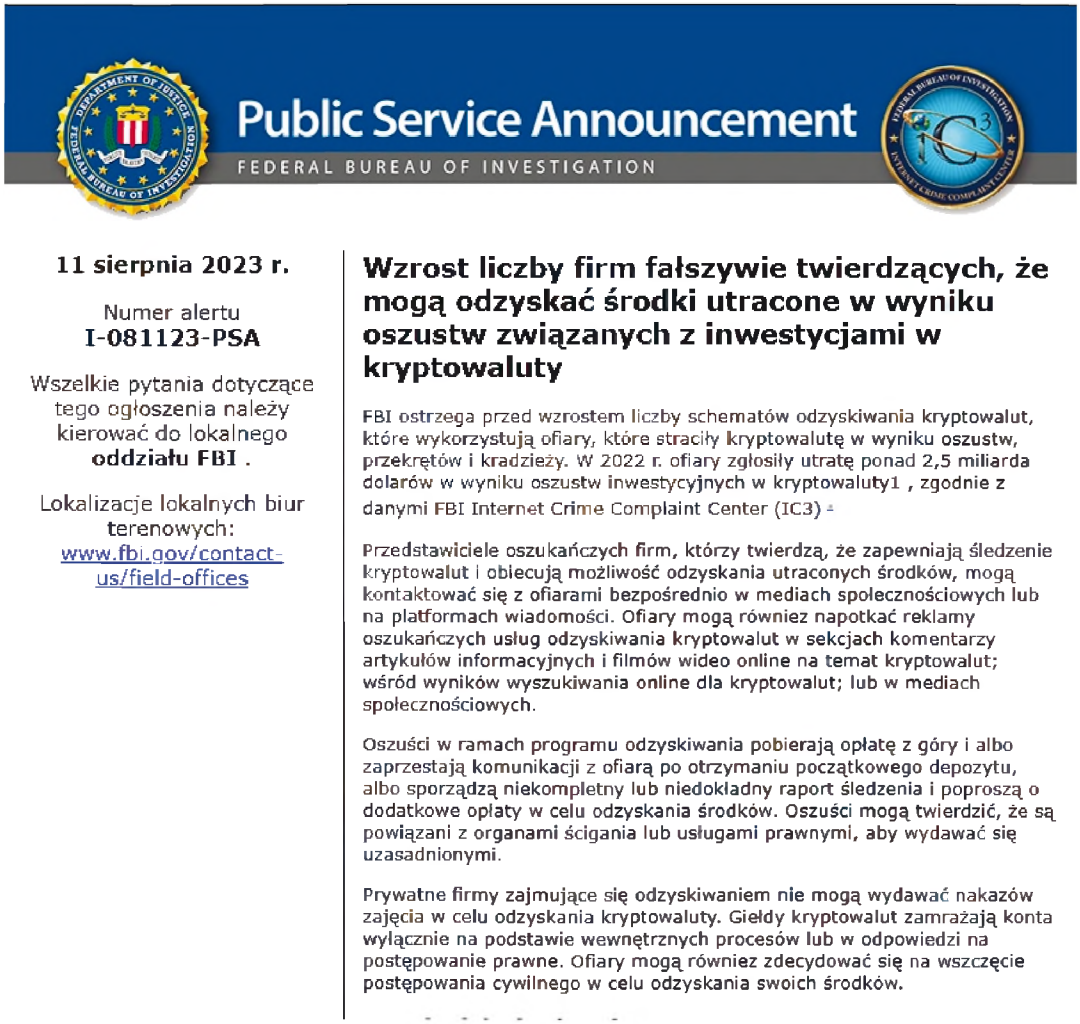
Cyberprzestępcy nawiązują kontakt z ofiarą wcześniejszego oszustwa – sami oszuści często kupują tzw. „listy naiwnych" (ang. sucker lists), czyli dane osób, które już kiedyś zostały oszukane. Często podszywają się pod instytucje – cyberprzestępcy udają pracowników organów nadzoru, kancelarii prawnych, firm windykacyjnych, a nawet organizacji rządowych.

Obiecują odzyskanie pieniędzy – oferują „odzyskanie środków" lub „pomoc prawną" w zamian za opłatę wstępną (np. „prowizję", „opłatę administracyjną"). Po otrzymaniu pieniędzy kontakt się urywa, a ofiara zostaje oszukana po raz drugi.

W mojej ocenie firmy, które oferują usługi odzyskiwania środków z oszustw inwestycyjnych można podzielić na dwie kategorie. Pierwsza to „recovery scam" co do zasady też oszuści ukierunkowani na zwiktymizowanie po raz drugi pokrzywdzonego. Sprawcy podszywają się pod istniejące instytucje bądź tworzą fikcyjne byty. Druga kategoria to firmy, kancelarie występujące pod własną marką, które oferują pomoc prawną i pomoc w odzyskaniu kryptowalut. W swojej dotychczasowej pracy miałem do czynienia z działalnością kancelarii lub firm (bo nie we wszystkich pracują adwokaci czy radcowie prawni) świadczących usługi pomocy prawnej pokrzywdzonym i o ile miałbym oceniać polega to na wysyłaniu pism do banków, giełd kryptowalutowych i instytucji. Pisma te opracowywane są na podstawie jakichś szablonów i co do zasady są mało skuteczne ale dokumentują, że robione jest coś w sprawie klienta. Natomiast twierdzenie, że ktoś pomaga odzyskiwać czy wcześniej śledzić kryptowaluty jest twierdzeniem na tyle nieuprawnionym, że prywatne podmioty – nawet jak to jest renomowana kancelaria prawna – nie mają możliwości zabezpieczenia kryptowalut, bo to może zrobić jedynie organ procesowy. Sama specyfika śledzenia transakcji kryptowalutowych również wymaga pozyskiwania danych z podmiotów świadczących usługi kryptowalutowe, gdyż nawet

jak trafią śledząc jakąś transakcje na giełdę kryptowalut to nie są w stanie pozyskać informacji na temat danych personalnych osoby na konto której trafiły środki, a także uzyskać dane transakcji wyjściowych (co uniemożliwia dalsze śledzenie). Jedynymi podmiotami uprawnionymi do pozyskania tych danych są organy ścigania.

Bardzo trafnie zauważyło to FBI wydając w tej sprawie ostrzeżenia.



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

11 sierpnia 2023 r.

Numer alertu
I-081123-PSA

Wszelkie pytania dotyczące tego ogłoszenia należy kierować do lokalnego **oddziału FBI .**

Lokalizacje lokalnych biur terenowych:
www.fbi.gov/contact-us/field-offices

Wzrost liczby firm fałszywie twierdzących, że mogą odzyskać środki utracone w wyniku oszustw związanych z inwestycjami w kryptowaluty

FBI ostrzega przed wzrostem liczby schematów odzyskiwania kryptowalut, które wykorzystują ofiary, które straciły kryptowalutę w wyniku oszustw, przekrętów i kradzieży. W 2022 r. ofiary zgłosiły utratę ponad 2,5 miliarda dolarów w wyniku oszustw inwestycyjnych w kryptowaluty1 , zgodnie z danymi FBI Internet Crime Complaint Center (IC3)

Przedstawiciele oszukańczych firm, którzy twierdzą, że zapewniają śledzenie kryptowalut i obiecują możliwość odzyskania utraconych środków, mogą kontaktować się z ofiarami bezpośrednio w mediach społecznościowych lub na platformach wiadomości. Ofiary mogą również napotkać reklamy oszukańczych usług odzyskiwania kryptowalut w sekcjach komentarzy artykułów informacyjnych i filmów wideo online na temat kryptowalut; wśród wyników wyszukiwania online dla kryptowalut; lub w mediach społecznościowych.

Oszuści w ramach programu odzyskiwania pobierają opłatę z góry i albo zaprzestają komunikacji z ofiarą po otrzymaniu początkowego depozytu, albo sporządzą niekompletny lub niedokładny raport śledzenia i poproszą o dodatkowe opłaty w celu odzyskania środków. Oszuści mogą twierdzić, że są powiązani z organami ścigania lub usługami prawnymi, aby wydawać się uzasadnionymi.

Prywatne firmy zajmujące się odzyskiwaniem nie mogą wydawać nakazów zajęcia w celu odzyskania kryptowaluty. Giełdy kryptowalut zamrażają konta wyłącznie na podstawie wewnętrznych procesów lub w odpowiedzi na postępowanie prawne. Ofiary mogą również zdecydować się na wszczęcie postępowania cywilnego w celu odzyskania swoich środków.

40. Ostrzeżenie FBI https://www.ic3.gov/PSA/2023/PSA230811 (dostęp 10.06.2025 r.)

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Numer alertu: I-062424-PSA
24 czerwca 2024 r.

Fikcyjne kancelarie prawne atakujące ofiary oszustw kryptowalutowych oferujące odzyskanie środków

Federalne Biuro Śledcze (FBI) wydaje to ogłoszenie, aby poinformować opinię publiczną o nowej taktyce przestępczej wykorzystywanej do dalszego oszukiwania ofiar oszustw kryptowalutowych. Niniejsze PSA jest aktualizacją Alert Number I-081123-PSA, opublikowanego 08/11/2023, zatytułowanego „ Wzrost liczby firm fałszywie twierdzących o możliwości odzyskania środków utraconych w oszustwach inwestycyjnych w kryptowaluty ".

Korzystając z mediów społecznościowych lub innych platform do przesyłania wiadomości, oszuści podszywający się pod prawników reprezentujących fikcyjne kancelarie prawne mogą kontaktować się z ofiarami oszustw i oferować swoje usługi, twierdząc, że mają upoważnienie do badania spraw odzyskiwania funduszy. Aby potwierdzić kontakt, „prawnicy" twierdzą, że współpracują z FBI, Consumer Financial Protection Bureau (CFPB) lub inną agencją rządową lub otrzymali od nich informacje na temat sprawy ofiary oszustwa. W niektórych przypadkach ofiary oszustw kontaktowały się z oszustami na fałszywych stronach internetowych, które wydają się legalne, mając nadzieję na odzyskanie swoich funduszy.

Aby udoskonalić oszustwo związane z odzyskiwaniem pieniędzy, „prawnicy" mogą:

- Poproś ofiary o potwierdzenie swojej tożsamości poprzez podanie danych osobowych lub danych bankowych, aby odzyskać pieniądze;
- Poproś ofiary o podanie kwoty wyroku, której domagają się od pierwotnego oszusta;
- Poproś ofiary o zapłatę części opłat początkowych z góry, a resztę należności zapłać po odzyskaniu środków;
- Nakazać ofiarom zapłatę zaległych podatków i innych opłat w celu odzyskania środków; lub
- Odwołaj się do rzeczywistych instytucji finansowych i kantorów wymiany walut, aby zbudować wiarygodność i rozwijać ich programy.

Według Centrum Zgłaszania Przestępstw Internetowych FBI (IC3) między lutym 2023 r. a lutym 2024 r. ofiary oszustw kryptowalutowych, które padły ofiarą fikcyjnych kancelarii prawnych, odnotowały straty o łącznej wartości ponad 9,9 mln dolarów.

41. Ostrzeżenie FBI https://www.ic3.gov/PSA/2024/PSA240624 (dostęp 10.06.2025 r.)

Zakończenie

Oszustwa inwestycyjne XXI wieku to inteligentnie zaprojektowane pułapki emocjonalno- finansowe, które żerują na ludzkiej chciwości, samotności i niewiedzy, a ich skala i poziom zaawansowania sprawiają, że stają się jednym z największych wyzwań współczesnego cyberbezpieczeństwa.

Ekosystem rynku kryptowalut ulega nieustannym zmianom. Ewoluują też przestępcze metody dostosowując się do nowych technologii, a co najgorsze wykorzystując je w sposób z jakim do tej pory nie mieliśmy do czynienia.

Państwa i organy regulacyjne starają się dostosować przepisy nie tylko rynku kryptowalut, ale także bankowe tak aby inwestorzy byli bardziej chronieni, a cały system finansowy będzie musiał dostosować model swoich zachowań do sytuacji adekwatnych do zagrożeń opisanych w tym artykule. Nie bez znaczenia jest też podejście do tematu organów ścigania, które jak wspomniałem mają sporo do zrobienia ażeby sprostać eskalującemu zagrożeniu. Zresztą należy tu patrzeć szeroko bo oprócz oszustw inwestycyjnych inne cyberprzestępstwa również wymagają przygotowania zawodowego i reakcji.

Celem artykułu było ustalenie, jaką skalę zagrożeń niesie zjawisko oszustwa inwestycyjnego oraz przedstawienie jak ono przebiega i jakie mechanizmy powodują, że jest ono takim zagrożeniem. Tego typu ataki są i będą się pojawiać w coraz to nowych odsłonach i coraz bardziej wyrafinowane. Ze względu na rozwój technologii społeczeństwo, instytucje finansowe oraz organy ścigania muszą być przygotowane na nowe metody przestępców, ale co istotne podejmować współpracę w tym zakresie. Czas na szerokie partnerstwo publiczno-prywatne.

Bibliografia

1. J. Kosiński.: Paradygmaty cyberprzestepczosci Wydawnictwo DIFIN Warszawa 2015.
2. Bentyn S., Grzybkowski M.: Kryptowalut, Dlaczego jeden bitcoin wart będzie milion dolarów?. Poznań: Wydawnictwo: Crypto-logic 2018.
3. P. Rodwald.: Kryptowaluty z perspektywy informatyki śledczej Gdynia 2021.
4. Zob. Steciak M., Szymański P., Boroszko K., Zwalczanie nielegalnych działań w zakresie pośredniczenia w transakcjach finansowych przez zorganizowane grupy przestępcze wykorzystujące mechanizm zdalnego pulpitu. Modus operandi działania sprawców [w:] J. Kosiński, R. Janczewski (red.), Przestępczość teleinformatyczna 2021, Gdynia, 2022 s. 72.

Raporty i analizy

1. Chainalysis: The 2025 Crypto Crime Report. Nowy Jork: Chainalysis, 2025.
2. ComplyAdvantage: The State of Financial Crime 2024, Londyn: ComplyAdvantage, 2024.
3. Elliptic: Typologies Report 2023 – Preventing Financial Crimein Cryptoassets, Londyn: Elliptic Enterprises Limited, 2023.
4. Raport opracowany przez iKsync oraz Uniwersytet Ekonomiczny w Krakowie: Polak Inwestor 2023, Kraków: iKsync, 2023.
5. Raport opracowany przez Łukasik K, Witczak J, Polski Instytut Ekonomiczny w Warszawie: Popularność kryptowalut w Polsce, Warszawa 2023.
6. Raport CERT Orange Polska za rok 2024.
7. INTERPOL Globalna ocena oszustw finansowych 2024 Lyon.
8. Raport Roczny CSIRT KNF 2024.
9. Raport Roczny 2024 z działalności CERT Polska.

Źródła internetowe

1. Urząd Komisji Nadzoru Finansowego: Encyklopedia Cyberbezpieczeństwa. Fałszywe inwestycje. 2022 [online], https://cebrf.knf.gov.pl/encyklopedia-cyberbezpieczenstwa/schematy-oszustw/falszywe-inwestycje [dostęp: 14.06.2025r.].
2. Centralne Biuro Zwalczania Cyberprzestępczości: Oszustwa związane z fałszywymi inwestycjami. 2023 [online], https://cbzc.policja.gov.pl/bzc/zagrozenia-w-sieci/106,Oszustwa-zwiazane-z-falszywymi-inwestycjami.html [dostęp: 14.06.2025r.].
3. Public Service Announcemenent – Federal Bureau of Investigation (FBI): Cryptocurrency Investment Schemes. 2022, [online], https://www.ic3.gov/Media/Y2022/PSA221003 [dostęp: 10.06.2025r.].
4. https://www.statista.com/statistics/863917/number-crypto-coins-tokens/.
5. https://www.triple-a.io/cryptocurrency-ownership-data (dostęp 14.06.2025).
6. https://crypto.com/en/research/2023-review-2024-ahead (dostęp 10.06.2025).
7. https://cebrf.knf.gov.pl/deepfake. (dostęp 10.06.2025).
8. https://cryps.pl/ostrzezenie/uwaga-na-kryptowalutowe-oszustwa-na-tinderze/ (dostęp 10.06.2025).
9. https://forexrev.pl/belgijskie-fsma-uwaga-na-oszustwa-na-tinderze/ (dostęp 10.06.2025).
10. https://www.youtube.com/watch?v=QMdnfJveOaU (dostęp 10.06.2025).
11. https://www.knf.gov.pl/dla_konsumenta/kampanie_informacyjne/cyberoszustwa_inwestycyjne/schematy_oszustw/oszustwa_inwestycyjne (dostęp 10.06.2025).
12. https://www.trustpilot.com/review/litegap.com?languages=pl (dostęp 10.06.2025).

13. https://www.ic3.gov/PSA/2024/PSA240624 (dostęp 10.06.2025).
14. https://www.ic3.gov/PSA/2023/PSA230811 (dostęp 10.06.2025).
15. https://bezpiecznymiesiac.pl/bm/baza-wiedzy/1232,Oszustwa-inwestycyjne.html?utm_source=perplexity (dostęp 10.06.2025).
16. https://www.knf.gov.pl/dla_konsumenta/kampanie_informacyjne/cyberoszustwa_inwestycyjne/schematy_oszustw/oszustwa_inwestycyjne (dostęp 10.06.2025).
17. https://zbp.pl/Aktualnosci/Wydarzenia/Cyberbezpieczenstwo-eksperyment-spoleczny (dostęp 10.06.2025).
18. (https://cert.pl/uploads/docs/Raport_CP_2024.pdf#page=39) (dostęp 10.06.2025).
19. https://businessinsider.com.pl/kryptowaluty/oszustwo-na-kryptowaluty (dostęp 10.06.2025).

Grzegorz Matyniak[1]

Czy biegły jest od wykrywania sprawców i z czego to może wynikać?

Streszczenie

Artykuł dotyka problemów związanych z powoływaniem biegłych, w szczególności z zakresu informatyki śledczej i analizy kryminalnej. Oprócz pojęcia biegłego sądowego oraz ciążących na nim podstawowych obowiązków wynikających z *Kodeksu postępowania karnego*, przedstawione zostały przykładowe pytania, z jakimi spotkałem się w trakcie swojej działalności biegłego. Wskazano, jakiego rodzaju pytania związane z informatyką śledczą mogą być wykorzystane w postanowieniu o powołaniu, jak również nieliczne przypadki pytań, które nie powinny w nim się pojawiać. Wskazano też czynności – niejednokrotnie pomniejszające koszty postępowania – jakie powinny być wykonane przez organy ścigania przed podjęciem decyzji o powołaniu biegłego.

Słowa kluczowe: biegły, organ ścigania, organ procesowy, pytania do biegłych

Biegły – co to za mistyczny stwór?

Biegły sądowy – bo o nim będziemy tym razem rozprawiać – to ekspert w danej dziedzinie, posiadający specjalną wiedzę teoretyczną i bogate doświadczenie zawodowe, powoływany w postępowaniu sądowym w celu przedstawienia fachowej opinii o okolicznościach mających znaczenie dla wyroku sprawy sądowej, a których wyjaśnienie wymaga specjalistycznej wiedzy.

Wymaga się od niego nie tylko posiadania niekwestionowanej wiedzy i najwyższych kwalifikacji zawodowych (art. 193 §1 i 2, art. 195 oraz art. 200 §2 pkt 1 *Kodeksu postępowania karnego* i art. 278 §1 oraz art.290–291 *Kodeksu postępowania karnego*), ale również zaufania publicznego, sumienności i bezstronności (art. 196 §3 i art. 197 §1 *Kodeksu postępowania karnego* oraz art. 282 §1 *Kodeksu postępowania cywilnego*). Ponadto wymagane jest zaufanie sądu do osoby biegłego (art. 198 §1 *Kodeksu postępowania karnego* i art. 284 *Kodeksu postępowania cywilnego*).

Na osobie biegłego ciążą obowiązki, które przedstawię poniżej (oczywiście są to tylko niektóre, wybrane subiektywnie przeze mnie):

- wydania opinii – gdyż biegły nie może odmówić wydania opinii w okręgu sądu okręgowego, przy którym został ustanowiony, zleconych przez sąd lub organ

[1] Grzegorz Matyniak – emerytowany oficer Policji, biegły sądowy Sądu Okręgowego w Krośnie z zakresu informatyki śledczej i analizy kryminalnej, nauczyciel akademicki Uczelnia Państwowa im. Jana Grodka w Sanoku.

prowadzący postępowanie przygotowawcze w sprawach karnych, z wyjątkiem wypadków określonych w przepisach regulujących postępowanie przed tymi organami (art. 196 §1 *Kodeksu postępowania karnego*);
- wydania opinii we wskazanym przez organ procesowy terminie;
- wydania opinii bezstronnej, zgodnie z obowiązującym stanem wiedzy w danej dziedzinie;
- wydania opinii jasnej, pełnej, pozbawionej wewnętrznych sprzeczności:
  a) JASNEJ (sformułowania pozwalają na zrozumienie wyrażonych w niej ocen i poglądów, a także sposobu dochodzenia do nich albo też wyjaśnia używaną w niej niezrozumiałą dla przeciętnego człowieka fachową terminologię oraz niezawierającej dwuznacznych sformułowań);
  b) PEŁNEJ (zawierającej udzielenie odpowiedzi na wszystkie postawione pytania, uwzględniającej wszystkie istotne dla rozstrzygnięcia konkretnej kwestii okoliczności oraz zawierającej uzasadnienie wyrażonych ocen lub poglądów);
  c) POZBAWIONEJ WEWNETRZNYCH SPRZECZNOŚCI (występują sprzeczności między wnioskami końcowymi opinii a jej treścią, tzn. treść opinii przy zastosowaniu zasad logicznego myślenia w żadnym wypadku nie mogłaby doprowadzić do podanych wniosków końcowych);
- zachowania w tajemnicy informacji niejawnych lub uzyskanych z postępowania przygotowawczego, zanim zostaną one ujawnione w postępowaniu sądowym.

Ale jak zauważamy, nie ma nic na temat tego, że biegły ma obowiązek ustalenia sprawcy lub wskazania chociażby podejrzanego, gdyż te ustalenia są celem postępowania przygotowawczego i de facto należą do obowiązków organów ścigania lub organu procesowego prowadzącego dane postępowanie przygotowawcze (art. 297 §1 pkt 2 *Kodeksu postępowania karnego*).

W trakcie prowadzonych postępowań zdarza się niejednokrotnie, że organ procesowy mierzy się z dylematami na temat tego, kiedy skorzystać z pomocy biegłego (czyli wydać postanowienie o jego powołaniu). Przykładowe okoliczności dotyczące przypadków powoływania biegłego wskazuję poniżej:
- okoliczności, które powinny być stwierdzone przez biegłego **muszą mieć istotne znaczenie dla sprawy**, a zatem brak jest podstaw, by dopuścić dowód z opinii biegłego dotyczący kwestii drugorzędnych;
- do stwierdzenia owych istotnych okoliczności mających znaczenie dla rozstrzygnięcia sprawy wymagane są **wiadomości specjalne**;
- **istotne znaczenie dla rozstrzygnięcia sprawy** – to dowody, których przeprowadzenie jest niezbędne z punktu widzenia możliwości przypisania oskarżonemu sprawstwa zarzucanego mu czynu, w tym ustalenia stopnia winy i jej

odcieni, zamiaru, z jakim działał, wysokości szkody wyrządzonej jego działaniem czy okoliczności popełnienia zarzucanego mu czynu;
- **wiadomości specjalne** – obejmują wiadomości faktyczne czy praktyczne (wiedza i doświadczenie), które to wykraczają poza normalną, powszechną wiedzę z uwzględnieniem faktu rozwoju i powszechności.

Zatem niespełnienie wskazanych wyżej powodów zdaje się poważnie utrudniać – a czasami wręcz wykluczać – wydanie postanowienia o zasięgnięciu opinii biegłego. Ale za każdym razem decyzję podejmują organ prowadzący postępowanie i indywidualny referent sprawy.

Pytania do biegłych – koncert życzeń czy może akt rozpaczy?

W swojej dotychczasowej historii zawodowej związanej z funkcją biegłego zdarzały mi się różnego rodzaju pytania ze strony organów procesowych – i nie chodzi w tym miejscu o napiętnowanie ich autorów, lecz raczej o ogólne wskazania, jak formułowane i jakiego rodzaju pytania powinny się ze strony organu procesowego pojawiać. Uważam, że kiedy organ procesowy decyduje się na zasięgnięcie opinii biegłego, powinien po prostu zadać pytanie lub pytania, na które chce uzyskać odpowiedź. Te i tylko te. Wydaje się, że jest to logiczne i zrozumiałe. Uważam, że zadawanie większej ilości pytań, gdy nie ma to uzasadnienia i związku z prowadzonym postępowaniem, jest niepotrzebną stratą czasu zarówno organu, jak i osoby powołanej w charakterze biegłego. Poniżej kilka ogólnych sugestii związanych z zadawaniem pytań do biegłego.
- Pytania kierowane do biegłych powinny być tak sformułowane, aby ich treść nie pozostawiała żadnych wątpliwości co do intencji pytającego (nie mogą to być pytania z zawartą tezą, którą biegły tak naprawdę ma potwierdzić, co często ma miejsce w przypadku adwokatów czy pełnomocników stron, przykładem takich pytań jest pytanie: *Czy zainstalowana na telefonie aplikacja AnyDesk umożliwiała sprawcy dokonanie wszystkich czynności na rachunku bankowym pokrzywdzonego?* Gdy w takim przypadku w materiałach sprawy nie ma informacji o badaniu wskazanego telefonu, nie ma informacji o instalacji wskazanej aplikacji oraz – co chyba najważniejsze – o podaniu przez pokrzywdzonego kodu sparowania między urządzeniami ewentualnemu sprawcy.
- Zadawane pytania są takimi, na które istnieje realna możliwość udzielenia odpowiedzi.
- Zadawane pytania nie mogą wykraczać poza dziedzinę wiedzy, którą reprezentuje biegły *(np. Czy na badanym telefonie znajdują się pliki wideo lub zdjęcia stanowiące pornografię dziecięcą?* – to pytanie wykracza poza zakres wiedzy biegłego z informatyki śledczej czy z analizy kryminalnej, ale z kolei pytanie

łudząco podobne do powyższego o treści: *Czy na badanym urządzeniu znajdują się pliki lub materiały których posiadanie jest zabronione?*, pozwala w choćby części udzielić odpowiedzi na interesujące organ procesowy zagadnienie.

- Pytania, które zadajemy biegłemu, muszą być sformułowane w sposób dla niego zrozumiały (pozwolą Państwo, że uznam, że pytania o długości zdań naszego wybitnego pisarza Henryka Sienkiewicza (cechującego się mocno rozbudowaną i bogatą w szczegóły narracją) nie są dobrym pomysłem).
- Jeżeli zadane pytania powiązane są ze znajomością okoliczności sprawy, to należy umożliwić biegłemu dostęp do akt sprawy (lub chociażby ich części w postaci określonych dokumentów lub ich kopii), w szczególności jeśli mówimy o dokonaniu analizy akt sprawy ze wskazaniem dalszych czynności lub możliwości pozyskania dodatkowych śladów czy dowodów, ewentualnie sugestii biegłego w tym zakresie (mam nadzieję, że Szanowni Czytelnicy zgodzą się ze mną, że opinia biegłego to nie owoc pracy umysłowej opartej wyłącznie na domysłach, przypuszczeniach lub chęci udzielenia odpowiedzi zadowalającej zleceniodawcę).

Poniżej kilka przykładów pytań stawianych biegłym (z zachowaniem pisowni oryginalnej oraz z moim *komentarzem*), które – w mojej ocenie – nie spełniają wskazanych wyżej kryteriów:

- Czy nadesłane do badań urządzenia są sprawne technicznie (mowa o przekazanych do badań telefonach)? – *gdy będą niesprawne, ich badanie najprawdopodobniej nie będzie możliwe.*
- Wskazanie ich typu, ustalenie cech fabrycznych, ujawnienie cech indywidualnych sprzętu pozwalającego na identyfikację właściciela, kont użytkownika – *czy wskazane dane naprawdę są potrzebne w sprawie zabójstwa, kradzieży z włamaniem, oszustwa albo groomingu?*
- Czy na przekazanych do badań urządzeniach utworzone zostały konta użytkownika, a jeżeli tak, to wskazanie ich nazw i dat utworzenia – *można by doprecyzować o jakiego rodzaju konta chodzi zleceniodawcy (konta pocztowe, konta użytkownika w mediach – jakich).*
- Wskazanie rodzaju zainstalowanego systemu operacyjnego, aplikacji ze szczególnym uwzględnieniem przeglądarek internetowych oraz komunikatorów internetowych – *jedyny uzasadniony w moim rozumieniu przypadek tego pytania to sprawdzenie legalności systemu pod kątem posiadania jego nielegalnej kopii, ale czy w pozostałych przestępstwach jest to informacja istotna?*
- Wyszukiwanie informacji w plikach tekstowych, archiwach przeglądarek internetowych, wyszukiwarek internetowych, korespondencji z poczty elektronicznej, komunikatorów internetowych, wiadomości (SMS, RCS, w tym zaszyfrowanych plików), których treść może świadczyć o zdarzeniu związanym

z przestępstwem, planowaniem przestępstwa, narzędziami mogącymi służyć do popełnienia przestępstwa, zacieraniem śladów przestępstwa – *tutaj zlecający badanie chyba poszedł zbyt szeroko, gdyż biegły z zakresu informatyki śledczej nie musi posiadać wiedzy na temat znamion wszystkich przestępstw.*

- Wyszukiwanie materiałów związanych z pornografią, homoseksualizmem, a także treści charakterystycznych – najczęściej internetowych – wskazujących na zainteresowania użytkownika urządzenia – *o ile mogę zgodzić się w części pierwszej pytania (pornografia), to pozostała część budzi już moje wątpliwości.*
- Czy na podstawie analizy zgromadzonego materiału dowodowego możliwe jest określenie: czy w dniu 30.07.2025 r. użytkownik telefonu komórkowego marki Motorola o ustalonym numerze IMEI wraz z kartą SIM o ustalonym numerze abonenckim znajdował się w pobliżu miejsca zdarzenia oznaczonego pomiarem GPS, a wskazanego jako miejsce zdarzenia? Czy możliwe jest wskazanie odległości logowania się w/w urządzenia (telefonu) od wskazanego miejsca? – *w tym przypadku powiedziałbym, że takie rzeczy wiedzą tylko: James Bond (agent 007), za starych czasów porucznik Borewicz, a z tych niedawnych to chyba tylko CSI Miami, Las Vegas lub może CSI Cyber.*
- Czy plik o oznaczeniu BACE0000000012345 znajdujący się w telefonie marki Samsung Galaxy S8 mógł zostać pobrany z Internetu na dysk telefonu podejrzanego „samoczynnie", niezależnie od woli i świadomości podejrzanego, podczas przeglądania przez niego artykułów w sieci w dniu 25.07.2025 r. w godzinach między 15:12 a 18:23?
- Czy osoba o przeciętnej wiedzy z zakresu działania przeglądarek internetowych mogła nie mieć świadomości obecności tego konkretnego pliku w pamięci podręcznej przeglądarki?

– *obydwa wskazane wyżej pytania o wolę i świadomość oraz stan wiedzy informatycznej osoby, której sprzęt zabezpieczono, są skierowane do biegłego z zakresu informatyki śledczej, a raczej powinny być do samego zainteresowanego. Jeżeli zaś chodzi o pytanie o stan wiedzy użytkownika komputera lub telefonu na temat działania technicznego przeglądarek internetowych, to moim zdaniem stan ten jest nikły, by nie powiedzieć, że żaden, gdyż wiedza techniczna (mam na myśli wiedzę specjalistyczną dotyczącą przebiegu procesów w przeglądarce, a nie jak włączyć przeglądarkę i z niej korzystać) nie jest w żaden sposób potrzebna użytkownikowi do korzystania z tych aplikacji, a jej brak nie jest przeszkodą w prawidłowym używaniu.*

- Czy i w jaki sposób doszło do ingerencji w telefon komórkowy lub komputer powoda przez osobę trzecią dla potrzeb uzyskania dostępu do rachunku bankowego powoda za pośrednictwem bankowości elektronicznej oraz czy stosowane

przez użytkownika telefonu programy antywirusowe na urządzeniu mobilnym zapewniały bezpieczeństwo urządzenia? – *bardzo trudne, a wręcz niemożliwe jest udzielenie odpowiedzi na tak postawione pytania, kiedy telefonu lub komputera (innego sprzętu, o którym jest mowa) nie poddano oględzinom, nie zlecono jego badania innemu biegłemu ani też nie przesłano go do badań mającemu wydać opinię w tym przypadku biegłemu. I wcale nie chodzi o fakt negowania złożonych zeznań w tej sprawie przez pokrzywdzonego twierdzącego, że programy były i że były aktualne.*

Podsumowanie

Podsumowując powyższe rozważania, pod rozwagę Szanownych Czytelników (będących referentami sprawy, pełnomocnikami pokrzywdzonych, obrońcami podejrzanych) podaję sugestie co do zasad wykonywania poszczególnych czynności w prowadzonych postępowaniach, jakie – moim zdaniem – mogą jedynie usprawnić lub ułatwić Wam (jako referentom) żmudną niejednokrotnie pracę.

- Prowadźmy sprawę w taki sposób, w jaki chcielibyśmy, aby nas potraktowano (a na marginesie – nie życzę nikomu, by musiał się znaleźć po drugiej stronie w charakterze pokrzywdzonego).
- Zanim zdecydujemy się na powołanie biegłego spróbujmy do niego zadzwonić i krótko powiedzieć, co mamy i czego od niego oczekujemy, czy jest to możliwe do wykonania, by udzielił odpowiedzi na nurtujące nas pytania (a co ważne – czy nurtujące nas pytanie lub pytania są istotne dla prowadzonej przez nas sprawy, czy też zabraliśmy telefon, komputer albo inny jeszcze nośnik elektroniczny i teraz coś trzeba z nim zrobić).
- Zanim zdecydujemy się na zabezpieczenie sprzętu (telefonu, komputera itp.), sami musimy mieć wiedzę albo co najmniej wizję tego, co chcemy tam znaleźć, czy te interesujące nas dane tam się znajdują lub mogą w ogóle się tam znajdować, a nie bądźmy zbieraczami złomu (bo przecież macie dużo spraw i jak zawsze mało czasu).
- Jeżeli już zabieramy sprzęt komputerowy czy telekomunikacyjny, to zapytajmy właściciela o dane umożliwiające dostęp do sprzętu (hasło, kody, wzory) albo jeżeli mamy to urządzenie w dłoni (bo takie przypadki się przecież zdarzają) i jest ono w tym czasie odblokowane, to usuńmy z niego blokady, co pozwoli zaoszczędzić czas i niejednokrotnie niemałe środki finansowe.
- Zabezpieczmy te urządzenia zgodnie z zasadami sztuki w tym zakresie (w taki sposób, techniczny i procesowy, by nikt nie miał możliwości ingerencji w te urządzenia, a co za tym idzie, by nikt nie miał możliwości podważania późniejszych wyników badań czy analiz).

- Jeżeli już zabraliśmy sprzęt i uważamy, że nie będzie na nim danych, śladów przydatnych dla prowadzonej sprawy – to po prostu zróbmy oględziny (do czego organy procesowe bezwzględnie mają prawo) i oddajmy sprzęt właścicielowi.

Na koniec gwoli przypomnienia rzeczy oczywistych wskazuję:

- Postępowanie przygotowawcze **prowadzi lub nadzoruje prokurator, a w zakresie przewidzianym w ustawie prowadzi je Policja**. W wypadkach przewidzianych w Ustawie uprawnienia Policji **przysługują innym organom** (art. 298 §1 *Kodeksu postępowania karnego*).
- **Śledztwo prowadzi prokurator** (art. 311 §1 *Kodeksu postępowania karnego*).
- **Dochodzenie prowadzi Policja** lub prowadzą je organy, o których mowa w art. 312 kpk, chyba że prowadzi je prokurator (art. 325a §1 *Kodeksu postępowania karnego*).
- Minister Sprawiedliwości w porozumieniu z właściwymi ministrami określi, w drodze rozporządzenia, **organy** uprawnione **obok Policji** do prowadzenia dochodzeń oraz organy uprawnione do wnoszenia i popierania oskarżenia przed sądem pierwszej instancji w sprawach, w których prowadzono dochodzenie, jak również zakres spraw zleconych tym organom, mając na uwadze określony przez ustawę zakres kompetencji tych organów (art. 325d *Kodeksu postępowania karnego*).
- **Jeżeli dokonanie oględzin**, przesłuchania przy użyciu urządzeń technicznych umożliwiających przeprowadzenie tej czynności na odległość, eksperymentu, ekspertyzy, zatrzymania rzeczy lub **przeszukania wymaga czynności technicznych, w szczególności takich jak wykonanie pomiarów, obliczeń, zdjęć, utrwalenie śladów, można do udziału w nich wezwać specjalistów** (art. 205 §1 *Kodeksu postępowania karnego*). *Ale czy biegły to specjalista?*

Jak widzimy powyżej, nie ma nigdzie w kodeksie postępowania karnego ani innych kodeksach dyspozycji, zaleceń, informacji dotyczących prowadzenia postępowań lub wykonywania wskazanych czynności mowy o biegłym – czy uważają Państwo, że nadszedł czas, by to zmienić?

Literatura:

1) Gruza Ewa, *Co biegły miał na myśli, czyli refleksje o języku opinii biegłych*, [w:] *Nauka wobec prawdy sądowej*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2005.
2) Habzda-Siwek Ewa, *Kwalifikacje do pełnienia funkcji biegłego – zarys problematyki*, [w:] *Iure et facto: księga jubileuszowa ofiarowana doktorowi Józefowi Gurgulowi*, Instytut Ekspertyz Sądowych, Kraków 2006.

3) Jaworski Ryszard, Szostak Maciej (red.), *Nauka wobec prawdy sądowej. Księga pamiątkowa ku czci profesora Zdzisława Kegla*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2005.
4) Kalinowski Stefan, *Biegły i jego opinia*, Warszawa 1994.
5) Koop I., *Kompetencje biegłego*, [w:] *Biegły w sądzie*, Wydawnictwo Instytutu Ekspertyz Sądowych, Kraków 2006.
6) Locard Edmond, *Dochodzenie przestępstw według metod naukowych*, Łódź 1937.
7) Pikulik Arkadiusz, *Obowiązki organu procesowego w przyjęciu pisemnej albo ustnej opinii biegłego*, „Problemy Współczesnej Kryminalistyki" 2010, t. XV.
8) Piotrowska Irena., *Pozycja i rola biegłego sądowego w świetle oczekiwań organu procesowego*, „Arch. Med. Sąd. Krym." 2007, LVII, s.196–199.
9) Powszek Artur, Powszek Władysław, *By biegli byli biegli. Poradnik dla biegłych sądowych i prawników*, cz. 1 i 2, Wydawnictwo Difin.
10) Rozporządzenie Ministra Sprawiedliwości z dnia 18 czerwca 2019 r., *Regulamin urzędowania sądów powszechnych* (tekst jednolity).
11) Rozporządzenie Ministra Sprawiedliwości z dnia 24 stycznia 2005 r. w sprawie biegłych sądowych.
12) Sehn Jan, *Dowód z biegłych w postępowaniu sądowym*, „Nowe Prawo" 1956, nr 3.
13) Ustawa z dnia 17 listopada 1964 r. *Kodeks postępowania cywilnego* (§278–291).
14) Ustawa z dnia 27 lipca 2001 r. *Prawo o ustroju sądów powszechnych*.
15) Ustawa z dnia 6 czerwca 1997 r. *Kodeks postępowania karnego* (§193–203, §318).

Wojciech Pilszak[1]

Otwarte źródła informacji jako wsparcie inwigilacji realizowanej w środowisku cyfrowym

Streszczenie

Publikacja omawia możliwości wykorzystania otwartych źródeł informacji w toku działań inwigilacyjnych prowadzonych przez instytucje uprawnione, w tym służby specjalne. Oprócz definicji inwigilacji i rozszerzonej na potrzeby niniejszego opracowania definicji danych otwartoźródłowych, przedstawione zostały możliwości wykorzystania otwartych źródeł informacji w toku czynności operacyjnych prowadzonych w środowisku cyfrowym, zarówno w zakresie rozpoznania przed właściwą inwigilacją, niezależnie od stosowania innych narzędzi oraz jako wsparcie i uzupełnienie informacji pozyskiwanych przy wykorzystaniu innych rozwiązań. Zasygnalizowana została także konieczność dokumentowania uzyskanych wyników oraz podjęto próbę określenia granic inwigilacji prowadzonej w środowisku cyfrowym.

Słowa kluczowe: Inwigilacja, otwarte źródła informacji, wykorzystanie danych cyfrowych, Internet.

Kiedy rozpoczynałem pracę nad niniejszą publikacją, w przestrzeni medialnej pojawiły się informacje o zawieszeniu prac nad Ustawą – Kodeks Pracy Operacyjnej[2]. Pomimo różnego rodzaju „ułomności", jakie możemy znaleźć w projekcie tego aktu prawnego, prace nad nim miały jedną bardzo istotną zaletę – miał on ująć w oficjalne ramy prawne całość pracy operacyjnej, rozrzuconej do tej pory w różnego rodzaju regulacjach o charakterze niejawnym, odrębnym dla każdej ze służb. Na dzień dzisiejszy to, jakie działania w stosunku do obywatela mogą podjąć różnego rodzaju służby państwowe, w tym te o charakterze specjalnym, jest dla większości społeczeństwa niejasne, co prowadzi do takich patologii jak osławiona „Afera Pegasusa"[3], w której bardzo specjalistyczne i dedykowane do pozyskiwania informacji o najcięższych kategoriach przestępstw oprogramowanie, wykorzystywane było – bardzo delikatnie rzecz ujmując – do szpiegowania aktualnej opozycji politycznej, lub osób z różnych powodów niewygodnych dla rządzących. Patrząc wstecz, postulaty dotyczące konieczności ujawnienia form i metod prowadzenia czynności

[1] Wojciech Pilszak – emerytowany oficer Policji, e-Detektywi sp. z o.o. / Pilszak Consulting, ORCID ID: 0009-0004-4439-6403, kontakt z Autorem: wojciech.pilszak@e-detektywi.pl.

[2] https://www.rp.pl/sluzby/art41579741-nie-bedzie-kodeksu-pracy-operacyjnej-rzad-wprowadza-obostrzenia-dla-sluzb-przez-rozporzadzenia – ostatni dostęp 16.02.2025 r.

[3] https://pl.wikipedia.org/wiki/Afera_Pegasusa – ostatni dostęp 16.02.2025 r.

operacyjno-rozpoznawczych były formułowane już w latach 90-tych ubiegłego wieku, między innymi przez prof. Tadeusza Hanauska. Do dnia dzisiejszego, temat ten jest skutecznie pomijany lub bagatelizowany w pracach legislacyjnych prowadzonych przez różnego rodzaju gremia powoływane przez polityków, niezależnie od opcji, której akurat obywatele powierzyli misję kierowania krajem. Tadeusz Hanausek formułował bardzo racjonalną tezę, iż społeczeństwo powinno posiadać możliwość zapoznania się z informacjami, jakiego rodzaju rozwiązania mogą być przeciwko niemu użyte i w jakich granicach, natomiast wiedza o tym, wobec kogo te rozwiązania są aktualnie używane powinna pozostawać niejawna i być domeną służb je stosujących. Wskazywał on, iż są kraje, które te zagadnienia regulują w wewnątrzresortowych instrukcjach o charakterze zazwyczaj tajnym lub poufnym. Nie jest to rozwiązanie najlepsze, gdyż jak jeszcze w roku 1764, pisał jeden z czołowych myślicieli Oświecenia C. Beccaria „Jeżeli władza postępować będzie samowolnie, nie zaś zgodnie z prawami ustanowionymi w kodeksie, który jest dostępny dla wszystkich obywateli, to wtedy stanie otworem droga do tyranii, która rozciąga się po wszystkie granice wolności politycznej". Dlatego znacznie lepszym rozwiązaniem wydaje się unormowanie realizacji zakresu i sposobu realizacji czynności operacyjno-rozpoznawczych w ogólnie dostępnym akcie prawnym[4]. Jak można zauważyć, pomimo upływu lat, teza ta nadal pozostaje aktualna, a niedawne wydarzenia pokazują, jak bardzo konieczne jest precyzyjne i ostre określenie granic w jakich mogą poruszać się wszelkiego rodzaju służby – nie tylko specjalne – w ramach realizacji nałożonych na nie ustawowo obowiązków. W szczególności, wydaje się, iż niezbędne będzie ponowne wprowadzenie, nie tyle do słownika pojęć – tam ten termin znajduje się od dawna – ale do regulacji prawnych, określających działania służb państwowych mogących ingerować w bardzo głębokie obszary prywatności, terminu „inwigilacja" wraz z precyzyjnym określeniem jej zasad i okoliczności, w jakich może ona być stosowana. Zrozumiałym jest, iż dla części obecnych polityków, wywodzących się jeszcze z czasów opozycji w PRL może to być pewnego rodzaju przeżycie traumatyczne, ale nie regulując tego obszaru działalności służb, byłe ofiary zaczynają zajmować stanowisko podobne ich oprawcom. Brak klarowności systemu prawa, może służyć – jak pokazały niedawne doświadczenia – wykorzystywaniu bardzo niebezpiecznych dla wolności obywatelskich rozwiązań, w kontekście partykularnych interesów jednej, aktualnie rządzącej, opcji światopoglądowo-politycznej. A ponieważ, jak napisał John Acton, a po nim wielu, wielu innych: „każda władza deprawuje, a władza absolutna deprawuje absolutnie"[5],

[4] Tadeusz Hanausek, Kryminalistyka: Poradnik detektywa, Biuro Wydawnictw Prawniczych „Polbod", Katowice 1993, s. 94.

[5] John Acton, List do biskupa Mandella Creightona, 3 kwietnia 1887.

przypuszczać można, iż zawsze może pojawić się chęć do wykorzystania rozwiązań jakie oferował „uskrzydlony koń" i wiele innych podobnych mu narzędzi dostępnych na rynku, ponownie. Teraz – podobnie jak w przeszłości – oczywiście w „jedynie słusznym celu"...

W tym miejscu należy w kilku słowach wyjaśnić dlaczego zdecydowałem się – pomimo nasuwających się wątpliwości, przede wszystkim o charakterze etycznym – na korzystanie z terminu „inwigilacja" w niniejszym opracowaniu. Patrząc obiektywnie na działalność Służby Bezpieczeństwa, która głównie tą metodę pracy operacyjnej stosowała, stwierdzić należy, iż była to formacja na swoje czasy bardzo nowoczesna, chętnie korzystająca z dostępnych rozwiązań technicznych i wdrażająca nowe rozwiązania, a w niektórych obszarach także tworząca własne i na bieżąco analizująca możliwości wykorzystania w pracy operacyjnej pojawiających się innowacji technicznych. Zauważyć należy, że wraz z rozwojem technologicznym tzw. technika operacyjna zaczęła odgrywać coraz większą rolę w sprawach realizowanych przez Służbę Bezpieczeństwa, a niekiedy opierano się tylko i wyłącznie na niej. Także w chwili obecnej niezbędne jest korzystanie przez służby powołane do ochrony prawa i porządku publicznego z jak największego wachlarza możliwości technicznych, z uwzględnieniem także rozwiązań nieoczywistych i nietypowych, a podejście tej instytucji – pomimo całej negatywnej otoczki z nią związanej – do nowoczesnych rozwiązań technicznych, może stanowić punkt odniesienia dla aktualnie funkcjonujących w Polsce służb państwowych.

Kończąc tą nieco przydługą wypowiedź o charakterze prawno-filozoficznym, zwrócić należy się do istoty niniejszej publikacji i określenia możliwości wykorzystania w procesie inwigilacji prowadzonej w środowisku cyfrowym materiałów pozyskanych w oparciu o otwarte źródła informacji. Zacznę od przywołania samego terminu „inwigilacja", a z uwagi na brak osadzonej w obowiązujących aktach prawnych definicji, wykorzystam tę, która funkcjonowała w obowiązującym w Polce do 1989 r. systemie prawnym. Inwigilacją nazywać będziemy zatem: „*metodę pracy operacyjnej polegającą na stałym lub okresowym kontrolowaniu zachowania i działania osób, które, zdaniem funkcjonariuszy, mogły w sprzyjających okolicznościach podjąć działalność antysystemową*"[6]. Oczywiście, w omawianym przypadku należałoby rozważyć, co w obecnej chwili rozumiemy przez działalność antysystemową i czy może być ona interpretowana np. jako działalność przestępcza wyczerpująca znamiona niektórych czynów opisanych w obowiązującym Kodeksie Karnym w Rozdziale XVII – Przestępstwa przeciwko Rzeczypospolitej Polskiej[7],

[6] Filip Musiał, Podręcznik Bezpieki, Wydawnictwo Diecezjalne i Drukarnia w Sandomierzu, Kraków-Warszawa 2020, s. 341.

[7] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny – t. j. Dz.U.2024.17.

czy też jej zakres należy rozszerzyć lub ograniczyć. Niejako na marginesie zauważyć należy, iż w zawieszonym projekcie prac nad Kodeksem Pracy Operacyjnej termin „inwigilacja" także nie występuje, a rozwiązania mogące być elementami składowymi inwigilacji zostały podzielone na odrębne czynności, co w ostatecznym rozrachunku może skutecznie utrudnić ich wykorzystanie w warunkach realnych, które z reguły pozycjonowane są w znacznej odległości od teoretycznie wypracowanych założeń[8].

Mamy więc trzy, istotne, składowe przyjętej definicji inwigilacji, które obejmują:

- obszar kontroli (zachowania i działania osób);
- czas jej trwania (stała lub okresowa);
- powód kontroli (podejrzenie możliwości podjęcia działalności antysystemowej).

Niezbędnym elementem zastosowania tej metody pracy operacyjnej będzie wystąpienie wszystkich tych trzech elementów łącznie, przy czym za najbardziej istotny i konieczny warunek rozpoczęcia inwigilacji należy uznać podejrzenie możliwości podjęcia działalności antysystemowej.

Na tak przygotowaną definicję nałożyć należy możliwości w zakresie inwigilacji w środowisku cyfrowym, jakie niesie ze sobą korzystanie z rozwiązań OSINT (ang. *Open-Source Intelligence*) czyli wywiadu otwartoźródłowego. Pomimo, iż problematyka ta od bardzo dawna pojawia się w działaniach militarnych, rozwój usług cyfrowych, wkraczających praktycznie w każdą dziedzinę życia ludzkiego, sprawił, że temat wyszukiwania i analizy ogólnodostępnych informacji stal się przedmiotem zainteresowania wielu instytucji i osób, niezależnie od ich profilu czy legalności prowadzonych działań[9]. Ponieważ kwestia wykorzystania otwartych źródeł informacji poruszana była wielokrotnie w kontekście działań różnego rodzaju organizacji czy grup dziennikarzy śledczych, w niniejszym opracowaniu skoncentruję się jedynie na wykorzystaniu danych pochodzących z otwartych źródeł informacji przez służby państwowe, w tym służby specjalne. W kontekście tym zauważyć należy, iż różnego rodzaju instytucje mające charakter służby specjalnej, czyli części instytucji państwowych odpowiedzialnych za zewnętrzne i wewnętrzne bezpieczeństwo państwa[10] i działające w jego interesie, mają potencjalnie większe możliwości – zarówno techniczne jak i prawne – niż nawet największe grupy pasjonatów. Prowadzone przez służby specjalne działania mające charakter inwigilacji

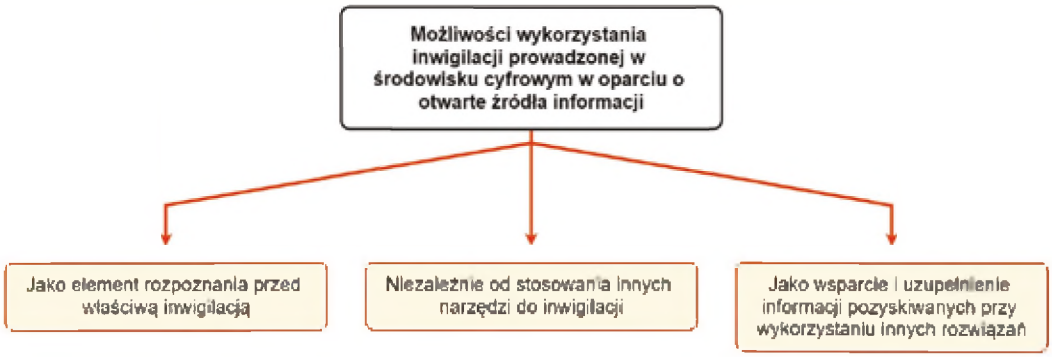
[8] Jako elementy inwigilacji można uznać między innymi wskazane w art. 14 Ustawy w punkcie 12 – kombinację operacyjną oraz w pkt. 22 i 23 niejawną ingerencję i niejawne przeszukanie. Należy jednak zauważyć, iż okoliczności, w których zastosowanie tych metod pracy operacyjnej będzie dopuszczalne, nie zawsze muszą się pokrywać, jak również rezultat czynności podejmowanych w trakcie korzystania z tych metod pracy nie będzie tak kompletny jak w przypadku samej inwigilacji.

[9] Krzysztof Wosiński, Bezpieczeństwo osób i systemów IT z wykorzystaniem białego wywiadu, Wydawnictwo Naukowe PWN S.A., Warszawa 2024, s. 1.

[10] http://encyklopediaap.uw.edu.pl/index.php/Służby_specjalne – ostatni dostęp 16.03.2025 r.

w oparciu o dane uzyskane z publicznie dostępnych informacji, które każdy może pozyskać na żądanie poprzez zakup lub obserwację[11] mogą być znakomicie wspierane poprzez dostęp do baz danych wrażliwych i innych baz szczegółowych, z których informacje – przynajmniej teoretycznie – są niedostępne dla podmiotów nieposiadających stosownych uprawnień. Oczywiście nie będziemy wówczas mówić wyłącznie o danych uzyskanych z publicznie dostępnych źródeł informacji, a sam OSINT nie będzie nim w sensie ścisłym, jednak rozszerzenie na potrzeby niniejszego opracowania definicji danych otwartoźródłowych do postaci „danych uzyskanych z publicznie dostępnych źródeł informacji, które każdy może pozyskać na żądanie poprzez zakup lub obserwację lub danych, do dostępu do których jest uprawniony na podstawie obowiązujących unormować prawnych i kompetencji", wydaje się dopuszczalne. Taka rozszerzona interpretacja definicji pozwoli na uniknięcie dysonansu poznawczego, w wyniku którego można by odnieść wrażenie, iż służby mogące korzystać z różnego rodzaju dostępnych państwowych i prywatnych źródeł danych z premedytacją nie będą do nich sięgały i niejako samoograniczały swoje możliwości, co jest oczywistą nieprawdą.

Na poniższym schemacie, w sposób ramowy, zostały przedstawione możliwości wykorzystania inwigilacji prowadzonej w środowisku cyfrowym w oparciu o otwarte źródła informacji:



Informacje, czyli przetworzone i poddane analizie dane, pozyskiwane w trakcie inwigilacji prowadzonej w środowisku cyfrowym w oparciu o otwarte źródła informacji mogą znaleźć swoje zastosowanie w różnych sytuacjach, których przykłady zostaną omówione poniżej:

[11] Krzysztof Wosiński, Bezpieczeństwo osób…, s. 11.

1. Inwigilacja realizowana w oparciu o otwarte źródła informacji jako element rozpoznania przed właściwą inwigilacją

Taki sposób wykorzystania wartościowych materiałów zgromadzonych w trakcie analizy dostępnych zasobów sieciowych, pozwala na bardziej precyzyjne ukierunkowanie właściwej inwigilacji wszczynanej w oparciu o szczegółowe unormowania prawne obejmujące zasady korzystania z tej formy pracy operacyjnej przez uprawnione służby państwowe. Oczywiście, mamy w tym przypadku do czynienia z pewnego rodzaju uogólnieniem, ponieważ – jak pamiętamy – aktualnie obowiązujące uregulowania prawne, tak jawne jak i niejawne, nie zawierają w sobie tej formy pracy operacyjnej jako takiej, ale nic nie stoi na przeszkodzie, aby wykorzystać zgromadzone materiały przy okazji przygotowania do realizacji innej formy pracy operacyjnej, np. kontroli operacyjnej. Należy pamiętać, iż w przeciwieństwie do wykorzystania systemu „Pegasus", w tym przypadku, nie mamy do czynienia z hipotetycznym nawet naruszeniem prawa, wynikającym np. z nieuprawnionego dostępu do informacji poprzez przełamanie zabezpieczeń urządzenia, jak to mogło mieć miejsce w przypadku przywołanego wyżej rozwiązania. Należy także wziąć pod uwagę, iż informacje zgromadzone w toku analizy danych pozyskanych z tzw. otwartych źródeł lub baz danych dostępnych na podstawie obowiązującego prawa, mogą służyć jako materiał wyjściowy, do przygotowania dalszych czynności, ograniczając w ten sposób czas i koszty, jakie prawdopodobnie należałoby ponieść, gdyby materiały te nie były wykorzystywane. Każdorazowo należy uwzględnić także kluczowy aspekt korzystania z danych otwartoźródłowych, jakim jest konieczność stałej analizy pozyskanych informacji oraz ich weryfikacja w zakresie autentyczności i przydatności w toku realizowanych później czynności inwigilacyjnych. Szczególnie na obecnym etapie rozwoju możliwości manipulacji grupami ludzi oraz łatwości w tworzeniu treści istniejących jedynie w rzeczywistości wirtualnej, czynności te mogą odgrywać kluczową rolę w procesie rozpoznania realizowanego jako etap przygotowania właściwej inwigilacji z wykorzystaniem dostępnych metod i środków technicznych.

Weryfikacja materiałów cyfrowych, które mogą zostać ujawnione w toku przeszukiwania sieci Internet powinna dotyczyć następujących obszarów związanych z informacją:

- Autentyczność – oczywistym jest, iż tylko prawdziwe dane to wartościowy materiał na informacje wykorzystane jako materiały kierunkowe w dalszym procesie prowadzenia inwigilacji. Weryfikacja autentyczności pozyskanych informacji powinna stanowić pierwszy etap prac z danymi. Skupianie się na pozostałych obszarach i ich weryfikacja bez uzyskania wcześniejszej pewności co ich autentyczności jest jedynie marnotrawieniem sił i środków. Należy pamiętać także o tym, aby jasno i precyzyjnie określić czas, jaki chcemy poświęcić na weryfikację

określonych treści. Obsesyjne poszukiwanie dowodów na prawdziwość zabezpieczonego materiału może spowodować, iż pominięte lub zmarginalizowane zostaną przesłanki sprzeczne z założoną pod wpływem „zafiksowania się" na udowodnieniu autentyczności materiałów tezą. Należy pamiętać, iż zawsze istnieje możliwość wykorzystania materiałów wcześniej opublikowanych, w celu stworzenia potencjalnie nowej informacji, dlatego gromadząc materiał, który ma być wykorzystany jako późniejsza baza do właściwego procesu inwigilacji, należy bezwzględnie zweryfikować, czy pozyskany materiał jest treścią pierwotną i autentyczną, czy też stanowi element cyfrowego „kolażu".

- Źródło – materiały, które poddawane są analizie nie zawsze muszą pochodzić od osoby, która ma być objęta procesem inwigilacji. Z bardzo dużym prawdopodobieństwem mogą to być materiały opublikowane w Internecie przez inne osoby, w bliższy lub dalszy sposób związane z podmiotem potencjalnej inwigilacji. Ustalenie i zweryfikowanie źródła pozwala na określenie jego roli w procesie wytworzenia bądź udostepnienia informacji.
- Czas – określenie czasu publikacji informacji w sieci oraz okresu, w jakim mogło mieć miejsce publikowane zdarzenie, pozwala na umieszczenie go w tworzonej linii czasu obejmującej aktywność osoby pozostającej „w zainteresowaniu" w ramach przygotowywanej inwigilacji, a tym samym określenie np. rodzaju zdarzenia (jednorazowe lub cykliczne).
- Lokalizacja – ustalenie geolokalizacji zdarzenia, o którym informacja została umieszczona w mediach cyfrowych, pozwala na zdobycie dodatkowych informacji o przyzwyczajeniach osoby, która ma być poddana późniejszej inwigilacji. Należy przy tym odróżnić rzeczywiste miejsce wykonania np. fotografii, od treści wskazywanych w części opisowej oraz od informacji znajdujących się w metadanych pliku. Nie należy pomijać także analizy innych pozyskanych materiałów dotyczących osoby potencjalnego „figuranta" znajdujących się w sieci Internet, a pochodzących zarówno od niego jak i od osób z nim powiązanych oraz przypadkowych (np. w sytuacji umieszczenia relacji z imprezy masowej), w celu wykluczenia ewentualnych przypadków bilokacji, a tym samym obniżenia wiarygodności zabezpieczonych treści. Wszelkie ujawnione rozbieżności powinny być starannie weryfikowane, aby uniknąć wprowadzenia do materiałów danych nieprawdziwych. Warto w trakcie ustalania lokalizacji korzystać z rozwiązań systematyzujących działania przygotowawcze, pozwalających np. na szczegółową analizę elementów wyposażenia wnętrz jak i infrastruktury zewnętrznej[12].

[12] Przykładem takich rozwiązań pozwalających na usystematyzowanie elementów poddawanych analizie są opracowana przez Krzysztofa Wosińskiego mapy myśli, które można znaleźć w jego repozytorium w serwisie GitHub, pod adresem: https://seintpl.github.io/ – ostatni dostęp 01.04.2025 r.

- Motywacja – na ostatnim etapie weryfikacji materiałów cyfrowych, ujawnionych w toku przeszukiwania sieci Internet należy pochylić się nad motywacją, jaką kierowała się osoba, udostępniając określone treści szerokiej rzeszy odbiorców. W przypadku zorganizowanych grup przestępczych, wykorzystujących zaawansowane techniki kontrwywiadowcze, należy zawsze pamiętać o możliwość wystąpienia celowych działań zmierzających do ukrycia rzeczywistego miejsca pobytu lub zamiarów. W takim samym zakresie zasadę „ograniczonego zaufania" należy stosować wobec każdej, opracowywanej na potrzeby przyszłych procedur inwigilacyjnych, osoby.

Zgromadzone i zweryfikowane w opisany powyżej, z konieczności bardzo ogólnie, sposób informacje, stanowić będą bazę do wykonywania dalszych czynności obejmujących działania wpisujące się w ogólne znaczenie terminu inwigilacja, zarówno realizowane przez uprawnione instytucje państwowe jak i przez różnego rodzaju podmioty prywatne.

2. Niezależnie od stosowania innych narzędzi do inwigilacji

Kolejna możliwość wykorzystania materiałów otwartoźródłowych w ramach procesu inwigilacji, pojawia się już w trakcie jej stosowania przez podmioty uprawnione. Ponownie należy przypomnieć, iż pomimo braku występowania terminu „inwigilacja" w polskim systemie prawnym, działania te mogą wpisywać się w inne metody pracy operacyjnej realizowane przez instytucje państwowe. Brak ustawowo zdefiniowanego terminu, nie przeszkadza zaś na pewno podmiotom oraz osobom fizycznym realizującym różne czynności obejmujące gromadzenie danych i ich późniejsze wykorzystanie zarówno w granicach obowiązującego prawa jak i poza nim[13], jednakże w niniejszej publikacji nie będziemy poruszać tej problematyki, lub w ostateczności – o ile taka konieczność zaistnieje – bardzo powierzchownie. Koncentrując się na działaniach inwigilacyjnych prowadzonych w środowisku cyfrowym równolegle do działań o charakterze operacyjnym – w tym niekoniecznie inwigilacyjnych – podejmowanych w oparciu o uprawnienia ustawowe, wspomnieć należy, iż dane pozyskane w wyniku wykorzystania dostępnych materiałów otwartoźródłowych zgromadzonych w sieci Internet mogą być wykorzystane w co najmniej dwojaki sposób. Pierwszy z nich pozwala na wykorzystanie materiałów zgromadzonych podczas przeszukiwania i analizy dostępnych zasobów sieciowych, jako uzupełnienie już posiadanych informacji. Na szczególną uwagę zasługuje fakt, iż

[13] Np. Doxing, czyli działanie polegające na gromadzeniu i wykorzystywaniu danych zebranych w Internecie na temat innych osób w celu zawstydzenia, zastraszenia, zniesławienia, bądź wywołania u ofiary poczucia zagrożenia. Termin jest neologizmem powstałym na bazie anglojęzycznych wyrażeń docs (dokumenty) i compiling / releasing (przetwarzać, upubliczniać) – https://www.gov.pl/web/baza-wiedzy/doxing--nowe-zjawisko-i-cyberzagrozenie – ostatni dostęp 01.04.2025 r.

inwigilacja, dotycząca konkretnej osoby, nawet przy wykorzystaniu tak inwazyjnych metod gromadzenia informacji jak system Pegasus, dostarcza najczęściej treści tylko bezpośrednio z tą osobą związanych. Uzupełnienie jej o dane gromadzone podczas inwigilacji dodatkowo wspieranej przez wykorzystanie otwartych źródeł informacji, pozwala na rozszerzenie obszaru zainteresowania, uzupełniając go nie tylko o inne materiały z najbliższego otoczenia „figuranta", ale także o treści, które nie byłyby do pozyskania w trakcie standardowych procedur inwigilacyjnych. Zauważyć tutaj należy, iż inwigilacja realizowana o materiały otwartoźródłowe, najczęściej nie ma miejsca w „czasie rzeczywistym", lecz jest opóźniona w stosunku do realnych zdarzeń, z uwagi na sposób dostarczania treści np. do zasobów sieci Internet. Taka specyfika pozwala na mapowanie sposobu przedstawienia np. określonych wydarzeń, przez osoby w nich uczestniczące na ich rzeczywisty przebieg, a co za tym idzie otwiera drogę do dalszej analizy i interpretacji.

3. Jako wsparcie i uzupełnienie informacji pozyskiwanych przy wykorzystaniu innych rozwiązań

W ostatnim z omawianych przypadków, inwigilacja realizowana przy wykorzystaniu otwartych źródeł informacji pełni zdecydowanie służebną rolę w stosunku do inwigilacji realizowanej za pomocą środków technicznych i osobowych. Pewne jej elementy mają charakter ściśle powiązany z omówionymi w punktach poprzedzających ponieważ, zarówno wykorzystanie materiałów pochodzących z otwartych źródeł jako swoistego rodzaju „mapy drogowej" pozwalającej na ukierunkowanie procesu późniejszej inwigilacji na obszary potencjalnie istotne, jak i jej realizacja niezależnie od stosowania innych narzędzi do inwigilacji wyczerpuje – przynajmniej w części – powyżej zdefiniowany obszar. Elementem istotnym, na który należy zwrócić uwagę, jest jej mniej uprzywilejowany status, w stosunku do dwóch wcześniej omawianych. O ile wykorzystanie inwigilacji w oparciu o dane otwartoźródłowe zostało w wyczerpujący sposób omówione w poprzednich punktach, o tyle wykorzystanie jej w celu uzupełnienia informacji pozyskanych przy wykorzystaniu innych rozwiązań wymaga uzupełnienia. Nie można bezkrytycznie zakładać, iż w wyniku inwigilacji zrealizowanej w zakresie posiadanych uprawnień przez służby państwowe, zgromadzone zostaną informacje, które będzie można przetworzyć w toku dalszego postepowania na w pełni wartościowy, kompletny i zupełny materiał dowodowy. Doświadczenie uczy, iż takie sytuacje zdarzają się niezmiernie rzadko – znacznie częściej zgromadzony w trakcie procesu inwigilacji materiał operacyjny zawiera jedynie szczątkowe – w mniejszym lub większym zakresie – informacje, które i tak, prawie zawsze, wymagają poszerzenia w toku dalszych czynności operacyjnych lub procesowych. W takim przypadku rola inwigilacji realizowanej przy wykorzystaniu

ogólnodostępnych zasobów w przestrzeni cyfrowej, może okazać się kluczowa. Dysponując wstępnymi informacjami pochodzącymi z innych źródeł, możemy dążyć do ich weryfikacji, rozszerzenia lub doprecyzowania poprzez wykorzystanie materiałów dostępnych np. w sieci Internet. Rozszerzenie wykorzystywanych metod dostępu do informacji o te nie zawsze oczywiste, pozwala na uzyskanie znacznie lepszych wyników niż kurczowe trzymanie się rozwiązań opisanych np. w przepisach wewnątrzresortowych. Na marginesie, warto zauważyć, iż bardzo często mamy do czynienia z sytuacją wręcz odwrotną – osoby realizujące w organach ścigania czynności operacyjno-rozpoznawcze związane z wykorzystaniem otwartych źródeł informacji czują się – z chwilą opuszczenia szeregów instytucji państwowych i przejściu do sektora prywatnego – pozbawione częściowo czegoś, co można określić mianem „mocy sprawczej", jaką mieli w organach ścigania. Odczucie to związane jest nierozerwalnie z rozszerzonymi możliwościami, jakie daje im wykorzystanie specjalistycznych baz danych, jako wsparcia czy usprawnienia typowych czynności wywiadowczych, do których uzyskują dostęp na podstawie kompetencji ustawowych. W mojej ocenie, taka zmiana środowiska pracy pozwala raczej na ponowne przeanalizowanie i – jeśli to konieczne – odświeżenie wykorzystywanych metod pracy, a nie jest elementem ograniczającym czy wręcz deprecjonującym uzyskiwane rezultaty.

Konkludując – mając świadomość ograniczeń stosowanych rozwiązań, nie należy się ograniczać wyłącznie do nich, a wręcz przeciwnie – tym częściej powinniśmy korzystać z możliwości ich uzupełnienia – a inwigilacja realizowana w oparciu o materiały otwartoźródłowe nadaje się do tego celu doskonale.

Na marginesie należy także zwrócić także uwagę na bardzo istotny element procesu inwigilacji realizowanej w oparciu o materiały otwartoźródłowe, jakim jest dokumentowanie uzyskanych informacji. Pracując w szczególności w obszarze sieci Internet, zwłaszcza w środowisku mediów społecznościowych należy pamiętać, iż wiele z prezentowanych treści może mieć charakter chwilowy, ulotny. Często najbardziej wartościowe materiały pojawiają się w sieci pod wpływem błędu czy impulsu, i tak samo szybko jak się pojawiły – znikają. Systematyczne wykonywanie zrzutów ekranów zawierających ujawnione treści, nagrywanie aktywności związanej z przeglądanymi zasobami czy też zabezpieczenie kluczowych stron internetowych, jest niezbędne do utrwalenia danych ujawnianych w tak dynamicznie funkcjonującym środowisku jakim jest sieć Internet.

Na zakończenie należałoby odnieść się także do pytania o granicę inwigilacji cyfrowej, a w szczególności tej wykorzystującej materiały otwartoźródłowe. Ze smutkiem należy stwierdzić, iż granice te znajdą się dokładnie tam, gdzie sami je ustanowimy. Ulubioną postawą człowieka piśmiennego było bowiem zawsze „obserwowanie z przerażeniem" lub „wskazywanie z dumą", przy jednoczesnym

skrupulatnym ignorowaniu tego, co się naprawdę dzieje[14]. Nasze życie prywatne i zawodowe stało się procesem informacyjnym tylko dlatego, że wynieśliśmy nasz ośrodkowy układ nerwowy na zewnątrz nas samych w postaci elektrotechniki[15]. Obserwując jednak postępy w raczej nietypowym – jak dla gatunku homo sapiens – ekshibicjonizmie cyfrowym należy raczej przypuszczać, iż będą one przesuwały się coraz dalej, w myśl zasady, iż jeśli odpowiednio długo będziemy prezentowali kontrowersyjne treści bądź zachowania, to w końcu staną się one normą, a przynajmniej za takie uzna je większość. Potwierdzeniem tej tezy zdaje się być popularność wszelkiego rodzaju patoinfluencerów czy patostreamerów prezentujących treści, które bardzo łagodnie można opisać określeniem „kontrowersyjne", jednakże nie możemy zapominać, że to my sami stoimy za wzrostem ich popularności, w myśl stwierdzenia iż popyt generuje podaż. Należy zwrócić uwagę, że jeszcze kilka lat temu, mało kto prognozował pojawienie się w mediach społecznościowych „wyzwań" polegających na wkładaniu do produktów żywnościowych ostrych przedmiotów, czy kont dla kilkuletnich dzieci, dzisiaj zaś, coraz częściej, mamy z tego rodzaju zjawiskami do czynienia. Paradoksem jednak jest to, że przesuwanie się granic inwigilacji cyfrowej przy wykorzystaniu otwartych źródeł informacji raczej nie będzie dotyczyło organów ścigania – te skierują się w stronę rozwiązań komercyjnych, posiadających możliwości inwazyjnego dostępu do urządzeń czy zautomatyzowanego dostępu do zasobów przechowujących dane i ich automatycznej agregacji i kategoryzacji. Granice inwigilacji cyfrowej przesuną się raczej w przypadku działań podejmowanych przez różnego rodzaju samozwańczych cyfrowych detektywów i będzie to połączone ze wzrostem tolerancji na sieciową patologię połączoną z coraz większą chęcią zaistnienia w świecie cyfrowym, a co za tym idzie umieszczaniem tam treści coraz bardziej osobistych, które stanowić będą prawdziwą kopalnię wiedzy o naszym i naszego otoczenia życiu prywatnym.

Literatura

1. John Acton, *List do biskupa Mandella Creightona*, 3 kwietnia 1887.
2. Tadeusz Hanausek, *Kryminalistyka: Poradnik detektywa*, Biuro Wydawnictw Prawniczych „Polbod", Katowice 1993.
3. Marshall McLuhan, *Zrozumieć media. Przedłużenie człowieka*, Wydawnictwa Naukowo-Techniczne, Warszawa 2004.
4. Filip Musiał, *Podręcznik Bezpieki*, Wydawnictwo Diecezjalne i Drukarnia w Sandomierzu, Kraków-Warszawa 2020.

[14] Marshall McLuhan, Zrozumieć media. Przedłużenie człowieka, Wydawnictwa Naukowo-Techniczne, Warszawa 2004, s. 265.
[15] Tamże, s. 94.

5. Krzysztof Wosiński, *Bezpieczeństwo osób i systemów IT z wykorzystaniem białego wywiadu*, Wydawnictwo Naukowe PWN S.A., Warszawa 2024.
6. Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny* – t. j. Dz.U.2024.17.
7. Ustawa *Kodeks pracy operacyjnej* – projekt z dn. 17.04.2023 r.

Źródła internetowe

1. *https://www.rp.pl/sluzby/art41579741-nie-bedzie-kodeksu-pracy-operacyjnej-rzad-wprowadza-obostrzenia-dla-sluzb-przez-rozporzadzenia* – ostatni dostęp 16.02.2025 r.
2. *https://pl.wikipedia.org/wiki/Afera_Pegasusa* – ostatni dostęp 16.02.2025 r.
3. *http://encyklopediaap.uw.edu.pl/index.php/Służby_specjalne* – ostatni dostęp 16.03.2025 r.
4. *https://seintpl.github.io/* – ostatni dostęp 01.04.2025 r.
5. *https://www.gov.pl/web/baza-wiedzy/doxing-nowe-zjawisko-i-cyberzagrozenie* – ostatni dostęp 01.04.2025 r.

Marek Stawarczyk[1]

O manipulacjach w obrazie cyfrowym

Rejestracja obrazów cyfrowych stała się powszechnie dostępnym sposobem dokumentowania rzeczywistości. Urządzenia, którymi tego dokonujemy pozwalają nie tylko zapisywać je ale również modyfikować poprzez wbudowane oprogramowanie czy filtry. Wraz z obrazem rejestrowane są także inne parametry takie jak data, czas, miejsce tj. współrzędne geograficzne, itd. Prezentacja obrazu niejednokrotnie stanowi dowód bycia w danym miejscu, uczestnictwa w zdarzeniu czy stwierdzenia stanu. Dysponując zatem cyfrowymi narzędziami możemy ingerować w zapisany obraz. Poprawa jakości obrazu (jasność, ostrość, kadrowanie czy wyrównanie) nie jest jednak traktowana jako modyfikacja mająca istotny wpływ na zawartość – czyli manipulacja.

Zgodnie z definicją pojęcia (w psychologii) manipulacja[2] to dążenie do osiągnięcia celu przez manipulatora – modyfikatora obrazu czyt. fałszerza. Motywacje wprowadzania zmian mogą być różne poczynając od chęci ośmieszenia, zrobienia żartu, poprzez stworzenia dokumentacji fałszywych faktów, „dokumentowanie" nieprawdziwych zdarzeń politycznych po szeroko rozumianą dezinformację. Modyfikacje obrazu cyfrowego stały się usługą[3].

Wykrywanie manipulacji w obrazie cyfrowym to ważna dziedzina w analizie mediów cyfrowych i kryminalistyce cyfrowej. Istnieje wiele metod – zarówno wizualnych, jak i technicznych – które pozwalają zidentyfikować, czy obraz został zmodyfikowany.

Analiza prosta

Analizę prostą możemy określić jako analizę dwuetapową. Analizę wizualną związaną z analizą treści i jakości obrazu oraz analizę metadanych jakie zostały przypisane automatycznie przez urządzenie rejestrujące.

Analiza wizualna

Człowiek może czasem zauważyć oznaki edycji:

- **Nienaturalne cienie lub oświetlenie** – niespójne źródła światła. Wskazania – podejrzenia wielu źródeł światła np. naturalne i sztuczne, także kierunki cieni obiektów względem źródeł światła.

[1] Marek Stawarczyk – biegły sądowy Sądu Okręgowego w Krośnie z zakresu informatyki oraz informatyki śledczej.

[2] https://pl.wikipedia.org/wiki/Manipulacja_(psychologia)

[3] https://fixthephoto.com/pl/image-manipulation-service

- **Zniekształcenia i rozmycia** – szczególnie w miejscach edycji (tj. przy wycinaniu obiektów i wstawianiu obiektów). Szczególnie istotne jest wskazanie usunięć i przesłonięć innymi obiektami z tej samej fotografii.
- **Dziwne odbicia i proporcje** – np. brak odbicia obiektu w wodzie/lustrze, tzw „martwe oko" w przypadku postaci.
- **Nieciągłość tekstur i krawędzi**. Czasami widoczne działanie narzędzi edycyjnych – „dorysowane" kropki, linie itd. bądź zmieniony kolor fragmentu obiektu.

Taki wstęp – oględziny czy nawet analiza wizualna pozwala jedynie na wskazanie potencjalnie modyfikowanych fragmentów czy obiektów znajdujących się na fotografii. Nawet największa spostrzegawczość jest mało wiarygodna bez wsparcia narzędzi.

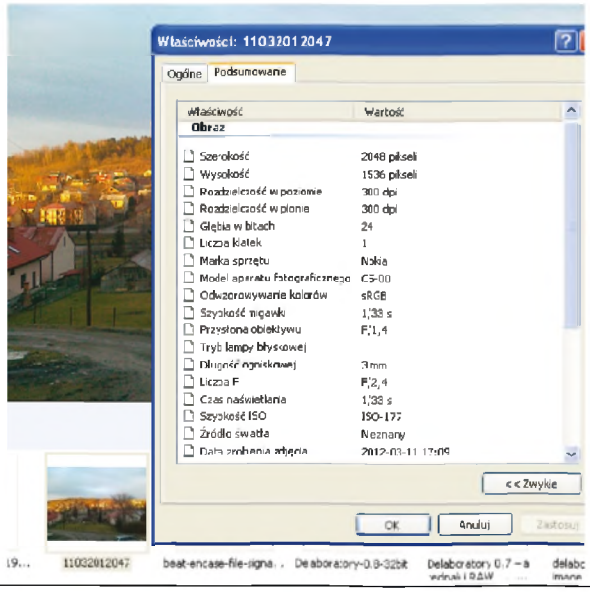
Analiza metadanych (Exif)

Metadane mogą zawierać informacje o:

- Aparacie/kamerze, lokalizacji GPS, czasie wykonania zdjęcia.
- Programach użytych do edycji (np. Photoshop, GIMP).

Podstawowe narzędzia:

- ExifTool[4], Exif Pilot,
- Jeffrey's Image Metadata Viewer,
- JPEGSnoop.[5]

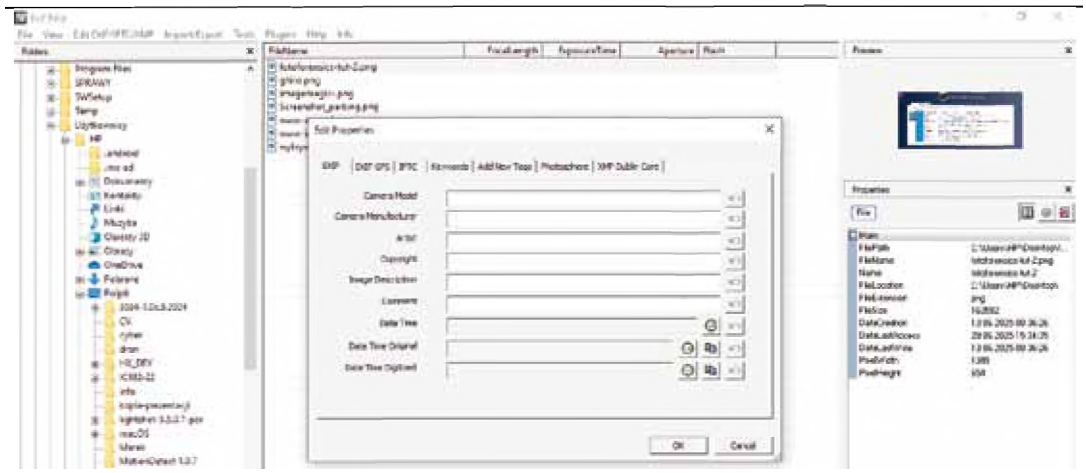


Rys. 1. Przykład metadanych zdjęcia wykonanego telefonem

[4] https://exiftool.org/

[5] https://github.com/ImpulseAdventure/JPEGsnoop

Oprogramowanie **Exif Pilot**[6] pozwala nie tylko na odczyt metadanych lecz również na ich modyfikację czy usunięcie.



Rys. 2. Możliwości modyfikacji metadanych

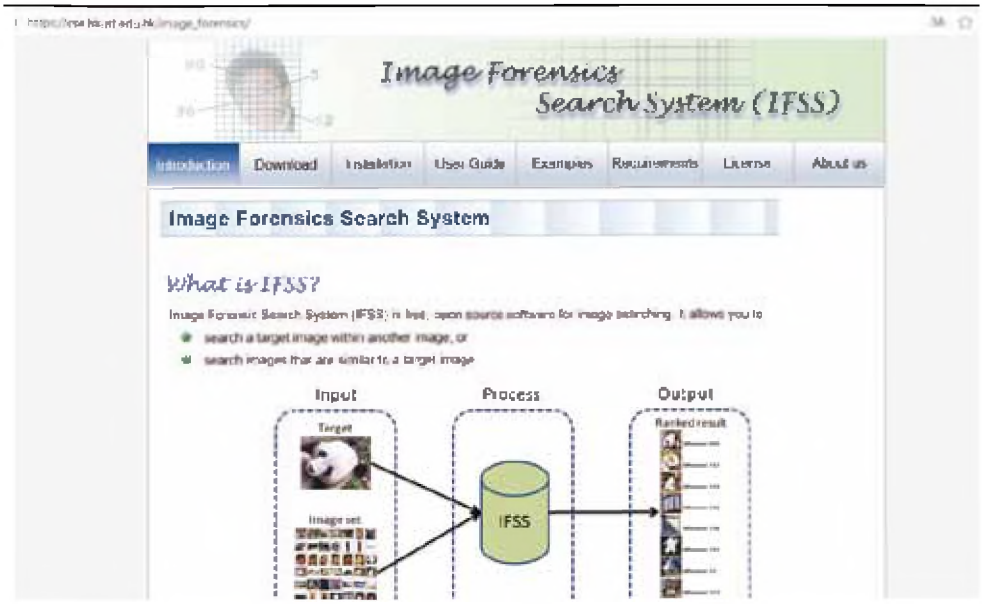
Brak metadanych lub obecność wpisów typu „Adobe Photoshop", „Gimp" czy nazw innych narzędzi edycji obrazów cyfrowych może wskazywać na edycję. Oprogramowanie może wskazać również urządzenie, którym został zarejestrowany obraz cyfrowy.

Wyszukiwanie obrazem

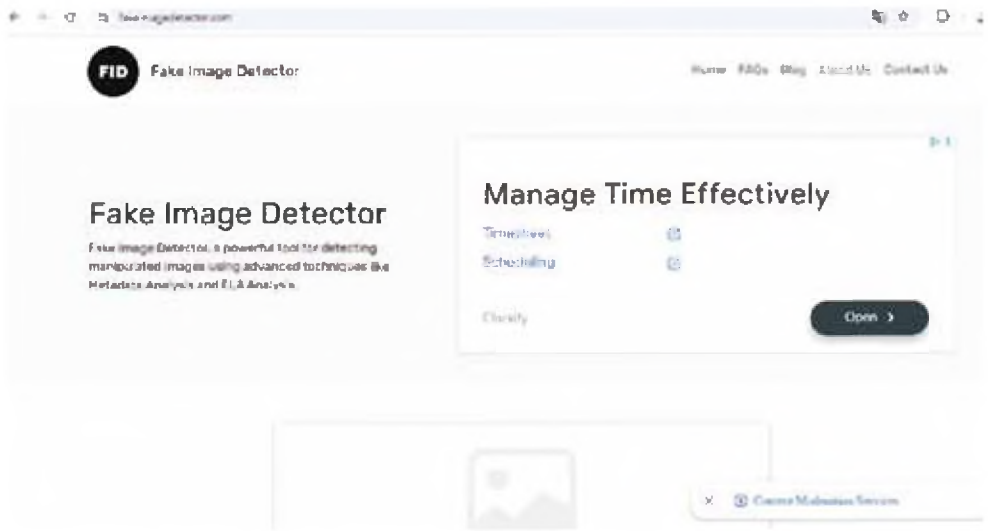
Niezależnie od wspomnianej powyżej analizy prostej stosuje się wyszukiwanie obrazem oraz wyszukiwanie tzw. wsteczne. Wyszukiwanie to pozwala na ujawnienie czy obraz lub jego fragmenty nie zostały wcześniej opublikowane lub użyte. W szczególności przeszukiwane są media społecznościowe. Niejednokrotnie do tego wyszukiwania tworzy się galerię fragmentów całości obrazu i wyszukuje się poszczególne fragmenty. Technika ta jest szczególnie przydatna przy wyszukiwaniu twarzy. Analizę tą nazywamy **analizą zgodności z kontekstem (konfrontacja faktów).** Analiza pozwala ustalić czy sceny, stroje, miejsca pasują do deklarowanego czasu i lokalizacji. Porównanie zdjęcia z innymi źródłami (np. z Google Images, **TinEye**[7]) lub **Image Forensics Search System**[8]. Analizę stosujemy w autentykacji obrazów (np. w mediach) czy aplikacjach AI do detekcji deepfake'ów. Obecnie

[6] https://www.colorpilot.com/exif.html
[7] https://tineye.com/
[8] https://cse.hkust.edu.hk/image_forensics/

wykorzystuje się zaawansowane narzędzia Open-Source: **DeepFake Detection Tools**[9], **FaceForensics++**[10] lub onlinowe **Fake Image Detector.**[11]



*Rys. 3. Serwis systemu **Image Forensics Search System***



Rys. 4. Interface serwisu webowego Fake Image Detector

[9] https://arya.ai/apex-apis/deepfake-detection-api, https://sensity.ai/
[10] https://github.com/ondyari/FaceForensics
[11] https://www.fakeimagedetector.com/

Analiza zaawansowana

Analiza zawansowana polega na wykorzystaniu narzędzi analitycznych w celu wykrycia anomalii w ramach struktury obrazu. Każda matryca, na której powstał obraz cyfrowy zawiera swoją specyfikę i niedokładności, a oprogramowanie rejestrujące obraz dokonuje wg ustalonego algorytmu kompresji i zapisu obrazu. Ponadto należy tu zauważyć, że najbardziej wiarygodnym badaniem, jakie można byłoby przeprowadzić, byłoby porównanie surowego obrazu z matrycy z obrazem zarejestrowanym. Każdy z liczących się producentów urządzeń rejestrujących obraz opracował swój standard zapisu stanu matrycy podczas powstawania i rejestracji obrazu tzw. pliku typu **raw**.

Poniżej przykładowa lista urządzeń i typów plików obsługiwanych przez narzędzie analityczne[12]:

- *Windows bitmap .bmp*
- *Raw Canon .cr2*
- *Raw Canon .crw*
- *Encapsulated PostScript .eps*
- *Graphics Interchange Format .gif*
- *JPEG File Interchange Format .jpg or .jpeg*
- *Raw Minolta .mrw*
- *Raw Olympus .orf*
- *Portable Network Graphics .png*
- *Raw Photoshop .psd*
- *Raw Fujifilm .raf*
- *Raw Panasonic .rw2*
- *Raw TARGA .tga*
- *Tagged Image File Format .tiff*

W przypadku badania obrazu cyfrowego zapisanego na komputerze, dysku czy pamięci masowej warto podjąć próbę odzyskania danych, gdyż jest możliwe ujawnienie plików tymczasowych analizowanego obrazu. Po ujawnieniu takich plików możliwe jest wskazanie wówczas narzędzi i technik modyfikacji jak również określenie tzw. stempla czasowego operacji.

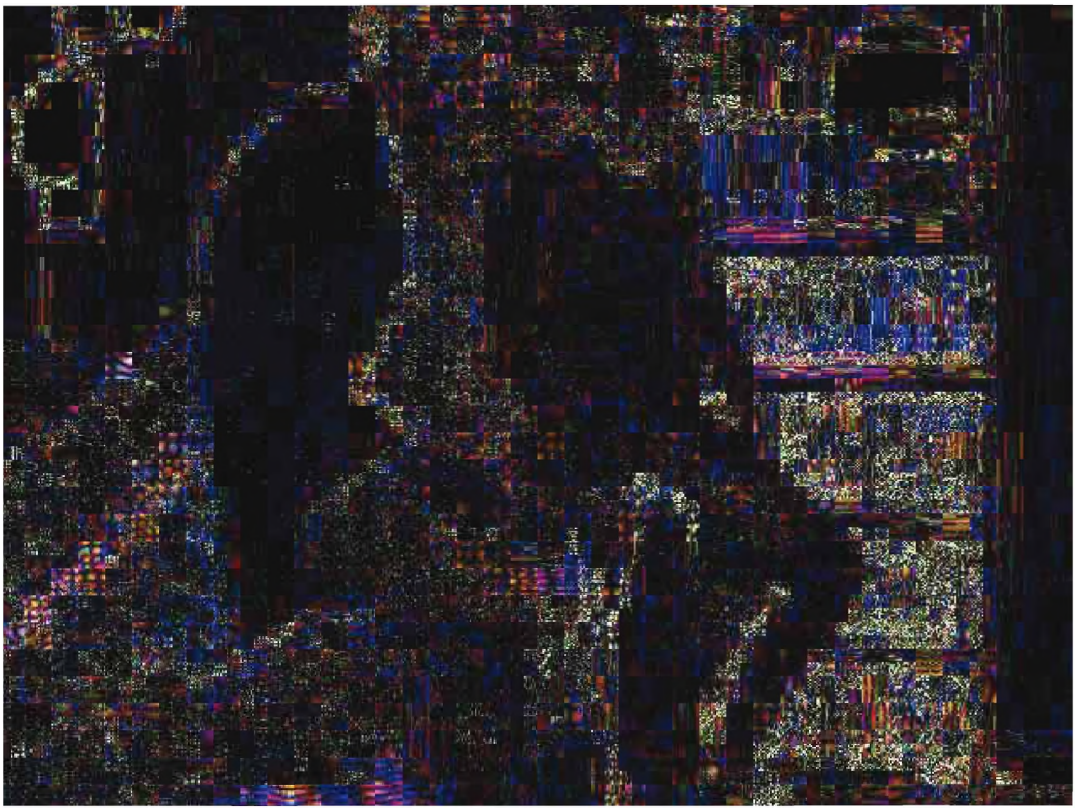
[12] https://docs.getghiro.org/en/ghiro-0.2.1/introduction/index.html#architecture

Analiza statystyczna i cyfrowa

Wykorzystuje różnice w danych cyfrowych obrazu:

a) Analiza błędów kompresji JPEG (ELA – Error Level Analysis).

Obszary edytowane mają inny poziom strat kompresji. Algorytm ten został wbudowany w narzędzia: serwis FotoForensics.com[13], oprogramowanie Ghiro[14] w postaci środowiska wirtualnego dla VirtualBox i Vmware.



Rys. 5. Przykład analizy ELA widoczne różnice w wielkości pikseli i bloków co potwierdza dodawanie obiektów i ponowny zapis. Zmiana szumu lokalnego w obrazie

b) Analiza poziomu szumu (Noise Inconsistency)

Każda kamera ma unikalny „szum matrycy". Analiza szumów w obrazie cyfrowym to technika pozwalająca wykrywać **manipulacje**, identyfikować źródło obrazu (np. model aparatu), a także ocenić jakość kompresji lub filtracji. Szumy w obrazie są bowiem często **charakterystyczne dla urządzenia rejestrującego** i **trudne do dokładnego podrobienia**. Edytowane fragmenty mogą mieć inny charakter szumu.

[13] https://fotoforensics.com/

[14] https://getghiro.org/

Należy zatem rozumieć, że każde urządzenie pozostawia tym samym indywidualny „odcisk", ślad na obrazie cyfrowym.

Rodzaje szumów w obrazie:

- **Gaussowski** – losowy, addytywny szum; modeluje zakłócenia od układów elektronicznych.
- **sól-pieprz (salt-and-pepper)** – pojedyncze, czarne lub białe piksele, zwykle efekt zakłóceń transmisji lub mikrouszkodzenia matrycy powstałe w produkcji czy montażu.
- **JPEG** – artefakty wynikające z kompresji stratnej.
- **chromatyczny i luminancyjny** – zależne od matrycy światłoczułej (np. CMOS); używane do identyfikacji aparatów.
- **PRNU (Photo Response Non-Uniformity)** – wzór unikalny dla każdego sensora, działający jak „odcisk palca" aparatu.

Cel	Metoda	Co się wykrywa?
Wykrycie manipulacji	Niespójność szumu lokalnego	Wklejki, retusze
Atrybucja obrazu	Dopasowanie PRNU	Model lub konkretne urządzenie
Wykrycie kompresji lub filtrów	Analiza statystyk częstotliwości	Edycja, ponowne zapisywanie
Odzyskiwanie jakości	Modelowanie szumu i jego usuwanie	Poprawa czytelności

Tab. 1. Tabela interpretacji analizy szumu

W odniesieniu do analizy szumów możemy mieć tzw. wskazania detekcyjne.

Obserwacja	Możliwa manipulacja
Brak szumu w fragmencie	Retusz, filtr wygładzający
Inny typ szumu lokalnie	Wklejenie z innego źródła
Artefakty blokowe	Kompresja JPEG, wielokrotna edycja
Brak zgodności z PRNU	Obraz zmodyfikowany, nieoryginalny
Obserwacja	Możliwa manipulacja

Tab. 2. Wskazania detekcyjne szumu

c) Analiza spójności kolorów i gradientów

Gradient opisuje zmiany jasności w przestrzeni obrazu – czyli wskazuje, **jak szybko i w jakim kierunku zmienia się jasność pikseli**. Naturalne obrazy mają ciągłe, spójne gradienty. Manipulacje (np. kopiowanie fragmentów z innego obrazu) mogą wprowadzić **nieciągłości lub nienaturalne różnice w gradientach.** Fałszywe fragmenty mogą mieć różną głębię koloru lub inne krzywe luminancji. Analiza spójności gradientów i jasności w obrazie cyfrowym to technika używana w **wykrywaniu manipulacji obrazu**, takich jak fotomontaże, retusze lub inne formy fałszowania opiera się na założeniu, że **naturalne obrazy mają spójną strukturę gradientów i rozkład jasności**, który może zostać zaburzony przez ingerencję.

Spójność gradientów – algorytmy mogą wykrywać „dziwne" krawędzie – np. te, które nagle się kończą lub mają nienaturalny kierunek sprawdza się **ciągłość kierunków gradientów** – np. przy krawędziach, które powinny być jednorodne.

- Do analizy często wykorzystywany jest MATLAB i zaawansowane techniki segmentacji możliwy do wykorzystania skrypt w Photoshopie.
- OpenCV[15] – analiza gradientów (cv2.Sobel, cv2.Laplacian).

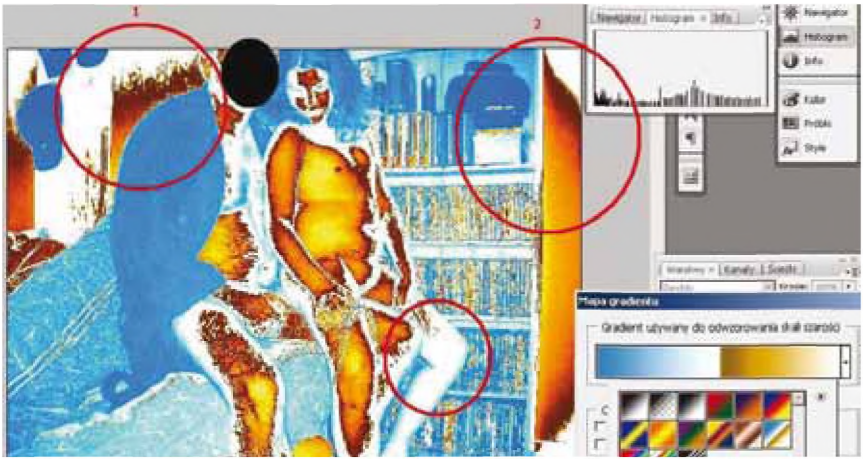
Badanie może wskazać granice wklejonych obiektów często pokazują nagłe zmiany gradientu.

Jasność (luminancja) odnosi się do **intensywności światła** odbieranego z danego punktu obrazu. W obrazach RGB można ją obliczyć jako ważoną sumę składników kolorów. W prawdziwych zdjęciach oświetlenie zwykle jest spójne. Jeśli część obrazu została dodana z innego zdjęcia, to może mieć **inną ekspozycję, kontrast lub kierunek oświetlenia**, co prowadzi do nienaturalnej jasności.

Analiza **mapy jasności** pozwala na sprawdzanie **lokalnych anomalii** – np. obszary zbyt jasne lub ciemne względem otoczenia, stworzenie mapy jasności całego obrazu (np. konwertując do skali szarości). Podczas badania możemy zastosować **modele oświetlenia** (np. metoda oświetlenia sferycznego) i sprawdzać, czy oświetlenie na różnych obiektach jest spójne.

Badanie powinno ujawnić obszary o nierealistycznym oświetleniu, które sugerują wklejenie z innego źródła.

[15] https://opencv.org/, https://sourceforge.net/projects/opencvlibrary/ zestawy – biblioteki skryptów dla różnych środowisk systemowych do wykorzystania i implementacji. Status open source.



Rys. 6. Analiza spójności gradientów – kolor pomarańczowy wskazuje na rzeczywiste źródło światła, elementy w kolorze niebieskim to modyfikacja – półka w tle po prawej i czapki po lewej



Rys. 7. Brak odbicia źródła światła u jednej z postaci tzw. „martwe oko". Twarze w bezpośredniej bliskości skierowane w obiektyw, różne wielkości pikseli: oczy z lewej a oczy z prawej



Rys. 8. Widoczne artefakty wstawianych obiektów z innych źródeł – różne wielkości pikseli i nieciągłości bloków

Kryterium	Oryginalny obraz	Zmanipulowany obraz
Gradienty	Spójne, ciągle	Przerwane, nienaturalne kierunki
Jasność	Jednorodne oświetlenie	Lokalna nieciągłość lub anomalie
Statystyki	Zgodne z modelem naturalnym	Odstępstwa od oczekiwanych wartości

Tab. 3. Tabela interpretacji analizy gradientów i jasności

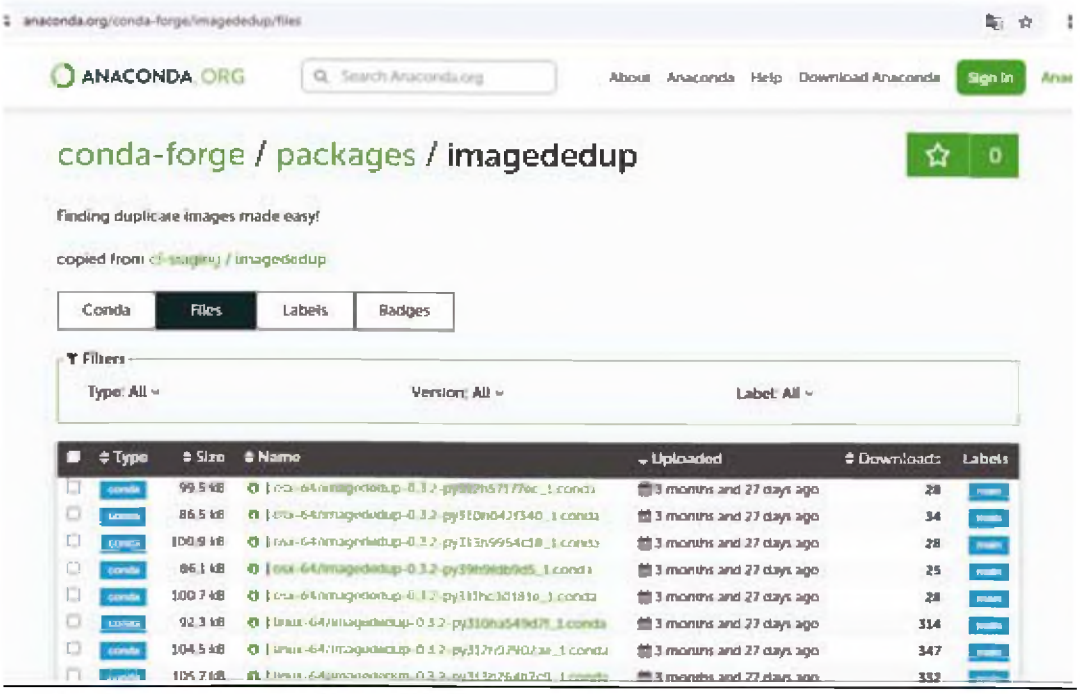


Rys. 9. ***PhotoWorks***[16] *– zaawansowany edytor umożliwiający korekty i ingerencję w obraz*

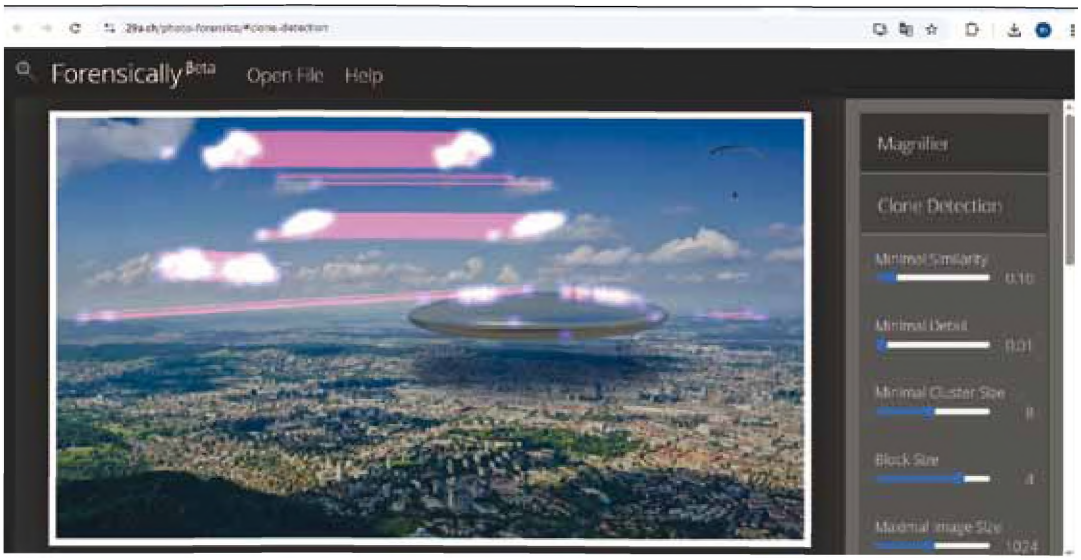
d) Analiza występowania duplikatów

Clone detection[17] – wykrywa duplikaty pikseli (np. używane do maskowania) natomiast serwis **Forensically**[18] posiada tę funkcjonalność wbudowaną w postaci skryptu.

[16] https://fixthephoto.com/pl/best-automatic-photo-editor.html
[17] https://www.sciencedirect.com/topics/computer-science/clone-detection
[18] https://29a.ch/photo-forensics/#clone-detection



Rys. 10. Serwis z oprogramowaniem realizującym funkcję znajdowania duplikatów – archiwum dla różnych systemów operacyjnych



Rys. 11. Wizualizacja działania skryptu w serwisie Forensically

e) Analiza tablic kompresji

JPEG kompresuje obraz powstały na matrycy z formatu **raw** na **jpg** w trakcie zapisywania na nośnik w blokach 8x8 pikseli, korzystając z:

- **Transformacji DCT** (Discrete Cosine Transform) Każdy blok 8×8 pikseli może mieć widoczne granice, szczególnie przy niskiej jakości kompresji. Po wklejeniu fragmentu może pojawić się niespójność między blokami. Widoczne są jako „kratka" lub „mozaika".
- **Kwantyzacji** (redukcji precyzji – główny element stratności).
- **Kompresji entropijnej** (np. Huffmana).

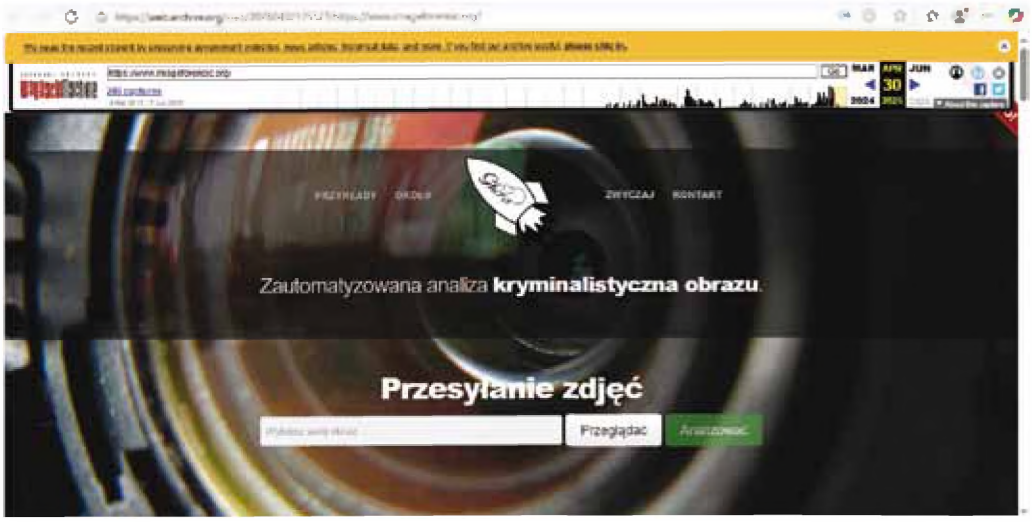
Te kroki zostawiają ślady, które mogą zostać zaburzone przez edycję lub podwójną kompresję. Analiza wykrywa, czy plik był zapisany więcej niż raz jako JPEG i może wskazywać na manipulację lub edycję (np. Photoshop -> eksport JPEG -> ponowne zapisanie).

Oprogramowanie wspomagające analizę

Narzędzie	Funkcje
JPEGsnoop	Odczyt Q-tables, analiza struktury JPEG, identyfikacja aparatu
Forensically (by 29a.ch), Fotoforensics	ELA, JPEG Ghost, analiza bloków JPEG
ExifTool	Wydobywanie metadanych JPEG
ImageMagick / PIL	Manipulacja obrazem, re-kompresja
OpenCV + NumPy	DCT, histogramy blokowe, analiza pikseli

Tab. 4. Narzędzia do analizy JPEG

Zastosowanie: weryfikacja autentyczności zdjęć (np. w dziennikarstwie, sądownictwie), identyfikacja fałszerstw dokumentów, automatyczne wykrywanie deepfake'ów lub montażu.



Rys. 12. Historyczna strona oprogramowania Ghiro z tłumaczeniem na język polski



Rys. 13. Główne cechy – strona z tłumaczeniem na język polski

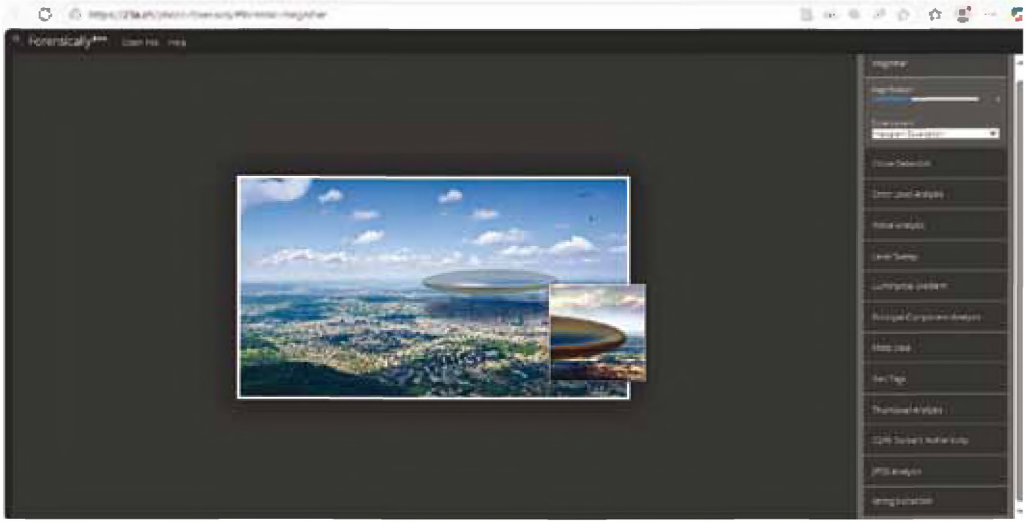
Ghiro umożliwia analizę wielu plików graficznych (batch processing), co czyni je przydatnym narzędziem w śledztwach cyfrowych i testach autentyczności obrazów. Ghiro to open-source'owe narzędzie do analizy kryminalistycznej obrazów cyfrowych, skoncentrowane na automatyzacji analizy metadanych i wykrywaniu manipulacji. Do systemu Ghiro analizowany plik jest ładowany przez API lub interfejs webowy. System wykonuje **wiele analiz równolegle** (np. metadane, ELA, wykrywanie ukrytych danych). Wyniki są zapisywane w bazie danych, a użytkownik

otrzymuje czytelny raport. Można filtrować obrazy wg wykrytych anomalii lub właściwości (np. „wszystkie obrazy z GPS", „obrazy z oznakami manipulacji").

Funkcja	Opis
Analiza metadanych EXIF, IPTC, XMP	Odczyt producenta, modelu aparatu, GPS, daty, softu
Wykrywanie manipulacji JPEG	Analiza kompresji, tablic kwantyzacji, wielokrotnego zapisu
Error Level Analysis (ELA)	Wizualne wskazanie miejsc potencjalnej edycji
Detekcja ukrytych danych (steganografia)	Próby wykrycia ukrytych plików lub danych w obrazie
Hashing (MD5, SHA1, SHA256)	Generowanie odcisków cyfrowych obrazu
Batch Processing	Możliwość analizy tysięcy plików w tle
Interfejs webowy	Intuicyjna przeglądarka z historią i raportami

Tab. 5. Najważniejsze cechy wg użytkowników systemu

Forensically to skuteczne, darmowe narzędzie do wstępnej analizy autentyczności zdjęć. Jest intuicyjne i dostępne w przeglądarce, więc stanowi świetne wsparcie zarówno dla profesjonalistów, jak i amatorów w dziedzinie śledztw cyfrowych. Nie zastępuje jednak specjalistycznych narzędzi komercyjnych (np. **Amped Authenticate** czy **Griffeye Analyze**), ale świetnie je uzupełnia ma on jednak swoje ograniczenia ponieważ nie obsługuje wideo (tylko obrazy statyczne), wymaga ręcznej interpretacji wyników – brak automatycznej decyzji o „fałszerstwie". Najlepiej działa na **obrazach JPEG** – PNG i inne formaty mogą dawać mniej informacji. Nie zapewnia 100% pewności co do autentyczności – to narzędzie wspomagające analizę, a nie orzekające.



Rys. 14. Ekran główny wraz z funkcjonalnościami systemu Forensically

Funkcje	Opis
Magnifer & Zoom	Lupa pozwalająca na dynamiczny podgląd w powiększeniu wskazanego fragmentu obrazu. Pozwala dokładnie przyglądać się szczegółom obrazu. Ułatwia porównanie krawędzi, tekstur, itp.
Error Level Analysis (ELA)	Pokazuje różnice w poziomach kompresji JPG. Pomaga zidentyfikować obszary edytowane. Zmodyfikowane fragmenty mogą mieć inny poziom błędu kompresji niż reszta.
Clone Detection (Wykrywanie klonów)	Wyszukuje powtarzające się fragmenty obrazu. Służy do wykrywania narzędzi typu „kopiuj-wklej" (np. w programie Photoshop). Przydatne w analizie usuniętych lub powielonych obiektów.
Metadata Viewer	Pokazuje dane EXIF z obrazu (np. model aparatu, lokalizacja GPS, data utworzenia). Umożliwia analizę autentyczności i źródła pliku.
Noise Analysis	Analizuje poziom szumu na obrazie. Wskazuje na niejednorodność, typową dla wklejanych elementów.
JPEG Ghosts	Wyszukuje artefakty sugerujące nałożenie obrazów o różnej kompresji. Pomocne w wykrywaniu kolaży lub fotomontaży.
Level Sweep / Histogram	Pomaga wykrywać nienaturalne zmiany jasności, które mogą być efektem edycji.

Tab. 6. Główne funkcje oprogramowania Forensically

MITIS[19]

Jak podaje artykuł w serwisie fotoblogia.pl:

„... **Tak wykrywa się manipulacje na zdjęciach w Polsce**

Naukowcy z krakowskiej AGH zostali nagrodzeni Srebrną Gwiazdą Policji za opracowanie systemu o nazwie MITIS, wykrywającego fałszerstwa w fotografii cyfrowej. Program umożliwia nie tylko wykrycie manipulacji, ale też przywrócenie oryginalnej wersji. Jakie są inne metody tropienia fałszerstw w fotografii?

[19] https://fotoblogia.pl/polski-patent-na-wykrywanie-manipulacji-w-fotografii,6793528252270209a



...”

Rys. 15. https://fotoblogia.pl/polski-patent-na-wykrywanie-manipulacji-w-fotografii,6793528252270209a

Podsumowanie

Metody, narzędzia, środowiska i algorytmy powstawania – tworzenia obrazów cyfrowych tj. zdjęć jak i video wymagają i wymuszają stosowanie coraz bardziej funkcjonalnych narzędzi ich analizy. W artykule wskazano jedynie na główne elementy analizy pomijając analizę treści i faktów związanych utrwalonym obrazem. W artykule pominięto całkowicie szeroko rozumiane zagadnienie „**Graficzny kontent cyfrowy vs AI**”. Obrazy cyfrowe mają jednak ogromny wpływ na wszystkie aspekty naszego życia. Kontent graficzny przestał być załącznikiem do docierającej do nas informacji, a stał się niejednokrotnie jej treścią dodając lub wzmacniając ładunek faktograficzny czy emocjonalny z nią związany. Analiza obrazów cyfrowych jest wymagająca i konieczna zarówno w obszarze treści, jak i technik powstania aby informacja wsparta obrazem była prawdziwa.

Bibliografia[20]

https://getghiro.org/
https://medium.com/@adihendro/photo-forensic-analysis-81f22b02c63a

[20] Dostęp do serwisów w okresie od 01-maja do 25 czerwca 2025.

https://www.fakeimagedetector.com/
https://cse.hkust.edu.hk/image_forensics/
https://www.swiatobrazu.pl/media-manipulacje-fotografia-sposoby.html
https://fixthephoto.com/pl/best-automatic-photo-editor.html
https://ifdetector.com/
https://repozytorium.uni.wroc.pl/Content/58880/PDF/03_Magdalena_Wolinska.pdf
https://pl.shaip.com/blog/15-free-image-datasets-to-train-facial-recognition-models/
https://www.unite.ai/pl/deepface-for-advanced-facial-recognition/
https://www.fakeimagedetector.com/
https://www.fotopolis.pl/warsztat/porady-fotograficzne/998-firmware-aparatu-cyfrowego-co-to-jest
http://mitis.kt.agh.edu.pl/index_pl.html
https://fotoblogia.pl/polski-patent-na-wykrywanie-manipulacji-w-fotografii,6793528252270209a
https://verifeye.online/
https://bgr.com/general/altered-photo-detection-software-verifeyed/
https://spidersweb.pl/2015/07/verifeyed.html
https://spidersweb.pl/tag/verifeyed
https://www.ksoin.pl/5001-2/
https://www.wykop.pl/link/2637245/verifeyed-algorytm-do-wykrywania-fotomontazy-utrudni-zycie-oszustom/
http://learnmem.cshlp.org/site/misc/tsg_JPEG_instructions.pdf
https://niebezpiecznik.pl/post/jak-wykryc-fotomontaz/
http://www.errorlevelanalysis.com/
http://www.euronews.com/2012/07/10/tungstene-the-fake-photo-finder/
https://services.tineye.com/TinEyeAPI
https://www.nchsoftware.com/photoeditor/index.html?kw=download%20software&gclid=EAIaIQobChMIoeKNmuS99AIVEd-yCh08ewBQEAMYASAAEgJNr_D_BwE

Tomasz Typrowicz[1]

Metody oraz zakres gromadzenia, przetwarzania i analizy danych mogących stanowić materiał dowodowy stosowane w Placówkach Straży Granicznej

Wprowadzenie

Artykuł poświęcony jest zaprezentowaniu stosowanych w polskiej Straży Granicznej metod gromadzenia, przetwarzania i analizy danych uzyskiwanych w trakcie realizacji zadań służbowych, do których należą w szczególności: ochrona granicy państwowej[2] oraz kontrola ruchu granicznego[3]. Opisano również inne zasoby bazodanowe, z których korzysta Straż Graniczna, a które w istotny sposób wspierają działania jej funkcjonariuszy. Uzyskane w trakcie realizacji zadań związanych z ochroną granicy państwowej czy kontroli ruchu granicznego dane, stanowią cenne źródło wiarygodnych informacji oraz mogą być wykorzystane jako materiał dowodowy również przez inne uprawnione instytucje.

Kontrola graniczna powinna przebiegać możliwie krótko, z jednoczesnym zachowaniem odpowiednio wysokiego poziomu jej dokładności i skuteczności. Taka kombinacja możliwa jest przede wszystkim dzięki odpowiedniemu wyszkoleniu funkcjonariuszy Straży Granicznej. Chodzi zarówno o znajomość przepisów regulujących zasady wjazdu oraz pobytu jak i sprawne obsługiwanie systemów wspomagających proces kontroli. Mowa tutaj o systemie odpraw granicznych Zintegrowany System Ewidencji 6 (ZSE6), będący jednym z najważniejszych elementów na platformie Centralnych Systemów Informatycznych w Straży Granicznej (CSI SG). ZSE6 pozwala na gromadzenie i przetwarzanie informacji dotyczących podróżnych, ich dokumentów oraz środków transportu z jednoczesną możliwością sprawdzenia w krajowych i międzynarodowych systemach poszukiwawczych. Dodatkowo wykorzystanie w ZSE6 możliwości sprzętu zapewniającego pobieranie i weryfikację danych biometrycznych sprawiło, że możliwe jest obecnie wprowadzenie automatycznych kontroli – bramki biometryczne Automated Border Control (ABC). ZSE6 dzięki swoim modułom weryfikacyjnym, pozwala

[1] Tomasz Typrowicz – oficer Straży Granicznej, Starszy Specjalista Referatu Kryminalnej Analizy Operacyjnej i Przetwarzania Danych GOŚ PSG w Sanoku, biegły sądowy Sądu Okręgowego w Krośnie oraz Sądu Okręgowego w Rzeszowie z zakresu analizy kryminalnej.

[2] Ochrona granicy państwowej (na lądzie i na morzu) – czynności polegające głównie na eliminowaniu przypadków bezprawnego jej przekraczania przez osoby, środki transportu.

[3] Kontrola ruchu granicznego, kontrola graniczna (realizowana w przejściach granicznych) – czynności związane z weryfikacją legalności przekraczania granicy państwowej, spełnienia zasad wjazdu i pobytu.

również na wykonywanie czynności zleconych na polecenie sądu i prokuratury oraz innych właściwych organów państwowych.

Gromadzenie danych

W dniu dzisiejszym termin „granica" odmieniany jest przez wszystkie przypadki. Dzieje się tak głównie z powodu niespokojnej sytuacji na granicy białorusko-polskiej oraz ukraińsko-polskiej co jest wynikiem trwającego konfliktu pomiędzy Ukrainą i Rosją. W ostatnich miesiącach pojawiło się również napięcie na granicy niemiecko-polskiej, będące wynikiem wieloletniego niekontrolowanego napływu nielegalnych migrantów na terytorium Unii Europejskiej (UE) z państw trzecich oraz obecnej „polityki" migracyjnej. Pojawia się dużo pytań na temat znaczenia i zadań formacji granicznych w poszczególnych krajach UE oraz ich zdolności do skutecznej ochrony granic zewnętrznych całej UE oraz strefy Schengen. Ale czy tylko granice zewnętrzne trzeba chronić? Czy obecne granice wewnętrzne UE pozbawione systemu kontroli są bezpieczne?

W Polsce za ochronę granicy państwowej odpowiada Straż Graniczna, opisana jako „jednolita, umundurowana i uzbrojona formacja przeznaczona do ochrony granicy państwowej, kontroli ruchu granicznego oraz zapobiegania i przeciwdziałania nielegalnej migracji"[4]. Ustawodawca jasno i zwięźle określił do czego w głównej mierze została powołana Straż Graniczna, choć obecnie zakres realizowanych przez nią zadań jest znacznie szerszy[5]. Katalog zadań uległ znacznemu rozszerzeniu w chwili wstąpienia Polski do Unii Europejskiej (1 maja 2004 r.) a następnie przystąpienia do Układu z Schengen (21 grudnia 2007 r.). Polska wzięła na siebie obowiązek ochrony zewnętrznych granic Unii Europejskiej – granica lądowa i morska z Rosją, granica lądowa z Białorusią i Ukrainą. W naszym kraju zniesiona została kontrola bezpośrednia na granicy zachodniej (Niemcy) oraz południowej (Czechy, Słowacja). Rozszerzono również zasięg działań Straży Granicznej na obszar całego kraju, oraz dodano nowe zadania m.in. uprawniające do prowadzenia kontroli legalności zatrudnienia (KLZ) oraz kontroli legalności pobytu (KLP).

Na przestrzeni ostatnich 34 lat zmianie ulegały zarówno struktura jak i nazwy jednostek organizacyjnych oraz ich zasięg terytorialny. Struktura Straży Granicznej to w chwili obecnej Komenda Główna SG w Warszawie, Biuro Spraw Wewnętrznych SG, dwa Ośrodki Szkolenia SG (Centrum Szkolenia Straży Granicznej, Ośrodek Szkoleń Specjalistycznych Straży Granicznej), Wyższa Szkoła Straży Granicznej oraz dziewięć oddziałów na terenie całej Polski (Warmińsko-Mazurski Oddział SG, Podlaski Oddział SG, Nadbużański Oddział SG, Bieszczadzki Oddział SG, Karpacki

[4] Art. 1 pkt 1 Ustawy z dnia 12.10.1990 r. o Straży Granicznej.
[5] Rawski 2016, s. 198.

Oddział SG, Śląski Oddział SG, Nadodrzański Oddział SG, Morski Oddział SG i Nadwiślański Oddział SG). W strukturze każdego oddziału funkcjonuje Komenda Oddziału oraz placówki lub w przypadku Morskiego Oddziału – również dywizjony[6]. Pod pojęciem placówki Straży Granicznej należy rozumieć jednostki, które obsługują: drogowe przejścia graniczne, lotnicze przejścia graniczne, kolejowe przejścia graniczne, morskie przejścia graniczne, piesze przejścia graniczne, jednostki przy granicy zielonej i morskiej oraz jednostki w głębi kraju.

Kontrola ruchu granicznego nadal jest jednym z kluczowych zadań dla funkcjonariuszy pełniących służbę w placówkach zlokalizowanych na granicy zewnętrznej: przejścia lotnicze, morskie, drogowe, kolejowe i piesze. W celu usprawnienia kontroli granicznej wprowadzono system dwóch linii kontroli: pierwsza linia (bezpośrednia kontrola) oraz druga linia (czynności wyjaśniające). Funkcjonariusz na pierwszej linii kontroli granicznej, jest osobą, która decyduje czy zezwolić podróżnemu na przekroczenie granicy państwowej, czy też nie. W przypadku wątpliwości przekazuje sprawę do rozpatrzenia na drugiej linii. Trudno sobie nawet wyobrazić na jakiej podstawie taki funkcjonariusz mógłby podjąć słuszną decyzję, gdyby nie miał dostępu do wyników sprawdzeń danych osoby, jej dokumentu lub pojazdu, zapisanych w odpowiednich systemach poszukiwawczych oraz informacyjnych. Dlatego też niezbędne jest posiadanie specjalistycznej aplikacji, wspomagającej kontrolę ruchu granicznego.

Należy pamiętać, że funkcjonariusze, prowadząc działania w strefie przygranicznej (placówki przy granicy zielonej i morskiej) oraz wewnątrz kraju (placówki w głębi kraju), również muszą mieć możliwość dokonania analogicznych sprawdzeń jak w przypadku kontroli ruchu granicznego. Doskonałym przykładem jest choćby konieczność przeprowadzenia legitymowania osoby[7] bądź sprawdzenia dokumentu czy pojazdu, podczas czynności realizowanych w terenie. W takim przypadku funkcjonariusze wykorzystują urządzenia mobilne, zapewniające bezpieczny dostęp do tych samych aplikacji i baz danych co w jednostkach „odprawowych", poprzez sieć telefonii komórkowej.

Nim jednak Straż Graniczna uruchomiła obecnie używany system, przeszła długą drogę w testowaniu i wdrażaniu tego typu aplikacji. Rozwój systemów wspomagających kontrolę ruchu granicznego oraz wykorzystanie technologii informatycznych w Straży Granicznej nabrał rozpędu w chwili przystąpienia do strefy Schengen. Główne prace skierowano wówczas na obsługę międzynarodowego

[6] Źródło https://www.strazgraniczna.pl/pl/straz-graniczna/struktura-sg [dostęp: 31.05.2025 r.].

[7] Legitymowanie osób jest uprawnieniem jakie posiadają funkcjonariusze Straży Granicznej, polegającym na ustaleniu lub potwierdzeniu tożsamości osoby. Wynika ono z art. 11 pkt. 4 Ustawy o Straży Granicznej.

systemu informatycznego o nazwie Schengen Information System (SIS, SIS II)[8] – obecnie SIS RECAST oraz Visa Information System (VIS)[9], jak również na możliwość obsługi danych biometrycznych.

Bazując na posiadanych doświadczeniach w zakresie funkcjonalności, jakie powinna posiadać aplikacja wspomagająca kontrolę ruchu granicznego, powołano w strukturach Straży Granicznej grupę projektową[10], która rozpoczęła w 2012 roku prace nad nową wersją Zintegrowanego Systemu Ewidencji. W pracach uwzględniono doświadczenia zdobyte podczas użytkowania wcześniejszych rozwiązań tj. skorowidze papierowe, lokalne komputery (ROL), rozwiązanie sieciowe (ZSE2, ZSE4, ODPRAWA SG, ZSE5)[11]. W dniu 30 września 2014 r., miało miejsce masowe wdrożenie Zintegrowanego Systemu Ewidencji generacji 6 (ZSE6). System jest zintegrowany z systemami poszukiwawczymi i informacyjnymi na trzech poziomach: lokalnym, krajowym oraz europejskim. Dodatkowo system współpracuje z czytnikami umożliwiającymi, poza klasycznym odczytem dokumentu, także kontrolę biometryczną. Na uwagę zasługuje fakt, iż już od wersji ZSE4 Straż Graniczna ma możliwość weryfikowania danych zawartych w chipie biometrycznym, a od wersji ODPRAWA SG – także pobierania w celach identyfikacji oraz weryfikacji tożsamości osoby odcisków linii papilarnych. Jednakże dopiero wersja ZSE6 zapewnia pełne wykorzystanie biometrii podczas realizacji czynności służbowych. Straż Graniczna wykorzystuje obecnie całostronicowe czytniki dokumentów oraz czteropalcowe czytniki linii papilarnych[12]. Dodatkowo w przejściach lotniczych trwa proces wprowadzania rozwiązania w postaci automatycznych bramek, określanych jako „bramka ABC" lub „e-gate", które umożliwiają podróżnemu samodzielną odprawę graniczną.

[8] SIS, SIS II, SIS RECAST – jest to największa w Europie baza danych, w której przetwarzane są określone przepisami kategorie danych osób i przedmiotów, poszukiwanych i wprowadzanych do systemu przez państwa strefy Schengen. źródło https://home-affairs.ec.europa.eu/policies/schengen/schengen-information-system_pl [dostęp: 31.05.2025 r.].

[9] VIS – System Informacji Wizowej jest to centralny system służący do wymiany informacji wizowej pomiędzy Państwami Członkowskimi Unii Europejskiej. źródło https://home-affairs.ec.europa.eu/policies/schengen/visa-information-system_en [dostęp: 31.05.2025 r.].

[10] Grupa projektowa została powołana decyzją 159 Komendanta Głównego Straży Granicznej z dnia 24 września 2012 r. w sprawie powołania zespołu do wykonywania prac związanych z budową, wdrażaniem i rozwojem centralnych systemów informatycznych Straży Granicznej oraz powołania Komitetu Sterującego nadzorującego prace zespołu.

[11] Rawski 2016, s. 199.

[12] Rawski 2016, s. 203.

ZSE6 współpracuje z następującymi bazami poszukiwawczymi[13]:

1. Ewidencja Zleceń 2 (EZ2) – czynności związane z zatrzymaniem osoby lub poszukiwanego przedmiotu, zakazem wyjazdu z kraju, wręczeniem wezwania lub ustaleniem miejsca pobytu.
2. Wykaz osób niepożądanych w kraju (WYKAZ) – dotyczy osób (cudzoziemców), których wjazd na terytoriom Polski jest zakazany.
3. Krajowy System Informacji Policji (KSIP) – zlecenia dotyczące poszukiwanych osób i przedmiotów w ramach prowadzonych śledztw.
4. System Informacyjny Schengen (SIS RECAST) – państwa strefy Schengen umieszczają czynności zlecone w ramach środka kompensacyjnego za zlikwidowanie kontroli granicznej na granicach wewnętrznych państw strefy; w ramach SIS RECAST państwa wymieniają się informacjami poprzez Biura SIRENE na temat osób i przedmiotów poszukiwanych celem zatrzymania, ustalenia miejsca pobytu lub odnalezienia, czy też kontrolnego rozpytania, jednak sposób i zakres realizacji zlecenia jest uzależniony od prawa krajowego państwa, gdzie zostanie ujawniony alert.
5. INTERPOL – Międzynarodowa Policja Kryminalna zrzeszająca 196 państw umieszcza wpisy dotyczące poszukiwanych osób, dokumentów i przedmiotów, realizacja wpisów jest również uzależniona od norm prawa krajowego.
6. Passenger Name Record (PNR) – dane od przewoźników lotniczych dotyczące przelotu pasażera, umieszczone z 48-godzinnym wyprzedzeniem i zawierają kilka różnych rodzajów informacji, takich jak daty i plan podróży, dane kontaktowe, biuro podróży, w którym zarezerwowano lot, informacje o bagażu itp.; dane są wykorzystywane do oceny pasażerów celem zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń i ścigania sprawców.

Dodatkowo do ZSE6 podpięte są bazy informacyjne takie jak[14]:

1. Powszechny Elektroniczny System Ewidencji Ludności (PESEL), na podstawie którego można zweryfikować tożsamość osoby i jego najbliższej rodziny, miejsce zamieszkania na terenie Polski, posiadane, wydane bądź zgłoszone jako zagubione dokumenty tożsamości.
2. Centralny Rejestr Zezwoleń (CRZ) – dotyczy małego ruchu granicznego (MRG) obecnie tylko z Ukrainą, gdzie odnotowano wnioski o przyznanie zezwolenia oraz status wydanego, zatrzymanego bądź zagubionego zezwolenia.
3. Wizowy System Informacyjny (VIS) – państwa strefy Schengen umieszczają informację o wydanych jednolitych wizach uprawniających na wjazd do państw

[13] Pawłowski, Użyczyn 2023, s. 29.
[14] tamże, s. 29–30.

strefy; można zweryfikować ważność wizy i dane biometryczne posiadacza wizy, czyli wizerunek twarzy i linie papilarne dłoni.
4. Krajowy Rejestr Dokumentów Paszportowych (RDP) – baza weryfikująca dane dotyczące dokumentów paszportowych wydanych przez władze RP.
5. System Wspomagania Kierowania (SWK) – gromadzący szczegółowe informacje dotyczące zdarzeń z udziałem osób i pojazdów odnotowanych przez Straż Graniczną.
6. Krajowy Rejestr Dowodów Osobistych (RDO) – baza gromadząca dane na temat unieważnionych polskich dowodów osobistych.
7. POBYT – baza wydanych cudzoziemcom decyzji administracyjnych związanych z zezwoleniem na osiedlenie się, zezwoleniem na zamieszkanie w Polsce; baza decyzji o nadanie statusu uchodźcy, udzieleniu azylu, informacji o repatriacji i krajowe wnioski wizowe.
8. Baza Dokumentów Uzupełniających (BDU) – baza gdzie na bieżąco rejestrowane i uaktualniane są dane pozwoleń na pracę przedstawionych przez cudzoziemców podczas wjazdu do Polski, celem uwierzytelnienia powodu wjazdu na podstawie okazanej wizy. W bazie rejestrowane są również wszystkie fikcyjne, zamknięte, zawieszone działalności gospodarcze niezgodne z bazą REGON. Informacje te są wykorzystywane do ujawniania prób nielegalnego wjazdu na podstawie wyłudzonej wizy o pracę.

Szczegółowy zakres danych przetwarzanych przez systemy odprawowe zawarto w Zarządzeniu nr 1 Komendanta Głównego Straży Granicznej z dnia 2 stycznia 2015 r. w sprawie sposobu i trybu gromadzenia i przetwarzania informacji z zakresu ochrony granicy państwowej, kontroli ruchu granicznego oraz zapobiegania i przeciwdziałania nielegalnej migracji, aktualizowanego w miarę rozbudowywania oraz pojawiania się nowych baz[15].

Jak już wspomniano wyżej, proces prawidłowego wprowadzania danych do bazy ZSE6 jest ściśle określony przepisami i ma istotne znaczenie z prawnego punktu widzenia, gdyż jest nieodzowny do wydania decyzji np. o odmowie wjazdu, zatrzymania poszukiwanych osóbi przedmiotów, realizacji zleceń sądu i prokuratury, itp. Dlatego czynności te wykonują funkcjonariusze, którzy posiadają odpowiednie przeszkolenie i gwarantują prawidłowe wykorzystanie możliwości systemu. W celu uniknięcia pomyłek podczas wprowadzania danych zastosowano szereg zabezpieczeń w samej bazie, m.in. rozdzielono dostęp dla czynności związanych z odprawą graniczną – moduł ODPRAWA, od czynności związanych z legitymowaniem –

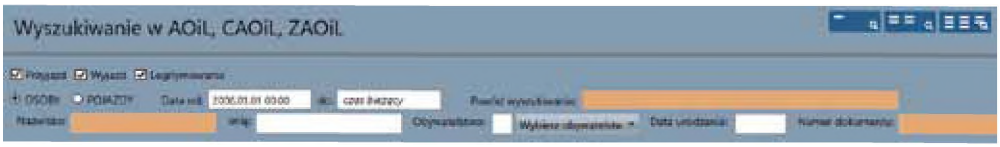
[15] Zarządzenie oraz jego aktualizacje (dostępne na stronie https://e-dziennik.strazgraniczna.pl) opisują wszystkie systemy związane z gromadzenia i przetwarzania informacji z zakresu ochrony granicy państwowej, kontroli ruchu granicznego oraz zapobiegania i przeciwdziałania nielegalnej migracji.

moduł LEGITYMOWANIE. Stosowane są też procedury weryfikacyjne związane z poprawnością i kompletnością wprowadzonych danych, w ramach których wychwytywane są ewentualne błędy lub nieścisłości, które są następnie eliminowane.



Fot. 1. Widok przykładowych modułów CSI SG. Źródło: materiały własne, 2023.

W celu odpytania bazy ZSE6 stworzono osobny moduł ZAOiL – Zintegrowane Archiwum Odpraw i Legitymowania, który umożliwia dokonanie sprawdzenia w archiwalnych danych zgromadzonych w systemach AOiL (ODPRAWA SG, ZSE2), CAOiL (ZSE4, ZSE5), ZAOiL (ZSE6). Dane są dostępne w bazie już w chwili rozpoczęcia prowadzenia kontroli granicznej lub legitymowania. Natomiast okres czasu za jaki możemy odpytać bazę to 10 lat wstecz. ZSE6 posiada również specjalny interfejs dla uprawnionych organów, dzięki któremu mogą one w sposób pośredni, korzystać z informacji dostępnych w systemach Straży Granicznej[16].



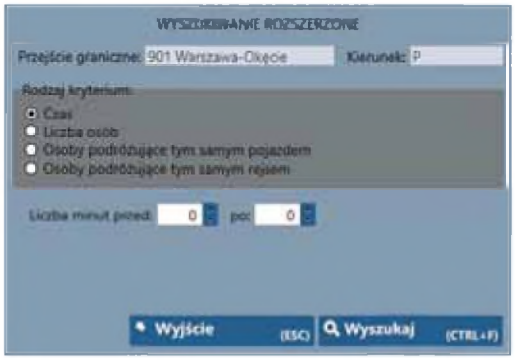
Fot. 2. Widok zakładek podczas wyszukiwania danych osoby lub dokument u podróży w ZSE6 – AOiL, CAOiL, ZAOiL (kolorem pomarańczowym zaznaczono pola wymagane). Źródło: materiały własne, 2023.

[16] Gontarz 2024, s. 1.

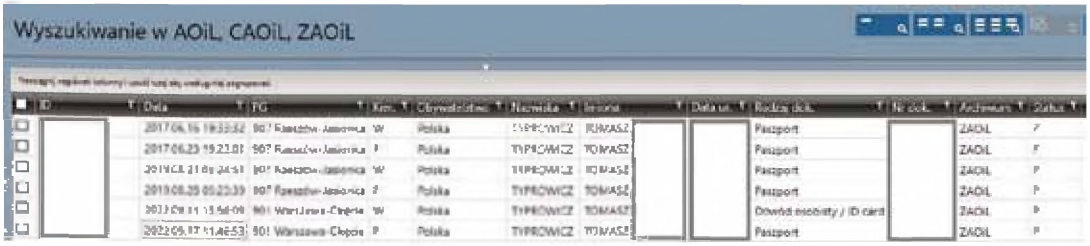


Fot. 3. Widok zakładek podczas wyszukiwania danych pojazdu w ZSE6 – AOiL, CAOiL, ZAOiL (kolorem pomarańczowym zaznaczono pola wymagane). Źródło: materiały własne, 2023.

Baza umożliwia również wyszukiwanie na zasadzie typowania osób czy pojazdów, które przekraczały granicę w danym przejściu granicznym, łącznie z uzyskaniem danych osób towarzyszących. Ma to istotne znaczenie w przypadku ustalenia lub potwierdzenia powiązań pomiędzy osobami, które granicę przekraczały w tym samym okresie czasu: w różnych pojazdach, w środkach komunikacji zbiorowej (autobus, pociąg, samolot), bądź w różnych okolicznościach – w przypadku przejścia obsługującego ruch drogowy i pieszy.

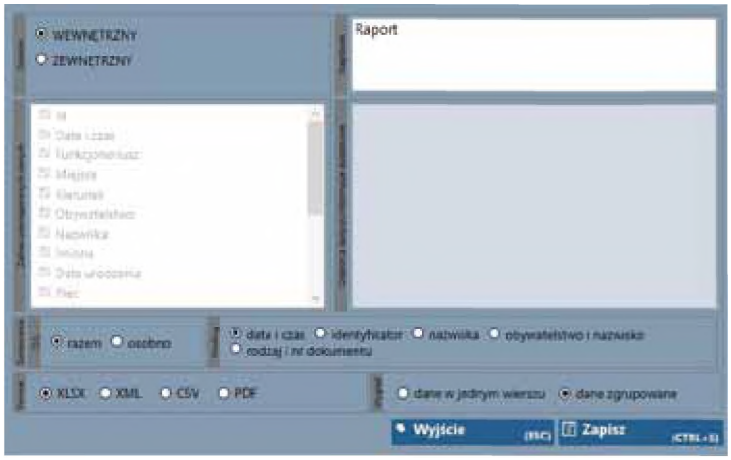


Fot. 4. Widok zakładek podczas wyszukiwania rozszerzonego w ZSE6. Źródło: materiały własne, 2023.



Fot. 5. Widok uzyskanych wyników wyszukiwania osoby w ZSE6. Źródło: materiały własne, 2023.

Wyniki wyszukania można przedstawić w raportach, które mają dwa szablony – dla użytku wewnętrznego SG oraz dla zapytań zewnętrznych. Raporty mogą zostać posortowane razem lub osobno dla ODPRAWY (O) i LEGITYMOWANIA (L) według kryterium daty i czasu, identyfikatora systemowego, nazwiska, obywatelstwa czy rodzaju dokumentu. Ale co najważniejsze raport można uzyskać w postaci edytowalnej (.xlsx, .xml, .csv) lub nieedytowalnej (.pdf).



Fot. 6. Widok zakładek podczas eksportu danych z ZSE6. Źródło: materiały własne, 2023.

Sposób składania wniosków o udostępnienie powyższych danych reguluje Zarządzenie Nr 57 Komendanta Głównego Straży Granicznej z dnia 23 sierpnia 2019 r. w sprawie udostępniania przez Straż Graniczną uprawnionym organom państwowym informacji z zakresu ochrony granicy państwowej, kontroli ruchu granicznego oraz zapobiegania i przeciwdziałania nielegalnej migracji[17]. W dokumencie znajdziemy informacje zawierające wzór wniosku o udostępnienie danych oraz w jakiej formie i do kogo należy go przesłać.

Należy pamiętać, iż system zawiera dane osób, które stawiły się do kontroli granicznej na jednym z Polskich przejść granicznych (lotnicze, morskie, drogowe, kolejowe, piesze) lub zostały wylegitymowane na terytorium Polski. Dlatego nie będzie zwierał danych osób, które wjechały na terytorium naszego kraju przez granicę wewnętrzną UE. Dlatego warto korzystać z innych baz, które mogą uzupełnić tą lukę informacyjną, takich jak: PNR, POBYT, POL-on[18].

[17] Zarządzenia dostępne na stronie https://e-dziennik.strazgraniczna.pl

[18] POL-on system informatyczny, który zbiera dane na temat nauki i szkolnictwa wyższego w całej Polsce.

Przetwarzanie i analiza danych

Jak wspomniano na początku artykułu, Straż Graniczna jest również odpowiedzialna za zapobieganie i przeciwdziałanie nielegalnej migracji. Dlatego w strukturach oddziałów i wybranych placówek funkcjonują komórki odpowiedzialne za prowadzenie czynności dochodzeniowo-śledczych oraz operacyjno-rozpoznawczych. Informacje uzyskiwane przez te komórki, są również gromadzone w celu ich późniejszego wykorzystania oraz poddania analizie m.in. w następujących bazach:

1) CBD EWIDA – Centralna Baza Danych EWIDA, zawiera informacje uzyskane w ramach prowadzonych postępowań przygotowawczych, czynności postępowania przygotowawczego powierzonych przez prokuratora Straży Granicznej do wykonania, postępowań sprawdzających oraz spraw o wykroczenia,
2) A-EWIDA – Centralna Baza Danych EWIDA Analityczna, gdzie przetwarza się do celów analizy kryminalnej zasoby pionu operacyjno-śledczego Straży Granicznej zgromadzone w Centralnej Bazie Danych Analizy Kryminalnej „Analityk",
3) P-EWIDA – Centralną Bazę Danych EWIDA Poufna, w której gromadzi się i przetwarza informacje uzyskane w ramach wykonywanych czynności operacyjno-rozpoznawczych.

Szczegółowy opis funkcjonowania tych baz danych określa Zarządzenie Nr 69 Komendanta Głównego Straży Granicznej z dnia 8 listopada 2019 r. w sprawie organizacji i nadzorowania prowadzonych przez Straż Graniczną postępowań przygotowawczych, czynności postępowania przygotowawczego i postępowań sprawdzających. Okres czasu przez jaki dostępne są dane to 10 lat od dnia uzyskania informacji.



Fot. 7. Widok obiektów wprowadzanych do bazy A-EWIDA. Źródło: materiały własne, 2023.

Wsparciem procesów wykrywczych, zwłaszcza w przypadku dużej ilości danych z różnych źródeł i baz danych zajmuje się analiza kryminalna. Analiza kryminalna to przede wszystkim umiejętne kojarzenie informacji, ich uzupełnianie i wykorzystanie w ramach czynności operacyjno-rozpoznawczych lub dochodzeniowo-śledczych[19]. Narzędzie to jest sukcesywnie implementowane i wykorzystywane w Straży Granicznej od 2003 roku. W chwili obecnej każdy analityk kryminalny ma możliwość korzystania z narzędzi i programów, które ułatwiają mu pracę m.in.: IBM i2 Analyst's Notebook ver. 9.0.6, IBM i2 iBase ver. 8.9.11, Link AGH ver. 2.5.0. Warunkiem prowadzenia czynności analitycznych na odpowiednio wysokim poziomie, jest nieustanne pogłębianie wiedzy z różnych dziedzin. Służą temu m.in. szkolenia specjalistyczne organizowane przez Ośrodki Szkolenia SG ale również instytucje zewnętrzne umożliwiające szkolenia online, takie jak: CEPOL (https://leed.cepol.europa.eu), EUROPOL (https://epe.europol.europa.eu), CISCO (https://www.netacad.com).

Również udział w konferencjach krajowych i międzynarodowych jest okazją do uzupełnienia wiedzy i wymiany doświadczeń. Część z nich jest organizowana regularnie, inne mają charakter jednorazowy. Do najciekawszych, w których miałem okazję brać udział, można zaliczyć te organizowane przez: TeleStrategies (https://www.issworldtraining.com/ ISS_EUROPE/); Centralne Biuro Antykorupcyjne (LEAF2022 https://www.leaf2022.com); Akademię Górniczo Hutniczą (CrimCon https://crimcon.fslab.agh.edu.pl/), Polską Platformę Bezpieczeństwa Wewnętrznego (CINTiA https://ppbw.pl/en/cintia-conference/), Instytut Kościuszki (CYBERSEC https://cybersecforum.eu/), Międzynarodowe Targi Poznańskie (IN.SEC.ON https://insecon.pl).

Straż Graniczna bierze również udział w projektach finansowany przez Narodowe Centrum Badań i Rozwoju w ramach projektów w zakresie badań naukowych i prac rozwojowych na rzecz obronności i bezpieczeństwa państwa. Jako analityk kryminalny miałem możliwość badać przydatność użytkową aplikacji MOBINT, która była realizowana w ramach projektu: „zaawansowane techniki analizy informacji pozyskiwanych z cyfrowych nośników, w szczególności z urządzeń mobilnych" (www.ctb.agh.edu.pl).

Przyszłość

W dzisiejszych czasach naznaczonych tak intensywnym rozwojem technologicznym, instytucje porządku publicznego takie jak Straż Graniczna, mają nie tylko możliwość ale i obowiązek wykorzystania nowych technologii do sprawnego realizowania swoich zadań. Ma to zneutralizować zagrożenie wynikające z wykorzystania tych samych

[19] Nawrocki, 2022, s. 14.

technologii przez osoby niemające czystych intencji i ograniczyć równie dynamiczny rozwój świata przestępczego.

Aby nadążyć za oczekiwaniami zwiększającymi bezpieczeństwo w ruchu, trwają prace nad dwoma systemami wymiany i integracji danych na poziomie UE. Pierwszy z nich o nazwie Entry/Exit System (EES)[20] to system rejestracji cudzoziemców wjeżdżających do jednego z 29 krajów UE na pobyt krótkoterminowy – planowane uruchomienie w październiku 2025 r. Drugi z nich o nazwie European Travel Information and Authorisation System (ETIAS)[21] to system autoryzacji podróżnych z krajów bezwizowych. Podróżni sami będą wypełniać specjalny formularz, na podstawie którego będą sprawdzane warunki ich wjazdu zanim jeszcze dotrą do granic strefy Schengen i wjadą na teren UE – planowane uruchomienie ostatni kwartał 2026 r.

Polska Straż Graniczna odpowiada za wdrożenie tych rozwiązań i jej zadaniem jest stworzenie interfejsu do zadawania zapytań w trybie migracyjnym oraz poszukiwawczym,z którego będą mogły korzystać inne uprawnione organy i służby.

Bibliografia

1. Gontarz A., 2024, Ochrona granicy informatyką stoi, https://crn.pl/wywiady-i-felietony/ochrona-granicy-informatyka-stoi/ [dostęp: 31.05.2025 r.]
2. Kuptel D., 2022, Bramka ABC – jako narzędzie wspomagające odprawę graniczną, „Nowoczesne systemy bezpieczeństwa wspomagające prace Straży Granicznej", Ochrona i Bezpieczeństwo Obiektów i Biznesu, Wydanie Specjalne.
3. Nawrocki D., 2022, Geneza i system szkolenia analityków kryminalnych w Straży Granicznej, „Nowoczesne systemy bezpieczeństwa wspomagające prace Straży Granicznej", Ochrona i Bezpieczeństwo Obiektów i Biznesu, Wydanie Specjalne.
4. Pawłowski M., Użyczyn Ł., 2023, Zintegrowany system ewidencji – początek i jego rozwój na przestrzeni ostatnich 30 lat, „Nowoczesne systemy bezpieczeństwa wspomagające prace Straży Granicznej", Ochrona i Bezpieczeństwo Obiektów i Biznesu, Wydanie Specjalne.
5. Rawski M., 2016, Współczesne konteksty bezpieczeństwa [w:] Informatyczno-techniczne wsparcie działań Straży Granicznej w zakresie kontroli ruchu granicznego oraz ochrony granicy państwowej Rzeczypospolitej Polskiej, red. M. Sitek i in., Józefów, wyd. WSGE.
6. Rozporządzeniu Rady Ministrów z dnia 6 grudnia 2023 r. w sprawie wykonywania niektórych uprawnień przez funkcjonariuszy Straży Granicznej (Dz.U.2023.2693).

[20] źródło https://travel-europe.europa.eu/ees_en [dostęp: 31.05.2025].
[21] źródło https://travel-europe.europa.eu/etias_en [dostęp: 31.05.2025].

7. Ustawa z dnia 12.10.1990 r. o Straży Granicznej (Dz.U.2024.0.915 t.j.).
8. Zarządzenie nr 1 Komendanta Głównego Straży Granicznej z dnia 2 stycznia 2015 r. w sprawie sposobu i trybu gromadzenia i przetwarzania informacji z zakresu ochrony granicy państwowej, kontroli ruchu granicznego oraz zapobiegania i przeciwdziałania nielegalnej migracji (Dz.Urz.KGSG.2015.1).
9. Zarządzenie Nr 57 Komendanta Głównego Straży Granicznej z dnia 23 sierpnia 2019 r. w sprawie udostępniania przez Straż Graniczną uprawnionym organom państwowym informacji z zakresu ochrony granicy państwowej, kontroli ruchu granicznego oraz zapobiegania i przeciwdziałania nielegalnej migracji (Dz.Urz. KGSG.2019.59).
10. Zarządzenie Nr 69 Komendanta Głównego Straży Granicznej z dnia 8 listopada 2019 r. w sprawie organizacji i nadzorowania prowadzonych przez Straż Graniczną postępowań przygotowawczych, czynności postępowania przygotowawczego i postępowań sprawdzających (Dz.Urz.KGSG.2019.73).

inż. Ireneusz Wasiewicz[1]

Tajemnice zawodowe w Polsce – czyli rzecz o pragmatyce procesowej przy zabezpieczaniu nietypowych i wrażliwych dowodów cyfrowych

1. Wprowadzenie

Tajemnica zawodowa to prawnie chroniony obowiązek zachowania w poufności informacji uzyskanych w związku z wykonywaniem określonego zawodu. Jej naruszenie może prowadzić do odpowiedzialności karnej, cywilnej, a także dyscyplinarnej. W polskim systemie prawnym tajemnice zawodowe mają swoje umocowanie zarówno w przepisach szczególnych jak ustawy branżowe, jak i ogólnych (np. Kodeks karny, Kodeks postępowania karnego, Kodeks postępowania cywilnego).

Jeżeli konieczne jest zabezpieczenie dowodowe danych zawierających jedną z przytoczonych w niniejszym opracowaniu tajemnic zawodowych, należy dopasować metodologię i sposób zabezpieczenia, tak by technicy kryminalni i informatycy śledczy oraz kolejne osoby w toku postępowania i łańcuchu dowodowym, nie naraziły zabezpieczonego materiału na nieautoryzowane zapoznanie się z przedmiotowymi informacjami oraz w taki sposób, by nie były kwestionowane podjęte działania procesowe. Do czasu podjęcia decyzji przez sąd i prokuratora gospodarza postępowania, informacja pozostaje zablokowana, zamknięta i niedostępna (np. w kopertach bezpiecznych zabezpieczona np. jak środki finansowe).

Historycznie rzecz ujmując, informacja zawsze była cenna – łacińskie *„informare"* oznacza; *„kształtować, wyobrażać, określać"* – niesiona treść i jej wartość w określonych okolicznościach zawsze mały niebagatelne znaczenie dla odpowiednich osób.

Zestaw informacji posiadający dodatkowo określone atrybuty jak kompletność, aktualność, adresowalność mógł być informacją, co najmniej wrażliwą i cenną, a w skrajnym przypadku informacją objętą tajemnicą. Jednocześnie nie ma znaczenia, czy niniejsza informacja była wyrażona ustnie, pisemnie, elektronicznie, czy też jest to przekaz skutecznie zakodowany. Sam fakt istotności przekazu jest wystarczający dla podejmowania odpowiednich środków, w tym technicznych, kryptograficznych i proceduralnych, by dbać o ograniczone i identyfikowalne grono dysponentów i odbiorców informacji. Utrata ścisłej kontroli nad nośnikiem przekazu, naraża

[1] Ireneusz Wasiewicz – funkcjonariusz państwowych służb fiskalnych i mundurowych RP z 30 letnim stażem, zajmujący się, na co dzień cyberprzestępczością, bezpieczeństwem teleinformatycznym oraz identyfikowaniem, utrwalaniem oraz analizą artefaktów i śladów cyfrowych.

informację poufną na niekontrolowane ujawnienie a osobę lub organizację, do której należy na poważną szkodę.

2. Ogólne podstawy prawne

Konstytucja RP (art. 47, 49, 51) – ochrona prywatności, korespondencji i danych osobowych.

Kodeks karny (art. 266 §1–2) – przestępstwo ujawnienia tajemnicy zawodowej.

Kodeks postępowania karnego (art. 180 §1–2) – przesłuchanie osób zobowiązanych do zachowania tajemnicy zawodowej.

Kodeks postępowania cywilnego (art. 261 §2) – odmowa zeznań ze względu na tajemnicę zawodową.

Zawodowe ustawy branżowe.

3. Wykorzystanie informatyki

Tajemnice zawodowe i branżowe, nie wykluczając także tajemnic państwowych, to w obecnym czasach, w znaczącej ilości dane przechowywane i przetwarzane w sposób elektroniczny oraz przetwarzane cyfrowo i przekazywane w sposób zdalny, najczęściej zakodowane różnorodnymi mechanizmami szyfrowania kryptograficznego. Procedura ta w sposób oczywisty i celowy zabezpiecza przechowywanie, przetwarzanie i transmisję tych danych przed ujawnieniem osobom nieuprawnionym.

W procedurze procesowego utrwalenia informacji w celu dowodowym wyróżniamy:

- źródło dowodowe zawierające informację czyli środek dowodowy (ślad kryminalistyczny), np. dawniej tablica kamienna, płótno, zapisany papier, zaschnięte błoto, fotografia napisu na murze, korespondencja elektroniczna, utrwalony ślad daktyloskopijny, zeznanie świadka, kaseta z zapisem audio-video, zapis na dysku komputerowym, nośnik wymienny typu flash, nośnik CD/DVD/BD, informacje pobrane z serwera sieci komputerowej czy też dane transmitowane przez medium cyfrowe itp.;
- informacja elektroniczna – wg informatyki sądowej (ang. computer forensic) – elektroniczny ślad kryminalistyczny na określonym nośniku;
- ślad kryminalistyczny – weryfikowalny zapis informacji lub stanu, prowadzący do odtworzenia i ustalenia przebiegu zdarzeń, będących przedmiotem postępowania, zgodnie z rzeczywistością w celu ustalenia prawdy obiektywnej (prawdy materialnej).

3.1. Informacja elektroniczna

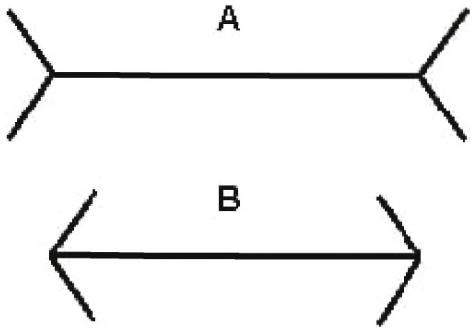
Ogólne cechy informacji:

- niematerialna forma,
- trwałość informacji jest uzależniona od rodzaju nośnika,
- możliwość utrwalania, gromadzenia, zwielokrotniania i przetwarzania,
- możliwość przesyłania,
- możliwość zdalnego dostępu (także anonimowego),
- łatwość modyfikacji lub zniszczenia.

A gdzie podziały się:

- jednoznaczność i trwałość dowodu, a przynajmniej w zakresie wyglądu, brzmienia, znaczenia lub sensu,
- niepodważalność stanu faktycznego,
- poufność,
- trwałe umiejscowienie dowodu, co do miejsca, strefy i czasu – tzw. znaczniki czasowe?





Atrybuty informacji wg teorii zarządzania [patrz norma ISO/IEC 2382-8:2001]:

- dostępność,
- aktualność,
- rzetelność,
- kompletność,
- porównywalność,
- przetwarzalność,
- koszt,

- adresowalność,
- użyteczność,
- priorytetowość,
- wartość,
- poufność,
- jednoznaczność,
- szczegółowość,
- przejrzystość.

Informacja – atrybuty (wg normy ISO 27001):

- podstawowe:
- integralność,
- poufność,
- dostępność;
- dodatkowe:
- autentyczność,
- rozliczalność,
- niezaprzeczalność,
- niezawodność,
- prywatność,
- anonimowość.

3.2 Dokument elektroniczny

Dokument elektroniczny, to:

- informacja przesyłana lub utrwalona elektronicznie (cyfrowo), która może mieć znaczenie dowodowe,
- stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych.

Dokumenty elektroniczne, podział ze względu na sposób pozyskania:

- dowody pozyskane w wyniku procesowego utrwalenia danych,
- dowody przechowywane w systemach elektronicznych,
- dowody pochodzące z systemów retencyjnych publicznych operatorów,
- dowody utrwalone nielegalnie.

Dokument elektroniczny, cechy nietrwałe:

- ulotność,
- nietrwałość rozumiana jako zmienność stanu informacji,
- łatwość manipulacji,
- łatwość utracenia lub usunięcia.

Dokument elektroniczny w rozumieniu kpk: stanowi źródło informacji prowadzące do weryfikacji faktów, umożliwiające tym samym dowodzenie w prowadzonym postępowaniu.

3.3 Dokument i informacja elektroniczna w prawie

A co jeżeli dowód zawiera informacje niejawne ?

Art. 180. kpk [Tajemnica zawodowa i służbowa]

§ 1. Osoby obowiązane do zachowania w tajemnicy informacji niejawnych o klauzuli tajności „zastrzeżone" lub „poufne" lub tajemnicy związanej z wykonywaniem zawodu lub funkcji mogą odmówić zeznań co do okoliczności, na które rozciąga się ten obowiązek, chyba że sąd lub prokurator dla dobra wymiaru sprawiedliwości zwolni te osoby od obowiązku zachowania tajemnicy, jeżeli ustawy szczególne nie stanowią inaczej. Na postanowienie w tym przedmiocie przysługuje zażalenie.

§ 2. Osoby obowiązane do zachowania tajemnicy notarialnej, adwokackiej, radcy prawnego, doradcy podatkowego, lekarskiej, dziennikarskiej lub statystycznej oraz tajemnicy Prokuratorii Generalnej, mogą być przesłuchiwane co do faktów objętych tą tajemnicą tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu. W postępowaniu przygotowawczym w przedmiocie przesłuchania lub zezwolenia na przesłuchanie decyduje sąd, na posiedzeniu bez udziału stron, w terminie nie dłuższym niż 7 dni od daty doręczenia wniosku prokuratora. Na postanowienie sądu przysługuje zażalenie.

§ 3. Zwolnienie dziennikarza od obowiązku zachowania tajemnicy nie może dotyczyć danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również identyfikację osób udzielających informacji opublikowanych lub przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie powyższych danych.

§ 4. Przepisu § 3 nie stosuje się, jeżeli informacja dotyczy przestępstwa, o którym mowa w art. 240 § 1 Kodeksu karnego.

§ 5. Odmowa przez dziennikarza ujawnienia danych, o których mowa w § 3, nie uchyla jego odpowiedzialności za przestępstwo, którego dopuścił się publikując informację.

Gdzie jest zatem problem ?

Art. 225. kpk

[Postępowanie z dokumentami zawierającymi informacje niejawne znalezionymi w toku przeszukania]

§ 1. Jeżeli kierownik instytucji państwowej lub samorządowej albo też osoba, u której dokonano zatrzymania rzeczy lub u której przeprowadza się przeszukanie,

oświadczy, że wydane lub znalezione przy przeszukaniu pismo lub inny dokument zawiera informacje niejawne lub wiadomości objęte tajemnicą zawodową lub inną tajemnicą prawnie chronioną albo ma charakter osobisty, organ przeprowadzający czynność przekazuje niezwłocznie pismo lub inny dokument bez jego odczytania prokuratorowi lub sądowi w opieczętowanym opakowaniu.

§ 2. Tryb wskazany w §1 nie obowiązuje w stosunku do pism lub innych dokumentów, które zawierają informacje niejawne o klauzuli „zastrzeżone" lub „poufne" albo dotyczą tajemnicy zawodowej lub innej tajemnicy prawnie chronionej, jeżeli ich posiadaczem jest osoba podejrzana o popełnienie przestępstwa, ani w stosunku do pism lub innych dokumentów o charakterze osobistym, których jest ona posiadaczem, autorem lub adresatem.

§ 3. Jeżeli obrońca lub inna osoba, od której żąda się wydania rzeczy lub u której dokonuje się przeszukania, oświadczy, że wydane lub znalezione w toku przeszukania pisma lub inne dokumenty obejmują okoliczności związane z wykonywaniem funkcji obrońcy, organ dokonujący czynności pozostawia te dokumenty wymienionej osobie bez zapoznawania się z ich treścią lub wyglądem. Jeżeli jednak oświadczenie osoby nie będącej obrońcą budzi wątpliwości, organ dokonujący czynności przekazuje te dokumenty z zachowaniem rygorów określonych w § 1 sądowi, który po zapoznaniu się z dokumentami zwraca je w całości lub w części, z zachowaniem rygorów określonych w §1, osobie, od której je zabrano, albo wydaje postanowienie o ich zatrzymaniu dla celów postępowania.

§ 4. Wydaną, odebraną lub znalezioną w toku przeszukania dokumentację psychiatryczną organ przeprowadzający czynność przekazuje, z zachowaniem rygorów określonych w §1, sądowi lub prokuratorowi.

Art. 226. kpk

[Wykorzystanie jako dowodów dokumentów zawierających informacje niejawne]

W kwestii wykorzystania dokumentów zawierających informacje niejawne lub tajemnicę zawodową, jako dowodów w postępowaniu karnym, stosuje się odpowiednio zakazy i ograniczenia określone w art 178–181.

Jednakże w postępowaniu przygotowawczym o wykorzystaniu, jako dowodów, dokumentów zawierających tajemnicę lekarską decyduje prokurator.

Art. 236a. kpk

[Odpowiednie stosowanie przepisów rozdziału do danych informatycznych lub systemu informatycznego]

Przepisy rozdziału niniejszego 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.

Art. 236b. kpk

[Odpowiednie stosowanie przepisów rozdziału do danych informatycznych lub systemu informatycznego]

§ 1. Rzeczą lub przedmiotem w rozumieniu przepisów niniejszego rozdziału są również środki na rachunku.

§ 2. Postanowienie w przedmiocie dowodów rzeczowych może dotyczyć środków na rachunku, jeżeli zostały zatrzymane jako dowód w sprawie.

4. Klasyfikacja tajemnic

4.1. Podział tajemnic ze względu na przepisy prawa

- informacje niejawne – tajemnica państwowa,
  zgodnie z przepisami Ustawy o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. jest to informacja wymagająca ochrony przed nieuprawnionym ujawnieniem, która spowodowałaby lub mogłaby spowodować szkody dla Rzeczypospolitej Polskiej, niezależnie od formy i sposobu jej wyrażania. Informacjom niejawnym nadaje się klauzulę tajności, adekwatną do szkody jaka może zostać wyrządzona przez jej ujawnienie (tzw. szkoda potencjalna),
- informacje prywatne,
  konstytucyjnie chronione prawo do wolności, prywatności i ochrony dóbr osobistych;
  - prawo do ochrony danych osobowych;
  - prawo do obrony siebie/swoich bliskich przed sądami i organami państwa;
  - prawo do nieujawniania sympatii politycznych i wyborczych;
  - prawo do nieujawniania preferencji seksualnych ...
- tajemnice zawodowe,
  informacje pozyskane lub udostępnione w wyniku wykonywania zawodu.

4.2. Podział ze względu na potoczne rozumienie prawa

- chronione informacje publiczne (państwowe)
  to samo, co informacje niejawne zgodnie z przepisami Ustawy o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r., a jednocześnie znacznie szerzej rozumiane jako informacje przetwarzane w ramach obowiązków służbowych i potencjalnie wymagające ochrony (czasami nadmiernej – z uwagi na prawo do jawności życia publicznego) przed nieuprawnionym ujawnieniem;

- informacje wrażliwe
  to samo co ochrona prywatności każdej osoby, konstytucyjnie chronione prawo do wolności, prywatności, wiary i ochrony dóbr osobistych, etc.;
- tajemnica służbowa
  to samo lub podobnie co tajemnica zawodowa oraz tajemnica państwowa zdefiniowana w latach 1999–2010 w ustawie o ochronie informacji niejawnych (obecnie wycofana), czyli potocznie informacje pozyskane lub udostępnione w wyniku wykonywania zawodu, także rozumiane szerzej jako ochrona informacji firmowych i publicznych (firm, urzędów, organów i instytucji), do których pracownik ma dostęp z racji wykonywanej funkcji lub zawodu.

4.3. Terminy nieaktualne w obiegu prawnym:

- tajemnica państwowa
  termin funkcjonujący do roku 2010 i wycofany przepisami Ustawy o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r., oznaczał wyjątkowo wrażliwe informacje państwowe sygnowane klauzulą ściśle tajne i tajne (art. 2 pkt 1);
- tajemnica służbowa
  termin funkcjonujący do roku 2010 i wycofany przepisami Ustawy o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r., oznaczał informację niejawną niebędącą tajemnicą państwową – poufną i zastrzeżoną, uzyskaną w związku z czynnościami służbowymi albo wykonywaniem prac zleconych, której nieuprawnione ujawnienie mogłoby narazić na szkodę interes państwa, interes publiczny lub prawnie chroniony interes obywateli albo jednostki organizacyjnej (art. 2 pkt 2);
- tajemnica wojskowa
  termin funkcjonujący w II RP, wycofany po roku 1945 i określający wówczas informacje niejawne dotyczące funkcjonowania sił zbrojnych, których to nieuprawnione ujawnienie mogłoby spowodować istotne zagrożenie dla niepodległości i nienaruszalności terytorium kraju oraz dla podstawowych interesów obronności, bezpieczeństwa państwa i obywateli.

4.4. Bezwzględne zakazy dowodowe oraz prawa

Art. 178. kpk

Nie wolno przesłuchiwać jako świadków:

1) obrońcy albo adwokata lub radcy prawnego działającego na podstawie art. 245 (kontakt zatrzymanego z adwokatem lub radcą prawnym, zawiadomienie o zatrzymaniu § 1), co do faktów, o których dowiedział się udzielając porady prawnej lub prowadząc sprawę;

2) duchownego co do faktów, o których dowiedział się przy spowiedzi.

Art. 178a. kpk

Nie wolno przesłuchiwać jako świadka mediatora co do faktów, o których dowiedział się od oskarżonego lub pokrzywdzonego prowadząc postępowanie mediacyjne, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 karalne niezawiadomienie o czynie zabronionym § 1 Kodeksu karnego (ludobójstwo, masowy zamach, stosowanie środków masowej zagłady, zamach stanu, szpiegostwo, zabójstwo, pedofilia, zamach na życie i zdrowie (...)

Art. 179. kpk

Zwolnienie od obowiązku zachowania tajemnicy państwowej:

§ 1. Osoby obowiązane do zachowania w tajemnicy informacji niejawnych o klauzuli tajności „tajne" lub „ściśle tajne" mogą być przesłuchane co do okoliczności, na które rozciąga się ten obowiązek, tylko po zwolnieniu tych osób od obowiązku zachowania tajemnicy przez uprawniony organ przełożony.

§ 2. Zwolnienia wolno odmówić tylko wtedy, gdyby złożenie zeznania wyrządzić mogło poważną szkodę państwu.

§ 3. Sąd lub prokurator może zwrócić się do właściwego naczelnego organu administracji rządowej o zwolnienie świadka od obowiązku zachowania tajemnicy, jeżeli ustawy szczególne nie stanowią inaczej.

Art. 180. kpk

Przesłuchiwanie osób obowiązanych do zachowania tajemnicy zawodowej:

§ 1. Osoby obowiązane do zachowania w tajemnicy informacji niejawnych o klauzuli tajności „zastrzeżone" lub „poufne" lub tajemnicy związanej z wykonywaniem zawodu lub funkcji mogą odmówić zeznań co do okoliczności, na które rozciąga się ten obowiązek, chyba że sąd lub prokurator dla dobra wymiaru sprawiedliwości zwolni te osoby od obowiązku zachowania tajemnicy, jeżeli ustawy szczególne nie stanowią inaczej.

Na postanowienie w tym przedmiocie przysługuje zażalenie.

§ 2. Osoby obowiązane do zachowania tajemnicy notarialnej, adwokackiej, radcy prawnego, doradcy podatkowego, lekarskiej, dziennikarskiej lub statystycznej oraz tajemnicy Prokuratorii Generalnej, mogą być przesłuchiwane co do faktów objętych tą tajemnicą tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność nie może być ustalona na podstawie innego dowodu. W postępowaniu przygotowawczym w przedmiocie przesłuchania lub zezwolenia na przesłuchanie decyduje sąd, na posiedzeniu bez udziału stron, w terminie nie dłuższym niż 7 dni od daty doręczenia wniosku prokuratora. Na postanowienie sądu przysługuje zażalenie.

§ 3. Zwolnienie dziennikarza od obowiązku zachowania tajemnicy nie może dotyczyć danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również identyfikację osób

udzielających informacji opublikowanych lub przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie powyższych danych.

§ 4. Przepisu § 3 nie stosuje się, jeżeli informacja dotyczy przestępstwa, o którym mowa w art. 240 karalne niezawiadomienie o czynie zabronionym § 1 Kodeksu karnego.

§ 5. Odmowa przez dziennikarza ujawnienia danych, o których mowa w § 3, nie uchyla jego odpowiedzialności za przestępstwo, którego dopuścił się publikując informację.

5. Przegląd tajemnic zawodowych

5.1. Tajemnica adwokacka i radcowska

Dotyczy wszelkich informacji i danych uzyskanych przez adwokata lub radcę prawnego w związku z udzielaniem pomocy prawnej (porady, obrona, reprezentacja).

Podstawa prawna:

Art. 6 ustawy Prawo o adwokaturze [Dz.U. 1982 nr 16 poz. 124]

1. Adwokat obowiązany jest zachować w tajemnicy wszystko, o czym dowiedział się w związku z udzielaniem pomocy prawnej.
2. Obowiązek zachowania tajemnicy zawodowej nie może być ograniczony w czasie.
3. Adwokata nie można zwolnić od obowiązku zachowania tajemnicy zawodowej co do faktów, o których dowiedział się udzielając pomocy prawnej lub prowadząc sprawę.
4. Obowiązek zachowania tajemnicy zawodowej nie dotyczy informacji; udostępnianych na podstawie przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, przekazywanych na podstawie przepisów rozdziału 11a działu III ustawy z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa (Dz. U. z 2021 r. poz. 1540, 1598, 2076, 2105, 2262 i 2328), w zakresie określonym tymi przepisami.

Art. 3 ust. 3 ustawy o radcach prawnych

Pragmatyka procesowa:

1. Adwokat odmawia zeznań przed sądem, powołując się na nienaruszalność tajemnicy obrończej.
2. Wniosek obrońcy o wyłączenie jawności rozprawy, by nie naruszyć poufności danych klienta.

5.2. Tajemnica postępowania przygotowawczego

Zapis regulowany w polskim prawie (dot. także rozpraw przed sądami):

- w ustawie z dnia 28 stycznia 2016 r. Prawo o prokuraturze [t.j. Dz.U. 2024 poz. 1564],

- w ustawie z dnia 6 czerwca 1997 r. Kodeks karny [t.j. Dz.U. 2025 poz. 383].

Podstawa prawna: Ustawa Prawo o prokuraturze

Art. 102 Obowiązek zachowania tajemnicy

§ 1. Prokurator jest obowiązany zachować w tajemnicy okoliczności sprawy, o których w postępowaniu przygotowawczym, a także poza jawną rozprawą sądową, powziął wiadomość ze względu na swoje stanowisko prokuratora.

§ 2. Obowiązek zachowania tajemnicy trwa także po ustaniu stosunku służbowego.

§ 3. Obowiązek zachowania tajemnicy ustaje, gdy prokurator składa zeznania jako świadek w postępowaniu przygotowawczym lub przed sądem, chyba że ujawnienie tajemnicy zagraża dobru Państwa albo takiemu ważnemu interesowi prywatnemu, który nie jest sprzeczny z celami wymiaru sprawiedliwości. W takich przypadkach od obowiązku zachowania tajemnicy może zwolnić prokuratora Prokurator Krajowy, a Prokuratora Krajowego – Prokurator Generalny.

Ustawa Kodeks karny

Art. 241

§ 1. Kto bez zezwolenia rozpowszechnia publicznie wiadomości z postępowania przygotowawczego, zanim zostały ujawnione w postępowaniu sądowym, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Tej samej karze podlega, kto rozpowszechnia publicznie wiadomości z rozprawy sądowej prowadzonej z wyłączeniem jawności.

5.3. Tajemnica sędziowska

Termin wprowadzony ustawą z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych i ustawa o Sądzie Najwyższym z dnia 23 listopada 2002 r.

Podstawa prawna: Prawo o ustroju sądów powszechnych [Dz.U. 2001 Nr 98 poz. 1070]

§ 1. Sędzia jest obowiązany zachować w tajemnicy okoliczności sprawy, o których powziął wiadomość ze względu na swój urząd, poza jawną rozprawą sądową.

§ 2. Obowiązek zachowania tajemnicy trwa także po ustaniu stosunku służbowego.

§ 3. Obowiązek zachowania tajemnicy ustaje, gdy sędzia składa zeznania jako świadek przed sądem, chyba że ujawnienie tajemnicy zagraża dobru państwa albo takiemu ważnemu interesowi prywatnemu, który nie jest sprzeczny z celami wymiaru sprawiedliwości. W tych przypadkach od obowiązku zachowania tajemnicy może zwolnić sędziego Minister Sprawiedliwości.

§ 4. Wobec osoby pełniącej urząd na stanowisku sędziego postępowania sprawdzającego przewidzianego w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742) nie przeprowadza się. Przed przystąpieniem do pełnienia obowiązków sędzia zapoznaje się z przepisami o ochronie

informacji niejawnych i składa oświadczenie o znajomości tych przepisów. Informacje niejawne mogą być udostępnione sędziemu tylko w zakresie niezbędnym do pełnienia urzędu na stanowisku sędziowskim, pełnienia powierzonej funkcji lub wykonywania powierzonych czynności.

5.4. Tajemnica prokuratorska

Termin wprowadzony ustawą z dnia 28 stycznia 2016 r. Prawo o prokuraturze

Podstawa prawna: ustawa Prawo o prokuraturze [t.j. Dz.U. 2024 poz. 390]

§ 1. Prokurator jest obowiązany zachować w tajemnicy okoliczności sprawy, o których w postępowaniu przygotowawczym, a także poza jawną rozprawą sądową, powziął wiadomość ze względu na swoje stanowisko prokuratora.

§ 2. Obowiązek zachowania tajemnicy trwa także po ustaniu stosunku służbowego.

§ 3. Obowiązek zachowania tajemnicy ustaje, gdy prokurator składa zeznania jako świadek w postępowaniu przygotowawczym lub przed sądem, chyba że ujawnienie tajemnicy zagraża dobru Państwa albo takiemu ważnemu interesowi prywatnemu, który nie jest sprzeczny z celami wymiaru sprawiedliwości. W takich przypadkach od obowiązku zachowania tajemnicy może zwolnić prokuratora Prokurator Krajowy, a Prokuratora Krajowego – Prokurator Generalny.

5.5. Tajemnica Prokuratorii Generalnej RP

Termin wprowadzony ustawą z dnia 15 grudnia 2016 r. Prawo o Prokuratorii Generalnej RP.

Podstawa prawna: ustawa Prawo o Prokuratorii Generalnej RP [Dz.U. 2016 poz. 2261]

Rozdział 4,

Art. 38 i Art. 39. [Tajemnica Prokuratorii Generalnej]

1. Czynności Prokuratorii Generalnej związane z wykonywaniem zastępstwa, wydawaniem opinii, sporządzaniem raportów, analiz i stanowisk, udziałem w negocjacjach i mediacjach oraz w postępowaniach przed organami międzynarodowymi, a także informacje i dokumenty stanowiące podstawę dokonania takich czynności są objęte tajemnicą Prokuratorii Generalnej.

2. Dokumenty sporządzone w związku z czynnościami, o których mowa w ust. 1, przez Prokuratorię Generalną, podmiot reprezentujący Skarb Państwa, organ lub osobę zastępowaną mogą być udostępnione przez właściwą jednostkę albo osobę prawną po zakończeniu sprawy.

3. W przypadku gdy dokumenty zakończonej sprawy są związane z inną sprawą prowadzoną przez Prokuratorię Generalną, podmiot reprezentujący Skarb Państwa, organ lub osobę zastępowaną mogą być one udostępnione po zakończeniu tej sprawy.

(...)

5.6. Tajemnica autorska

Obejmuje źródła informacji wykorzystane w utworze, dotyczy wydawcy i producenta.

Podstawa prawna: ust. o prawie autorskim i prawach pokrewnych [Dz.U. 1992 nr 24 poz. 83]

Pragmatyka procesowa:

Autor lub producent dzieła może odmówić zeznań przed sądem, powołując się na nienaruszalność tajemnicy autorskiej.

5.7. Tajemnica lekarska

Obejmuje wszelkie informacje uzyskane przez lekarza podczas udzielania świadczeń zdrowotnych i opieki medycznej.

Cytując Hipokratesa:

„Cokolwiek bym podczas leczenia, czy poza nim, z życia ludzkiego ujrzał, czy usłyszał, czego nie należy na zewnątrz rozgłaszać, będę milczał, zachowując to w tajemnicy".

Podstawa prawna:

Art. 40 ust. 1 ustawy o zawodach lekarza i lekarza dentysty [Dz.U. 1997 nr 28 poz. 152]

Art. 14 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta [Dz.U. 2009 nr 52 poz. 417]

Pragmatyka procesowa:

1. Lekarz odmawia zeznań przed sądem bez zgody pacjenta lub sądu.
2. Sąd zwraca się do okręgowej izby lekarskiej o opinię, czy uchylenie tajemnicy jest zasadne.

5.8. Tajemnica dziennikarska

Chroni źródła informacji dziennikarza oraz tożsamość informatorów.

Podstawa prawna:

art. 180 §3 Kodeksu postępowania karnego [Dz.U. 1997 nr 89 poz. 555],

art. 15 ust. 2 ustawy Prawo prasowe [Dz. U. 1984 nr 5 poz. 24]

Dziennikarz ma obowiązek zachowania w tajemnicy:

- danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również innych osób udzielających informacji opublikowanych albo przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie powyższych danych,
- wszelkich informacji, których ujawnienie mogłoby naruszać chronione prawem interesy osób trzecich.

Pragmatyka procesowa:

1. Redaktor naczelny odmawia wydania materiałów źródłowych bez postanowienia sądu.
2. Dziennikarz odmawia odpowiedzi na pytania prokuratora dot. źródła informacji.

5.9. Tajemnica zawodowa psychologa

Dotyczy danych pozyskanych w trakcie diagnozy, terapii i konsultacji psychologicznej.

Podstawa prawna: art. 14 ustawy o zawodzie psychologa i samorządzie zawodowym psychologów [Dz.U. 2001 nr 73 poz. 763].

Pragmatyka procesowa:

1. Psycholog wzywany jako świadek wnosi o zwolnienie z obowiązku składania zeznań.
2. Sąd może przeprowadzić przesłuchanie psychologa na posiedzeniu niejawnym.

5.10. Tajemnica komornicza (dotyczy komorników sądowych)

Termin w prawie polskim zdefiniowany w ustawie z dnia 22 marca 2018 r. o komornikach sądowych.

Podstawa prawna: ustawa o komornikach sądowych [t.j. Dz.U. 2018 poz. 771]

Art. 27

§ 1. Komornik jest obowiązany zachować w tajemnicy okoliczności sprawy, o których powziął wiadomość ze względu na wykonywane czynności.

§ 2. Obowiązek, o którym mowa w ust. 1, trwa także po odwołaniu komornika z zajmowanego stanowiska albo wygaśnięciu powołania na stanowisko komornika z mocy prawa.

§ 3. Obowiązek, o którym mowa w ust. 1, ustaje gdy komornik składa zeznanie jako świadek lub strona przed sądem lub prokuratorem, chyba że ujawnienie tajemnicy zagraża dobru państwa. W tym przypadku od obowiązku może zwolnić komornika Minister Sprawiedliwości.

§ 4. W postępowaniu dyscyplinarnym oraz postępowaniu o odwołanie komornika z zajmowanego stanowiska w trybie przewidzianym w art. 19 ust. 2 przepis ust. 3 stosuje się odpowiednio.

5.11. Tajemnica bankowa

Dotyczy wszelkich informacji dotyczących czynności bankowych, w tym kont, operacji i danych klientów.

Podstawa prawna: ustawa Prawo bankowe [Dz.U. 1997 nr 140 poz. 939]

Art. 104

ust. 1 Bank, osoby w nim zatrudnione oraz osoby, za których pośrednictwem bank wykonuje czynności bankowe, są obowiązane zachować tajemnicę bankową, która obejmuje wszystkie informacje dotyczące czynności bankowej, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje.

ust. 2 (...) 15 wyjątków od zapisów ust. 1

Pragmatyka procesowa:

1. Bank przekazuje dane tylko na pisemny wniosek sądu lub prokuratora.
2. Pracownik banku odmawia ujawnienia danych przed organami administracyjnymi bez stosownej zgody.

5.12. Tajemnica organów informacji finansowej

Termin w prawie zdefiniowany w ustawie z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

Podstawa prawna: ustawa o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu [Dz.U. 2018 poz. 723]

Art. 54

1. Instytucje obowiązane, ich pracownicy oraz inne osoby działające w imieniu i na rzecz instytucji obowiązanych zachowują w tajemnicy:

1) fakt przekazania Generalnemu Inspektorowi lub innym właściwym organom informacji określonych w rozdziałach 7 i 8;

2) informacje o planowaniu wszczęcia oraz o prowadzeniu analizy dotyczącej prania pieniędzy lub finansowania terroryzmu.

2. Obowiązek zachowania w tajemnicy informacji, o których mowa w ust. 1, nie dotyczy przekazywania informacji pomiędzy:

1) instytucjami kredytowymi i finansowymi w rozumieniu art. 3 pkt 1 i 2 dyrektywy (...),

2) instytucjami obowiązanymi, o których mowa w art. 2 ust. 1 pkt 13–15a i 17, oraz osobami z państw trzecich, które podlegają wymogom określonym w dyrektywie 2015/849 (...), (...).

3. Informacje o powzięciu podejrzenia, że określone wartości majątkowe mogą pochodzić z działalności o charakterze przestępczym lub mieć związek z finansowaniem terroryzmu, są przekazywane pomiędzy podmiotami wchodzącymi w skład grupy. Generalny Inspektor może nakazać instytucji obowiązanej wchodzącej w skład grupy zachowanie w tajemnicy faktu powzięcia takiego podejrzenia. (...)

Pragmatyka procesowa:
1. Bank przekazuje dane tylko na pisemny wniosek sądu lub prokuratora.
2. Pracownik banku odmawia ujawnienia danych przed organami administracyjnymi, bez stosownej zgody.

5.13. Tajemnica Spółdzielczych Kas Oszczędnościowo-Kredytowych (SKOK)

Obejmuje informacje uzyskane w związku z prowadzeniem i obsługiwaniem rachunków w spółdzielczych kasach oszczędnościowo-kredytowych.

Podstawa prawna: ustawa o spółdzielczych kasach oszczędnościowo-kredytowych [Dz.U. 2012 poz. 855]

Art. 9e

1. *Kasa jest obowiązana do zachowania tajemnicy zawodowej obejmującej wszystkie informacje dotyczące czynności, o których mowa w art. 3 ust. 1, w tym także informacje uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której kasa tę czynność wykonuje.*
2. *Dostęp do tajemnicy, o której mowa w ust. 1, mają wyłącznie członkowie organów kasy, niezależnie od podstawy prawnej pełnienia funkcji członka organu kasy, oraz osoby pozostające z kasą w stosunku pracy.*
3. *Osoby, o których mowa w ust. 2, są obowiązane do zachowania tajemnicy, zarówno w trakcie pełnienia funkcji lub pozostawania w stosunku pracy, jak również po zakończeniu pełnienia funkcji lub ustaniu stosunku pracy.*

Pragmatyka procesowa:

Procedura jest zbieżna z przepisami dot. usług bankowych.

5.14. Tajemnica ubezpieczeniowa

Obejmuje informacje uzyskane w związku z umowami ubezpieczenia, także zdrowotnymi.

Podstawa prawna: ustawa o działalności ubezpieczeniowej i reasekuracyjnej [Dz.U. 2015 poz. 1844]

Art. 35

1. *Zakład ubezpieczeń i osoby w nim zatrudnione, a także osoby i podmioty, za pomocą których zakład ubezpieczeń wykonuje czynności ubezpieczeniowe, są obowiązane do zachowania tajemnicy dotyczącej poszczególnych umów ubezpieczenia.*
2. *Obowiązek zachowania tajemnicy, o którym mowa w ust. 1, nie dotyczy informacji udzielanych na wniosek:*
   1) sądu lub prokuratury, o ile są niezbędne w toczącym się postepowaniu;
   2) Policji (...),
   2a) Inspektora Nadzoru Wewnętrznego (...)

3) Agencji Bezpieczeństwa Wewnętrznego (...);
4) Żandarmerii Wojskowej (...);
5) komornika sądowego;
6) administracyjnego organu egzekucyjnego oraz centralnego biura łącznikowego (...);
7) minister właściwy do spraw finansów publicznych oraz pracownicy urzędu obsługującego tego ministra;
8) organu nadzoru (...);
9) Najwyższej Izby Kontroli (...);
10) organów Krajowej Administracji Skarbowej (...)
11) (...)

Pragmatyka procesowa:

1. Ubezpieczyciel odmawia udzielenia informacji bez zgody ubezpieczonego lub decyzji sądu.
2. W toku sprawy cywilnej sąd może zażądać dokumentacji tylko w zakresie niezbędnym.

5.15. Tajemnica systemu ubezpieczeń społecznych

Obejmuje informacje uzyskane w związku z umowami ubezpieczenia, także zdrowotnymi.

Podstawa prawna: ustawa o systemie ubezpieczeń społecznych [Dz.U. 1998 nr 137 poz. 887]

Art. 3

zadania z zakresu nin. ustawy wykonują:

1. *Zakład Ubezpieczeń Społecznych;*
2. *otwarte fundusze emerytalne, określone w przepisach o organizacji i funkcjonowaniu funduszy emerytalnych, w zakresie gromadzenia i lokowania składki na ubezpieczenie emerytalne, o której mowa w art. 22 ust. 3 pkt 1 lit. a;*
3. *płatnicy składek.*

Art. 79

1. *Indywidualne dane zawarte na kontach ubezpieczonych i kontach płatników składek, a także w rejestrach prowadzonych przez Zakład oraz dane źródłowe będące podstawą zapisów na tych kontach i w rejestrach stanowią tajemnicę prawnie chronioną Zakładu. Do przestrzegania tej tajemnicy obowiązani są:*
   1) pracownicy Zakładu;
   2) członkowie Rady Nadzorczej Zakładu.
2. *Przepis ust. 1 stosuje się również do indywidualnych danych osób, przetwarzanych w Zakładzie w zakresie przyznawania, ustalania i wypłaty świadczeń z ubezpieczeń*

społecznych, a także świadczeń finansowanych z budżetu państwa oraz o dokonanych wypłatach, w związku z realizacją zadań zleconych Zakładowi na podstawie odrębnych przepisów.

5.16. Tajemnica tłumacza przysięgłego

Obejmuje informacje uzyskane w związku z wykonywaniem usług tłumacza przysięgłego w myśl ustawy zawodowej tłumaczy przysięgłych.

Podstawa prawna: ustawa o zawodzie tłumacza przysięgłego [Dz.U. 2004 nr 273 poz. 2702]

Art. 14

1. *Tłumacz przysięgły jest obowiązany do:*
   1) *wykonywania powierzonych mu zadań ze szczególną starannością i bezstronnością, zgodnie z zasadami wynikającymi z przepisów prawa;*
   2) *zachowania w tajemnicy faktów i okoliczności, z którymi zapoznał się w związku z tłumaczeniem;*
   3) *doskonalenia kwalifikacji zawodowych.*
2. *Dokonując tłumaczenia imion i nazwisk z języków nieposługujących się alfabetem łacińskim lub posługujących się innym systemem pisma, tłumacz dokonuje transliteracji lub transkrypcji tych imion i nazwisk na podstawie dokumentów podróży lub ich kopii, a w przypadku braku tych dokumentów dokonuje tłumaczenia zgodnie z regułami pisowni obowiązującymi w kraju, w którym został sporządzony tłumaczony dokument.*

Pragmatyka procesowa:

Tłumacz przysięgły występuje w roli biegłego, to jest osoby posiadającej informacje specjalne. Dowód z opinii świadka będącego biegłym, to środek dowodowy w postępowaniu sądowym, polegający na wykorzystaniu wiedzy specjalistycznej osoby trzeciej, zwanej biegłym, do wyjaśnienia okoliczności sprawy, które wymagają specjalistycznej wiedzy. Dowód z opinii biegłego jest bardzo ważnym i twardym dowodem procesowym. Biegły sporządza opinię, która ma pomóc sądowi w podjęciu rozstrzygnięcia.

5.17. Tajemnica notarialna

Dotyczy informacji uzyskanych przez notariusza przy sporządzaniu aktów i czynności notarialnych.

Podstawa prawna: art. 18 ustawy Prawo o notariacie [Dz.U. 1991 nr 22 poz. 91]

Pragmatyka procesowa:

1. Notariusz odmawia ujawnienia treści testamentu bez zgody zainteresowanego.
2. Obowiązek zachowania tajemnicy trwa także po odwołaniu notariusza.

3. Sąd żąda od notariusza aktów tylko na podstawie wniosku strony i po uprawdopodobnieniu interesu prawnego. Możliwość zwolnienia z obowiązku zachowania tajemnicy należy wyłącznie do Ministra Sprawiedliwości.

5.18. Tajemnica dostawcy usług płatniczych

Dotyczy informacji uzyskanych przez podmiot świadczący usługi płatnicze na terenie RP.

Podstawa prawna: ustawa o usługach płatniczych [Dz.U. 2011 nr 199 poz. 1175]

Art. 11 *Zakres tajemnicy zawodowej dostawców usług płatniczych*

§ 1. Do zachowania tajemnicy zawodowej dotyczącej działalności, o której mowa w art. 3 ust. 1, w charakterze dostawcy, a także działalności w zakresie wydawania pieniądza elektronicznego oraz działalności polegającej na świadczeniu usług ściśle powiązanych z usługami płatniczymi lub wydawaniem pieniądza elektronicznego są obowiązane:

1) osoby zarządzające oraz inne osoby wchodzące w skład organów statutowych dostawcy lub wydawcy pieniądza elektronicznego;

2) osoby pozostające z dostawcą lub wydawcą pieniądza elektronicznego w stosunku pracy;

3) osoby lub podmioty pozostające z dostawcą lub wydawcą pieniądza elektronicznego w stosunku zlecenia lub innym stosunku prawnym o podobnym charakterze, w tym agenci dostawcy lub wydawcy pieniądza elektronicznego, inni przedsiębiorcy dokonujący wykupu pieniądza elektron. oraz podmioty wykon. niektóre czynności operacyjne na podstawie umowy, o której mowa w art. 86 ust. 1 lub art. 132v ust. 1;

4) osoby lub podmioty pozostające w stosunku pracy, zlecenia lub innym stosunku prawnym o podobnym charakterze z podmiotem pozostającym z dostawcą lub wydawcą pieniądza elektronicznego w stosunku, o którym mowa w pkt 3.

§ 2. Obowiązek zachowania tajemnicy zawodowej istnieje również po zakończeniu pełnienia funkcji lub ustaniu stosunków prawnych, o których mowa w ust. 1. (...)

Pragmatyka procesowa:

Pragmatyka procesowa w kontekście tajemnicy usług płatniczych dotyczy przede wszystkim zasad i procedur związanych z ochroną danych osobowych i informacji dotyczących transakcji finansowych realizowanych za pomocą usług płatniczych. Kluczowe jest przestrzeganie przepisów prawa, w tym ustawy o usługach płatniczych oraz zasad etycznych, aby zapewnić poufność i bezpieczeństwo danych użytkowników.

5.19. Tajemnica kontroli państwowej

Termin prawniczy wprowadzony w Polsce ustawą z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli. Tajemnica kontrolerska w NIK, to obowiązek zachowania poufności informacji uzyskanych w związku z wykonywaniem czynności kontrolnych. Obejmuje ona zarówno zakres podmiotowy, przedmiotowy, jak i czasowy. Celem jest ochrona informacji, które mogą naruszać interes publiczny lub prywatny.

Podstawa prawna: ustawa o Najwyższej Izbie Kontroli [Dz.U. 1995 nr 13 poz. 59]

Art. 28a

(...)

3. *Program kontroli i tematyka kontroli są dokumentami chronionymi tajemnicą kontrolerską, udostępnianymi pracownikom Najwyższej Izby Kontroli w związku z wykonywaniem zadań służbowych. Innym osobom program kontroli lub tematyka kontroli może zostać udostępniona w uzasadnionych przypadkach za zgodą Prezesa Najwyższej Izby Kontroli.*

(...)

Art. 73.

1. *Informacje, które pracownik Najwyższej Izby Kontroli uzyskał w związku z wykonywaniem obowiązków służbowych stanowią tajemnicę kontrolerską, z zastrzeżeniem art. 10.*
2. *Obowiązek zachowania tajemnicy kontrolerskiej ma również członek Kolegium Najwyższej Izby Kontroli, o którym mowa w art. 22 ust. 2 pkt 1, w zakresie informacji, jakie uzyskał w wyniku rozpatrywania zastrzeżeń.*
3. *Obowiązek zachowania tajemnicy trwa również po ustaniu zatrudnienia lub upływie albo wygaśnięciu kadencji członka Kolegium Najwyższej Izby Kontroli.*

(...)

Pragmatyka procesowa:

1. W toku postępowania kontrolnego, dostęp do akt i informacji posiadają kontrolerzy oraz kierownik jednostki kontrolowanej lub osoba przez niego upoważniona.
2. NIK może współdziałać z innymi organami (np. prokuraturą) w ramach prowadzonych kontroli, w tym w zakresie wymiany informacji, zachowując zasady tajemnicy kontrolerskiej.
3. NIK jest zobowiązana do przekazywania Sejmowi określonych dokumentów, w tym analizy wykonania budżetu państwa i założeń polityki pieniężnej.

5.20. Tajemnica doradcy podatkowego

Obejmuje informacje związane z doradztwem podatkowym, planowaniem podatkowym i reprezentacją podatnika. Doradca podatkowy obowiązany jest do

zachowania w tajemnicy faktów i informacji, z którymi zapoznał się w związku z wykonaniem zawodu. Zasady te stosuje się odpowiednio do osób zatrudnionych przez doradcę podatkowego oraz podmioty, o których mowa w art. 4 ust. 1 ustawy o doradztwie podatkowym, w zakresie wykonywania przez te osoby czynności doradztwa podatkowego. Przepis ten jest podobny w treści do analogicznych przepisów innych ustaw korporacyjnych (np. art. 18 ust. 1 ustawy Prawo o notariacie, art. 6 ust. 1 ustawy Prawo o adwokaturze czy art. 3 ust. 3 ustawy o radcach prawnych).

Podstawa prawna: art. 37 ustawy o doradztwie podatkowym [Dz.U. 1996 nr 102 poz. 475]

Pragmatyka procesowa:

Doradca podatkowy, podobnie jak radca prawny, ma zapewnioną formalną ochronę i gwarancję przed próbą uzyskania od niego przez jakikolwiek organ czy sąd tego, co zostało mu powierzone w najgłębszej tajemnicy przez klienta. To fundament zawodu doradcy podatkowego, jako zawodu zaufania publicznego.

1. Doradca podatkowy odmawia złożenia wyjaśnień bez uchylenia tajemnicy przez klienta.
2. Prokurator występuje o zgodę do sądu na przesłuchanie doradcy w charakterze świadka.

5.21. Tajemnica ksiąg rachunkowych

Termin w prawie polskim został zdefiniowany w ustawie z dnia 29 września 1994 r. o rachunkowości. Z ustawy wynika, że należy chronić zbiory danych (tj. księgi rachunkowe, dowody księgowe, dokumenty inwentaryzacyjne i sprawozdania finansowe) oraz należy przechowywać w należyty sposób i chronić (...)

Podstawa prawna: ustawa o rachunkowości [Dz.U. 1994 nr 121 poz. 591]

Art. 71

1. *Dokumentację, o której mowa w art. 10 ust. 1, księgi rachunkowe, dowody księgowe, dokumenty inwentaryzacyjne i sprawozdania finansowe, zwane dalej także „zbiorami", należy przechowywać w należyty sposób i chronić przed niedozwolonymi zmianami, nieupoważnionym rozpowszechnianiem, uszkodzeniem lub zniszczeniem.*
2. *Przy prowadzeniu ksiąg rachunkowych przy użyciu komputera ochrona danych powinna polegać na stosowaniu odpornych na zagrożenia nośników danych, na doborze stosownych środków ochrony zewnętrznej, na systematycznym tworzeniu rezerwowych kopii zbiorów danych zapisanych na informatycznych nośnikach danych, pod warunkiem zapewnienia trwałości zapisu informacji systemu rachunkowości, przez czas nie krótszy od wymaganego do przechowywania ksiąg rachunkowych, oraz na zapewnieniu ochrony programów komputerowych i danych systemu informatycznego rachunkowości (...)*

Pragmatyka procesowa:

Zakres odpowiedzialności biura rachunkowego, to jeden z zasadniczych elementów umowy i kontraktu z klientem. Ale trzeba pamiętać też o rzetelności współpracy stron tej umowy. Praktyka i orzecznictwo sądów pokazują, że poprawne ułożenie stosunków z klientem, jest nie mniej ważne niż prawidłowość rozliczeń podatkowych i rozliczeń z ZUS.

5.22. Tajemnica statystyczna

Chroni dane indywidualne pozyskane w badaniach statystycznych publicznych i niepublicznych. Jest to jedna z tajemnic bezwzględnych i jej wykorzystanie może służyć wyłącznie do opracowań, zestawień i analiz statystycznych oraz do tworzenia przez Prezesa Głównego Urzędu Statystycznego operatu do badań statystycznych. Udostępnianie lub wykorzystywanie tych danych dla innych niż podane w ustawie celów jest zabronione.

Podstawa prawna: art. 10 ustawy o statystyce publicznej [Dz.U. 1995 nr 88 poz. 439]

Dotyczy również osób fizycznych i firm – nawet informacje z pozoru publiczne mogą być objęte ochroną, jeśli ujawnienie umożliwiłoby identyfikację źródła.

Pragmatyka procesowa:

1. Pracownik GUS odmawia udzielenia informacji podmiotowi nieuprawnionemu.
2. Sąd dopuszcza wykorzystanie danych statystycznych tylko w formie zbiorczej, syntetycznej.

5.23. Tajemnica pocztowa

Termin prawniczy wprowadzony w Polsce ustawą z dnia 23 listopada 2012 r. Prawo pocztowe. Ustawa reguluje kwestie prawne związane z działalnością pocztową i określa zasady uzyskiwania uprawnienia do wykonywania działalności pocztowej oraz zasady świadczenia usług pocztowych jako usług powszechnych.

Podstawa prawna: ustawa Prawo pocztowe [Dz.U. 2012 poz. 1529]

Art. 41

1. *Tajemnica pocztowa obejmuje informacje przekazywane w przesyłkach pocztowych, informacje dotyczące realizowania przekazów pocztowych, dane dotyczące podmiotów korzystających z usług pocztowych oraz dane dotyczące faktu i okoliczności świadczenia usług pocztowych lub korzystania z tych usług.*
2. *Do zachowania tajemnicy pocztowej są obowiązani:*
   1) operator pocztowy;
   2) osoby, które z racji wykonywanej działalności mają dostęp do tajemnicy pocztowej.

3. Naruszeniem obowiązku zachowania tajemnicy pocztowej jest w szczególności:
1) ujawnianie lub przetwarzanie informacji albo danych objętych tajemnicą pocztową;
2) otwieranie zamkniętych przesyłek pocztowych lub zapoznawanie się z ich treścią;
3) umożliwianie osobom nieuprawnionym podejmowania działań mających na celu wykonywanie czynności, o których mowa w pkt 1 i 2.
(...)

Pragmatyka procesowa:

Sąd lub prokurator dla dobra wymiaru sprawiedliwości, może zwolnić pracowników operatorów pocztowych od obowiązku zachowania tajemnicy, jeżeli ustawy szczególne nie stanowią inaczej. Osoba, która jest zwalniana od obowiązku zachowania tajemnicy, może w terminie 7 dni od wydania postanowienia, złożyć zażalenie.

5.24. Tajemnica telekomunikacyjna, obecnie komunikacji elektronicznej

Termin zdefiniowany w poprzedniej ustawie z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, obecnie w ustawie z dnia 12 lipca 2024 r. Prawo komunikacji elektronicznej (Dz.U. 2024 poz. 1221). Nowe przepisy dotyczące tajemnicy komunikacji elektronicznej, wprowadzone przez Prawo komunikacji elektronicznej, nakładają na dostawców usług obowiązek ochrony danych użytkowników przed nieuprawnionym ujawnieniem. Oznacza to, że dostawcy muszą wdrożyć odpowiednie środki techniczne i zabezpieczenia, aby zapewnić poufność komunikacji. Ponadto, nowe przepisy regulują kwestie związane z przetwarzaniem danych transmisyjnych i innymi danymi użytkowników w kontekście marketingu i świadczenia usług. Tajemnica „komunikacji elektronicznej" jest ważnym elementem ochrony prywatności w społeczeństwie. Zapewnia ona, że komunikacja elektroniczna w sieciach telekomunikacyjnych jest chroniona przed nieuprawnionym dostępem i ujawnieniem. Utrzymanie tej tajemnicy jest kluczowe dla budowania zaufania do usług telekomunikacyjnych i zachowania praw obywatelskich. Wszelkie formy komunikacji elektronicznej muszą być traktowane jako poufne, a dostawcy nie mogą ujawniać ich treści bez zgody użytkownika lub sądu w prowadzonym postępowaniu. Dostawcy usług są zobowiązani do zachowania należytej staranności w zabezpieczaniu urządzeń telekomunikacyjnych i zbiorów danych przed ujawnieniem tajemnicy komunikacji.

Podstawa prawna: ustawa Prawo komunikacji elektronicznej [Dz.U. 2024 poz. 1221]

Nowe przepisy mają na celu dostosowanie regulacji rynku telekomunikacyjnego do dynamicznie zmieniającej się rzeczywistości i zapewnienie efektywnej ochrony danych użytkowników. Regulacja obejmuje dane i informacje zgromadzone przez operatorów dot. zarówno osób fizycznych jak i podmiotów. Wszelkie formy komunikacji elektronicznej muszą być traktowane jako poufne, a dostawcy nie mogą ujawniać ich treści bez zgody użytkownika.

Pragmatyka procesowa:

Tajemnica komunikacji elektronicznej, zgodnie z polskim prawem, to obowiązek ochrony danych użytkowników oraz treści komunikacji i komunikatów przesyłanych w sieciach telekomunikacyjnych. Obejmuje ona zarówno dane dotyczące użytkownika, jak i treść samych komunikatów, a także dane transmisyjne i lokalizacyjne. Podmioty świadczące usługi komunikacji elektronicznej są zobowiązane do zachowania tej tajemnicy i stosowania odpowiednich środków technicznych oraz zabezpieczeń.

5.25. Tajemnica a obowiązek zeznania – kompetencja sądu

Konieczność zachowania tajemnicy działa w przypadku, gdy osoba zobowiązana do zachowania tajemnicy zawodowej zostaje wezwana na świadka.

Podstawa prawna: ustawa kodeks postępowania karnego [Dz.U. 1997 nr 89 poz. 555]

Art. 180 §2

Uchylenie obowiązku zachowania tajemnicy zawodowej może nastąpić tylko, gdy jest to konieczne dla dobra wymiaru sprawiedliwości.

Postanowienie o zwolnieniu z tajemnicy wydaje sąd, a nie prokurator (wyjątki: tajemnica bankowa, ubezpieczeniowa – mogą być uchylone ustawowo).

W przypadku, gdy osoba zobowiązana do zachowania tajemnicy zawodowej zostaje wezwana na świadka.

Art. 180 §2

Uchylenie obowiązku zachowania tajemnicy zawodowej może nastąpić tylko, gdy jest to konieczne dla dobra wymiaru sprawiedliwości.

Postanowienie o zwolnieniu z tajemnicy wydaje sąd, a nie prokurator (wyjątki: tajemnica bankowa, ubezpieczeniowa – mogą być uchylone ustawowo).

5.26. Tajemnica geologiczna

Obejmuje informacje geologiczne uzyskane w toku prac badawczych lub dokumentacyjnych, zwłaszcza dotyczące zasobów naturalnych. Tajemnica obowiązuje przez 5 lat od zatwierdzenia dokumentacji, chyba że właściciel wyrazi zgodę na ujawnienie.

Podstawa prawna: ustawa Prawo geologiczne i górnicze [Dz.U. 2011 nr 163 poz. 981]

Pragmatyka procesowa:

1. Biegły sądowy z zakresu geologii odmawia ujawnienia danych geologicznych nieupublicznionych bez zgody inwestora.
2. Sąd wydaje postanowienie o zwróceniu się do właściwego organu (ministra klimatu) o dostęp do dokumentacji geologicznej w sprawie sporu o eksploatację złóż.

5.27. Tajemnica Urzędu Ochrony Konkurencji i Konsumentów

Termin obejmuje wszelkie informacje i dowody uzyskane przez Prezesa Urzędu w związku z zastosowaniem art. 89a i art. 113a–113k, w tym informacje o wystąpieniu przedsiębiorcy lub osoby zarządzającej o odstąpienie od wymierzenia kary pieniężnej lub jej obniżenie oraz informacje uzyskane w procedurze dobrowolnego poddania się karze pieniężnej, nie podlegają udostępnieniu, z zastrzeżeniem ust. 2 i 3.

Podstawa prawna: ustawa o ochronie konkurencji i konsumentów [Dz.U. 2007 nr 50 poz.331]

Pragmatyka służbowa:

Prezes Urzędu udostępnia stronom informacje i dowody, o których mowa w ust. 1, przed wydaniem decyzji. Przepisu nie stosuje się, w przypadku gdy przedsiębiorca lub osoba zarządzająca występuje o odstąpienie od wymierzenia kary pieniężnej lub jej obniżenie lub przedsiębiorca lub osoba zarządzająca przystępuje do procedury w sprawie dobrowolnego poddania się karze pieniężnej, wyrażą pisemną zgodę na udostępnienie informacji i dowodów, o których mowa w ust. 1.

5.28. Tajemnica mediatora

Dotyczy informacji uzyskanych w trakcie prowadzonych mediacji w sprawach sądowych. Ma charakter absolutny i nie może zostać uchylona żadnym aktem świeckim. Tajemnica mediatora została potwierdzona także w Kodeksie postępowania karnego, który w art. 178a włącza także tajemnicę mediacji do katalogu osób, które nie mogą być przesłuchiwane.

Podstawa prawna: ustawa Kodeks postępowania karnego [Dz.U. 1997 nr 89 poz. 555]

art. 178a

Nie wolno przesłuchiwać jako świadka mediatora, co do faktów o których dowiedział się od oskarżonego lub pokrzywdzonego prowadząc postępowanie mediacyjne, z wyłączeniem informacji o przestępstwach, o których mowa w art. 240 § 1 Kodeksu karnego.

5.29. Tajemnica rzeczoznawcy majątkowego

Termin w prawie polskim zdefiniowany w ustawie z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami. Informacje uzyskane przez rzeczoznawcę majątkowego w związku z wykonywaniem zawodu stanowią tajemnicę zawodową. W szczególności informacje uzyskane w toku wykonywania czynności zawodowych nie mogą być przekazywane osobom trzecim, chyba że odrębne przepisy stanowią inaczej.

Podstawa prawna: ustawa o gospodarce nieruchomościami [Dz.U. 1997 nr 115 poz. 741]

art. 175

1. *Rzeczoznawca majątkowy jest zobowiązany do wykonywania czynności, o których mowa w art. 174 ust. 3 i 3a, zgodnie z zasadami wynikającymi z przepisów prawa, ze szczególną starannością właściwą dla zawodowego charakteru tych czynności oraz z zasadami etyki zawodowej, kierując się zasadą bezstronności w wycenie nieruchomości.*
2. *(...)*
3. *Informacje uzyskane przez rzeczoznawcę majątkowego w związku z wykonywaniem zawodu stanowią tajemnicę zawodową. W szczególności informacje uzyskane w toku wykonywania czynności zawodowych, nie mogą być przekazywane osobom trzecim, chyba że odrębne przepisy stanowią inaczej (...).*

5.30. Tajemnica spowiedzi

Dotyczy informacji uzyskanych w sakramencie pokuty. Ma charakter absolutny i nie może zostać uchylona żadnym aktem świeckim. Tajemnica spowiedzi została potwierdzona także w Kodeksie postępowania karnego, który w art. 178 włącza tajemnicę obrończą i tajemnicę spowiedzi do katalogu osób, które nie mogą być przesłuchiwane.

Podstawa prawna:

Kodeks Prawa Kanonicznego, kan. 983–984 [Kodeks 1983]

art. 53 Konstytucji RP, tajemnica respektowana na mocy wolności religijnej

Kodeks postępowania karnego

Pragmatyka procesowa:

1. Kapłan powołuje się na tajemnicę spowiedzi i odmawia składania zeznań nawet pod groźbą sankcji.
2. Sąd rezygnuje z przesłuchania duchownego po formalnym zgłoszeniu sprzeciwu w oparciu o klauzulę sumienia i prawo do wolności religijnej.

5.31. Tajemnica funkcjonariusza Centralnego Biura Antykorupcyjnego (CBA)

Dotyczy wszelkich informacji uzyskanych w toku czynności operacyjno-rozpoznawczych, kontroli lub działań specjalnych prowadzonych przez CBA.

Podstawa prawna:

Art. 54 ustawy o CBA [Dz.U. 2006 nr 104 poz. 708] – obowiązek zachowania tajemnicy także po ustaniu służby.

Uzupełnienie: art. 180 §2 i §5 kpk – przesłuchanie funkcjonariusza tylko po uchyleniu tajemnicy przez przełożonego lub sąd.

Pragmatyka procesowa:

1. Funkcjonariusz CBA odmawia zeznań, powołując się na nieujawnioną kategorię czynności operacyjnych.
2. Prokurator składa wniosek do Prezesa Rady Ministrów lub Szefa CBA o zgodę na zwolnienie funkcjonariusza z tajemnicy w konkretnym zakresie.

5.32. Tajemnica skarbowa

Obejmuje wszelkie dane związane z rozliczeniami podatkowymi, celnymi, kontrolami skarbowymi i deklaracjami podatkowymi.

Podstawa prawna: art. 293–299 Ordynacji podatkowej [Dz.U. 1997 nr 137 poz. 926]

Pragmatyka procesowa:

1. Urzędnik KAS odmawia ujawnienia danych podatnika bez pisemnej zgody lub decyzji sądu.
2. Sąd zwraca się do dyrektora izby administracji skarbowej o częściowe uchylenie tajemnicy w postępowaniu karnym.

5.33. Tajemnica celna

Obejmuje wszelkie dane związane z rozliczeniami podatkowymi i celnymi, kontrolami i składanymi deklaracjami o zobowiązaniach celno-skarbowych.

Podstawa prawna: ustawa Prawo celne [t.j. Dz.U. 2022 poz. 2073]

Art. 95b

1. *Indywidualne dane zawarte w zgłoszeniu celnym oraz innych dokumentach składanych przez zgłaszającego objęte są tajemnicą celną.*
2. *Przepis ust. 1 stosuje się również do danych zawartych w:*
   1) *aktach postępowania celnego oraz aktach postępowania w sprawach o przestępstwa skarbowe lub wykroczenia skarbowe;*
   2) *dokumentacji rachunkowej organu celnego;*

3) informacjach uzyskanych przez Szefa Krajowej Administracji Skarbowej lub naczelnika urzędu celno-skarbowego z banków oraz z innych źródeł niż wymienione w ust. 1.3.

3. Do przestrzegania tajemnicy celnej obowiązani są funkcjonariusze Służby Celno-Skarbowej oraz członkowie korpusu służby cywilnej zatrudnieni w jednostkach organizacyjnych Krajowej Administracji Skarbowej, którzy w związku z wykonywaniem obowiązków uzyskali dostęp do informacji stanowiących tajemnicę celną. (...)

5.34. Tajemnica giełdowa

Oznacza wszystkie informacje dotyczące czynności giełdowych, uzyskane w czasie pracy. Obowiązek zachowania tajemnicy zawodowej istnieje również po ustaniu stosunków prawnych.

Podstawa prawna:

ustawa o giełdach towarowych [Dz.U. 2000 nr 103 poz. 1099],

art. 147 ustawy o obrocie instrumentami finansowymi [Dz.U. 2005 nr 183 poz. 1538].

Tajemnica zawodowa obejmuje informacje uzyskane, przez osobę wymienioną w art. 148 ust. 1, w związku z podejmowanymi czynnościami służbowymi w ramach pozostawania w stosunku pracy, zlecenia lub w innym stosunku prawnym o podobnym charakterze, dotyczącą chronionych prawem interesów podmiotów dokonujących czynności związanych z obrotem instrumentami finansowymi, lub innych czynności w ramach regulowanej ustawą działalności objętej nadzorem Komisji lub zagranicznego organu nadzoru, jak również dotyczącą czynności podejmowanych w ramach wykonywania tego nadzoru, oraz czynności związanych z prowadzeniem rejestru akcjonariuszy, w szczególności informację zawierającą:

- dane identyfikujące stronę umowy lub innej czynności prawnej;
- treść umowy lub przedmiot czynności prawnej;
- dane o sytuacji majątkowej strony umowy; (...).

5.35. Tajemnica zawodowa funkcjonariuszy służb specjalnych ABW i AW

Dotyczy informacji niejawnych oraz operacyjnych czynności służb.

Informacje zdobyte w toku działań kontrwywiadowczych, zabezpieczania cyberprzestrzeni, ochrony konstytucyjnego porządku państwa.

Podstawa prawna:

Ustawy o poszczególnych służbach – ustawa o ABW [Dz.U. 2002 nr 74 poz. 676]

Ustawa o ochronie informacji niejawnych [Dz.U. 2019 poz. 742]

Informacje zdobyte w toku działań kontrwywiadowczych, zabezpieczania cyberprzestrzeni, ochrony konstytucyjnego porządku państwa.

Pragmatyka procesowa:

1. Funkcjonariusz ABW lub AW zeznaje jedynie w zakresie nieobjętym klauzulą tajności lub po uzyskaniu formalnej zgody Szefa ABW. Funkcjonariusz ABW składa oświadczenie o niemożności zeznania bez zgody Szefa ABW.
2. Sąd prowadzi część rozprawy z wyłączeniem jawności przy przesłuchiwaniu świadka – funkcjonariusza.

5.36. Tajemnica urzędnicza (urzędnicy państwowi i samorządowi)

Obejmuje informacje uzyskane w związku z pełnieniem obowiązków służbowych, które nie są publicznie dostępne, a mogą mieć znaczenie dla interesu publicznego, prywatności obywateli lub prawidłowego działania instytucji.

Podstawa prawna:

Art. 5 i 6 ustawy o pracownikach samorządowych [Dz.U. 2008 nr 223 poz. 1458]

Art. 24 ustawy o służbie cywilnej [Dz.U. 2008 nr 227 poz. 1505]

Art. 266 §2 Kodeksu karnego – karalność ujawnienia [Dz.U. 1997 nr 88 poz. 553]

Pragmatyka procesowa:

1. Urzędnik gminy odmawia odpowiedzi na pytania dotyczące niejawnych aspektów przetargu publicznego bez zgody przełożonego.
2. Sąd, na wniosek obrońcy, występuje do burmistrza o zgodę na ujawnienie danych w ramach jawności dowodów.

5.37. Tajemnica żołnierzy zawodowych i tajemnica wojskowa

Obejmuje dane dotyczące obronności państwa, działań operacyjnych, planów mobilizacyjnych, logistyki oraz wewnętrznych procedur wojskowych.

Podstawa prawna:

Art. 15–18 ustawy o obronie Ojczyzny [Dz.U. 2022 poz. 2305]

Ustawa o ochronie informacji niejawnych [Dz.U. 2010 nr 182 poz. 1228].

Pragmatyka procesowa:

1. Żołnierz odmawia zeznań dotyczących operacji poligonowej zaklasyfikowanej jako niejawna.
2. Prokurator wojskowy wnosi o zgodę do Ministerstwa Obrony Narodowej na przesłuchanie żołnierza w zakresie danych o uzbrojeniu.

5.38. Tajemnica służby wywiadu wojskowego i służby kontrwywiadu wojskowego

Ochrona wszelkich informacji związanych z działaniami wywiadowczymi i kontrwywiadowczymi Sił Zbrojnych RP.

Podstawa prawna:

Ustawa o SWW i SKW

Ustawa o ochronie informacji niejawnych

Pragmatyka procesowa:

1. Funkcjonariusz SWW odmawia składania zeznań dotyczących misji zagranicznej w ramach NATO.
2. Prokurator wojskowy wnioskuje o przesłuchanie świadka na posiedzeniu niejawnym po uzyskaniu zgody MON.

5.39. Tajemnica służby celno-skarbowej (funkcjonariusze KAS)

Obejmuje dane operacyjne, kontrolne i podatkowe oraz tajemnice przedsiębiorców, uzyskane przez funkcjonariuszy Krajowej Administracji Skarbowej.

Podstawa prawna:

Art. 297 i 299 ustawy o KAS [Dz.U. 2016 poz. 1947]

Art. 293–299 Ordynacji podatkowej (tajemnica skarbowa) [Dz.U. 1997 nr 137 poz. 926]

Pragmatyka procesowa:

1. Funkcjonariusz KAS odmawia ujawnienia danych z kontroli celnej bez zgody Szefa KAS.
2. Sąd zwraca się do ministra finansów o uchylenie tajemnicy dla konkretnej sprawy karnej.

5.40. Tajemnica funkcjonariuszy Policji i Straży Granicznej

Dotyczy danych operacyjnych, informacji pozyskanych w toku postępowania przygotowawczego, czynności operacyjnych lub pracy rozpoznawczej.

Podstawa prawna:

Art. 61 ustawy o Policji

Art. 180 §2 kpk – uchylenie tajemnicy przez sąd

Pragmatyka procesowa:

1. Policjant odmawia ujawnienia metod operacyjnych wobec świadka koronnego.
2. Funkcjonariusz odmawia ujawnienia informacji objętych klauzulą poufności.
3. Sąd po zamknięciu posiedzenia dopuszcza niejawne przesłuchanie funkcjonariusza.

5.41. Tajemnica służbowa w Służbie Więziennej (SW)

Dotyczy informacji o działaniach związanych z bezpieczeństwem zakładów karnych, osadzonych i funkcjonariuszy Służby Więziennej.

Podstawa prawna:

Art. 71 ustawy o Służbie Więziennej [t.j. Dz.U. 2024 poz. 1869]

Ochrona danych zgodnie z ustawą o informacjach niejawnych

Pragmatyka procesowa:

1. Funkcjonariusz Służby Więziennej nie ujawnia procedury konwojowania osadzonego bez zgody przełożonego.
2. Sąd rozpoznaje wniosek o przesłuchanie w trybie niejawnym z udziałem obrońcy.

5.42. Tajemnica życia prywatnego, wynalazcza, negocjacji i tajemnica korespondencji

Kodeks cywilny chroni dobra osobiste, które mogą obejmować tajemnicę życia prywatnego, w tym informacje o życiu intymnym, rodzinny, wyznawanej religii czy zdrowiu. Naruszenie dóbr osobistych, w tym np. tajemnicy korespondencji może skutkować żądaniem zaniechania naruszenia i usunięcia skutków naruszenia prywatności a także roszczeniami o zadośćuczynienie lub odszkodowanie.

Podstawa prawna: Kodeks cywilny [t.j. Dz.U. 2024 poz. 1061]

Pragmatyka procesowa:

Wszystkie tajemnice powołane w treści Kodeksu cywilnego chronią prywatność, życie i dzieła człowieka przed nieuprawnionym zapoznaniem się i wykorzystaniem. Naprawienie wyrządzonej szkody zarządzone polubownie lub przez sąd, najczęściej niweluje poniesione straty. Dochodzenie jednak swoich praw następuje na drodze cywilnej.

5.43. Tajemnica Urzędu Regulacji Energetyki

Obejmuje informacje uzyskane od operatorów i dotyczące szczegółów umów wewnętrznych.

Podstawa prawna: art. 28b ustawy Prawo energetyczne [Dz.U. 1997 nr 54 poz. 348]

Pragmatyka procesowa:

1. Urząd udziela informacji wyłącznie na żądanie sądu, prokuratora lub organu Krajowej Administracji Skarbowej, w ściśle określonych prawem okolicznościach.
2. W toku sprawy sądowej organ może zażądać dokumentacji tylko w zakresie niezbędnym.

5.44. Tajemnica handlowa (przedsiębiorstwa)

Brak w polskim prawie definicji terminu „tajemnica handlowa", jest on jednak bardzo rozpoznawalny i dość powszechnie używany w formie potocznej. W praktyce termin „tajemnica handlowa" jest używany zamiennie z terminem „tajemnica przedsiębiorstwa".

Termin „tajemnica handlowa" kilkukrotnie został użyty przez ustawodawcę w różnych aktach prawnych, jednakże było to użycie incydentalne i nie towarzyszyło mu objaśnienie zakresu. Nie należy traktować jednak takiego postępowania ustawodawcy jako celowego odróżnienia od „tajemnicy przedsiębiorstwa".

Przez tajemnicę przedsiębiorstwa rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane.

Podstawa prawna: ustawa o zwalczaniu nieuczciwej konkurencji [Dz.U. 1993 nr 47 poz. 211]

Art. 11

1. *Czynem nieuczciwej konkurencji jest ujawnienie, wykorzystanie lub pozyskanie cudzych informacji stanowiących tajemnicę przedsiębiorstwa.*
2. *Przez tajemnicę przedsiębiorstwa rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności. (...)*

Znaczenie w postępowaniu procesowym:

1. Przedsiębiorcy często zastrzegają informacje jako tajemnicę przedsiębiorstwa, aby uniknąć ujawnienia danych wrażliwych konkurencji i utraty przewagi konkurencyjnej.
2. W postępowaniu cywilnym, ujawnienie tajemnicy przedsiębiorstwa bez zgody przedsiębiorcy może być naruszeniem prawa.
3. W postępowaniu karnym, dostęp do tajemnicy przedsiębiorstwa przez prokuratora musi być uzasadniony i podyktowany celami postępowania.
4. Należy rozważać możliwość naruszenia tajemnicy przedsiębiorstwa w wyniku działań konkurencji, np. poprzez pozyskiwanie informacji od byłych pracowników.

5.45. Tajemnica rejestru zapasów interwencyjnych

Termin prawniczy wprowadzony w Polsce ustawą z dnia 16 lutego 2007 r. o zapasach ropy naftowej, produktów naftowych i gazu ziemnego oraz zasadach postępowania w sytuacjach zagrożenia bezpieczeństwa paliwowego państwa i zakłóceń na rynku naftowym.

Podstawa prawna: ustawa o zapasach ropy naftowej, produktów naftowych i gazu ziemnego

Art. 13

1. *Tworzy się rejestr systemu zapasów interwencyjnych, zwany dalej „rejestrem".*

(...)

6. *Dane jednostkowe zawarte w rejestrze, z wyjątkiem danych, o których mowa w ust. 3a, stanowią tajemnicę prawnie chronioną i mogą być udostępnione jedynie na żądanie organów władzy publicznej dla celów prowadzonych przez nie postępowań lub innym organom, w tym organizacjom międzynarodowym, jeżeli taki obowiązek wynika z ustawy, umowy międzynarodowej albo przepisów Unii Europejskiej.*
7. *Dokumenty stanowiące podstawę wpisów w rejestrach przechowuje się przez okres co najmniej 5 lat od dnia dokonania wpisu.*

(...)

Obowiązki przedsiębiorcy – ochrona tajemnicy przedsiębiorstwa:

Przedsiębiorca powinien podjąć racjonalne działania w celu zachowania poufności informacji. Obejmuje to m.in. wdrożenie procedur zabezpieczających, klauzule poufności w umowach, szkolenia pracowników. Ważne jest również, aby informacje nie były łatwo dostępne dla osób nieuprawnionych.

6. Tajemnica państwowa

Najważniejsze tajemnice naszego kraju, tajemnica państwowa Rzeczpospolitej Polskiej, to zbiory informacji, których ujawnienie osobom nieuprawnionym mogłoby narazić, na wyjątkowo poważną szkodę, najważniejsze interesy naszego kraju – obronność, bezpieczeństwo, niezależność gospodarczą, zakłócenie porządku konstytucyjnego i publicznego, suwerenność, pogorszenie stosunków międzynarodowych, utrudnienie funkcjonowania sił zbrojnych i inne ważne interesy państwa. Ujawnienie tajemnicy państwowej jest ciężkim przestępstwem. Tajemnica państwowa klasyfikowana jest w czterech kategoriach ochrony, jako informacje; „*zastrzeżone*", „*poufne*", „*tajne*" i „*ściśle tajne*". Klauzule te określają stopień ochrony, jaki należy zapewnić określonym informacjom w zależności od potencjalnych skutków ich nieuprawnionego ujawnienia.

Dawniej, istniały pojęcia „tajemnica państwowa" i „tajemnica służbowa", ale obecnie w polskim ustawodawstwie funkcjonuje wyłącznie „tajemnica państwowa" i przytoczone powyżej klauzule tajności.

Przykłady tajemnicy państwowej:

- plany obronne państwa;
- informacje o uzbrojeniu i siłach zbrojnych;
- dane dotyczące bezpieczeństwa wewnętrznego państwa;
- informacje o stosunkach międzynarodowych;
- informacje gospodarcze, których ujawnienie mogłoby zaszkodzić państwu.

Informacje niejawne

Pojęcie „informacja niejawna" pojawia się w art. 1 ustawy o ochronie informacji niejawnych, zgodnie z którym ustawa określa zasady ochrony takich informacji których *„nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania"*.

Stwierdzenie to jest na tyle szerokie, że trudno w ogóle przyznać mu cechę *„definicji"* pojęcia *„informacje niejawne"*, jako narzędzia umożliwiającego rzetelną analizę prawną. Zostało wyrażone za pomocą określeń nieostrych, odwołujących się do ocen, jak w szczególności *„mogłoby powodować"*, czy *„niekorzystne z punktu widzenia interesów"* [cytat za dr hab. Dobrosława Szumiło-Kulczycka, Warszawa 2014].

Wskazane wyrażenia normatywne nie pozwalają na dokonanie żadnego ścisłego rozgraniczenia pomiędzy kręgiem informacji, które powinny pozostać niejawne, a kręgiem innych informacji, które są obojętne z tego punktu widzenia. Nie da się jednoznacznie, in abstracto określić rodzajów informacji, których ujawnienie byłoby niekorzystne *„z punktu widzenia interesów Rzeczypospolitej Polski"*.

6.1. Tajemnica państwowa – klauzule tajności

Zgodnie z aktualnymi przepisami, poszczególne klauzule przyznaje się w następujących przypadkach:

1. „ściśle tajne",

jeżeli nieuprawnione ujawnienie informacji spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej, a które dotyczą polityki międzynarodowej, obronności państwa, czynności operacyjno-rozpoznawczych służb wywiadu i kontrwywiadu, bądź też mają bezpośrednie znaczenie dla niepodległości i porządku konstytucyjnego RP. Ujawnienie takie:

- zagrozi niepodległości, suwerenności lub integralności terytorialnej Rzeczypospolitej Polskiej;
- zagrozi bezpieczeństwu wewnętrznemu lub porządkowi konstytucyjnemu Rzeczypospolitej Polskiej;
- zagrozi sojuszom lub pozycji międzynarodowej Rzeczypospolitej Polskiej;
- osłabi gotowość obronną Rzeczypospolitej Polskiej;
- doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;
- zagrozi lub może zagrozić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie;
- zagrozi lub może zagrozić życiu lub zdrowiu świadków koronnych lub osób dla nich najbliższych albo świadków, o których mowa w art. 184 ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. Nr 89, poz. 555, z późn. zm.), lub osób dla nich najbliższych.

2. „tajne",

jeżeli nieuprawnione ujawnienie informacji spowoduje poważne szkody dla Polski w obszarze polityki międzynarodowej, obronności, ochrony suwerenności i porządku konstytucyjnego, interesów gospodarczych państwa, a także działań operacyjno-rozpoznawczych służb do tego uprawnionych. Ujawnienie takie:

- uniemożliwi realizację zadań związanych z ochroną suwerenności lub porządku konstytucyjnego Rzeczypospolitej Polskiej;
- pogorszy stosunki Rzeczypospolitej Polskiej z innymi państwami lub organizacjami międzynarodowymi;
- zakłóci przygotowania obronne państwa lub funkcjonowanie Sił Zbrojnych Rzeczypospolitej Polskiej;
- utrudni wykonywanie czynności operacyjno-rozpoznawczych prowadzonych w celu zapewnienia bezpieczeństwa państwa lub ścigania sprawców zbrodni przez służby lub instytucje do tego uprawnione;
- w istotny sposób zakłóci funkcjonowanie organów ścigania i wymiaru sprawiedliwości;
- przyniesie stratę znacznych rozmiarów w interesach ekonomicznych Rzeczypospolitej Polskiej.

3. „poufne",
jeżeli nieuprawnione ujawnienie informacji spowoduje szkodę Rzeczypospolitej Polskiej w obszarze polityki międzynarodowej, obronności, porządku publicznego lub bezpieczeństwa obywateli, utrudniłoby wykonywanie ustawowych zadań przez organy, służby lub instytucje odpowiedzialne za ochronę bezpieczeństwa, osłabiłoby system finansowy Polski lub naraziłoby na szkodę interesy ekonomiczne lub funkcjonowanie gospodarki narodowej. Ujawnienie takie:

- utrudni prowadzenie bieżącej polityki zagranicznej Rzeczypospolitej Polskiej;
- utrudni realizację przedsięwzięć obronnych lub negatywnie wpłynie na zdolność bojową Sił Zbrojnych Rzeczypospolitej Polskiej;
- zakłóci porządek publiczny lub zagrozi bezpieczeństwu obywateli;
- utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę bezpieczeństwa lub podstawowych interesów Rzeczypospolitej Polskiej;
- utrudni wykonywanie zadań służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw i przestępstw skarbowych oraz organom wymiaru sprawiedliwości;
- zagrozi stabilności systemu finansowego Rzeczypospolitej Polskiej;
- wpłynie niekorzystnie na funkcjonowanie gospodarki narodowej.

4. „zastrzeżone",
jeżeli nie nadano informacjom wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów ekonomicznych Rzeczypospolitej Polskiej.

Na podkreślenie zasługuje fakt, iż w nowej ustawie zrezygnowano z „Wykazu informacji niejawnych, które mogą stanowić tajemnicę państwową". Z powyższego jasno wynika, iż przy przyznawaniu danej klauzuli musimy kierować się wyłącznie nowymi definicjami klauzul oraz przede wszystkim świadomością nieuprawnionego ujawnienia danej informacji oraz jego ewentualnymi skutkami.

Uważam, iż w celu ułatwienia osobom uprawnionym dokonywania właściwej klasyfikacji informacji, w każdej jednostce organizacyjnej wskazane byłoby opracowanie, w porozumieniu z szefami komórek organizacyjnych, „Wykazu podstawowych rodzajów dokumentów niejawnych wytwarzanych w jednostce organizacyjnej, zawierających informacje niejawne". Takie rozwiązanie pozwoli na uniknięcie naruszeń w zakresie zawyżania lub zaniżania klauzul. Warto zauważyć, iż zgodnie z postanowieniami zawartymi w art. 9 przewidziano nowy tryb postępowania

w przypadku stwierdzenia zawyżenia lub zaniżenia klauzuli tajności. Zgodnie z przedmiotowymi zapisami:

- odbiorca materiału, w przypadku stwierdzenia zawyżenia lub zaniżenia klauzuli tajności, może zwrócić się do osoby, która ją nadała, albo przełożonego tej osoby z wnioskiem o dokonanie stosownej zmiany;
- w przypadku odmowy dokonania zmiany lub nieudzielenia odpowiedzi w ciągu 30 dni od daty złożenia wniosku, odbiorca materiału może zwrócić się odpowiednio do ABW lub SKW o rozstrzygnięcie sporu;
- spór, o którym mowa powyżej, ABW lub SKW rozstrzyga w terminie 30 dni od daty złożenia wniosku o rozstrzygnięcie sporu.

Podstawa prawna:
ustawa o ochronie informacji niejawnych, ustawa z dnia 5 sierpnia 2010 r. [t.j. Dz.U. 2019 poz. 742];
ustawa Kodeks karny [t.j. Dz.U. 2025 poz. 383]

6.2. Tajemnica państwowa – opis

Ujawnienie tajemnicy państwowej w Polsce może prowadzić do surowych kar zgodnie z artykułem 265 Kodeksu karnego. Funkcjonariusze publiczni mogą być skazani na karę pozbawienia wolności do 10 lat, podczas gdy niezamierzone naruszenia mogą skutkować karą odosobnienia do lat 3. Takie naruszenia nie tylko zagraża bezpieczeństwu narodowemu, ale może również zaszkodzić zaufaniu publicznemu. Dodatkowo, istnieją istotne reperkusje zawodowe, w tym możliwość utraty zatrudnienia lub odpowiedzialności dyscyplinarnej. Zrozumienie tych implikacji prawnych jest kluczowe, ponieważ podkreśla znaczenie przestrzegania przepisów i ochrony wrażliwych informacji.

Tak przeprowadzone rozgraniczenie pomiędzy poszczególnymi rodzajami tajności jest niezmiernie elastyczne i niewątpliwie:

- ułatwia organom dobór stopnia tajności;
- ułatwia dobór sposobu ochrony danych informacji przed ich nieuprawnionym ujawnieniem;
- wymaga stałej i prowadzonej na bieżąco oceny ryzyka zagrożenia interesów państwa w związku z ich ujawnieniem.

Taka regulacja niestety nie tworzy rozwiązań o charakterze pewnym, pozwalających na jednoznaczne klasyfikowanie oznaczonych typów informacji, a w konsekwencji otwiera pole do arbitralnych decyzji w tej dziedzinie [cytat za dr hab. Dobrosława Szumiło-Kulczycka, Warszawa 2014].

Tak przeprowadzona regulacja oznacza, że objęte są nią „informacje", bez względu na formę oraz sposób, w jaki dana informacja jest wyrażana (art. 1 ust. 1 u.o.i.n.).

Oznacza to, że dla określenia tego, co faktycznie może być objęte klauzulą tajności, jedyne znaczenie ma wiążąca się z tym treść. Sam nośnik informacji nie tylko nie ma decydującego znaczenia, ale w zasadzie nie ma w ogóle żadnego znaczenia.

Może to być zatem zarówno nośnik tradycyjny, taki jak papier, zdjęcie, film, szkic, taśma, może to być przedmiot, rzecz, może to być substancja, może to być wreszcie nośnik danych elektronicznych, płyta CD/DVD, pendrive, dysk, może to być jednak również zapis elektromagnetyczny, jeżeli tylko służy do przenoszenia informacji i jeżeli jego przechwycenie doprowadzi do ujawnienia informacji, którą przenosił.

6.3. Tajemnica państwowa – informacje niejawne a nośnik danych

Ustawa posługuje się, na oznaczenie nośników informacji pojęciem „materiał" i uznaje za materiał, każdy dokument lub przedmiot albo dowolną ich część, chronione jako informacja niejawna, a zwłaszcza urządzenie, wyposażenie lub broń wyprodukowane albo będące w trakcie produkcji, a także składnik użyty do ich wytwarzania (art. 2 pkt 4 u.o.i.n.).

Natomiast za dokument uznaje każdą utrwaloną informację niejawną (art. 2 pkt 3 u.o.i.n.). Jakkolwiek sformułowania te, zwłaszcza sformułowanie odnoszące się do pojęcia dokumentu, w którym ustawodawca niestety pomieszał kwestię nośnika informacji z samą informacją, są nieprecyzyjne, to jednoznacznie wskazują na wolę objęcia zakresem rzeczywistej ochrony jak najszerszego spektrum materiałów, które mogą być nośnikiem informacji.

6.4. Tajemnica państwowa – materiały niejawne w czynnościach procesowych

Do przygotowania niniejszego opracowania i statystyki, autor opracowania wykorzystał informacje pochodzące z ankiet, jakie przedstawiono sędziom sądów okręgowych oraz prokuratorom prokuratur okręgowych w Polsce.

Ankieta była przygotowana i rozesłana w roku 2014 do poszczególnych sądów okręgowych i prokuratur okręgowych w formie elektronicznej. Z każdego stanowiska (komputera) możliwe było tylko jednorazowe wypełnienie ankiety, co miało wyeliminować ryzyko ewentualnej wielokrotności jej wypełnienia przez jednego badanego. Ostatecznie ankietę wypełniło 73 respondentów.

Pytania ankietowe:

„1. Czy uzyskane podczas stosowania kontroli operacyjnej, transakcji pozornej, niejawnego nadzorowania przesyłki lub działania tajnego agenta dowody, z którymi zetknąłeś w procesie w latach 2012–2013, były:"

1.	Jawne;	liczba 4,	waga 5,5%
2.	Czasem jawne, czasem objęte klauzulą tajności;	liczba 26,	waga 35,6%
3.	Objęte klauzulą tajności;	liczba 34,	waga 46,6%
4.	Nie pamiętam;	liczba 9,	waga 12,3%
5.	Ogółem;	liczba 73	

„2. Jeżeli materiały te objęte były klauzulą tajności, to proszę wskazać, jaki był to rodzaj klauzuli:"

1.	Ściśle tajne,	liczba 13,	waga 12,5%	przypadki 19%
2.	Tajne,	liczba 23,	waga 22%	przypadki 33%
3.	Poufne,	liczba 39,	waga 38,5%	przypadki 57%
4.	Zastrzeżone,	liczba 10,	waga 10%	przypadki 15%
5.	Nie pamiętam,	liczba 17,	waga 17%	przypadki 25%
6.	Ogółem,	liczba 102		

Podsumowując; dobór klauzuli i tym samym poziomu ochrony przywołanych informacji wrażliwych był bardzo subiektywny i nieostry. Wydaje się, że zamysł ustawodawcy w tym zakresie nie był aż tak nieprecyzyjny i niejasny, choć efekt tego badania jest zaskakująco nieoczywisty.

6.5. Tajemnica państwowa – materiały niejawne w procesie

Ponadto w procesie karnym wyróżnia się jawność wewnętrzną i jawność zewnętrzną. Jawność zewnętrzna, to w istocie publiczność, jest to zatem dostępność informacji procesowych dla nieograniczonej liczby osób postronnych. Jawność wewnętrzna natomiast to jawność wobec stron – uczestników procesu, a zatem osób bezpośrednio zainteresowanych jego wynikiem i rozstrzygnięciem.

Szczególną postacią jawności wewnętrznej jest jawność informacji o podejmowanych czynnościach, w tym o zebranych materiałach wobec podejrzanego (oskarżonego).

Materiały niejawne w sposób oczywisty mogą zostać udostępnione stronom wyłącznie w trybie przewidzianym przepisami prawa, w ściśle rygorystycznych

warunkach – w strefie II przetwarzania informacji niejawnych oraz w pomieszczeniach kancelarii tajnych.

Stąd zasada udostępniania kompletnych akt wraz z materiałami niejawnymi w postępowaniu sądowym ustępuje fakultatywności w postępowaniu przygotowawczym. Przedwczesne żądanie ujawnienia podejrzanemu lub jego obrońcy wszystkich posiadanych informacji i dowodów mogłoby nierzadko zniweczyć podejmowane czynności śledcze.

Co do zasady, przyjmuje się więc konieczność zapewnienia oskarżonemu i jego obrońcy prawa pełnego zapoznania się z materiałami sprawy na etapie postępowania sądowego i dopuszcza ograniczenia w tym zakresie na etapie postępowania przygotowawczego. Zapewnienie możliwości zapoznania się przez oskarżonego i jego obrońcę z pełnym zebranym materiałem dowodowym aktualizuje się zatem z chwilą przekazania sprawy do sądu, przy czym prawo to powinno być tak zagwarantowane, aby mogło być zrealizowane przed rozprawą [cytat z wyroku Wyrok TK z 3.06.2008 r., K 42/07, OTK-A 2005, nr 5, poz. 77; P. Wiliński, Kraków 2003, Odmowa dostępu do akt sprawy w postępowaniu przygotowawczym, „Prokuratura i Prawo" 2006, nr 11, s. 79; T. Grzegorczyk, Kodeks postępowania karnego wraz z komentarzem do ustawy o świadku koronnym, s. 410].

Na przeciwległym biegunie wobec zasady jawności oraz wobec prawa do informacji o przebiegu postępowania i treści zebranych w jego toku materiałów jest konieczność zachowania przez państwo w tajemnicy pewnej kategorii informacji. Konieczność istnienia mechanizmów pozwalających na utajnienie oznaczonych informacji przed ich ogólnym rozpowszechnianiem jest powszechnie akceptowana.Zwykle uzasadnia się ją potrzebą ochrony takich wartości jak: bezpieczeństwo państwa, integralność terytorialna, bezpieczeństwo publiczne (art. 10 EKPCz, art. 19 ust. 3 MPPOiP).

W polskiej Konstytucji podstawa taka została sformułowana w art. 61 ust. 3 stwierdzającym, że ograniczenie prawa do informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne może nastąpić wyłącznie ze względu na określone w ustawach, ochronę wolności i praw innych osób i podmiotów gospodarczych oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa.

Jak już wyżej wskazano, z mocy samej reguły konstytucyjnej (art.45 ust. 2 Konstytucji) zasada jawności zewnętrznej postępowania sądowego zostaje wyłączona tam, gdzie w grę wchodzi konieczność ochrony informacji, które powinny zostać zachowane w tajemnicy ze względu na inne prawnie chronione wartości.

6.6. Tajemnica państwowa – orzecznictwo sądów europejskich

W serii orzeczeń wydanych w sprawach przeciwko Polsce, dotyczących postępowań karnych Trybunał wypowiadał się na temat zgodności z EKPCz regulacji, która pozwalała obwinionym i ich obrońcom zapoznawać się z materiałami postępowania, których jawność została wyłączona, w rygorze procedury kancelarii tajnej, pozwalała także robić notatki z tych akt, składane jednak w specjalnych przechowywanych, również w kancelarii tajnej, prowadzonych osobno dla każdego zaznajamiającego się zbiorach dokumentów, nie pozwalała jednak na uzyskiwanie kopii z tych akt ani na korzystanie z wskazanych notatek podczas rozprawy.

Analizując takie ograniczenia dostępu obwinionego do materiału dowodowego sprawy, Trybunał stwierdził, że: *„ograniczenia w dostępie do akt sprawy związane były z faktem, że znaczna część dowodów miała charakter niejawny"*. Trybunał nie uważa, aby decyzja władz o zachowaniu w tajemnicy dowodów uzyskanych przy wykorzystaniu przez policję tajnych metod dochodzeniowych mogła zostać uznana za arbitralną lub w inny sposób nieuzasadnioną w niniejszej sprawie.

Tutaj Trybunał dostrzegł istnienie rzeczywistego interesu społecznego w zachowaniu niejawności dowodów uzyskanych przez policję przy wykorzystaniu tajnych metod dochodzeniowych związanych ze ściganiem poważnych przestępstw.

Ponadto obowiązki wynikające z ustawy, a związane z koniecznością respektowania tajemnicy objętej klauzulą „ściśle tajne" i „tajne", zostały rozciągnięte na wszystkich uczestników obrotu prawnego [dr hab. Dobrosława Szumiło-Kulczycka, Warszawa 2014].

Podmiotem tego przestępstwa może być także oskarżony, jeżeli uzyska w procesie karnym dostęp do materiałów obejmujących informacje chronione wskazanymi klauzulami, a następnie ujawni je lub wykorzysta do innych celów niż prowadzona w sprawie karnej obrona. Udostępniając oskarżonemu (ale także jego obrońcy lub pokrzywdzonemu i jego pełnomocnikowi oraz każdej innej uprawnionej osobie) dokumenty, akta lub przedmioty oznaczone klauzulą tajności, poucza się ich o obowiązku zachowania w tajemnicy informacji niejawnych albo tajemnicy związanej z wykonywaniem zawodu lub funkcji oraz o zasadach sporządzania kopii, odpisów wyciągów i notatek, a także przyjmuje się pisemne oświadczenie o udzieleniu pouczenia oraz o obowiązku zachowania w tajemnicy uzyskanych wiadomości.

6.7. Tajemnica państwowa – podsumowanie

Jak można wysnuć z powyższego opisu, tajemnice branżowe i informacje niejawne pozostają niejawnymi, niezależnie od celu czy też okoliczności ich wykorzystania i ujawnienia osobom uprawnionym. Wykorzystanie tych informacji przez osoby uprawnione w procesie, nie zwalnia tych podmiotów z obowiązku chronienia ich,

wg zasad określonych w odpowiednich przepisach prawa. Dochowanie należytej staranności przy przetwarzaniu, gromadzeniu i udostępnianiu uprawnionym organom tych informacji, jest obowiązkiem każdego urzędnika i funkcjonariusza naszego państwa.

Podsumowanie

Tajemnica państwowa oraz tajemnice zawodowe, branżowe, służbowe i instytucjonalne stanowią złożony system ochrony informacji w państwie prawa. Każda z nich ma inne podstawy prawne, zakres, obostrzenia i warunki uchylenia – co wymaga precyzyjnego działania w toku procesów sądowych i administracyjnych.

Tajemnice branżowe są jednym z fundamentów zaufania społecznego do zawodów zaufania publicznego i instytucji publicznych. Ich ochrona stanowi o jakości usług, prawach obywateli i rzetelności procesów sądowych. Każdorazowe ich uchylanie wymaga ważenia wartości – dobra jednostki i dobra wymiaru sprawiedliwości.

Bibliografia

1. Encyklopedia zarządzania, http://mfiles.pl/pl/index.php/Encyklopedia_Zarządzania, 2022.
2. Praca zbiorowa, PTI 2011, Elementy informatyki sądowej.
3. Norma ISO/IEC 2382-8:2001.
4. Norma ISO/IEC 17799:2007,
5. Błażej Kwiatek, Wyd. Wolters Kluwer 2020, Dokument elektroniczny w ogólnym postępowaniu administracyjnym.
6. dr hab. Dobrosława Szumiło-Kulczycka, Warszawa 2014, Dostęp w procesie karnym do materiałów objętych klauzulą tajne lub ściśle tajne, Instytut Wymiaru Sprawiedliwości.
7. S. Spurek, Palestra 2014, nr 7-8, s. 27, Dostęp do akt postępowania przygotowawczego na podstawie przepisów ustawy o dostępie do informacji publicznej w świetle orzecznictwa sądów administracyjnych.
8. Wyrok TK z 03.06.2008 r., K 42/07, OTK-A 2005, nr 5, poz. 77.
9. P. Wiliński, Kraków 2003, s. 410, Odmowa dostępu do akt sprawy w postępowaniu przygotowawczym.
10. T. Grzegorczyk, „Prokuratura i Prawo" 2006, nr 11, s. 79, Kodeks postępowania karnego wraz z komentarzem do ustawy o świadku koronnym.

Teresa Wierzbowska, Zbigniew Taraś[1]

Skuteczność zgłoszeń naruszeń treści audio video (AV) – raport z badania

O badaniu

W październiku 2023 roku Stowarzyszenie Sygnał przeprowadziło badanie wśród największych dostawców treści audiowizualnych w Polsce, którego celem było zrozumienie wybranych mechanizmów i skali nieautoryzowanej dystrybucji materiałów. Do grona badanych podmiotów należały: CANAL+ Polska, Polsat, TVN i TVP. Zbierane dane objęły okres od września 2022 roku do sierpnia 2023 roku. Dzięki odpowiednio dobranej metodologii, obejmującej kluczowych nadawców oraz długi okresu pomiaru, możliwe było przeprowadzenie analizy przedmiotowych zjawisk. Należy jednak zauważyć, że badanie nie objęło całego ekosystemu dostawców treści AV a tylko jej znaczącą próbkę, zatem skala opisywanych zjawisk została jedynie zarysowana. Badanie było próbą uchwycenia w skali rynkowej kluczowych kwestii będących przedmiotem analizy prowadzonej przez Komisję Europejską i EUIPO w 2024 roku wśród wszystkich krajów członkowskich, zarówno wśród administracji, indywidualnych uprawnionych, jak i poszczególnych platform. Celem trzyfalowej ankiety prowadzonej przez Komisję Europejską była weryfikacja, na ile skuteczne są rozwiązania z kategorii tzw. soft law, które zostały wydane w tym zakresie przez Komisję Europejską. W 2021 roku Komisja wydała Rezolucję wskazującą na konieczność blokowania nielegalnych transmisji sportowych w ciągu maksymalnie 30 minut (live blocking). Z kolei w 2023 roku ukazał się Komunikat Komisji Europejskiej wskazujący na kluczową rolę pośredników w zatrzymaniu nielegalnej dystrybucji treści. Ankieta Komisji Europejskiej skupiała się na transmisjach na żywo oraz reakcjach platform. Niniejszy raport obejmuje szerszy zakres zagadnienia, próbując uchwycić także kwestie innego typu naruszeń treści audiowizualnych (nie tylko transmisje na żywo) oraz inne typy serwisów dystrybuujących w sposób nieautoryzowany treści (nie tylko platformy). W przypadku kraju takiego jak Polska, gdzie nie ma metod blokowania dostępu do serwisów pirackich typu web blocking czy dynamic blocking, znanych z innych krajów europejskich, pominięcie tak istotnych obszarów dałoby zbyt cząstkowe dane, by móc wyciągnąć wnioski na temat kondycji polskiego rynku.

[1] Teresa Wierzbowska – prezeska Zarządu Stowarzyszenia Sygnał; Zbigniew Taraś – Stowarzyszenie Sygnał, kierownik Sekcji dw z Piractwem Canal+ Polska.

6,1 mln naruszeń prawa do dystrybucji rocznie

Przedmiotem ochrony praw do dystrybucji w badanym okresie było 2155 tytułów, które obejmowały zarówno materiały VOD (stanowiące nieco ponad trzy czwarte tej puli), jak i wydarzenia transmitowane na żywo. Od września 2022 roku do sierpnia 2023 roku zarejestrowano ponad 6,1 mln naruszeń prawa do ich dystrybucji. Dotyczyły one głównie materiałów VOD co stanowiło 99,8% przypadków. Oznacza to, że średnio każdy z tych materiałów był dystrybuowany w sposób nielegalny ponad 3600 razy w skali roku, co daje ponad 300 przypadków miesięcznie oraz 10 dziennie na każdy tytuł. Warto w tym miejscu przypomnieć, że dane te odnoszą się jedynie do kilku wybranych uprawnionych biorących udział w badaniu, którzy udostępnili dane na potrzeby badania, zatem wyniki nie ukazują całej skali zjawiska w Polsce a jedynie mechanizmy.

Jak jednak wynika z danych, liczba naruszeń transmisji na żywo stanowi znikomy ułamek zjawiska nielegalnej dystrybucji treści. Należy przy tym wziąć pod uwagę, że kosztowność wyprodukowania treści transmitowanych na żywo i skala strat w przypadku kradzieży takiego sygnału jest wielokrotnie większa niż w przypadku treści VOD, co wymaga szczególnego podejścia a co jest istotne w odniesieniu do konsultacji Komisji Europejskiej, które koncentrują się na reagowaniu na nielegalną dystrybucję treści Audio Video. Przedmiotem wyjątkowej troski regulatorów UE jest bowiem ochrona wydarzeń sportowych na żywo, których naruszenia z naszej nadwiślańskiej perspektywy stanowią czubek góry lodowej (stanowią 0,13%), a mechanizmy ochrony w innych modelach dystrybucji i wobec innego typu treści niż sportowe są pomijane w podejmowanych obecnie działaniach. Wynika to z faktu, że z europejskiej perspektywy nowe regulacje dotyczące live blocking stanowić mają element uzupełniający wobec stosowanych już mechanizmów blokowania stron pirackich.

W przypadku krajów takich jak Polska konieczne jest ujęcie szerszej perspektywy, a tym samym wdrożenie kompleksowych rozwiązań, które będą odpowiednie nie tylko wobec transmisji na żywo, ale także naruszeń w modelu VOD.

Mechanizmy zgłaszania naruszeń

Poza analizą naruszeń pod kątem typów treści, przedmiotem badania było poznanie skali zjawiska ze względu na typy serwisów, które tych naruszeń się dopuszczają. Kluczowy podział obejmuje dwa typy podmiotów:

- takie, które same w sobie nie działają w intencji kradzieży treści (mogą to być na przykład platformy, na których sami użytkownicy Internetu udostępniają treści audio video),

- tzw. serwisy pirackie, których model funkcjonowania jest stworzony w celu czerpania korzyści z nielegalnej dystrybucji treści.

Jak wynika z danych, te pierwsze co do zasady współpracują z właścicielami materiałów. Posiadają narzędzia przeznaczone do obsługi zgłaszanych naruszeń w postaci zautomatyzowanych systemów bądź niezautomatyzowanych – formularzy i dedykowanych adresów mailowych. We współpracy tej zdecydowanie dominuje model niezautomatyzowany, który w badanym okresie pokrywał 88% zgłoszeń skierowanych do platform. Współpraca ta jednak nie jest w pełni efektywna – około jedna trzecia zgłoszeń

34% to tzw. „zgłoszenia iluzoryczne", gdyż treści – pomimo ich usunięcia – pojawiają się ponownie w miejscach, z których już były zdejmowane. Wynika to z faktu, iż funkcjonujący w Polsce mechanizm N&TD (ang. notice and take down) nie powoduje zablokowania możliwości udostępnienia tych treści ponownie i ogranicza się jedynie do jednorazowego działania. Skuteczniejszy w tej kwestii jest mechanizm NSD (ang. notice and stay down) – uwzględniony w Dyrektywie Prawnoautorskiej jako odpowiedź regulatora europejskiego na analizę ograniczonej skuteczności mechanizmu N&TD. **Ostatecznie procedura notice and stay down została wprowadzona do polskiego porządku prawnego we wrześniu 2024 roku.**

8,2 mln zgłoszeń naruszenia praw do dystrybucji skierowano do serwisów pirackich. To 99% wszystkich przypadków

Masę krytyczną (ponad 8,2 mln) zgłoszeń stanowiły te, które były wysyłane do serwisów pirackich, a więc intencjonalnie prowadzonych w celu czerpania korzyści z nielegalnej dystrybucji treści. To 99% wszystkich przypadków. Prawie wszystkie takie zgłoszenia, poza nielicznymi wyjątkami, były wysyłane za pomocą niezautomatyzowanej formy. Wśród nich aż 70% to wspomniane wcześniej problematyczne zgłoszenia iluzoryczne (prawie 6 mln przypadków). W przypadku tego typu serwisów zautomatyzowany mechanizm zgłoszeń praktycznie nie funkcjonuje. Istnieją także takie serwisy, które nie dają w ogóle możliwości przesłania zgłoszenia (brak formularzy, danych kontaktowych itp.). Z tego powodu prawie 1600 naruszeń nie zostało w ogóle zgłoszonych. W obydwu przypadkach – zarówno platform, jak i serwisów pirackich – 58% stanowiły zgłoszenia skuteczne.

Czas reakcji na zgłoszenie

Czas, w jakim zgłoszenia przynoszą zamierzony rezultat, jest kluczowym wymiarem efektywności podejmowanych działań. W badanym okresie w odniesieniu do materiałów VOD w przypadku większości zgłoszeń wynosił on do 24 godzin. Odsetek ten wahał się jednak w zależności od odbiorcy (platformy vs. serwisy

pirackie) oraz sposobu zgłoszenia (system zautomatyzowany vs. inna forma) od 73% do 85%.

94% zgłoszeń naruszenia praw do dystrybucji wydarzeń na żywo nie przynosi rezultatu

Zdecydowanie gorsze wyniki odnotowano w odniesieniu do wydarzeń transmitowanych na żywo. W przypadku tego typu treści kluczowe jest, aby reakcja na zgłoszenie przynosiła rezultat jeszcze w trakcie nadawania treści. Niestety, jedynie w 5% przypadków zgłoszeń skierowanych do serwisów pirackich (które – jak odnotowano wcześniej – stanowią masę krytyczną zjawiska) zareagowano w ciągu pierwszych 30 minut od momentu zgłoszenia, zaś dodatkowo 1% w pozostałym czasie trwania transmisji. Oznacza to, że w przypadku 94% zgłoszeń nie zareagowano w czasie, jaki ma w ogóle sens w odniesieniu do wydarzeń na żywo.

Kluczowe wnioski

Analizując powyższe dane w odniesieniu do działań Komisji Europejskiej w zakresie analizy sposobu reagowania na zgłoszenia naruszeń należy zwrócić uwagę, iż:

- Komisja Europejska w swym badaniu realizowanym w 2024 roku skupia się jedynie na transmisjach na żywo. Na polskim rynku stanowią one 0,13% odnotowanych przypadków naruszeń treści audiowizualnych, co wynika nie tyle z niskiej skali naruszeń wobec transmisji na żywo, co braku skutecznej ochrony względem innych modeli dystrybucji treści jak VOD;
- Komisja Europejska skupia się na treściach sportowych pomijając w bieżącej analizie inne typy treści;
- Komisja Europejska koncentruje się na współpracy uprawnionych z platformami, podczas gdy 99% zgłoszeń naruszeń w analizowanym roku było kierowanych nie do platform, lecz do serwisów pirackich.

Z powyższych wniosków wynika, że należy z ostrożnością odnosić się do danych, jakie zostaną zebrane w ankiecie przygotowanej przez Komisję Europejską, gdyż w przypadku Polski odnosić się one będą do wąskiego wycinka procederu piractwa z jakim mierzą się uprawnieni w naszym kraju. Konieczne jest wypracowanie w Polsce kompleksowego mechanizmu wzorem najlepszych rozwiązań europejskich, który będzie pomagał chronić treści prawno-autorskie poprzez blokowanie dostępu do stron nielegalnie dystrybuujących treści. Mechanizm taki powinien obejmować zarówno przypadki nielegalnych transmisji sportowych, jak i wszelkich treści audio video bezprawnie oferowanych, które generują olbrzymie straty tak po stronie uprawnionych jak i Budżetu Państwa.

O Stowarzyszeniu Sygnał

Stowarzyszenie Sygnał działa na rzecz poszanowania własności intelektualnej, praw nadawców, dystrybutorów, licencjodawców oraz odbiorców programów telewizyjnych i innych treści multimedialnych. Stowarzyszenie powstało w 2001 roku. W skład wchodzą czołowe firmy i eksperci z branży mediów i telekomunikacji. Główny obszar działań Stowarzyszenia to szeroko pojęte inicjatywy edukacyjne, badawcze i działania na rzecz usprawnienia procesu egzekwowania praw własności intelektualnej. Od lat realizuje na szeroką skalę unikalne szkolenia i warsztaty nt. ochrony własności intelektualnej i walki z naruszeniami praw autorskich dla przedstawicieli organów ścigania, m.in. dla policjantów z Wydziałów do Walki z Przestępczością Gospodarczą, Prokuratury i Szkół Policji, a także warsztatów dla przedstawicieli firm członkowskich. W ramach propagowania idei ochrony własności intelektualnej Stowarzyszenie inicjuje i prowadzi kampanie edukacyjne, przygotowuje raporty, badania, analizy i stanowiska, bierze udział w procesie legislacyjnym istotnych dla gospodarki aktów prawnych.



ZWALCZANIE PRZESTĘPCZOŚCI INTERNETOWEJ

UCZELNIA PAŃSTWOWA
im. Jana Grodka w Sanoku

ISBN 978-83-61802-62-4