Solidarni z Ukrainą

Kwartalnik Policyjny

Nr 2(77)/2026
Rok XX
ISSN 1898-1453

CZASOPISMO
CENTRUM SZKOLENIA POLICJI
W LEGIONOWIE
www.kwartalnik.csp.edu.pl

CYBERBEZPIECZEŃSTWO

W numerze m.in.:

- Cyberprzestępczość – wywiad z biegłym sądowym
- Policja w erze cyberataków
- Kryptowaluty
- Metody OSINT
- Patostreaming
- Nowe technologie w Policji
- Prawo
- Oględziny miejsca pożaru
- Hulajnoga elektryczna w edukacji
- Komisariat Młodego Policjanta
- Wyszkolenie strzeleckie
- Techniki interwencji

Policja w erze cyfrowej transformacji

Cyfrowa transformacja na świecie przyspiesza i doświadczamy zarówno płynących z niej dobrodziejstw, jak i wielu zagrożeń i strat. Rewolucjonizująca medycynę, gospodarkę, a nawet życie codzienne sztuczna inteligencja z jednej strony daje ogromne możliwości automatyzacji i analizy danych oraz odciążenia pracowników i funkcjonariuszy służb, a z drugiej – dzięki właśnie tym możliwościom – oznacza gwałtowną eskalację cyberprzestępczości, w tym m.in. cyberataków, szpiegostwa i dezinformacji, wyłudzenia danych i oszustw finansowych, pedofilii.

Niniejsze wydanie „Kwartalnika Policyjnego" przybliża wyzwania związane z zapobieganiem i zwalczaniem cyberprzestępczości nie tylko z punktu widzenia policjantów, ale także biegłego sądowego oraz ekspertów z instytucji współpracujących ze służbami w tym zakresie. Uświadamia, jak fundamentalne znaczenie ma edukacja funkcjonariuszy i pracowników Policji w zakresie cyberbezpieczeństwa, a także ochrona infrastruktury informatycznej, oraz prezentuje wprowadzane w Policji zaawansowane rozwiązania oparte na nowych technologiach.

Polecamy również lekturę materiałów poświęconych innej problematyce, w tym rzeszowskich projektów dotyczących bezpieczeństwa w ruchu drogowym czy artykułów z zakresu prawa. Dla zainteresowanych praktyką policyjną kadra dydaktyczna CSP przygotowała zagadnienia wyszkolenia strzeleckiego i technik interwencji.

redaktor naczelny
mł. insp. Agnieszka Gorzałczyńska-Mróz

Nr 2(77)/2026

Kwartalnik Policyjny

Do pobrania na stronie:
www.kwartalnik.csp.edu.pl

CZASOPISMO CENTRUM SZKOLENIA POLICJI W LEGIONOWIE

Wydawca: Centrum Szkolenia Policji w Legionowie

Adres redakcji: ul. Zegrzyńska 121, 05-119 Legionowo
sekretariat tel. 47 72 558 81, faks 47 72 535 80,
e-mail: kwartalnik@csp.edu.pl

ZESPÓŁ REDAKCYJNY

Druk: Wydział Wydawnictw i Poligrafii CSP w Legionowie

Nakład: 1000 egz.

Numer zamknięto 26.06.2026 r.

W NUMERZE

CYBERBEZPIECZEŃSTWO

2 Agnieszka Gorzałczyńska-Mróz
Policja w erze cyfrowej transformacji. Wstęp

5 Urszula Wróblewska, Michał Podbielski
O szczepieniach na cyberprzestępczość i nie tylko. Wywiad z biegłym sądowym z zakresu informatyki śledczej

12 Marcin Tęgos
Cyfrowy paraliż państwa. Czy Policja wytrzyma starcie w wojnie hybrydowej nowej generacji?

14 Przemysław Szczerba
Zabezpieczanie kryptowalut w postępowaniu karnym. Aspekty procesowe, techniczne i praktyczne

24 Michał Królik
Kryptowaluty na biurku. Jak czytać cyfrowe ślady i nie zgubić tropu?

28 Norbert Ptak
Deanonimizacja sprawców cyberprzestępstw metodami OSINT. Od nicku do wyroku

30 Łukasz Cepok
Jakie cyberzagrożenia czyhają na polskich użytkowników urządzeń mobilnych?

33 Arkadiusz Paciorek
Patostreaming jako zjawisko kryminogenne

NOWE TECHNOLOGIE W POLICJI

37 Adam Bogucki, Kamil Jurczyk, Sławomir Sobolewski, Justyna Biegańska
Nowoczesne narzędzia, realne wsparcie. Jak powstają systemy sztucznej inteligencji dla Policji

43 Adam Bochenek, Iwona Gierczak
Łączność radiowa w Policji. Podstawy, procedury i technologie

PRAWO

50 Jarosław Bakuła
Przygotowanie i zlecenie zabójstwa

54 Beata Spinek
Zgwałcenie jako przestępstwo implikujące konsekwencje na płaszczyźnie kryminologii, socjologii i psychologii

59 Karol Józef Rosik
Glosa do wyroku Sądu Rejonowego w Bielsku Podlaskim z 29.03.2018 r., VII W 881/17 – aprobująca

TECHNIKA KRYMINALISTYKI

64 Marek Wrzosek, Kamila Poloczek
Pożar. Metody zabezpieczania śladów kryminalistycznych w trakcie oględzin miejsca pożaru

BEZPIECZEŃSTWO RUCHU DROGOWEGO

70 Mateusz Szarek
Hulajnoga elektryczna w edukacji komunikacyjnej ucznia. Praktyczne wnioski z projektu edukacyjnego realizowanego w Rzeszowie

78 Małgorzata Dencikowska
Komisariat Młodego Policjanta w Rzeszowie. Pionierska przestrzeń edukacji na rzecz bezpieczeństwa, która zmienia podejście do profilaktyki w Policji

WYSZKOLENIE STRZELECKIE I TI

81 Krystian Chudziński
AR-15 bez tajemnic. 10 krytycznych błędów, których musi unikać każdy użytkownik

85 Adam Kryszajtys
Siła fizyczna jako środek przymusu bezpośredniego. Obezwładnienie osoby agresywnej za pomocą obalenia z uchwytu za nogi

UMUNDUROWANIE POLICJANTA

89 Wojciech Pudło
Czapka zimowa policyjna

O szczepieniach na CYBERPRZESTĘPCZOŚĆ i nie tylko

z nadkom. w st. spocz. Michałem Podbielskim
rozmawia podkom. Urszula Wróblewska, Zakład Kryminalny CSP

Dyrektor Biura Cyberbezpieczeństwa w Polskim Towarzystwie Ekspertów i Biegłych Sądowych. Wieloletni instruktor Akademii Policji w Szczytnie z zakresu informatyki, informatyki śledczej, cyberprzestępczości oraz cyberbezpieczeństwa. Wykładowca akademicki w Akademii Nauk Stosowanych WSGE im. A. De Gasperi w Józefowie. Twórca autorskich szkoleń z zakresu cyberprzestępczości, cyberbezpieczeństwa, informatyki śledczej oraz cyberbezpieczeństwa osobistego. Od 12 lat biegły sądowy z zakresu informatyki o specjalizacji „Telefonia komórkowa i urządzenia mobilne". Ekspert w zakresie nadzoru oraz wdrażania procedur, polityk bezpieczeństwa, analizy ryzyka, bezpieczeństwa systemów informatycznych. Odznaczony przez Prezydenta Rzeczypospolitej Polskiej „Krzyżem Zasługi za Dzielność" za uratowanie życia przy narażeniu własnego.

Droga służbowa:
2009 – wstąpienie do Policji – Wydział Patrolowy Komendy Miejskiej Policji w Ostrołęce,
2010 – Wydział Patrolowy. Ogniwo Wywiadowcze KMP w Ostrołęce,
2012 – Zespół do Walki z Korupcją, Wydział dw. z Przestępczością Gospodarczą i Korupcją KMP w Ostrołęce,
2015 – Zarząd w Radomiu Wydział w Ostrołęce Centralnego Biura Śledczego Policji,
2020–2026 – Akademia Policji w Szczytnie.

PTEiBS
POLSKIE TOWARZYSTWO EKSPERTÓW I BIEGŁYCH SĄDOWYCH

W dobie cyfrowej transformacji niemal każdy aspekt naszego życia pozostawia ślad w cyberprzestrzeni. Wraz z rozwojem nowych technologii rośnie jednak także skala zagrożeń – od oszustw internetowych i kradzieży danych po zaawansowane ataki wymierzone w instytucje publiczne oraz przedsiębiorstwa. W takich realiach szczególnego znaczenia nabierają eksperci, którzy potrafią nie tylko analizować cyfrowe ślady przestępstw, ale również skutecznie przeciwdziałać zagrożeniom. Biegli sądowi – bohaterowie drugiego planu. Ich praca wymaga nie tylko specjalistycznej wiedzy technicznej, ale również umiejętności analitycznego myślenia, dociekliwości i odpowiedzialności.

Wprowadzenie

Naszym gościem jest biegły sądowy z zakresu informatyki, ekspert z dziedziny cyberprzestępczości, cyberbezpieczeństwa oraz informatyki śledczej, Dyrektor Biura Cyberbezpieczeństwa w Polskim Towarzystwie Ekspertów i Biegłych Sądowych, były funkcjonariusz i instruktor Akademii Policji w Szczytnie, który przez lata łączył praktykę śledczą z działalnością dydaktyczną. Dzięki doświadczeniu zdobytemu zarówno w trakcie służby, jak i w związku z pełnieniem funkcji biegłego sądowego oraz w pracy na sali wykładowej, ma unikalną wiedzę na temat współczesnych wyzwań związanych z cyberprzestępczością, bezpieczeństwem informacji oraz edukacją przyszłych specjalistów. W swojej karierze zajmował się analizą cyberprzestępstw, zabezpieczaniem dowodów cyfrowych oraz wspieraniem organów ścigania i wymiaru sprawiedliwości w wyjaśnianiu skomplikowanych spraw. Dziś dzieli się swoją wiedzą z przyszłymi funkcjonariuszami i specjalistami, pokazując, że bezpieczeństwo w cyberprzestrzeni zaczyna się od świadomości, edukacji i profesjonalizmu.
Zapraszam do rozmowy o zagrożeniach cyfrowego świata, metodach działania cyberprzestępców, roli organów ścigania oraz znaczeniu świadomości społecznej w budowaniu bezpieczeństwa w sieci.

Jest Pan biegłym od przeszło 11 lat, jak wyglądała Pana droga zawodowa od służby w formacjach mundurowych do pracy biegłego sądowego?

Na wstępie chciałbym bardzo serdecznie podziękować za zaproszenie do wywiadu w Państwa kwartalniku. Niejednokrotnie czytałem Państwa czasopismo i nigdy nie przypuszczałem, że będę miał możliwość zagościć na jego stronach.
Odpowiedź na pytanie nie jest całkiem oczywista. Musimy cofnąć się o ponad 20 lat. Wówczas, jako młody człowiek, zacząłem serwisować pierwsze telefony komórkowe. Wielu czytelników zapewne już nie pamięta czasów, kiedy telefony komórkowe służyły do dzwonienia i pisania SMS oraz posiadały blokady nie tylko urządzeń, ale również blokady sieciowe, tzw. simlock. Zajmowałem się usuwaniem blokad oraz naprawą telefonów. Policja, jak i inne służby w tamtym czasie, nie miała zbyt wielu rozwiązań, a tym bardziej specjalistów w zakresie telefonów, którzy mieliby jakąkolwiek wiedzę dotyczącą obejścia zabezpieczeń czy odczytu danych z urządzeń. Najciekawsze jest to, iż do dnia dzisiejszego najwięcej problemów przysparzają właśnie te starsze telefony. Gdy prowadziłem serwis, zwracało się do mnie wiele służb, w tym Policja, o udzielenie pomocy i podzielenie się wiedzą w tym zakresie. Niejednokrotnie dokonywałem odczytu danych czy naprawy uszkodzonych telefonów przy asyście policjantów, umożliwiając dostęp do źródła dowodowego w prowadzonych sprawach. Współpraca trwała kilka lat, pomyślałem: „Dlaczego miałbym nie spróbować pracy w Policji, żeby wspierać ją od środka?”. I tak zaczęła się moja służba w szeregach Policji. Po kilku latach pracy w Wydziale Patrolowym Komendy Miejskiej Policji w Ostrołęce podjąłem decyzję o podzieleniu się moją wiedzą i doświadczeniem z innymi instytucjami, takimi jak sądy i prokuratury. Zwróciłem się do Prezesa Sądu Okręgowego w Ostrołęce z wnioskiem o ustanowienie mnie biegłym sądowym z zakresu informatyki i tak dzielę się swoją wiedzą do dnia dzisiejszego. Początkowo współpraca obejmowała rejon Sądu Okręgowego w Ostrołęce, a z czasem podjąłem współpracę na terenie całego kraju.

Każdego dnia słyszymy w przekazach medialnych o różnego rodzaju przestępstwach internetowych, w których niekiedy ofiary tracą dorobek życia. Jakie rodzaje cyberprzestępstw spotyka Pan najczęściej w swojej pracy?

Rozpoczynając swoją drogę jako biegły sądowy, myślałem, że większość spraw będzie dotyczyć przestępstw narkotykowych i związanej z tym korespondencji dotyczącej handlu, zakupu, produkcji. Na przestrzeni lat wraz z rozwojem sieci Internet zmieniała się charakterystyka przestępstw oraz danych, jakie można było uzyskać z urządzeń – i mówię tu już nie tylko o telefonach komórkowych, lecz także o komputerach, tabletach, nawigacjach czy pojazdach. Rozwój Internetu pozwolił przestępcom zmienić metody działania i przejść w świat wirtualny, by mogli popełniać przestępstwa anonimowo i bez większych obaw o ujawnienie sprawcy. Tak właśnie narodziła się cyberprzestępczość. To, co kiedyś wiązało się z bezpośrednim kontaktem przestępcy z ofiarą, teraz posiada kurtynę w postaci komputera. Jakie rodzaje cyberprzestępstw najczęściej spotykam? Niezmiennie prym wiodą oszustwa internetowe i to pod każdą możliwą postacią. Obecnie wróciła metoda oszustwa na zaliczkę lub przedpłatę. Na jednym ze znanych portali ogłoszeniowych zostają wystawiane do sprzedaży przedmioty w atrakcyjnej, ale nie przesadnie, cenie. Dochodzi do kontaktu – w tym również telefonicznego – kupującego ze sprzedającym. Kontakt telefoniczny ma utwierdzić przyszłą ofiarę o wiarygodności oferty. Sprzedający w związku z nieufnością do kupującego prosi o pełną wpłatę za przedmiot – a w razie nieufności ze strony kupującego – prosi o wpłatę zaliczki. Po wpłacie kontakt sprzedającego z kupującym zostaje utrzymany, żeby ogłoszenie jak najdłużej było aktywne i aby sprawca mógł oszukać jak najwięcej osób. Sprzedający często zmienia termin wysyłki, wskazując przeróżne problemy z tym związane. Na koniec twierdzi, że to on został oszukany i ktoś przejął jego konto bankowe, kradnąc pieniądze wpłacone za przedmiot. Oczywiście jest to totalne kłamstwo. Niekiedy kupujący odpuszczają i nie zawiadamiają Policji. Ogłoszenie zostaje zdjęte i po kilku dniach ogłoszenie powraca wystawione przez inną osobę. Należy zwrócić szczególną uwagę, że do oszustw są wykorzystywane konta istniejące kilka lat, a często również z wystawionymi innymi przedmiotami, co znacznie utrudnia weryfikację sprzedającego. Kupują na serwisach ogłoszeniowych konta z wyrobioną już historią. Zdają sobie bowiem sprawę, że są prowadzone kampanie informacyjne w mediach i Internecie ujawniające metody oszustw i pokazujące sposoby weryfikacji, dlatego też dostosowują się do tych zaleceń i instrukcji. Serwisy ogłoszeniowe

bardzo często oferują możliwość bezpiecznego kupowania z ochroną kupującego. Jeśli osoba sprzedająca nie chce się zgodzić na transakcję z ochroną, jest to pierwszy sygnał tego, że coś jest nie tak.

Biorąc pod uwagę opiniowane przez Pana sprawy – czy mógłby Pan wskazać, jakie błędy najczęściej popełniają użytkownicy Internetu, które prowadzą do utraty danych lub pieniędzy?

Niejednokrotnie w różnego rodzaju wystąpieniach ekspertów czy osób, które prowadziły profilaktykę w zakresie cyberprzestępczości słyszałem: „Nie klikaj w nieznane linki". Dziś nasze całe życie wirtualne opiera się na różnego rodzaju linkach czy kodach QR i jest ciężko nie klikać w linki. Faktycznie, wiele lat wstecz nieznane linki prowadziły do zainfekowania komputera i utraty danych czy przejęcia systemu. Obecnie cyberprzestępcy mniej korzystają z tego typu metody podpinania np. złośliwego oprogramowania pod linki, co oczywiście nie oznacza, że tego nie robią. Chodzi o pracę, jaką muszą włożyć w oszukanie ofiary i zysk, jaki osiągną. Łatwiej jest cyberprzestępcy wysłać link z fałszywą stroną, na której ofiara sama wpisze dane, które chce otrzymać przestępca, aniżeli tworzyć program, infekować komputer, obsługiwać narzędzia do odczytu i pobierania danych, co wiąże się również z łatwiejszym namierzeniem sprawcy. Cyberprzestępcy wykorzystują linki prowadzące do stworzonych przez siebie do stron internetowych, które są takie same jak oryginalne strony internetowe różnych firm (tzw. phishing) – głównie banków. Fałszywe strony są zakładane na serwerach zagranicznych, do których polskie służby mają znacznie utrudniony dostęp. Użytkownicy Internetu niestety nie sprawdzają dokładnego adresu URL strony, do której prowadzi link. Bez namysłu, bardzo często pod presją czasu, wypełniają tam żądane dane, takie jak loginy, hasła i autoryzują logowanie na aplikacjach mobilnych banków, nie odczytując informacji zawartych w tych wiadomościach. Tak więc najczęstszym błędem użytkowników Internetu jest pośpiech i brak refleksji przy wpisywaniu danych, autoryzowaniu działań wyświetlanych za pośrednictwem aplikacji na urządzeniach mobilnych, takich jak np. smartfon. Rozważmy najczęstszy scenariusz oszustwa – osoba wystawia przedmiot do sprzedaży. Ze sprzedającym kontaktuje się zainteresowany kupnem i wysyła sprzedającemu instrukcję pobrania pieniędzy poprzez logowanie się na stronie bankowości internetowej za pośrednictwem wysłanego przez niego linku. Niestety opisany przykład sprzedaży/zakupu prowadzi do utraty niejednokrotnie dużych sum pieniędzy. Oszuści przejmują władzę nad naszym kontem bankowym i dochodzi do wyprowadzenia pieniędzy z konta czy zaciągnięcia pożyczek.

Jest Pan ekspertem w dziedzinie informatyki śledczej. Jak powinien wyglądać proces zabezpieczania cyfrowych dowodów podczas postępowania przygotowawczego? Z jakimi najczęstszymi błędami można się spotkać podczas zabezpieczania dowodów?

Wydawałoby się, że proces zabezpieczania dowodów cyfrowych jest znacznie prostszy od zabezpieczania klasycznych dowodów/śladów, zważywszy na rozwój technologiczny i cyfrowy. Właśnie nie. Zabezpieczanie dowodów cyfrowych wymaga od informatyków śledczych dużej wiedzy, doświadczenia i stosowania zasad. Błędne zabezpieczenie dowodu cyfrowego może doprowadzić do modyfikacji, czyli zmiany danych, podważenia wiarygodności dowodu, a czasem nawet trwałego usunięcia danych. W swojej pracy spotkałem się z przypadkami utraty wszystkich danych przez specjalistów w dziedzinie informatyki śledczej, w tym też służb, i co gorsze – nadpisu tych danych. Dlatego podczas zabezpieczania dowodów cyfrowych każdy informatyk śledczy powinien się kierować pewnymi zasadami, które pozwolą nam na zabezpieczenie dowodu w sposób bezsporny. Zasady te obejmują: odizolowanie osób od sprzętu i uniemożliwienie jakiejkolwiek w nim ingerencji oraz zachowanie integralności danych (dowód w żaden sposób nie może ulec najmniejszej zmianie od momentu jego przejęcia), protokołowanie – informatyk śledczy powinien pamiętać o procedurze dokumentowania związanej z zatrzymaniem, dostępem, przechowywaniem, składowaniem, opakowaniem dowodu, czynności powinny zostać w pełni udokumentowane i być dostępne dla niezależnej oceny, korzystanie ze wsparcia eksperckiego w zakresie wykraczającym poza nasze umiejętności, przeszkolenie – osoba zajmująca się zabezpieczaniem dowodów cyfrowych powinna stale poszerzać swoją wiedzę, aby móc prawidłowo wykonywać czynności.
Najczęstsze błędy spotykane podczas zabezpieczania dowodów są ściśle powiązane z nieprzestrzeganiem wymienionych zasad. Jednym z takich przykładów jest podejmowanie czynności na miejscu przez funkcjonariuszy nieposiadających dostatecznej wiedzy informatycznej pozwalającej we właściwy sposób zabezpieczyć sprzęt czy dane. Prowadzi to niejednokrotnie do utraty wartości dowodowej lub co gorsze – całkowitej utraty dowodu cyfrowego. Kolejny przykład błędu popełnianego przez funkcjonariuszy to prowadzenie niepełnej dokumentacji, która nie odpowiada na kluczowe pytania: kto, kiedy i w jaki sposób posiadał dostęp do danego dowodu. Tych błędów jest znacznie więcej. Przytoczyłem te, które mają największy wpływ na wartość dowodową zabezpieczanych śladów i danych.

Współpracuje Pan z różnymi służbami. Jak wygląda współpraca biegłego sądowego z Policją, prokuraturą oraz sądem? Czy któraś z tych instytucji ma szczególne wymagania dotyczące wydawania opinii?

Cel i wymagania każdej z instytucji przy sporządzaniu opinii przez biegłego te same, czyli wydanie rzetelnej, obiektywnej i zgodnej ze stanem faktycznym ekspertyzy. Sporządzając opinię, staram się używać prostego języka,

zrozumiałego dla każdego. Należy pamiętać, że nie każdy jest specjalistą i nie musi się znać na wszystkim. Niekiedy opinia dotyczy zabezpieczenia dowodów w postaci np. zdjęć, dokumentów, plików, informacji dotyczących m.in. logowania się urządzeń czy zainstalowanych aplikacji, a czasem jest merytoryczne wypowiedzenie się w przedmiocie zagadnienia, które nie jest do końca jasne dla każdej ze stron, tak jak to jest np. w przypadku kradzieży pieniędzy z kont bankowych ofiary metodą phishingową. Wówczas należy odpowiedzieć na pytanie, czy banki dochowały wszelkich procedur bezpieczeństwa oraz na podstawie akt określić krok po kroku *modus operandi* cyberprzestępcy. Zakres spraw opiniowanych dla instytucji zlecających jest naprawdę szeroki i czasem potrafi zaskoczyć mnie samego. Współpraca z poszczególnymi instytucjami wygląda podobnie, niemniej jednak są różnice mające znaczenie z punktu widzenia biegłego. Policja w znacznej większości przesyła urządzenia wraz z pytaniami, na które biegły ma odpowiedzieć bez żadnych dodatkowych informacji. Odstępstwem od tej zasady są dwie jednostki Policji – KMP w Ostrołęce i KPP w Wałczu – z nimi współpraca jest ściślejsza, co przekłada się na wyjaśnienie wszelkich okoliczności sprawy.
Prokuratury cenią sobie bliższą współpracę. Oznacza to, że biegły jest bardziej szczegółowo wprowadzany w sprawę. Prokuratorzy bardzo często spotykają się lub dzwonią i konsultują z biegłym kwestię, jakie wartości dowodowe można wydobyć z urządzeń; a także czy istnieją inne informacje, które mogą pomóc w wyjaśnieniu sprawy lub udowodnieniu winy czy niewinności. Instytucja biegłych została stworzona właśnie w takim celu, aby przychodzili z pomocą i wspomagali instytucje swoją wiedzą i umiejętnościami.
Natomiast sąd, zwracając się z pytaniami do biegłego, udostępnia cały materiał dowodowy w postaci akt sprawy. Umożliwia to biegłemu na zebranie znacznie większej ilości informacji niezbędnych do wydania opinii i wyjaśnienie wszelkich wątpliwości.
Z doświadczenia mogę powiedzieć, że najbardziej owocna współpraca ma miejsce wówczas, gdy wprowadzimy biegłego w szczegóły sprawy. Oczywiście, czasem nie ma potrzeby większego wprowadzania biegłego w sprawę, niemniej jednak biegły, mając dostęp choćby tylko do protokołów przesłuchań, może zauważyć coś więcej niż prowadzący sprawę, w szczególności gdy biegły ma duże doświadczenie w tym zakresie.

Jakie rady może Pan przekazać osobom rozpoczynającym karierę w dziedzinie cyberbezpieczeństwa?

Bardzo często spotykam się z pytaniem: „Jesteś informatykiem i nie wiesz?". Zawsze staram się wyjaśniać, że informatyków można porównać po części do lekarzy. Na początku zdobywamy podstawową wiedzę, np. dotyczącą funkcjonowania, działania sprzętu, systemu oraz rozwiązywania podstawowych problemów, a dopiero później określamy specjalizację, jaką chcemy podążać. Informatyk będący programistą nie musi znać się na politykach bezpieczeństwa tak jak lekarz ortopeda nie musi leczyć chorób oczu. Nawet ja jako biegły czasem odmawiam wydania opinii z uwagi na brak dostatecznej wiedzy w jakiejś konkretnej specjalizacji. Nie chciałbym doprowadzić do sytuacji podważenia wydanej przeze mnie opinii.
Myślę, że najważniejsze, by osoby rozpoczynające karierę koncentrowały się właśnie nad tą konkretną specjalizacją i starały się być w niej jak najlepsze. Powinny poszerzać swoją wiedzę i umiejętności poprzez szkolenia i korzystać z wiedzy bardziej doświadczonych. Nie przejmować się porażkami i przekuwać je w sukces. Z doświadczenia wiem, że pracodawcy znacznie bardziej cenią osobę, która potrafi coś zrobić, niż taką, która zna definicje.

Czy – Pana zdaniem – przestępcy internetowi wykorzystają rozwój sztucznej inteligencji?

Od wielu lat mówiłem głośno o tym, że sztuczna inteligencja przyniesie wiele dobrego, ale również i złego. Rozwój cyberprzestępczości znacznie przyśpieszył i stanowi to ogromne wyzwanie dla służb. Dobrze, że w Polsce zostało powołane Centralne Biuro Zwalczania Cyberprzestępczości Policji, ale dziś potrzebne jest też korzystanie z wiedzy i doświadczenia praktyków policyjnych. W dobie tak bardzo rozwiniętej sztucznej inteligencji nie możemy już ufać, czy po drugiej stronie słuchawki lub monitora siedzi osoba, za którą się podaje. Oczywiście, że cyberprzestępczość korzysta z dobrodziejstwa AI. Większość poważniejszych cyberprzestępców korzysta z w pełni zautomatyzowanych funkcji sztucznej inteligencji. Przestępcy nie tworzą nowych rodzajów ataków, korzystają z tych już sprawdzonych, ale sztuczna inteligencja pomaga dziś przestępcom w automatyzacji, skalowaniu i zwiększaniu wiarygodności istniejących oszustw. Na ataki z użyciem sztucznej inteligencji narażony jest zarówno przeciętny człowiek, jak i instytucje. Możemy sobie wyobrazić sytuację, w której dzwoni do nas przełożony i prosi o wykonanie jakiejś czynności. W słuchawce oczywiście słyszymy jego głos i nie mamy żadnej wątpliwości, że po drugiej stronie jest ta właśnie osoba. Bezrefleksyjnie wykonujemy jego polecenia, co sprawia, że przestępca osiąga swój skutek. Każdy z nas widział efekty *deepfake* obrazu i głosu, pozostaje kwestią czasu, jak *deepfake'owy* głos będzie wykorzystywany masowo. Kolejnym przykładem wykorzystania sztucznej inteligencji może być przeprowadzenie oszustwa biznesowego (BEC – Business Email Compromise). Rozważmy przykład przesłania na skrzynkę służbową wiadomości email przesłanej masowo do wielu pracowników, funkcjonariuszy opatrzoną wszystkimi cechami naszego przełożonego. W wiadomości załączony został załącznik, a z treści wiadomości możemy wyczytać o przesłaniu zestawienia premii, dodatków z listą osób w celu transparentności przyznawania nagród. Takiego badania nie przeprowadziłem, ale myślę, że znaczna większość otworzyłaby załącznik, nawet z ciekawości. Wraz z otwarciem załącznika można doprowadzić do zainfekowania komputera, a to z kolei otwiera dalszą drogę cyberprzestępcy do osiągnięcia z góry założonego celu.
W praktyce człowiek pozostaje najsłabszym ogniwem, a AI sprawia, że manipulowanie ludźmi staje się tańsze, szybsze i bardziej przekonujące. Dlatego

umiejętność weryfikacji informacji i tożsamości rozmówcy jest dziś jednym z najważniejszych elementów cyberbezpieczeństwa.

Pracując na co dzień z przestępczością internetową, specjaliści napotykają wiele problemów. Które przypadki cyberprzestępczości, z jakimi miał Pan do czynienia, były najtrudniejsze?

Najtrudniejsze nie są te, które sprawiają problemy techniczne, a te, które są ciężkie moralnie, np. pedofilia. Sprawy tej kategorii przysparzają najwięcej problemów, żeby móc się od nich zdystansować. To biegły jest na tej pierwszej linii, gdzie musi przygotować materiał dowodowy dla prokuratury czy Policji. Wiąże się to niestety z wyselekcjonowaniem m.in. materiałów w postaci zdjęć czy filmów. Są oczywiście gotowe rozwiązania w postaci odpowiedniego oprogramowania, które pozwala na wyodrębnienie takiej zawartości, lecz nie są zbyt dokładne. Dlatego muszę osobiście dokonać skrupulatnej analizy danych, by odnaleźć wszystkie dowody oraz osoby pokrzywdzone. Prowadząc sprawy dotyczące pedofilii, człowiek nie zdaje sobie sprawy, jak przebiegli i bez kręgosłupa moralnego są pedofile. Podczas moich wystąpień w szkołach zawsze staram się uświadamiać dzieci, młodzież, ale również rodziców o tego typu zagrożeniach. Staram się przedstawiać sprawy, które były opiniowane – oczywiście w zakresie, w jakim je mogę przedstawić – i pokazywać, jak przestępcy sterują i manipulują dziećmi, żeby osiągnąć swój cel. Zawsze zaczyna się niewinnie: zaczepka przez komunikator internetowy, rozmowy, zrozumienie, te same zainteresowania, dostępność na każde zawołanie i próba zdystansowania dziecka od rodziców. Dlatego wprowadźmy delikatną kontrolę, co nasze dzieci piszą i z kim. Analizując sprawy, zauważyłem, że zawsze były wysyłane przez dziecko sygnały do rodziców, osób bliskich, że coś jest nie tak. Odzwierciedlenie ma to później w rozmowach bardzo często z innym dzieckiem, kolegą, koleżanką, którym to dziecko zwierza się, że nikt go nie rozumie i nie potrafił wysłuchać.

Od jakiegoś czasu można wyraźnie zauważyć, że na świecie przyśpieszył rozwój technologiczny. Parędziesiąt lat wstecz jedynym urządzeniem do korzystania z Internetu był komputer. Obecnie korzystamy ze smartfonów, tabletów i innych urządzeń pozwalających na łączenie się z siecią Internet. Jak Pan uważa, czy urządzenia mobilne są obecnie większym źródłem zagrożeń niż tradycyjne komputery? A może są inne urządzenia, które mogą przynieść równie poważne zagrożenia jak komputer czy smartfon?

Wszystko zależy od tego, co chce osiągnąć przestępca. Są pewne typy przestępstw, jak np. ransomware (blokowanie dostępu do danych komputera poprzez zaszyfrowanie), gdzie przestępca będzie miał na celu osiągnięcie jak największej korzyści finansowej – stosowane głównie na komputerach, serwerach. Urządzenie mobilne jest niezbędne przy zastosowaniu metody phishingu, gdzie ofiara klika w link przesłany przez sprawcę i zostaje przekierowana na stronę identyczną jak strona banku, z żądaniem zalogowania. W tym momencie jest niezbędny smartfon w celu uwierzytelnienia logowania się przestępcy do bankowości. Czasem pewnego typu metody stosuje się i na komputery, i na urządzenia mobilne – mówię o zdalnym pulpicie. Dochodzi do kontaktu rzekomego pracownika banku, który informuje o podejrzanych działaniach na naszym koncie bankowym, po czym proponuje zainstalowanie aplikacji umożliwiającej blokowanie tych działań. Aplikacja, którą proponuje sprawca, to nic innego jak zdalny pulpit umożliwiający mu przejęcie pełnej kontroli nad naszym urządzeniem. Analizując skuteczność cyberataków, myślę, że zwiększy się liczba zagrożeń wobec smartfonów. Niejednokrotnie uświadamiam słuchaczom, że dziś naszą tożsamością nie jest tylko imię, nazwisko, wizerunek itp. Naszą tożsamością jest również smartfon. Nasze urządzenia zawierają ogrom informacji, autoryzują transakcje czy wytyczają drogę. Kto może znać nas lepiej niż nasz smartfon. Przez niego prowadzimy rozmowę, wysyłamy wiadomości, dokonujemy płatności, a niektórzy popełniają przestępstwa. Smartfony wiedzą o nas wszystko. Ale cyberprzestępstwa można popełnić na wiele różnych sposobów i przy wykorzystaniu różnego rodzaju urządzeń, takich jak np. IoT – internet of things (z ang. internet rzeczy). Na co dzień wykorzystujemy rzeczy podłączone do Internetu, nie zastanawiając się nad odpowiednim zabezpieczeniem, więc można je łatwo wykorzystać do ataków.

Jak wygląda analiza telefonu lub komputera zabezpieczonego jako materiał dowodowy?

Przy wykonywaniu czynności najważniejsze jest odpowiednie zachowanie na miejscu oraz dokumentowanie. Na zajęciach z prowadzenia czynności na miejscu podczas zabezpieczania danych zawsze podkreślałem, iż odpowiednie dokumentowanie i wykonywanie czynności pozwoli na uniknięcie jakichkolwiek zarzutów dotyczących umyślnego popełniania błędów czy podważenia wartości dowodowych. Błędy czasem się zdarzają i jest to naturalne, ważne, by było ich jak najmniej lub w ogóle, a jeśli już są – to żeby inny specjalista lub biegły mógł je naprawić. I tu bardzo pomocna jest dokumentacja. Zapoznając się z nią, szybko można wyłapać, do jakiego błędu doszło i w jaki sposób go naprawić.
Każdorazowo przy zabezpieczaniu danych z urządzeń jest niezbędny odpowiedni sprzęt – programy informatyki śledczej, pokrowce blokujące sygnał, przewody i powerbanki, ale również śrubokręty i inne narzędzia niezbędne czasem do rozebrania urządzenia. Najważniejsze jest, by nie doszło do naruszenia integralności danych zawartych

w urządzeniach, dlatego w pierwszej kolejności tworzymy kopię binarną pamięci urządzenia, a dopiero po tej czynności możemy przejść do analizy danych zawartych w kopii. Należy pamiętać, że w idealnym świecie kopie takie powinny być trzy – jedna do prowadzenia badań, druga kopia bezpieczeństwa w razie popełnienia błędu przez badającego i trzecia do udostępniania wraz z materiałami sprawy. W każdym razie jedna z kopii powinna pozostać bez otwierania dla bezpieczeństwa danych. Mając kopię, można przejść do analizy danych. W tym miejscu ma znaczenie, jakie dane chcemy uzyskać z pamięci urządzenia. Czasem wystarczą programy do przeszukiwania pamięci, ale czasem nawet jest niezbędne postawienie kopii na nowym dysku i uruchomienie go w formie działającego systemu. Wszystko zależy od zlecenia. Najważniejsze, by odpowiednio dokumentować postęp prac.

Jest Pan autorem wielu autorskich szkoleń dla różnych grup zawodowych. Uczestniczył Pan w licznych konferencjach, debatach i spotkaniach profilaktycznych w szkołach. Jakie znaczenie ma edukacja społeczeństwa w zakresie cyberbezpieczeństwa?

Myślę, że społeczeństwo jest coraz bardziej świadome zagrożeń w sieci. Niemniej jednak uważam, że znacznie za mało jest prowadzonych kampanii informacyjnych o zagrożeniach. Przestępcy korzystają niezmiennie z tych samych metod, modyfikując i dostosowując się do tego, co dzieje się na świecie, w państwie, w mieście. Opinia publiczna powinna być częściej informowana o aktualnych trendach cyberprzestępstw, które należy przekazywać w sposób zrozumiały dla przeciętnej osoby. Trzeba pamiętać, że większość skutecznych cyberataków wykorzystuje błędy ludzkie, a nie luki techniczne. Prowadzenie edukacji na szerszą skalę w znacznym stopniu ogranicza skuteczność oszustw, chroni gospodarkę i instytucje, zwiększa bezpieczeństwo dzieci i młodzieży. Jak można zauważyć, edukacja w tym zakresie przynosi same korzyści. Technologia rozwija się szybciej niż świadomość społeczna. Narzędzia oparte na AI, deepfake i coraz bardziej przekonujące oszustwa internetowe sprawiają, że edukacja nie może być jednorazowym zastrzykiem wiedzy. Powinna być procesem ciągłym, obejmującym dzieci, dorosłych i seniorów. Można powiedzieć, że w cyberbezpieczeństwie edukacja pełni podobną rolę jak szczepienia w zdrowiu publicznym: nie eliminuje wszystkich zagrożeń, ale znacząco zmniejsza ich skalę i skutki.

Czy według Pana dzieci i młodzież są dziś bardziej narażone na cyberprzestępczość niż dorośli?

Niezależnie od tego, czy są to dzieci, młodzież czy dorośli każdy z nas jest w takim samym stopniu narażony na cyberprzestępczość. Różnica dotyczy tylko rodzaju przestępstwa.

Najmłodsi w społeczeństwie najbardziej są narażeni na *grooming* – próba nawiązania przez dorosłego więzi z dzieckiem w celu wykorzystania seksualnego oraz *troll parenting* – zachowanie rodziców polegające na dzieleniu się w internecie materiałami ośmieszającymi ich dzieci lub ukazującymi je w sytuacjach trudnych, wstydliwych, a nawet upokarzających. Rodzice często nie zdają sobie sprawy, że mogą w ten sposób wyrządzić dziecku krzywdę.
Młodzież narażona jest najbardziej na cyberprzemoc ze strony rówieśników. Niezmiennie co jakiś czas słyszymy o znęcaniu się psychicznym nad rówieśnikami – o szkalowaniu, wyśmiewaniu i wykluczaniu kogoś z życia społecznego. Takie zachowanie ze strony rówieśników kończy się tragedią. Tragedią dla nastolatka, ale również rodziców, bliskich. Powinniśmy nieustannie o tym przypominać i uświadamiać.
Dorośli narażeni są na oszustwa internetowe, ale nie tylko. Bardzo niebezpiecznym zjawiskiem jest *sextortion* – szantaż seksualny poprzez wykorzystanie niefizycznej formy przymusu w celu wymuszenia przysług seksualnych lub pieniędzy od ofiary. Tego typu cyberprzestępstwo może dotknąć zarówno dorosłych, młodzież, ale również dzieci. Niejednokrotnie dzielimy się zdjęciami z osobami, które „znamy" tylko przez Internet, co może prowadzić do wykorzystania tych materiałów przeciwko nam. Zaczyna się od jednego zdjęcia, następnie przestępca szantażuje ofiarę i wymusza kolejne zdjęcia, kończąc na żądaniach pieniędzy.
Nie zapomnijmy o naszych seniorach, którzy są niejednokrotnie bardziej narażeni niż dzieci, młodzież czy dorośli. Grupa ta jest najchętniej atakowana z uwagi na niedostateczną wiedzę i skłonność do obdarowywania innych dużym zaufaniem.
W świecie, w którym coraz większa część naszego życia przenosi się do Internetu, bezpieczeństwo cyfrowe staje się równie ważne jak bezpieczeństwo w świecie rzeczywistym.

Obecnie Polska jest bardziej narażona na cyberataki. Każdego dnia dochodzi do kilkudziesięciu tysięcy, a nawet kilku milionów prób ataków na różne instytucje. Jakie są najczęstsze metody działania cyberprzestępców wobec instytucji publicznych?

W większości przypadków atak na instytucje publiczne jest ukierunkowany na dwa cele: pozyskanie danych i zysk finansowy. Ostatnio można również spotkać się ze szpiegostwem obcych krajów. Żeby atak był skuteczny i osiągnął zamierzony cel, sprawcy wykorzystują różne metody, a czasem łączą kilka z nich.
Jedną z nadal najskuteczniejszych metod jest *phishing* i *spear phishing* (spersonalizowany, dokładnie zaplanowany socjotechniczny atak). *Spear phishing* jest szczególnie niebezpieczny, ponieważ wiadomości są przygotowywane pod konkretną osobę lub urząd.

Kolejną z metod wykorzystywanych przez przestępców jest *ransomware* (złośliwe oprogramowanie szyfrujące dane), niejednokrotnie infekowany poprzez użycie metody *spear phisingu*.
Jedną z najwcześniej aktywnie wykorzystywanych metod przez przestępców na szerszą skalę były ataki DDoS – *Distributed Denial of Service* (z ang. rozproszona odmowa usługi). Polega na zalaniu atakowanego systemu bardzo dużą liczbą zapytań z wielu różnych źródeł. Celem jest przeciążenie systemu.
Instytucje planujące wdrożenie polityki bezpieczeństwa powinny mieć na względzie, że wiele poważnych incydentów zaczyna się od pozornie prostego błędu człowieka – kliknięcia w fałszywy link lub użycia słabego hasła. Dlatego obok technologii kluczową rolę odgrywają procedury i świadomość użytkowników.

Skoro rozmawiamy o atakach na instytucję, proszę wskazać, jakie błędy organizacyjne najczęściej występują w administracji publicznej, jeśli chodzi o bezpieczeństwo IT?

Znaczna większość instytucji jest dobrze zabezpieczona pod względem technologicznym. Posiada sprzęt oraz oprogramowanie czuwające nad bezpieczeństwem. Najczęściej występują błędy organizacyjne. Problemem jest podejście pracowników. Traktują cyberbezpieczeństwo wyłącznie jako problem działu IT, a bezpieczeństwo powinno być odpowiedzialnością całej instytucji. W momencie gdy kierownictwo nie angażuje się w zarządzanie ryzykiem, procedury bezpieczeństwa często pozostają tylko formalnością. Słabym punktem instytucji jest brak ciągłości i powtarzalności szkoleń. Ciągłe uświadamianie pracowników oraz wskazywanie najnowszych trendów cyberprzestępców może pomóc rozpoznać ataki. Instytucje zapominają również o aktualizacji procedur i polityk bezpieczeństwa. Widziałem polityki bezpieczeństwa przestarzałe i nieaktualizowane od wielu lat. Kolejnym błędem jest nadawanie nadmiernych uprawnień użytkownikom. Posiadają oni często dostęp do znacznie większej liczby systemów oraz danych, niż potrzebują do wykonywania swoich obowiązków. Narusza to zasadę najmniejszych uprawnień (*least privilege*). Instytucje nie testują planów reagowania na incydenty. Mają procedury reagowania, ale nigdy ich nie testują. W efekcie podczas wystąpienia rzeczywistego incydentu pojawia się chaos, opóźnienia i niejasny podział odpowiedzialności. Inny ważny błąd, jaki można zauważyć, to niedostateczne wsparcie kierownictwa. Cyberbezpieczeństwo postrzegane jest wyłącznie jako koszt i zbędny wydatek. Jest to jeden z najczęściej wskazywanych problemów przez audytorów i specjalistów ds. bezpieczeństwa.
Największe ryzyko w instytucjach czy administracji publicznej zwykle nie wynika z braku konkretnych narzędzi, lecz z połączenia trzech czynników: niewystarczającej świadomości, słabego zarządzania procesami bezpieczeństwa oraz niedostatecznego nadzoru nad ryzykiem. Dlatego skuteczne cyberbezpieczeństwo jest przede wszystkim zagadnieniem organizacyjnym i zarządczym, a dopiero w drugiej kolejności technologicznym.

Pracował Pan jako instruktor i szkoleniowiec w Akademii Policji w Szczytnie. Był Pan jedną z osób tworzących program studiów dla funkcjonariuszy CBZC. Jak wygląda proces szkolenia funkcjonariuszy w zakresie cyberbezpieczeństwa, cyberprzestępczości?

Obecnie każda z instytucji, w tym Policja, boryka się z brakiem specjalistów w zakresie cyberbezpieczeństwa i cyberprzestępczości, dlatego krok w kierunku utworzenia studiów z tego zakresu był jak najbardziej uzasadniony i oczywisty. Studia pierwszego stopnia są uzupełniane drugim stopniem, gdzie wiedza jest uszczegółowiana i uzupełniana. Treści programowe są merytoryczne, niemniej jednak wydaje się konieczne jeszcze kompleksowe rozwiązanie podpierające teorię cykliczną praktyką. Akademia Policji w Szczytnie ma możliwości do wprowadzenia stałych rozwiązań i wdrożenia szkoleń czysto praktycznych, które uświadomią funkcjonariuszom, jak działa przestępstwo z punktu widzenia sprawcy. Stworzenie odizolowanego środowiska do przeprowadzania ataków i zbierania śladów informacji jest niezbędne dla ustalenia sprawcy. Do tego potrzebni są wykładowcy posiadający wiedzę praktyczną z konkretnych specjalizacji. Przy tworzeniu praktycznego programu należałoby także korzystać ze wsparcia odpowiednich osób, mających dostateczną wiedzę i umiejętności. Niemniej jednak Akademia Policji w Szczytnie zmierza w dobrym kierunku, aczkolwiek trochę za wolno. Funkcjonariusze są głodni wiedzy i chcą tę wiedzę zdobywać i poszerzać.

Summary

Resilience to cybercrime and more... Interview with court expert in the field of computer forensics

In this interview, the Director of the Cybersecurity Office at the Polish Society of Experts and Court Experts (Polish: Polskie Towarzystwo Ekspertów i Biegłych Sądowych), a former police officer, a court expert in IT, an expert in the supervision and implementation of security procedures and policies, risk analysis and the security of IT systems, answers questions about the types of crimes he most often encounters in his work, as well as about the directions of cybercrime development. He emphasizes that the development of AI has already contributed to the automation, scaling and increasing the credibility of fraud in cyberspace. He also announces the next stages of development of AI-based crime. He points out common mistakes made by Internet users that are exploited by criminals and lead to loss of data or money.
As an expert in the field of computer forensics, he discusses the process of securing digital evidence during pre-trial proceedings, as well as the principles of securing digital evidence and the most common mistakes made by investigators in this area. He emphasizes the need to introduce into the training programs of police officers dealing with cybercrime regular, purely practical exercises conducted by lecturers with practical knowledge and skills in specific specializations.
He also explores issues related to cooperation between court experts and the Police, prosecutors, and courts. He pays special attention to the difficult issues of securing evidence and preparing expert opinions in cases involving pedophilia. He highlights the role of continuous education of the entire society regarding current threats posed by the Internet, with particular emphasis on the threats to which the youngest and seniors are exposed. Due to the rapidly growing number of cyberattacks on public administration and other institutions and companies, he calls for a responsible approach to cybersecurity by management and employees, as well as for compliance with policies and procedures in the field of the security of IT systems.

Tłumaczenie: Beata Pepłowska

CYFROWY PARALIŻ PAŃSTWA

Czy Policja wytrzyma starcie w wojnie hybrydowej nowej generacji?

Grafika wygenerowana z wykorzystaniem licencjonowanego programu Adobe Firefly.

Marcin Tęgos

Naczelnik Wydziału Cyberbezpieczeństwa Biura Łączności i Informatyki KGP
Przewodniczący Zespołu POL-CERT

W świecie, gdzie granica między pokojem a konfliktem uległa całkowitemu zatarciu, prawdziwe pole bitwy nie leży na polach czy w pasie przygranicznym, lecz w krzemowych obwodach naszych serwerów. Podczas gdy opinia publiczna patrzy na Policję przez pryzmat radiowozów i patroli, najważniejsza instytucja mająca za zadanie ochronę bezpieczeństwa i utrzymanie porządku publicznego walczy dziś na pierwszej linii frontu niewidzialnej wojny. Teza jest brutalnie prosta: jeśli zawiedzie cyberbezpieczeństwo infrastruktury Policji, całe państwo może doświadczyć cyfrowego paraliżu, zanim pierwszy funkcjonariusz zdąży wyciągnąć broń.

Przez lata popełnialiśmy błąd poznawczy. Myśleliśmy o cyberbezpieczeństwie w kategoriach „walki z przestępcami" – ścigania hakerów kradnących dane czy oszukujących emerytów. To myślenie jest anachroniczne i niebezpieczne. Dziś cyberbezpieczeństwo Policji to nie tylko kwestia łapania złodziei, to fundament bezpieczeństwa wewnętrznego państwa.

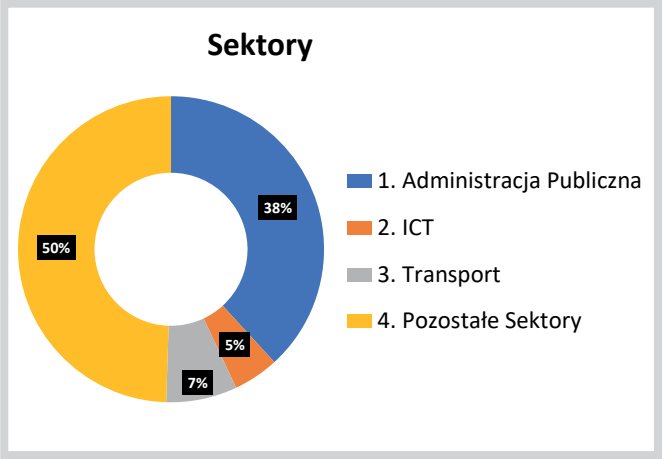
Spójrzmy na liczby, bo one nie kłamią i nie mają emocji. W roku 2025 Wydział Cyberbezpieczeństwa Biura Łączności i Informatyki Komendy Głównej Policji wraz z zespołem POL-CERT obsłużył ponad 17 tysięcy incydentów. To o ponad pięć tysięcy więcej niż rok wcześniej. To nie jest „wzrost statystyczny" – to potężna fala uderzeniowa, która każdego dnia rozbija się o mury naszej instytucji. I co najgorsze: ta fala nie słabnie, ona przybiera na sile, napędzana przez geopolityczne ambicje adwersarzy, dla których infrastruktura rządowa i policyjna jest celem priorytetowym.

Sektor publiczny w Polsce znajduje się pod bezprecedensową presją cyberataków. W 2024 r. cyberprzestępcy dokonywali średnio 2063 ataków miesięcznie na sektor publiczny oraz 2058 ataków na sektor wojskowo-rządowy[1]. W 2024 r. odnotowano wzrost liczby incydentów w sektorze publicznym o 58 procent w porównaniu do roku 2023[2].

Dane z pierwszej połowy 2025 r. wskazują na dalszą eskalację zagrożeń. W analizowanym okresie zgłoszono 485 tysięcy potencjalnych incydentów bezpieczeństwa, z czego potwierdzono 111 660 przypadków rzeczywistych naruszeń – wzrost o 23 procent. Szczególnie alarmujące są dane dotyczące ataków o poważnym charakterze, których liczba wzrosła o 57 procent, a naruszeń w sektorze publicznym o 58 procent[3].

Według raportu ENISA, polska administracja publiczna znalazła się w gronie pięciu państw najbardziej atakowanych w UE, z udziałem 15 procent incydentów w tej kategorii[4].

Wykres nr 1. Cele ataków cybernetycznych w stosunku do liczby zgłoszonych incydentów. (Zestawienie na podstawie danych Agencji Unii Europejskiej ds. Cyberbezpieczeństwa – ENISA 2024-2025 EU, dla sektorów określonych w dyrektywie NIS2[5]).



Wchodzimy w erę, w której grupy APT[6] nie szukają już tylko pieniędzy. Szukają chaosu. Szukają sposobu na wyłączenie systemów łączności, paraliż komunikacji kryzysowej i ośmieszenie instytucji państwowych. Co więcej, nadchodzi „cyfrowy darwinizm" – era wspierana przez sztuczną inteligencję (AI), gdzie automatyczne ataki będą generowane z prędkością, której ludzki operator nie jest w stanie się przeciwstawić. Standardowe procedury, które dziś wydają się solidne, jutro mogą stać się jedynie cyfrowym odpowiednikiem papierowych tarcz przeciwko pociskom rakietowym. W tym kontekście działania Biura Łączności i Informatyki KGP – choć wciąż będące zaledwie początkiem długiej drogi – jawią się jako niezbędna próba „podjęcia rękawicy". Nie możemy pozwolić sobie na reaktywność; musimy przejść do strategii proaktywnej. Reforma zarządzania, przebudowa struktury POL-CERT i dostosowanie do rygorystycznych wymogów nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa to nie są tylko biurokratyczne zabiegi. To budowa cyfrowego układu odpornościowego. Centralizacja zarządzania stacjami roboczymi oraz wprowadzenie twardej, sprzętowej autoryzacji (2FA[7]) to fundamenty, bez których każda próba obrony jest skazana na porażkę. Bez tego Policja pozostaje instytucją z „otwartymi drzwiami" w świecie, gdzie każdy atak jest zautomatyzowany i nieubłagany.

Musimy jednak zadać sobie pytanie: czy to wystarczy? Wyścig zbrojeń między państwową machiną a grupami hakerskimi wspieranymi przez obce mocarstwa to bieg, w którym stawką jest suwerenność informacyjna. Inwestycja w technologię to tylko połowa sukcesu. Drugą połową jest kapitał ludzki – szkolenie kadr, które będą potrafiły myśleć krok przed algorytmem przeciwnika.

Policja nie może być postrzegana jedynie jako instytucja reagująca na przestępstwa. Musi stać się twierdzą, której cyfrowe mury są równie szczelne, co fizyczne zapory. Jeśli nie zrozumiemy, że bezpieczeństwo infrastruktury IT Policji jest tożsame z bezpieczeństwem każdego obywatela, obudzimy się w państwie, które ma wszystkie paragrafy świata, ale nie posiada sprawnego systemu, by je wyegzekwować.

[1] ISBtech.pl. Serwis o tematyce technologicznej, *Ponad 4 000 ataków miesięcznie na polski sektor publiczny*, https://www.isbtech.pl/2025/05/ponad-4-000-atakow-miesiecznie-na-polski-sektor-publiczny/ [dostęp: 11.06.2026 r.].

[2] Z. Łochowska, *Statystyki cyberbezpieczeństwa: co mówią dane o wzroście zagrożeń w 2025 roku?*, Exorigo-Upos.pl, https://www.exorigo-upos.pl/blog/statystyki-cyberbezpieczenstwa-dane-z-2025-roku/ [dostęp: 11.06.2026 r.].

[3] J. Jaśkowiak, *Cyberzagrożenia w Polsce 2025: Najczęściej atakowana infrastruktura krytyczna*, Mikrokontroler.pl, 25.04.2025 r., https://mikrokontroler.pl/2025/04/25/cyberzagrozenia-w-polsce-2025-najczesciej-atakowana-infrastruktura-krytyczna/ [dostęp: 11.06.2026 r.].

[4] ENISA. European Union Agency For Cybersecurity, Enisa Threat Landscape 2025, październik 2025 r., s. 18,https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf [dostęp: 11.06.2026 r.].

[5] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2), Dz.U. L 333 z 27.12.2022, pp. 80–152.

[6] Grupy APT (*Advanced Persistent Threat* – zaawansowane trwałe zagrożenie) – grupy cyberprzestępców skupiające się na zaawansowanych, trwałych zagrożeniach. Są to zazwyczaj cyberprzestępcy z organizacji państwowych lub organizacji, które działają w imieniu państw. Koncentrują się one na ukierunkowanych i wyrafinowanych operacjach cybernetycznych, aby przeniknąć do systemów wysokiego szczebla (organizacji rządowych, korporacji) i pozostać w nich niewykrytymi przez dłuższy czas. Działają głównie w celu długoterminowego cyberszpiegostwa i kradzieży poufnych danych. Dysponują zaawansowanymi narzędziami, technikami, wiedzą i umiejętnościami. Źródło: ESET Online Help, ESET Glossary, https://help.eset.com/glossary/pl-PL/apt_group.html [dostęp: 11.06.2026 r.].

[7] Sprzętowa autoryzacja 2FA – jedna z najbezpieczniejszych form weryfikacji tożsamości polegająca na logowaniu się fizycznym kluczem – urządzeniem USB lub NFC, które generuje kryptograficzny podpis.

Summary

Digital paralysis of the state: can the Police withstand the new era of hybrid warfare?

The author, Head of the Cybersecurity Department at the Communications and Information Technology Bureau of the National Police Headquarters, outlines a fundamental shift in the way public security and public order are safeguarded. While the public often associates police work with patrol cars and officers on the streets, the Police are increasingly operating on the frontlines of cyberspace. The author argues that a failure to adequately protect police information and communication systems could lead to digital paralysis with consequences extending far beyond the Police itself. In 2025, the Cybersecurity Department of the National Police Headquarters and the POL-CERT team handled nearly 17,000 cybersecurity incidents – over 5,000 more than in the previous year. According to the author, this trend shows no sign of slowing down and is, in fact, becoming increasingly pronounced. Particular attention is paid to Advanced Persistent Threat (ATP) attacks aimed at creating chaos, disrupting communications, impairing crisis-management capabilities, and discrediting state institutions. The growing use of artificial intelligence is expected to further increase both the scale and sophistication of such threats. The article concludes that the Police must adopt a proactive approach strengthening cyber resilience. This will require organisational reform, the further development of the POL-CERT framework, compliance with the amended National Cybersecurity System Act, and continued investment in highly skilled cybersecurity professionals capable of staying ahead of increasingly sophisticated threats.

Tłumaczenie: Joanna Łaszyn

ZABEZPIECZANIE KRYPTOWALUT W POSTĘPOWANIU KARNYM

Aspekty procesowe, techniczne i praktyczne

Grafika wygenerowana z wykorzystaniem licencjonowanego programu Adobe Firefly.

podkom. Przemysław Szczerba

Wydział Informatyki Śledczej CBZC

Podkom. Przemysław Szczerba, radca w Wydziale Informatyki Śledczej w Centralnym Biurze Zwalczania Cyberprzestępczości (CBZC) w Warszawie. Posiada ponad 14-letnie doświadczenie w służbach ścigania, specjalizując się w informatyce śledczej oraz zabezpieczaniu dowodów cyfrowych. Certyfikowany specjalista w zakresie: SEC+, CCSK, CHFI, BTL1, eCDFP. Absolwent studiów z zakresu bezpieczeństwa wewnętrznego oraz inżynier informatyki. Trener cyberbezpieczeństwa w NASK. Wielokrotnie zapraszany do wsparcia dydaktycznego w przedsięwzięciach realizowanych przez Zakład Kryminalny Centrum Szkolenia Policji w Legionowie z zakresu szeroko pojętej cyberprzestępczości, analizy kryminalnej czy kryptowalut.

Obszary zainteresowań: blockchain forensics, analiza kryptowalut, OSINT/SOCMINT, geolokalizacja cyfrowa, ransomware, postępowanie dowodowe w sprawach cyberprzestępczości.

Artykuł przedstawia kompleksową analizę problematyki zabezpieczania kryptowalut w polskim postępowaniu karnym. Omówiono podstawy technologiczne walut cyfrowych, w tym technologię blockchain, mechanizmy kluczy kryptograficznych oraz rodzaje portfeli. Przedstawiono podstawy prawne zabezpieczania kryptowalut, procedury stosowane przez organy ścigania oraz wytyczne Prokuratury Krajowej z 2023 r. Szczególną uwagę poświęcono wyzwaniom technicznym i prawnym związanym z pozorną anonimowością transakcji, problemami jurysdykcyjnymi oraz przechowywaniem zabezpieczonych aktywów cyfrowych. Sformułowano rekomendacje dotyczące dobrych praktyk dla funkcjonariuszy organów ścigania i prokuratur.

WPROWADZENIE

Dynamiczny rozwój technologii rozproszonych rejestrów, zapoczątkowany publikacją koncepcji Bitcoina przez Satoshiego Nakamoto w 2008 r., wywołał fundamentalne zmiany nie tylko w sferze finansowej, ale również w obszarze prawa karnego materialnego i procesowego[1].

Kryptowaluty, początkowo postrzegane jako niszowy eksperyment technologiczny, stały się pełnoprawnym instrumentem obrotu gospodarczego, a jednocześnie narzędziem wykorzystywanym przez sprawców przestępstw do transferu i ukrywania środków pochodzących z działalności przestępczej. Zjawisko to wymaga od organów ścigania zarówno odpowiednich kompetencji technicznych, jak i znajomości procedur prawnych właściwych dla tej specyficznej kategorii mienia.

> „Informatyk śledczy powinien posiadać pełne zrozumienie technologii, na których opierają się waluty cyfrowe, gdyż tylko to pozwala na przeprowadzenie efektywnych analiz".
>
> P. Rodwald, *Kryptowaluty z perspektywy informatyki śledczej*, AMW, Gdynia 2021, s. 14.

Stwierdzenie to w równym stopniu dotyczy funkcjonariuszy organów ścigania i prokuratur, którzy coraz częściej stają przed koniecznością zabezpieczania aktywów cyfrowych w toku prowadzonych postępowań karnych. Brak specjalistycznej wiedzy technicznej może prowadzić nie tylko do utraty istotnych dowodów, ale również do nieodwracalnego przepadku mienia o znacznej wartości[2].
Niniejszy artykuł ma na celu przedstawienie kompleksowej analizy problematyki zabezpieczania kryptowalut w polskim postępowaniu karnym, z uwzględnieniem aspektów technologicznych, prawnych i praktycznych. Opracowanie uwzględnia aktualne wytyczne Prokuratury Krajowej, literaturę specjalistyczną z zakresu informatyki śledczej oraz doświadczenia praktyczne wynikające z dotychczasowych postępowań.

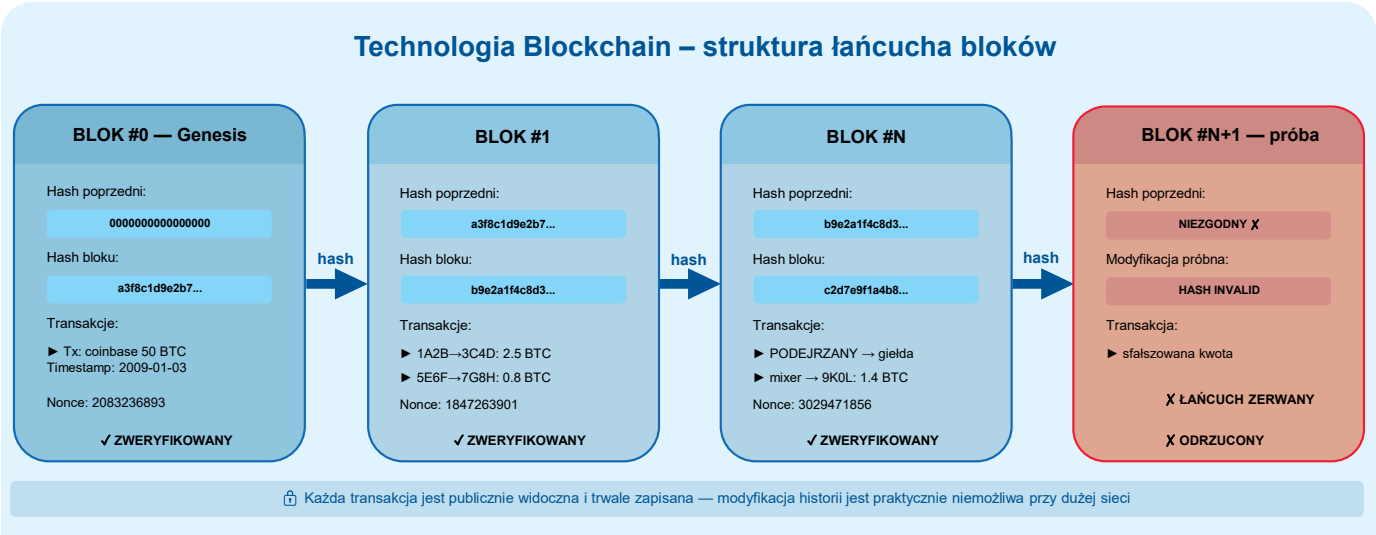
PODSTAWY TECHNOLOGICZNE KRYPTOWALUT

Pojęcie i definicja waluty wirtualnej

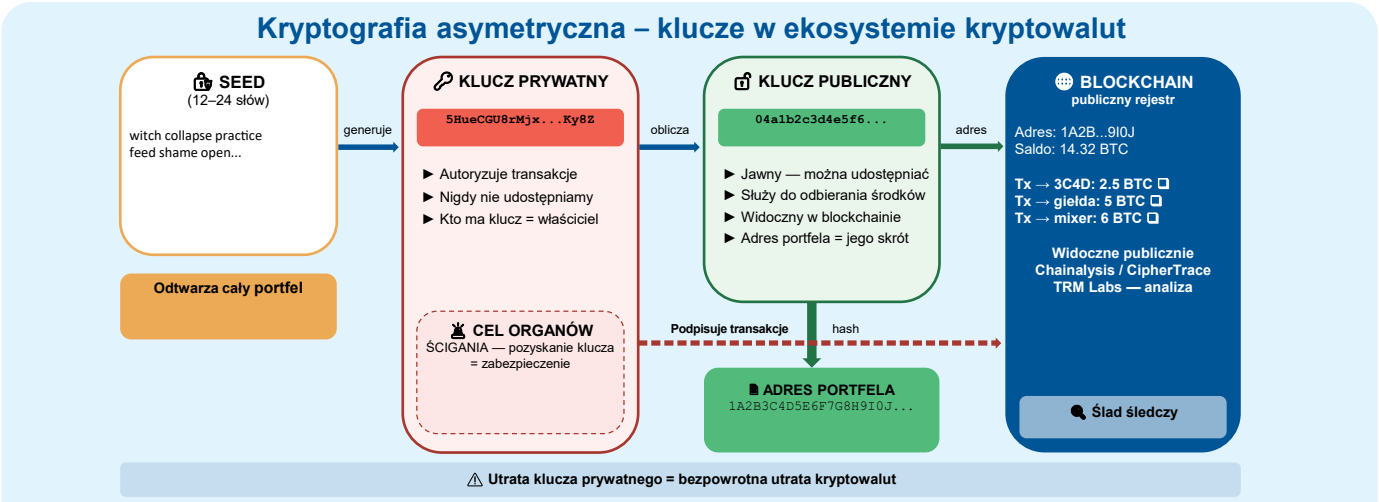
Ustawodawca polski zdecydował się na wprowadzenie definicji legalnej waluty wirtualnej w art. 2 ust. 2 pkt 26 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu. Zgodnie z przywołaną regulacją walutą wirtualną jest cyfrowe odwzorowanie wartości, które nie stanowi prawnego środka płatniczego, pieniądza elektronicznego, instrumentu finansowego ani weksla bądź czeku, lecz jest wymieniane w obrocie gospodarczym na prawne środki płatnicze i akceptowane jako środek wymiany[3]. Definicja ta, choć krytykowana w doktrynie za swoją negatywną konstrukcję, stanowi punkt wyjścia dla kwalifikacji prawnej kryptowalut w postępowaniu karnym.
M. Wnęk, analizując naturę prawną kryptowaluty, zwraca uwagę na konieczność rozróżniania pomiędzy pojęciami waluty wirtualnej, waluty cyfrowej i kryptowaluty. W świetle jego analiz termin „kryptowaluta" w sposób najprecyzyjniejszy oddaje istotę omawianych aktywów, akcentując ich kryptograficzny charakter. Rozróżnienie to ma istotne znaczenie praktyczne, ponieważ zakres pojęciowy waluty wirtualnej w rozumieniu ustawowym jest szerszy niż pojęcie kryptowaluty i obejmuje również aktywa nieoparte na technologii blockchain[4].

Technologia blockchain i mechanizmy kryptograficzne

Funkcjonowanie kryptowalut opiera się na technologii łańcucha bloków (blockchain), która stanowi zdecentralizowany i rozproszony system rejestracji transakcji. Każdy blok zawiera kryptograficzny skrót (hash) bloku poprzedniego, co tworzy nieprzerwany łańcuch zapewniający integralność danych. Próba modyfikacji jakiejkolwiek historycznej transakcji wymagałaby zmiany wszystkich następujących bloków, co przy odpowiednio dużej sieci jest praktycznie niemożliwe[5].
Zasadniczym elementem środowiska kryptowalut jest szyfrowanie asymetryczne, oparte na parze klucza publicznego i prywatnego. Klucz publiczny pełni funkcję adresu portfela – jest jawny i umożliwia otrzymywanie środków. Klucz prywatny natomiast służy do autoryzacji transakcji wychodzących i stanowi jedyny dowód dysponowania środkami zgromadzonymi pod danym adresem. Utrata klucza prywatnego oznacza bezpowrotną utratę dostępu do kryptowalut, co ma fundamentalne znaczenie dla procedur zabezpieczania – organy ścigania muszą dążyć do pozyskania tego klucza, aby efektywnie zabezpieczyć walutę cyfrową[6].



Ryc. 1. Struktura łańcucha bloków — każda modyfikacja historycznych danych unieważnia kolejne bloki. Źródło: opracowanie własne.



Ryc. 2. Kryptografia asymetryczna — relacja między seed, kluczem prywatnym, kluczem publicznym i adresem portfela. Źródło: opracowanie własne.

⚠ Kluczowe pojęcie: SEED (fraza odzyskiwania)

Seed to ciąg 12–24 słów w języku angielskim, służący do odtworzenia dostępu do portfela kryptowalutowego.

Samo posiadanie seeda umożliwia odzyskanie środków — bez fizycznego dostępu do urządzenia i bez znajomości kodu PIN. Seed zapisany na kartce papieru, ujawniony podczas przeszukania, może stanowić kluczowy element umożliwiający zabezpieczenie kryptowalut. Należy traktować go z taką samą uwagą jak gotówkę lub klucz do sejfu.

Obok pary kluczy, istotnym pojęciem jest tzw. seed (ziarno), czyli ciąg od 12 do 24 słów w języku angielskim, służący do odtworzenia dostępu do portfela kryptowalutowego. Z perspektywy czynności procesowych oznacza to, że seed ujawniony podczas przeszukania – nawet zapisany odręcznie na kartce papieru – może stanowić kluczowy element umożliwiający zabezpieczenie kryptowalut[7].

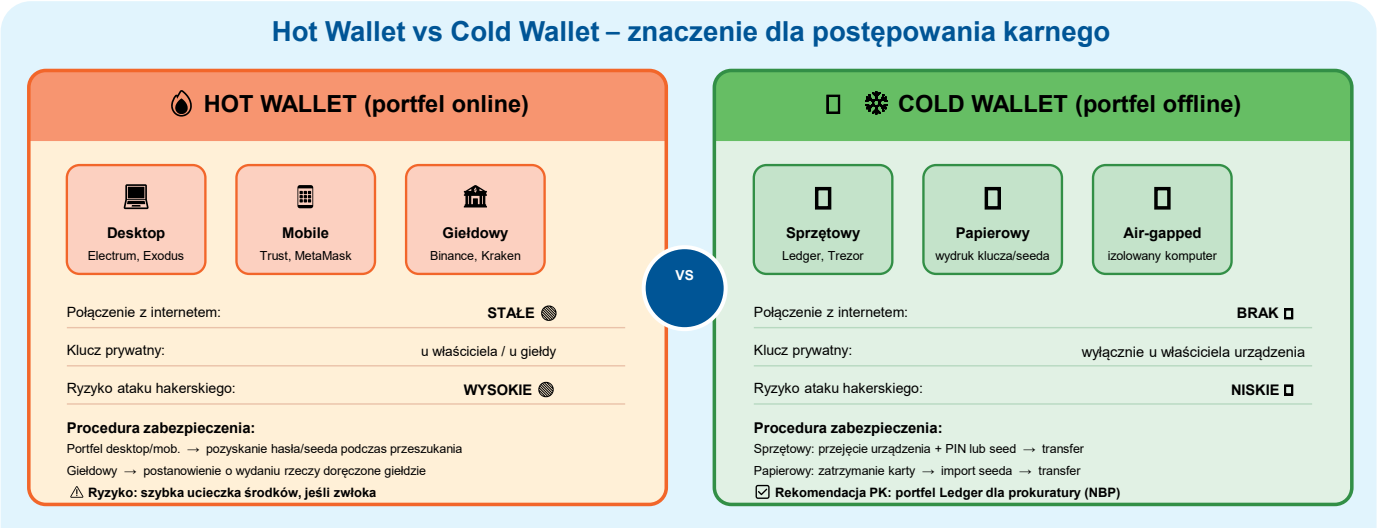
Rodzaje portfeli kryptowalutowych

Blockchain pełni w ekosystemie kryptowalut rolę rozproszonego rejestru transakcji, porównywalnego funkcjonalnie z księgą wieczystą. Istotne jest, że kryptowaluty nie są fizycznie przechowywane w portfelach – portfel zawiera je-

Tabela 1. Rodzaje portfeli kryptowalutowych a właściwa procedura zabezpieczenia.

TYP PORTFELA	PRZYKŁADY	KLUCZ PRYWATNY	PROCEDURA ZABEZPIECZENIA
PORTFEL SPRZĘTOWY (HARDWARE WALLET)	Ledger Nano X/S+, Trezor Model T/Safe 3	Wyłącznie u właściciela urządzenia	Przejęcie urządzenia + kod PIN lub seed → transfer na portfel prokuratury
PORTFEL PAPIEROWY (PAPER WALLET)	Wydruk klucza prywatnego lub frazy seed	Dokument papierowy w posiadaniu właściciela	Zatrzymanie dokumentu jako dowód rzeczowy → import seeda → transfer środków
PORTFEL DESKTOPOWY / MOBILNY (SOFTWARE WALLET)	Electrum, Exodus, Trust Wallet, MetaMask	Na urządzeniu użytkownika (zaszyfrowany plik)	Zabezpieczenie nośnika elektronicznego → pozyskanie hasła lub seeda → transfer
PORTFEL GIEŁDOWY (CUSTODIAL / EXCHANGE)	Binance, Kraken, Zonda, Coinbase	Giełda – użytkownik nie posiada klucza prywatnego	Postanowienie o wydaniu rzeczy doręczone giełdzie; ewentualnie MLA przy giełdach zagranicznych
STABLECOIN ZE SCENTRALIZOWANYM EMITENTEM	USDT (Tether), USDC (Circle)	Emitent zachowuje zdolność do zamrożenia portfela	Wniosek o zamrożenie (freeze) do Tether / Circle (LEA request); uwaga: zamrażany jest cały portfel

Objaśnienia skrótów: **MLA** (ang. *Mutual Legal Assistance*) – wzajemna pomoc prawna w sprawach karnych, formalna procedura współpracy między państwami, polegająca na wystąpieniu jednego państwa do drugiego z wnioskiem o wykonanie określonych czynności procesowych (np. przesłuchanie świadka, dostarczenie dokumentów, zajęcie majątku); **USDT (Tether)** – stablecoin (kryptowaluta powiązana z kursem dolara USD) emitowany przez Tether Operations Limited, jeden z najszerzej stosowanych stablecoinów w obrocie kryptowalutowym; **USDC (USD Coin)** – stablecoin emitowany przez Circle Internet Financial, podobnie jak USDT, utrzymuje parytet 1:1 z dolarem USD, obaj emitenci prowadzą procedury zamrażania portfeli na wniosek organów ścigania (LEA freeze request); **LEA** (ang. *Law Enforcement Agency*) – organ ścigania (policja, prokuratura lub inny właściwy organ uprawniony do ścigania przestępstw).
Źródło: opracowanie własne na podstawie wytycznych Prokuratury Krajowej z 2023 r. i literatury przedmiotu.



Ryc. 3. Portfel online (Hot Wallet) vs portfel offline (Cold Wallet) – porównanie z perspektywy procedur zabezpieczających. Źródło: opracowanie własne.

dynie klucze kryptograficzne umożliwiające dysponowanie środkami zarejestrowanymi w blockchainie. Rozróżnienie to jest kluczowe dla zrozumienia procedur zabezpieczania[8]. Z punktu widzenia czynności procesowych należy wyróżnić dwie zasadnicze kategorie portfeli: zewnętrzne (pozagiełdowe) oraz giełdowe. Kluczowa różnica polega na tym, że w przypadku portfeli giełdowych użytkownik nie dysponuje kluczem prywatnym – klucze te pozostają w gestii giełdy. Ma to bezpośrednie przełożenie na sposób postępowania organów ścigania.

W przypadku portfeli giełdowych zabezpieczenie kryptowalut wymaga współpracy z operatorem platformy, podczas gdy w przypadku portfela zewnętrznego niezbędne jest pozyskanie klucza prywatnego lub seeda[9].

PODSTAWY PRAWNE ZABEZPIECZANIA KRYPTOWALUT W POSTĘPOWANIU KARNYM

Kwalifikacja prawna kryptowalut jako przedmiotu zabezpieczenia

Status prawny kryptowalut w polskim systemie prawnym budzi w dalszym ciągu kontrowersje doktrynalne. Niemniej jednak z perspektywy prawa karnego procesowego kluczowe znaczenie ma ustalenie, że waluta wirtualna może zostać uznana zarówno za dowód w sprawie, jak i za mienie podlegające zabezpieczeniu majątkowemu. Okoliczność, że kryptowaluty stanowią jednocześnie cyfrowe odwzorowanie wartości i posiadają określoną wartość majątkową, nie wyklucza ich traktowania jako dowodów rzeczowych[10]. Kodeks postępowania karnego nie zawiera szczególnych przepisów dotyczących zabezpieczania walut cyfrowych. Jak wskazuje Prokuratura Krajowa w wytycznych z 2023 r., brak jest przeciwwskazań do poszukiwania i zabezpieczania dowodów w postaci kryptowalut z wykorzystaniem ujawnionych danych dostępowych. W odniesieniu do kryptowalut zastosowanie znajdują ogólne przepisy dotyczące zatrzymania rzeczy, przeszukania oraz zabezpieczenia majątkowego, uzupełnione o specyficzne dla aktywów cyfrowych aspekty techniczne[11, 12].

Dualny charakter zabezpieczenia

W toku prowadzonych postępowań karnych możliwe jest procedowanie w stosunku do waluty wirtualnej w dwojaki sposób. Po pierwsze, kryptowaluty mogą być zabezpieczane jako mienie podlegające zabezpieczeniu majątkowemu – w szczególności w celu orzeczenia zwrotu pokrzywdzo-

Tabela 2. Dualny charakter zabezpieczenia kryptowalut w postępowaniu karnym.

KRYTERIUM	DOWÓD RZECZOWY	ZABEZPIECZENIE MAJĄTKOWE
CEL PROCESOWY	Wykazanie okoliczności faktycznych przestępstwa	Orzeczenie przepadku lub zwrot korzyści pokrzywdzonemu
PODSTAWA PRAWNA	Art. 217 k.p.k., art. 228–236 k.p.k.	Art. 291–296 k.p.k., art. 232 § 1 k.p.k.
FORMA ORZECZENIA	Protokół zatrzymania rzeczy + postanowienie o uznaniu za dowód	Postanowienie o zabezpieczeniu majątkowym lub tymczasowym zajęciu mienia
ORGAN EGZEKUCYJNY	Prokurator / sąd	Komornik lub naczelnik urzędu skarbowego (sprzedaż – art. 232 § 1 k.p.k.)
KUMULACJA	Te same jednostki kryptowaluty mogą być jednocześnie dowodem rzeczowym i przedmiotem zabezpieczenia majątkowego	

Źródło: opracowanie własne na podstawie k.p.k. i Wytycznych PK 2023.

Ryc. 4. Mapa przepływu środków od przestępstwa do zabezpieczenia przez organy ścigania. Źródło: opracowanie własne.

* Obfuskacja (ang. obfuscation) – technika zaciemniania kodu lub danych cyfrowych, polegająca na takim przekształceniu programu lub informacji, że ich zrozumienie i analiza przez człowieka lub narzędzia są znacznie utrudnione, przy jednoczesnym zachowaniu ich pełnej funkcjonalności. Stosowana m.in. przez twórców złośliwego oprogramowania (malware) w celu ukrycia sposobu działania kodu przed analizą śledczą i narzędziami antywirusowymi.

nemu bądź przepadku. Po drugie, ujawnione jednostki cyfrowe mogą stanowić dowód rzeczowy. Nie wyklucza to sytuacji, w której te same jednostki cyfrowe będą jednocześnie dowodem rzeczowym i przedmiotem zabezpieczenia majątkowego[13].

Priorytetowym celem każdego postępowania przygotowawczego powinno być dążenie do wyrównania szkody wyrządzonej pokrzywdzonemu, w tym w drodze odzyskania utraconych środków. Ma to szczególne znaczenie w sprawach z zakresu cyberprzestępczości, gdzie jedyną drogą wyrównania szkody może okazać się właśnie zabezpieczenie i zwrot zajętych wartości majątkowych[14].

PROCEDURY I METODY ZABEZPIECZANIA KRYPTOWALUT

Czynności przygotowawcze i profilowanie majątkowe

Zgodnie z art. 217 § 1 k.p.k. rzeczy mogące stanowić dowód w sprawie lub podlegające zajęciu powinny być wydane na żądanie sądu lub prokuratora. Jedną z pierwszych czynności, w toku której może dojść do ujawnienia posiadania kryptowalut przez sprawcę, jest czynność przeszukania[15].

Etap profilowania majątkowego stanowi kluczowy element przygotowania do czynności zabezpieczających. Metodyka zabezpieczeń majątkowych Prokuratury Krajowej szczegółowo opisuje czynności poprzedzające zajęcie walut cyfrowych, obejmujące m.in. analizę rachunków bankowych pod kątem transakcji z giełdami kryptowalut, weryfikację źródeł otwartych (OSINT), a także ustalenia operacyjne dotyczące sposobu przechowywania aktywów cyfrowych. Podczas przeszukania należy zwracać szczególną uwagę na wszelkie zapiski mogące stanowić adresy kluczy, hasła, loginy, kody autoryzacyjne, portfele papierowe i sprzętowe oraz na nośniki elektroniczne[16].

Algorytm postępowania przy zabezpieczaniu kryptowalut

Tabela 3 oraz rysunek 4 prezentują schemat decyzyjny dla funkcjonariuszy organów ścigania i prokuratorów w zależności od rodzaju portfela i stopnia współpracy ze strony podejrzanego.

Zabezpieczanie kryptowalut na portfelu giełdowym

Odrębne zagadnienie stanowi sytuacja, gdy ustalono, że ujawniony adres publiczny stanowi portfel giełdowy. W przypadku dobrowolnego wydania loginów i haseł należy postępować analogicznie jak w przypadku portfela zewnętrznego. Natomiast w sytuacji braku ujawnienia kodów dostępowych niezbędne będzie wydanie postanowienia o żądaniu wydania rzeczy, doręczonego bezpośrednio giełdzie[17].

Możliwe jest również dokonanie blokady konta na giełdzie lub wstrzymania transakcji na podstawie art. 86 ust. 10 ustawy o przeciwdziałaniu praniu pieniędzy, ponieważ rachunek w rozumieniu tej ustawy obejmuje również prowadzony w formie elektronicznej zbiór danych identyfikacyjnych zapewniających możliwość korzystania z jednostek walut wirtualnych[18].

Przechowywanie i sprzedaż zabezpieczonych kryptowalut

Kwestia przechowywania zabezpieczonych kryptowalut została szczegółowo uregulowana w Wytycznych PK 2023. Rekomendowaną formą przechowywania jest portfel zewnętrzny – papierowy lub sprzętowy marki Ledger. Konfiguracja portfela sprzętowego powinna zostać przeprowadzona komisyjnie, przy udziale kierownika jednostki, wyznaczonego administratora portfela oraz – w razie potrzeby – specjalisty. Ustanowiony kod PIN oraz wygenerowany seed należy zapisać na odrębnych kartkach, bez sporządzania kopii,

Tabela 3. Algorytm postępowania przy zabezpieczaniu kryptowalut — schemat decyzyjny.

SYTUACJA FAKTYCZNA	WŁAŚCIWY TRYB POSTĘPOWANIA	KLUCZOWE CZYNNOŚCI I UWAGI PRAKTYCZNE
WŁAŚCICIEL DOBROWOLNIE WYDAJE HASŁA / SEED	Dobrowolne wydanie rzeczy (art. 293 § 6 k.p.k.)	Logowanie do portfela; natychmiastowy transfer na portfel prokuratury; protokół + screenshoty z każdego etapu
KLUCZ PRYWATNY LUB SEED UJAWNIONY PODCZAS PRZESZUKANIA (BRAK DOBROWOLNEGO WYDANIA)	Zatrzymanie rzeczy; logowanie i transfer bez odrębnych czynności egzekucyjnych	Udział specjalisty CBZC obligatoryjny; dokumentacja każdego kroku; transfer bez zbędnej zwłoki
BRAK KLUCZY – PORTFEL ZEWNĘTRZNY, SEED NIEZNANY	Eksperyment procesowy z biegłym lub tymczasowe zajęcie mienia (art. 295 § 1 k.p.k.)	Priorytet szybkości: współsprawcy z seedem mogą wyprowadzić środki; następcze postanowienie zatwierdzające
PORTFEL GIEŁDOWY — POLSKA GIEŁDA	Postanowienie o wydaniu rzeczy doręczone giełdzie (art. 217 § 1 k.p.k.)	Możliwa blokada na podstawie art. 86 ust. 10 ustawy AML; szybka reakcja polskich podmiotów
PORTFEL GIEŁDOWY — GIEŁDA ZAGRANICZNA	Kontakt bezpośredni (LEA e-mail); przy odmowie – MLA lub Europol (J-CAT)	Dobrowolna współpraca = dowód wydany dobrowolnie; brak konieczności MPP; dowody dopuszczalne
STABLECOIN USDT/USDC — PORTFEL ZIDENTYFIKOWANY	Wniosek LEA o freeze do Tether Operations Limited / Circle Internet Financial	Zamrażany jest cały portfel – konieczne uwzględnienie środków osób trzecich; procedura następczego odblokowania

Objaśnienia skrótów: **J-CAT** (ang. *Joint Cybercrime Action Taskforce*) — wspólna inicjatywa operacyjna Europolu skupiająca specjalistów ds. cyberprzestępczości z państw UE oraz krajów partnerskich, powołana do koordynacji działań przeciwko zagrożeniom cybernetycznym o zasięgu transgranicznym; **MPP** (postanowienie o przymusowym przekazaniu) — czynność procesowa zobowiązująca podmiot (np. operatora giełdy kryptowalut) do przymusowego udostępnienia określonych danych lub aktywów na podstawie postanowienia organu procesowego.
Źródło: opracowanie własne na podstawie Wytycznych PK 2023 i k.p.k.

a następnie zdeponować wraz z urządzeniem w Narodowym Banku Polskim jako depozyt wartościowy. Ochrona klucza prywatnego stanowi fundamentalny element bezpieczeństwa zabezpieczonych środków[19, 20, 21].

Co do zasady zaleca się niezwłoczną sprzedaż zabezpieczonych walut cyfrowych na podstawie art. 232 § 1 k.p.k., mając na uwadze niestabilność rynkowej wartości kryptowalut – różnica wartości mienia podlegającego zwrotowi mogłaby stanowić przedmiot roszczeń osoby uprawnionej. Sprzedaży dokonuje organ egzekucyjny – komornik lub naczelnik urzędu skarbowego – nie zaś prokurator[22,23].

Uwaga praktyczna: kryptowaluty prywatności

Monero (XMR), Zcash (ZEC) oraz Dash w trybie PrivateSend oferują zaawansowane mechanizmy prywatności (ring signatures, zk-SNARKs, CoinJoin), które w istotny sposób utrudniają śledzenie przepływów środków. W przypadku spraw z udziałem tych walut należy w trybie priorytetowym zaangażować Europol (J-CAT) oraz rozważyć użycie specjalistycznych narzędzi. Klasyczne heurystyki analityczne mogą okazać się niewystarczające.

WYZWANIA TECHNICZNE I PRAWNE

Problem anonimowości i identyfikacji posiadaczy

Pozorna anonimowość posiadaczy kryptowalut stanowi jedno z kluczowych wyzwań dla organów ścigania. Zakup jednostek waluty cyfrowej przez sprawcę często stanowi element procederu prania brudnych pieniędzy. W praktyce jednak transakcje w sieci Bitcoin są pseudoanonimowe, nie zaś całkowicie anonimowe – każda transakcja jest publicznie widoczna w blockchainie, a zaawansowane narzędzia analityczne umożliwiają identyfikację użytkowników[24].

Zastosowanie heurystyk (uproszczonych metod wnioskowania) w pracy informatyka śledczego umożliwia klasyfikowanie adresów kryptowalutowych i wiązanie ich z konkretnymi podmiotami. Połączenie tych metod z platformami analitycznymi, takimi jak Chainalysis Reactor, CipherTrace lub TRM Labs, pozwala na skuteczne śledzenie przepływów środków w sieciach kryptowalutowych[25].

Problemy jurysdykcyjne i współpraca międzynarodowa

Zdecentralizowany charakter blockchain powoduje istotne trudności w ustaleniu właściwości miejscowej organów ścigania. Transakcje kryptowalutowe mogą obejmować podmioty z różnych krajów, a giełdy kryptowalut często są zarejestrowane w jurysdykcjach oferujących korzystne regulacje prawne.

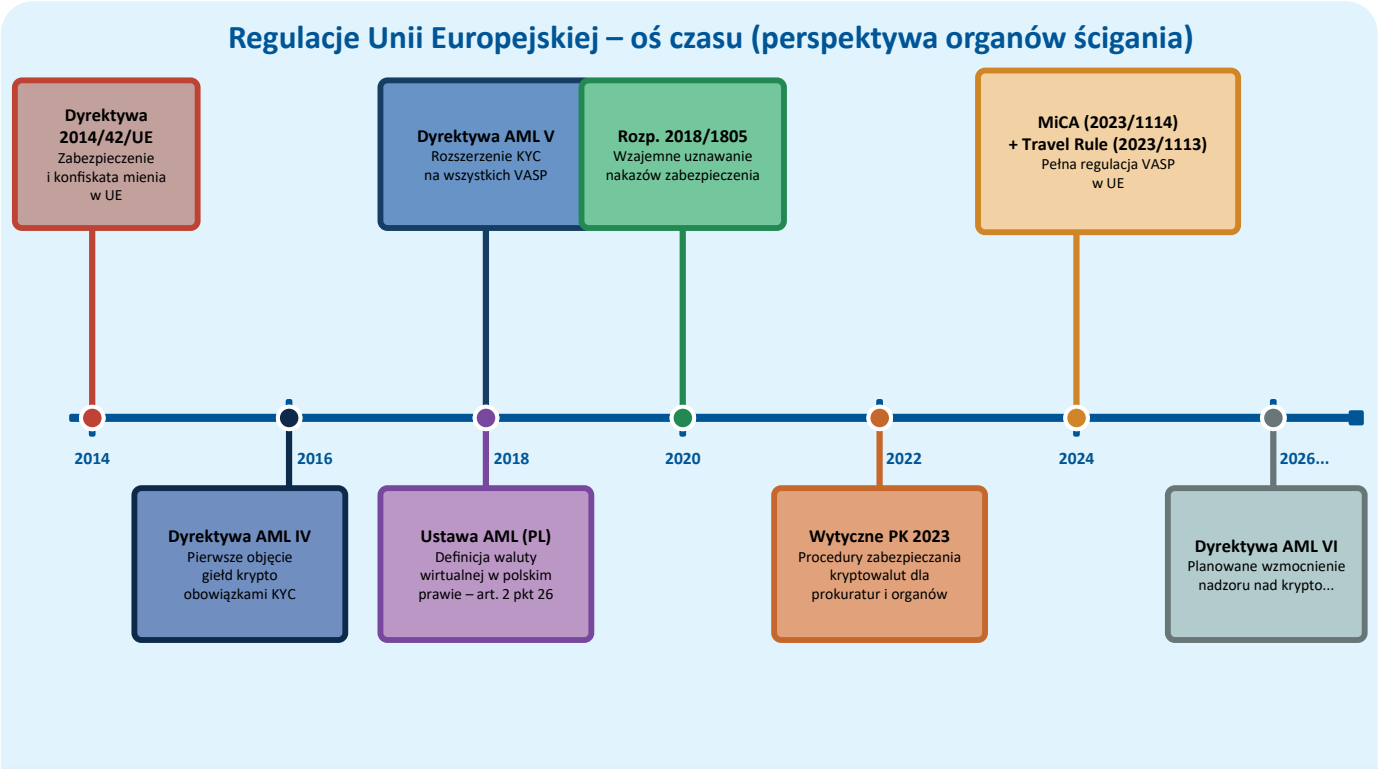
Istotnym przykładem współpracy międzynarodowej jest procedura współpracy z emitentami stablecoinów. Tether Operations Limited, emitent najpopularniejszego stablecoina USDT, dysponuje możliwością zamrożenia portfela zawierającego środki będące przedmiotem postępowania. Należy jednak pamiętać, że Tether zamraża całe portfele, nie zaś poszczególne tokeny[26].

Na poziomie Unii Europejskiej kluczowe znaczenie ma dyrektywa 2014/42/UE w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa, a także

Tabela 4. Kluczowe regulacje Unii Europejskiej – znaczenie dla organów ścigania.

AKT PRAWNY / INSTRUMENT	DATA WEJŚCIA W ŻYCIE	ZNACZENIE DLA ZABEZPIECZANIA KRYPTOWALUT PRZEZ ORGANY ŚCIGANIA
Dyrektywa 2014/42/UE (konfiskata i zabezpieczenie)	2014	Ramy prawne zabezpieczania i konfiskaty mienia w UE; zastosowanie wprost do kryptowalut jako mienia
Dyrektywa AML IV (2015/849) i AML V (2018/843)	2015 / 2018	Objęcie giełd kryptowalut obowiązkami KYC/AML; rejestracja VASP; ułatwienie identyfikacji posiadaczy
Ustawa z 1.03.2018 r. (PL) — implementacja AML IV	2018	Definicja legalna waluty wirtualnej (art. 2 ust. 2 pkt 26); podstawa kwalifikacji prawnej kryptowalut w RP
Rozporządzenie (UE) 2018/1805 (wzajemne uznawanie)	2020	Wzajemne uznawanie nakazów zabezpieczenia i konfiskaty między państwami UE; stosowalne do kryptowalut
Rozporządzenie MiCA — 2023/1114	2024–2025	Regulacja emitentów kryptoaktywów; obowiązek posiadania licencji VASP; wzmocnienie nadzoru i transparentności rynku
Travel Rule — rozporządzenie 2023/1113	2024	Obowiązek przekazywania danych o stronach transakcji powyżej 1000 EUR; kluczowy instrument trace'owania (śledzenia) środków

Objaśnienia skrótów: **KYC** (ang. *Know Your Customer*) – procedura weryfikacji tożsamości klientów, obowiązkowa dla podmiotów świadczących usługi finansowe i kryptowalutowe na mocy przepisów AML; AML (ang. *Anti-Money Laundering*) – przepisy i procedury dotyczące przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu; **VASP** (ang. *Virtual Asset Service Provider*) – dostawca usług w zakresie aktywów wirtualnych; definicja wprowadzona przez FATF (Financial Action Task Force) i transponowana do prawa UE dyrektywami AML IV i V, obejmuje giełdy kryptowalut, portfele powiernicze i inne podmioty świadczące usługi związane z kryptoaktywami; **MiCA** (ang. *Markets in Crypto-Assets Regulation*) – rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów, kompleksowe ramy prawne UE regulujące emisję i obrót kryptoaktywami, w tym obowiązek uzyskania licencji przez dostawców usług w zakresie kryptoaktywów; **dyrektywa AML IV** – dyrektywa 2015/849/UE w sprawie zapobiegania praniu pieniędzy; **dyrektywa AML V** – dyrektywa 2018/843/UE rozszerzająca obowiązki KYC na giełdy kryptowalut i dostawców portfeli; **Travel Rule** – rozporządzenie 2023/1113 nakładające obowiązek przekazywania danych identyfikacyjnych stron transakcji kryptowalutowych powyżej 1000 EUR.
Źródło: opracowanie własne na podstawie aktów prawa UE.



Ryc. 5. Regulacje UE w zakresie kryptowalut – oś czasu z perspektywy organów ścigania. Źródło: opracowanie własne.

rozporządzenie 2023/1113 (Travel Rule), nakładające na dostawców usług kryptoaktywów obowiązek gromadzenia i przekazywania informacji o stronach transakcji[27, 28].

DOBRE PRAKTYKI I REKOMENDACJE

Na podstawie analizy wytycznych Prokuratury Krajowej, literatury specjalistycznej oraz doświadczeń praktycznych sformułowano listę kontrolną dla funkcjonariuszy organów ścigania i prokuratur (tabela 5).

Tabela 5. Lista kontrolna – dobre praktyki przy zabezpieczaniu kryptowalut w postępowaniu karnym.

Lp.	ZALECANA CZYNNOŚĆ / DOBRA PRAKTYKA
1.	Przed czynnością – zapewnij udział specjalisty CBZC lub biegłego z zakresu kryptowalut i blockchain
2.	Przeprowadź profilowanie majątkowe: analiza rachunków bankowych, transakcji z giełdami krypto, OSINT, wywiad operacyjny
3.	Podczas przeszukania – poszukuj: fraz seed (kartek, notatników, zdjęć), portfeli sprzętowych, nośników elektronicznych, arkuszy z kluczami
4.	Sporządź protokół zatrzymania rzeczy z dokładnymi adresami publicznymi i liczbą jednostek na każdym adresie
5.	Dokumentuj każdy etap screenshotami: logowanie do portfela, saldo przed transferem, szczegóły transakcji, saldo po transferze
6.	Wykonaj natychmiastowy transfer na portfel prokuratury – nie zwlekaj (ryzyko wyprowadzenia środków przez współsprawcę dysponującego seedem)
7.	Portfel prokuratury – skonfiguruj komisyjnie; PIN i seed na odrębnych kartkach bez kopii; zdeponuj w NBP jako depozyt wartościowy
8.	Nie upubliczniaj adresu publicznego portfela prokuratury – wyłącznie na potrzeby konkretnych czynności procesowych
9.	Przy odmowie wydania przez giełdę zagraniczną – kieruj żądanie przez Europol (J-CAT) lub w drodze międzynarodowej pomocy prawnej (MLA)
10.	Rozważ niezwłoczną sprzedaż na podstawie art. 232 § 1 k.p.k. (niestabilność wartości rynkowej kryptowalut; ryzyko roszczeń)
11.	Przy USDT/USDC – złóż wniosek LEA o freeze do Tether / Circle; uwzględnij środki osób trzecich w portfelu; zaplanuj procedurę odblokowania
12.	Kryptowaluty prywatności (Monero XMR, Zcash ZEC) – zaangażuj Europol/J-CAT; klasyczne narzędzia analityczne mogą być niewystarczające

Źródło: opracowanie własne na podstawie Wytycznych PK 2023, Metodyki zabezpieczeń majątkowych PK (2018) i doświadczeń praktycznych autora.

Szczególne znaczenie ma udział specjalisty z zakresu informatyki lub kryptowalut przy każdej czynności zabezpieczającej. Brak specjalistycznej wiedzy technicznej może prowadzić do błędów skutkujących nieodwracalną utratą środków – np. przesłaniem kryptowaluty na nieprawidłowy adres. Współpraca z Centralnym Biurem Zwalczania Cyberprzestępczości stanowi w tym zakresie optymalne rozwiązanie[29, 30].

PRZESTĘPCZOŚĆ Z WYKORZYSTANIEM KRYPTOWALUT I PRAKTYKA ORZECZNICZA

Kryptowaluty są wykorzystywane w wielu przestępstwach, wśród których dominują: pranie brudnych pieniędzy, oszustwa inwestycyjne, działalność na rynkach darknetowych oraz wymuszenia z użyciem oprogramowania ransomware. A. Błażowska szczegółowo analizuje penalizację prania i fałszowania kryptowalut na gruncie art. 299 i art. 310 Kodeksu karnego, wskazując na rosnącą skalę tego zjawiska[31, 32].
Polskie orzecznictwo w zakresie kryptowalut jest wciąż stosunkowo skromne, choć systematycznie się rozwija. Kluczowe znaczenie mają rozstrzygnięcia dotyczące kwalifikacji prawnej kryptowalut jako mienia w rozumieniu prawa karnego oraz dopuszczalności ich zabezpieczenia majątkowego. Praktyka prokuratorska, ukształtowana wytycznymi Prokuratury Krajowej, potwierdza możliwość traktowania walut cyfrowych zarówno jako dowodów rzeczowych, jak i przedmiotu zabezpieczenia majątkowego.

> „Sprawy z udziałem kryptowalut wymagają od organów ścigania zdolności do śledzenia środków na poziomie transakcji blockchain, identyfikacji podmiotów powiązanych z adresami portfeli oraz współpracy z dostawcami usług kryptoaktywów. Brak którejkolwiek z tych zdolności praktycznie eliminuje szansę skutecznego zabezpieczenia środków".
>
> A. Błażowska, *Kryptowaluty w polskim prawie karnym*, C.H. Beck, Warszawa 2024, s. 91.

Na arenie międzynarodowej warto odnotować precedensowe działania amerykańskich organów ścigania, które wielokrotnie dokonywały zabezpieczenia kryptowalut o wartości setek milionów dolarów w sprawach związanych z działalnością darknetową i praniem pieniędzy. Doświadczenia te stanowią cenne źródło praktycznej wiedzy dla polskich organów ścigania[33].

PODSUMOWANIE

Zabezpieczanie kryptowalut w postępowaniu karnym stanowi jedno z najbardziej dynamicznie rozwijających się zagadnień na styku prawa karnego procesowego i technologii informatycznych. Przeprowadzona analiza prowadzi do kilku kluczowych wniosków.
Po pierwsze, polski system prawny – pomimo braku przepisów szczególnych dedykowanych walutom cyfrowym – zapewnia odpowiednią podstawę prawną do ich zabezpieczania w toku postępowania karnego. Przepisy k.p.k. dotyczące zatrzymania rzeczy, przeszukania i zabezpieczenia

majątkowego znajdują pełne zastosowanie do kryptowalut, co potwierdziły Wytyczne Prokuratury Krajowej z 2023 r.
Po drugie, kluczowym wyzwaniem pozostaje aspekt techniczny zabezpieczania. Skuteczność czynności zależy od umiejętności pozyskania kluczy prywatnych, seedów lub danych logowania, a także od szybkości działania – zwłoka może prowadzić do nieodwracalnej utraty środków. Nieodzowny jest udział specjalistów z zakresu informatyki śledczej w każdej czynności związanej z zabezpieczaniem walut cyfrowych.
Po trzecie, współpraca międzynarodowa – zarówno na poziomie instytucjonalnym (Europol, Eurojust), jak i bezpośrednim (giełdy, emitenci stablecoinów) – stanowi niezbędny element skutecznego zabezpieczania kryptowalut w sprawach o charakterze transgranicznym. Rozwój unijnych regulacji, w tym rozporządzenia MiCA i Travel Rule, powinien w nadchodzących latach ułatwić współdziałanie organów ścigania państw członkowskich.
Po czwarte, należy podkreślić pilną potrzebę systematycznego szkolenia funkcjonariuszy organów ścigania i prokuratur w zakresie technologii blockchain i kryptowalut. Dynamiczny rozwój tej technologii wymaga stałego aktualizowania kompetencji, a dotychczasowe doświadczenia wskazują, że braki wiedzy technicznej stanowią główną barierę skutecznego zabezpieczania walut cyfrowych w toku postępowań karnych.

[1] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, https://bitcoin.org/bitcoin.pdf [dostęp: 20.01.2025 r.].
[2] P. Rodwald, *Kryptowaluty z perspektywy informatyki śledczej*, Wydawnictwo Akademickie AMW, Gdynia 2021, s. 14–15.
[3] Art. 2 ust. 2 pkt 26 ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2025 r. poz. 644, z późn. zm.), dalej: ustawa AML.
[4] M. Wnęk, *Natura prawna kryptowaluty*, Wydawnictwo C.H. Beck, Warszawa 2023, s. 12–15.
[5] P. Rodwald, *Kryptowaluty z perspektywy informatyki śledczej*, s. 17–18.
[6] S. Bala, T. Kopyściański, W. Srokosz, *Kryptowaluty jako elektroniczne instrumenty płatnicze bez emitenta. Aspekty informatyczne, ekonomiczne i prawne*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2016, s. 52.
[7] P. Rodwald, *Kryptowaluty z perspektywy informatyki śledczej*, s. 36–38.
[8] Tamże, s. 46–60.
[9] A. Błażowska, *Kryptowaluty w polskim prawie karnym*, Wydawnictwo C.H. Beck, Warszawa 2024, s. 43–45.
[10] M. Wnęk, *Natura prawna kryptowaluty*, s. 45–48. Zob. też K. Zacharzewski, *Bitcoin jako przedmiot stosunków prawa prywatnego*, „Monitor Prawniczy" 2014, nr 21, s. 1132–1141.
[11] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2025 r. poz. 46, z późn. zm.), dalej: k.p.k.
[12] Pismo Departamentu do Spraw Cyberprzestępczości i Informatyzacji Prokuratury Krajowej z 2023 r., sygn. 1001-12.024.4.2023, dalej: Wytyczne PK 2023.
[13] Wytyczne PK 2023, s. 2.
[14] Prokuratura Krajowa, *Metodyka zabezpieczeń majątkowych*, Warszawa 2018, s. 290–291.
[15] Art. 217 § 1 k.p.k.
[16] Prokuratura Krajowa, *Metodyka zabezpieczeń majątkowych*, s. 293–296.
[17] Wytyczne PK 2023, s. 8–9.
[18] Art. 86 ust. 10 ustawy AML.
[19] Wytyczne PK 2023, s. 14–16.
[20] Tamże, s. 17–19.
[21] Prokuratura Krajowa, *Metodyka zabezpieczeń majątkowych*, s. 301.
[22] Art. 232 § 1 k.p.k.
[23] Wytyczne PK 2023, s. 12–14.
[24] A. Błażowska, *Kryptowaluty w polskim prawie karnym*, s. 71–93.
[25] P. Rodwald, *Kryptowaluty z perspektywy informatyki śledczej*, s. 11–12.
[26] Informacja uzyskana od Tether Operations Limited w ramach bezpośredniej współpracy z polskimi organami ścigania, 2024.
[27] Dyrektywa Parlamentu Europejskiego i Rady 2014/42/UE z dnia 3 kwietnia 2014 r. w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej (Dz. Urz. UE L 127 z 29.4.2014, s. 39).
[28] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1113 z dnia 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów (Travel Rule) (Dz. Urz. UE L 150 z 9.6.2023, s. 1).
[29] P. Opitek, *Kryptowaluty jako przedmiot zabezpieczenia i poręczenia majątkowego*, „Prokuratura i Prawo" 2017, nr 6, s. 45–62.
[30] Wytyczne PK 2023, s. 17–19.
[31] P. Rodwald, *Kryptowaluty z perspektywy informatyki śledczej*, s. 79–92.
[32] A. Błażowska, *Kryptowaluty w polskim prawie karnym*, s. 84–87. Zob. też art. 299 i art. 310 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2025 r. poz. 383, z późn. zm.).
[33] Prokuratura Krajowa, *Metodyka zabezpieczeń majątkowych*, s. 307–311.

Bibliografia

Literatura

Bala S., Kopyściański T., Srokosz W., K*ryptowaluty jako elektroniczne instrumenty płatnicze bez emitenta. Aspekty informatyczne, ekonomiczne i prawne*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław 2016.
Błażowska A., *Kryptowaluty w polskim prawie karnym*, Wydawnictwo C.H. Beck, Warszawa 2024.
Castronova E., *Synthetic Worlds: The Business and Culture of Online Games*, University of Chicago Press, Chicago 2005.

Kędzierska A., Korus K., *Kryptowaluty. Regulacje prawne i aspekty podatkowe*, Wolters Kluwer, Warszawa 2022.
Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008 [dokument elektroniczny – zob. netografia].
Opitek P., *Kryptowaluty jako przedmiot zabezpieczenia i poręczenia majątkowego*, „Prokuratura i Prawo" 2017, nr 6, s. 45–62.
Rodwald P., *Kryptowaluty z perspektywy informatyki śledczej*, Wydawnictwo Akademickie AMW, Gdynia 2021.
Srokosz W., *Definicja waluty wirtualnej – aspekty prawne*, Wrocławskie Studia Erazmiańskie 2019, t. XIII, s. 229–244.
Wnęk M., *Natura prawna kryptowaluty*, Wydawnictwo C.H. Beck, Warszawa 2023.
Zacharzewski K., *Bitcoin jako przedmiot stosunków prawa prywatnego*, „Monitor Prawniczy" 2014, nr 21, s. 1132–1141.

Akty prawne
Dyrektywa Parlamentu Europejskiego i Rady 2014/42/UE z dnia 3 kwietnia 2014 r. w sprawie zabezpieczenia i konfiskaty narzędzi służących do popełnienia przestępstwa i korzyści pochodzących z przestępstwa w Unii Europejskiej (Dz. Urz. UE L 127 z 29.4.2014, s. 39).
Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu (AML IV) (Dz. Urz. UE L 141 z 5.6.2015, s. 73).
Dyrektywa Parlamentu Europejskiego i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę 2015/849 (AML V) (Dz. Urz. UE L 156 z 19.6.2018, s. 43).
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1805 z dnia 14 listopada 2018 r. w sprawie wzajemnego uznawania nakazów zabezpieczenia i nakazów konfiskaty (Dz. Urz. UE L 303 z 28.11.2018, s. 1).
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1113 z dnia 31 maja 2023 r. w sprawie informacji towarzyszących transferom środków pieniężnych i niektórych kryptoaktywów (Travel Rule) (Dz. Urz. UE L 150 z 9.6.2023, s. 1).
Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów (MiCA) (Dz. Urz. UE L 150 z 9.6.2023, s. 40).
Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2025 r. poz. 383, z późn. zm.).
Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2025 r. poz. 46, z późn. zm.).
Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2025 r. poz. 644, z późn. zm.).

Dokumenty urzędowe i wytyczne
Pismo Departamentu do Spraw Cyberprzestępczości i Informatyzacji Prokuratury Krajowej z 2023 r., sygn. 1001-12.024.4.2023 (Wytyczne PK 2023).
Prokuratura Krajowa, *Metodyka zabezpieczeń majątkowych*, Warszawa 2018.
Wytyczne Departamentu do Spraw Przestępczości Gospodarczej Prokuratury Krajowej z dnia 20 marca 2020 r., sygn. PK VII PG 025.11.2017.
Europol, *Cryptocurrency: Tracing the Evolution of Criminal Finances*, EC3 Report, The Hague 2022.
Financial Action Task Force (FATF), Virtual Assets and Virtual Asset Service Providers – Updated Guidance, FATF, Paris 2021.

Netografia
Nakamoto S., *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, https://bitcoin.org/bitcoin.pdf [dostęp: 20.01.2025 r.].
Chainalysis Inc., *The 2024 Crypto Crime Report*, https://www.chainalysis.com/blog/crypto-crime-report-2024/ [dostęp: 20.01.2025 r.].
Europol, *IOCTA 2023 – Internet Organised Crime Threat Assessment*, https://www.europol.europa.eu/publications-events/main-reports/iocta-report [dostęp: 20.01.2025 r.].
Tether Operations Limited, *Law Enforcement Guide*, https://tether.to/en/transparency/#reports [dostęp: 20.01.2025 r.].
Prokuratura Krajowa, *Informacje dla organów ścigania*, https://pk.gov.pl [dostęp: 20.01.2025 r.].
CBZC – Centralne Biuro Zwalczania Cyberprzestępczości, *Informacja o działalności*, https://www.policja.pl/pol/cbzc [dostęp: 20.01.2025 r.].

Słowa kluczowe: kryptowaluty, blockchain, zabezpieczenie majątkowe, postępowanie karne, dowód rzeczowy, informatyka śledcza, klucz prywatny, Prokuratura Krajowa, CBZC, VASP.

Summary

Securing Cryptocurrencies in Criminal Proceedings. Procedural, Technical and Practical Aspects

The article presents a comprehensive analysis of the issues related to securing cryptocurrencies in Polish criminal proceedings. The technological foundations of digital currencies are discussed, including blockchain technology, cryptographic key mechanisms and types of wallets. The legal basis for securing cryptocurrencies, procedures applied by law enforcement agencies, and the 2023 guidelines of the National Public Prosecutor's Office are presented. Particular attention is paid to the technical and legal challenges associated with the pseudo-anonymity of transactions, jurisdictional problems, and the storage of secured digital assets. Recommendations of best practices for law enforcement officers and prosecution services are formulated.

Keywords: cryptocurrencies, blockchain, asset freezing, criminal proceedings, physical evidence, digital forensics, private key, National Prosecutor's Office, CBZC, VASP.

Tłumaczenie: Autor

KRYPTOWALUTY NA BIURKU

Jak czytać cyfrowe ślady i nie zgubić tropu?

Michał Królik

Akademia Informatyki Śledczej Mediarecovery

Zdj. Mediarecovery

Michał Królik – Crypto Product Area Manager w Mediarecovery – były funkcjonariusz Zarządu w Krakowie Centralnego Biura Zwalczania Cyberprzestępczości. Posiada międzynarodowe certyfikaty (m.in. TRM, Chainalysis, Europol, FBI), a w swojej karierze przeszkolił setki funkcjonariuszy i prokuratorów. Ponadto jest współtwórcą procedur zabezpieczania kryptowalut w Polsce i Europolu. Od 2017 r. kształtuje krajową praktykę analizy *blockchain* i wspiera rozwój kompetencji śledczych. Jest odpowiedzialny za rozwój portfolio produktów do analizy *blockchain* i śledzenia transakcji kryptowalutowych oraz usługi i prowadzenie szkoleń z serii *Kryptowaluty i analiza blockchain* w ramach Akademii Informatyki Śledczej Mediarecovery.

Autor artykułu w przejrzysty sposób przedstawia specyfikę czynności operacyjnych i procesowych, które należy wykonać w sprawach dotyczących przestępstw związanych z wykorzystywaniem kryptowalut. Podkreśla rolę analizy przepływów i zwraca uwagę na zabezpieczanie właściwych śladów w tego typu sprawach. Wskazuje na najczęstsze błędy popełniane przez funkcjonariuszy oraz wyjaśnia ich znaczenie dla prowadzonych postępowań.

Zwykłe przeszukanie i wirtualny sejf: zderzenie z nową rzeczywistością

Szósta rano. Wejście na adres. Klasyczna realizacja u figuranta. Przewracacie mieszkanie do góry nogami. Szukacie gotówki ukrytej w szafkach, rachunków bankowych, wartościowych przedmiotów. I nic. Pusto. Zabezpieczacie telefony i laptopy, technik wpisuje je do protokołu, a wy powoli zbieracie się do wyjścia.

Tymczasem na biurku, tuż obok kluczyków do samochodu, leży niewielkie urządzenie przypominające pendrive, a pod nim zwykła kartka z zapisanymi 24 angielskimi słowami. Dla osoby niewtajemniczonej to bezwartościowe przedmioty. Mijacie je obojętnie.

W rzeczywistości ten „pendrive” (czyli portfel sprzętowy) oraz kartka (tzw. *seed phrase*, czyli fraza odzyskiwania) to klucz do cyfrowego sejfu, w którym sprawca może

przechowywać równowartość setek tysięcy, a czasem milionów złotych. Zostawiając je na miejscu, przechodzicie obok jednego z najważniejszych dowodów w sprawie i majątku, który mógłby zostać zabezpieczony na poczet roszczeń pokrzywdzonych.
Jeszcze kilka lat temu takie znaleziska można było potraktować jako ciekawostkę. Dziś kryptowaluty stały się narzędziem wykorzystywanym w bardzo przyziemnych przestępstwach, od oszustw inwestycyjnych, przez obrót środkami odurzającymi, aż po pranie pieniędzy. Zrozumienie, na co patrzymy w trakcie przeszukania czy analizy materiału dowodowego, przestało być wyborem. Stało się rzemieślniczym obowiązkiem.

Mit pełnej anonimowości. Czym (operacyjnie) jest *blockchain*?

W wielu sprawach, które trafiają na nasze biurka, widać jedno: sprawcy traktują kryptowaluty jak cyfrową, w pełni anonimową gotówkę, niemożliwą do prześledzenia. Co istotne, często my sami również tak o nich myślimy. Gdy w materiałach pojawia się informacja, że środki trafiły na giełdę kryptowalut, łatwo uznać, że dalsze ustalenia będą niemożliwe.
To jeden z najczęstszych błędów na początku postępowania. W praktyce jest dokładnie odwrotnie.
Żeby skutecznie prowadzić tego typu sprawy, warto na chwilę odciąć się od technicznego żargonu. Nie trzeba rozumieć szczegółów kryptografii ani procesu „kopania". Z operacyjnego punktu widzenia blockchain to po prostu publiczny rejestr transakcji, swoista księga rachunkowa dostępna dla każdego.

> Różnica w stosunku do systemu bankowego jest zasadnicza. Przelew bankowy widzi wyłącznie bank, a dostęp do tych danych uzyskujemy dopiero po przeprowadzeniu odpowiednich czynności procesowych. Przelew w *blockchainie* jest widoczny publicznie 24 godziny na dobę, bez konieczności uzyskiwania zgód czy kierowania wniosków. Każda operacja pozostaje tam zapisana w sposób trwały.

Gdzie jest zatem ograniczenie? W tym rejestrze nie ma danych osobowych. Zamiast nazwisk i numerów PESEL widzimy jedynie adresy, czyli ciągi znaków przypisane do portfeli.

> Dlatego podstawowa zasada analizy kryptowalut brzmi: blockchain pokazuje przepływy, nie pokazuje osób.
> Z tego punktu widzenia nie jest to dziedzina zarezerwowana wyłącznie dla specjalistów IT. To w dużej mierze klasyczna praca operacyjna przeniesiona do środowiska cyfrowego: mamy ślad, który należy zabezpieczyć i powiązać z konkretną osobą.

Co faktycznie widać w analizie i… dlaczego nie zawsze ktoś zrobi to za nas?

Kiedy już wiemy, że *blockchain* to jawny rejestr, pojawia się naturalne pytanie: co tak naprawdę w nim widzimy? Nie ma tu efektownych wizualizacji rodem z filmów. Analiza *on-chain* to w praktyce żmudne łączenie kropek.
Widzimy ciągi znaków, czyli adresy (odpowiedniki kont), transakcje (przelewy), powiązania między nimi oraz powtarzalne wzorce zachowań. Możemy prześledzić, jak środki wyłudzone na „pewną inwestycję" trafiają na portfel sprawcy, są dzielone na mniejsze części, przechodzą przez kolejne adresy, a następnie trafiają na konto dużej giełdy kryptowalutowej. I tu pojawia się kluczowy element, jakim jest giełda. To nasz pierwszy realny punkt zaczepienia.
Zanim jednak do tego dojdziemy, warto zwrócić uwagę na pewien schemat myślowy. Gdy w sprawie pojawia się wątek kryptowalut, często pojawia się pokusa, aby przekazać ją w całości do wyspecjalizowanych jednostek.
W rzeczywistości zajmują się one najbardziej złożonymi sprawami, dotyczącymi zorganizowanych grup, zaawansowanej infrastruktury czy działań o dużej skali. Natomiast wiele podstawowych czynności, takich jak zabezpieczenie danych czy wstępne prześledzenie przepływu środków, może zostać wykonanych na poziomie jednostki prowadzącej postępowanie.
To właśnie ten etap często decyduje o powodzeniu dalszych działań. Zabezpieczenie cyfrowego śladu i jego wstępna analiza stają się dziś elementem podstawowego warsztatu.

Gdzie kończy się analiza *on-chain*, czyli operacyjne złoto

Wróćmy do naszego przykładu. Środki po kilku transferach trafiają na giełdę kryptowalutową. Co dzieje się dalej?
W tym miejscu dochodzimy do kluczowego momentu. Zgodnie z zasadą, że *blockchain* pokazuje przepływy, a nie osoby, ślad w publicznym rejestrze kończy się w momencie wejścia środków na scentralizowaną platformę.
Z punktu widzenia analizy *on-chain* oznacza to przerwę. Dalsze operacje nie są już widoczne w *blockchainie*, lecz zapisywane w wewnętrznych systemach giełdy.
I co ważne, to dobra wiadomość.
W tym miejscu kończy się analiza techniczna, a zaczynają się klasyczne czynności procesowe. Większe platformy kryptowalutowe oraz operatorzy usług podlegają regulacjom związanym z przeciwdziałaniem praniu pieniędzy i stosują procedury identyfikacji użytkowników.
Dla prowadzącego sprawę oznacza to możliwość uzyskania konkretnych danych: od informacji identyfikacyjnych, przez historię logowań, po szczegóły aktywności na koncie. W praktyce często pozwala to powiązać adres z konkretną osobą.
Od tego momentu ciężar działań przenosi się na znane obszary: analizę danych, pracę operacyjną, ustalenia osobowe i czynności terenowe. Kluczową rolę zaczyna odgrywać biały wywiad (OSINT – *Open Source Intelligence*). Aktywność w mediach społecznościo-

wych, powiązania z adresami e-mail, wpisy na forach czy ślady pozostawione w innych usługach często pozwalają powiązać adres kryptowalutowy z konkretną osobą lub środowiskiem. W praktyce dopiero połączenie analizy *on-chain* z działaniami poza *blockchainem* obejmującymi m.in. OSINT, dane pozyskane od podmiotów rynku kryptowalutowego oraz klasyczne czynności procesowe i operacyjne, umożliwia pełne odtworzenie przebiegu zdarzeń i identyfikację sprawcy.

Najczęstsze błędy w sprawach z wykorzystaniem kryptowalut

Przejdźmy do praktyki. Gdzie najczęściej popełniane są błędy już na początku postępowania? Z doświadczenia wynika, że powtarzają się trzy podstawowe schematy.

PO PIERWSZE: ZAŁOŻENIE, ŻE „JEDEN ADRES = JEDNA OSOBA".

Często myślimy schematem bankowym: skoro dana osoba ma jedno konto, to w świecie kryptowalut również korzysta z jednego adresu. W rzeczywistości jest inaczej. Nowoczesne portfele automatycznie generują nowe adresy dla kolejnych transakcji.

Błędne powiązanie kilku adresów tylko dlatego, że „wydają się podobne", może prowadzić do połączenia zupełnie niezwiązanych ze sobą wątków i skierowania postępowania na niewłaściwe tory.

PO DRUGIE: NIEUWAGA PODCZAS PRZESZUKANIA.

Wracając do sytuacji ze wstępu, w trakcie realizacji skupiamy się na gotówce, sprzęcie elektronicznym i oczywistych dowodach. Tymczasem kluczowe znaczenie mogą mieć rzeczy niepozorne: kartka z zapisanymi słowami lub niewielkie urządzenie przypominające pendrive.

Fraza odzyskiwania (tzw. *seed phrase*), najczęściej składająca się z 12 lub 24 słów, nie jest zwykłym hasłem. To w praktyce klucz do środków zgromadzonych w portfelu.

Zabezpieczenie samego urządzenia lub komputera nie gwarantuje dostępu do tych środków ani ich ochrony. Jeżeli sprawca posiada kopię frazy lub zapamiętał ją, może odzyskać dostęp do środków na dowolnym urządzeniu.

Dlatego w sprawach związanych z kryptowalutami kluczowe jest nie tylko zabezpieczenie sprzętu, ale również odnalezienie i zabezpieczenie frazy odzyskiwania.

PO TRZECIE: CZAS REAKCJI.

W odróżnieniu od systemu bankowego kryptowaluty funkcjonują bez przerw. Transakcje realizowane są przez całą dobę, niezależnie od dnia tygodnia.

Oznacza to, że środki mogą zostać przeniesione wielokrotnie w bardzo krótkim czasie. Zwłoka w podjęciu działań znacząco zmniejsza szanse na ich prześledzenie lub zabezpieczenie.

Co zabezpieczyć już na etapie zawiadomienia

W wielu sprawach kluczowe informacje znajdują się już po stronie pokrzywdzonego. Problem polega na tym, że często nie są one właściwie zabezpieczane na samym początku postępowania.

Z punktu widzenia analizy kryptowalut szczególne znaczenie mają:

- adres portfela, na który zostały przesłane środki,
- identyfikator transakcji (tzw. TXID),
- data i kwota transferu,
- nazwy wykorzystanych platform (giełd, kantorów),
- korespondencja ze sprawcą (np. komunikatory, e-mail),
- zrzuty ekranu z przebiegu „inwestycji".

Już na podstawie tych danych możliwe jest wstępne prześledzenie przepływu środków i określenie dalszego kierunku czynności.
Brak tych informacji lub ich niepełne zabezpieczenie na początku znacząco utrudnia dalszą analizę, a w niektórych przypadkach może uniemożliwić odtworzenie pełnego przebiegu zdarzeń.
Należy również zwrócić szczególną uwagę na poprawność zapisywanych danych. Adresy portfeli oraz identyfikatory transakcji (TXID) są ciągami znaków, w których nawet pojedyncza literówka lub pominięcie znaku może uniemożliwić ich odnalezienie w systemie. W praktyce oznacza to konieczność ponownego zbierania danych, a w niektórych przypadkach utratę możliwości odtworzenia pełnego przebiegu transferu środków.

Jak działają sprawcy, czyli mechanika z lotu ptaka

Kryptowaluty pojawiają się w różnych rodzajach przestępstw, od obrotu środkami odurzającymi po rozliczenia za nielegalne towary. Obecnie jednak najczęściej wykorzystywane są w oszustwach związanych z fałszywymi inwestycjami.
Sprawcy wykorzystują wizerunki znanych firm, instytucji publicznych lub osób rozpoznawalnych, często posługując się materiałami generowanymi przy użyciu sztucznej

inteligencji. Pokrzywdzony, przekonany o wiarygodności „inwestycji", sam kupuje kryptowaluty na legalnej platformie, a następnie przekazuje je na wskazany adres.
Z perspektywy sprawcy jest to rozwiązanie bardzo wygodne, ponieważ środki omijają tradycyjny system bankowy. Jednocześnie sprawca zdaje sobie sprawę, że przepływy w *blockchainie* są publiczne, dlatego podejmuje działania mające na celu ich ukrycie.

W tym celu wykorzystywane są m.in.:

- giełdy działające bez weryfikacji tożsamości,
- usługi mieszające środki (tzw. miksery),
- przenoszenie środków pomiędzy różnymi sieciami (*chain-hopping*).

Celem tych działań jest utrudnienie prześledzenia przepływu i zerwanie ciągłości analizy.
Końcowy etap często odbywa się już w świecie fizycznym. Środki trafiają do systemów umożliwiających ich wypłatę w gotówce, np. poprzez wpłatomaty kryptowalutowe. Wypłaty dokonują podstawione osoby, co dodatkowo utrudnia identyfikację sprawcy.
To właśnie na tych etapach, przy błędach popełnianych przez sprawców lub w punktach styku ze światem rzeczywistym, pojawia się największa szansa na skuteczne działania.

Dlaczego to nie jest proste

Skoro *blockchain* jest publiczny, a wiemy już, czego szukać na miejscu zdarzenia, pojawia się naturalne pytanie: dlaczego nie da się po prostu uruchomić ogólnodostępnego narzędzia i prześledzić przepływu środków?
Odpowiedź jest prosta: przestępcy również się uczą, a technologia rozwija się bardzo dynamicznie.
Nie operujemy już wyłącznie na jednej sieci, takiej jak Bitcoin. W praktyce mamy do czynienia z wieloma różnymi *blockchainami* (np. Ethereum czy Tron), które działają w odmienny sposób. Różnią się także modele zapisu transakcji, od modelu UTXO w Bitcoinie po model kont stosowany w innych sieciach.
W efekcie analiza szybko przestaje być intuicyjna. Próba śledzenia przepływów wyłącznie przy użyciu podstawowych narzędzi może być czasochłonna i obarczona ryzykiem błędnej interpretacji.

Kluczowym elementem są tzw. heurystyki, czyli reguły analityczne pozwalające na łączenie adresów i identyfikację wzorców działania. Bez ich znajomości łatwo o błędne wnioski, które mogą prowadzić do utraty czasu i skierowania postępowania na niewłaściwe tory.
Dlatego analiza kryptowalut nie polega na „zgadywaniu", lecz na uporządkowanym łączeniu danych. W praktyce wymaga to zarówno odpowiedniego przygotowania, jak i dostępu do specjalistycznych narzędzi analitycznych.

Zakończenie: nowa rzeczywistość

Kryptowaluty przestały być zjawiskiem niszowym. Stały się stałym elementem przestępczości gospodarczej i kryminalnej, z którym funkcjonariusze spotykają się coraz częściej.
Widać to również po zmianach w strukturach, od 1 marca 2026 r. we wszystkich komendach wojewódzkich Policji funkcjonują wydziały do walki z przestępczością cyfrową, których zakres obejmuje m.in. analizę informacji dostępnych w sieci (OSINT), zwalczanie oszustw internetowych oraz wsparcie lokalnych jednostek w sprawach technicznych. Zagadnienia związane z kryptowalutami stanowią już integralny element tego obszaru działań, obejmujący w szczególności zabezpieczenie materiału dowodowego, analizę przepływów oraz ich wstępną interpretację, a także transfer zabezpieczonych środków.
To wyraźny sygnał, że nie jest to już wiedza specjalistyczna zarezerwowana dla wąskiej grupy, lecz kompetencja, która staje się elementem codziennej pracy.
Jednocześnie w bardziej złożonych sprawach niezbędne pozostaje wsparcie wyspecjalizowanych jednostek. W praktyce oznacza to uzupełniający się model działania: od wstępnej analizy po zaawansowane działania operacyjne.
Doświadczenie pokazuje jednak, że wiele spraw, w szczególności dotyczących oszustw inwestycyjnych, można skutecznie ukierunkować już na etapie podstawowych czynności, pod warunkiem właściwego zabezpieczenia śladów i ich wstępnej analizy.
Środowisko pracy zmienia się dynamicznie, a wraz z nim rosną wymagania wobec funkcjonariuszy. Zrozumienie specyfiki kryptowalut oraz umiejętność właściwego zabezpieczenia cyfrowych śladów stają się dziś elementem podstawowego warsztatu.
Im szybciej zostanie to uwzględnione w codziennej praktyce, tym większe będą szanse na skuteczne prowadzenie postępowań i realne odzyskiwanie środków na rzecz pokrzywdzonych.

Summary

Cryptocurrencies. How to read digital footprints and avoid losing trail?

The author of this article presents the specific operational and procedural steps that must be taken in cases involving crimes related to the use of cryptocurrencies. The article highlights the role of flow analysis and draws attention to securing appropriate traces in such cases. The article also points out the most common mistakes made by officers and explains their importance for the proceedings conducted.

Tłumaczenie: Beata Pepłowska

Deanonimizacja sprawców cyberprzestępstw metodami OSINT

od <nicku> do wyroku

Zdj. Mediarecovery

Norbert Ptak

Ekspert ds. OSINT, Mediarecovery

W artykule omówiono zastosowanie nowoczesnych technik pozyskiwania i analizy informacji z powszechnie dostępnych źródeł internetowych jako narzędzia, które – łączone z tradycyjnymi metodami operacyjnymi i procesowymi – stanowi obecnie jeden z kluczowych elementów w walce z przestępczością, cyberprzestępczością i przestępstwami motywowanymi nienawiścią.

Wprowadzenie: od anonimowości do odpowiedzialności

Wielu sprawcom przestępstw w cyberprzestrzeni wydaje się, że nick, avatar bez twarzy i jednorazowy adres e-mail wystarczą, by zostać nieuchwytnym dla organów ścigania. Tymczasem nowoczesne techniki OSINT (*Open-Source Intelligence*), czyli wywiadu jawnoźródłowego, pozwalają krok po kroku przekuć pseudonim w imię, nazwisko i numer akt w prokuraturze. OSINT rozumiany jako systematyczne pozyskiwanie i analiza informacji z powszechnie dostępnych źródeł, takich jak media tradycyjne, dane administracji publicznej, publikacje profesjonalne i akademickie, dane z otwartych rejestrów handlowych czy finalnie Internetu – pod pojęciem WEBINT (*Web Intelligence*) – stał się dziś jednym z kluczowych narzędzi w śledztwach i nie ogranicza się tylko do cyberprzestępczości.

Nick jako punkt wyjścia – WEBINT

Media społecznościowe, fora, komunikatory, wycieki baz danych czy aktywność w Darknecie – wszystkie te elementy tworzą cyfrowy ślad, który przy odpowiedniej metodyce można skorelować i przypisać konkretnej osobie lub wykorzystać do uzyskania szerszego spojrzenia na śledztwo. W wielu sprawach pierwszym i jedynym punktem zaczepienia jest pseudonim używany na jednym z portali, w grze online, na forum czy w komunikatorze – dokładnie z takim scenariuszem na co dzień pracują policyjni analitycy, śledczy i prokuratorzy. Nick jest wartościowym selektorem, ponieważ użytkownicy mają tendencję do powtarzania raz wymyślonej nazwy na różnych platformach.

Zanim do gry wejdą zaawansowane narzędzia, wykonywana jest zwykle prosta analiza treści samego pseudonimu: czy zawiera imię, rok urodzenia, nazwę miasta albo inne wskazówki, które zawężają grupę potencjalnie podejrzanych osób. Kolejny krok to próba wyszukania kont należących do tej samej osoby w portalach i aplikacjach innych niż nasze pierwotne źródło.

Korelacja kont w mediach społecznościowych

To, co kiedyś wymagało żmudnej ręcznej pracy, dziś w dużej mierze wspiera automatyka i wyspecjalizowane narzędzia SOCMINT (*Social Media Intelligence*), ale kluczowe pozostaje analityczne spojrzenie człowieka.

Z jednego nicku prowadzi się ścieżkę do profilu na przykład na TikToku, Facebooku, forum dyskusyjnym czy niszowym komunikatorze – każde z tych miejsc może ujawniać inne informacje: zdjęcia, lokalizacje, listę znajomych, deklarowane miejsce pracy czy zainteresowania.

Analiza profili obejmuje między innymi treści postów, styl wypowiedzi, częstotliwość publikacji, geolokalizację zdjęć i relacji, a także powiązania społeczne – wspólne fotografie, komentarze, oznaczenia osób czy przynależność do konkretnych grup. Na tej podstawie może zostać zbudowany graf powiązań, który pozwala zidentyfikować osoby z bliskiego otoczenia sprawcy oraz zweryfikować hipotezy co do jego tożsamości i miejsca przebywania.

Fora, Darknet i komunikatory

Dla sprawców poważniejszych przestępstw naturalnym środowiskiem są zamknięte fora, serwisy w Darknecie i komunikatory, takie jak: Telegram, Signal czy Discord, które często oferują niższy poziom moderacji i większą swobodę działania. Także tam OSINT ma zastosowanie – analitycy, monitorując wybrane słowa kluczowe, nazwy kanałów, ogłoszenia sprzedaży czy oferty, mogą powiązać ujawnione nicki, adresy e-mail, numery telefonów z innymi aktywnościami w sieci.

W praktyce prowadzi to na przykład od pseudonimu sprzedawcy z darknetowego forum, przez jego konto na komunikatorze, aż po profil w serwisie programistycznym czy mediach społecznościowych, gdzie pojawia się to samo zdjęcie, charakterystyczny podpis albo e-mail.
Korelacja tych danych z informacjami z rejestrów publicznych czy danych abonenta pozyskiwanych przez służby w trybie procesowym pozwala już przejść z poziomu hipotezy OSINT do twardego dowodu łączącego konkretnego człowieka z określoną aktywnością w sieci.

Mowa nienawiści i nawoływanie do przemocy – dlaczego OSINT jest kluczowy

Razem ze stałym wzrostem liczby aktywnych użytkowników rośnie liczba przypadków szerzenia mowy nienawiści w sieci, a skrajne treści publikowane online mogą przekładać się na realne incydenty przemocy – od przestępstw z nienawiści po ataki motywowane ideologicznie.
Monitoring treści w mediach społecznościowych pokazuje, że największy udział w rozpowszechnianiu mowy nienawiści mają duże platformy – takie jak X (dawny Twitter) czy Facebook – ale nie można lekceważyć mniejszych serwisów, grup na komunikatorach ani lokalnych forów.
Deanonimizacja sprawców gróźb karalnych, uporczywego nękania, stalkingu czy nawoływania do przemocy wymaga nie tylko zabezpieczenia materiału dowodowego (screenshoty, logi, metadane), lecz także odtworzenia chronologii zdarzeń, eskalacji treści oraz struktury sieci, która sprzyjała rozprzestrzenianiu się nienawistnych komunikatów. Tak odtworzona historia aktywności w sieci bywa kluczowa przy kwalifikacji prawnej czynu i ocenie, czy mamy do czynienia z jednorazowym incydentem, czy z długotrwałą, zorganizowaną kampanią ataków na ofiarę lub określoną grupę społeczną.

Etapy współpracy służb z zespołem OSINT Mediarecovery

W pracy polskich organów ścigania coraz częściej pojawia się moment, w którym prowadzący sprawę prokurator lub policjant dysponuje jedynie fragmentarycznymi danymi – nickiem, adresem email, linkiem do kanału w komunikatorze – i potrzebuje specjalistycznego wsparcia w ich analizie. W takim przypadku z pomocą przychodzą wyspecjalizowane zespoły, takie jak Laboratorium Informatyki Śledczej i zespół OSINT Mediarecovery, które oferują ustandaryzowany proces realizacji usługi dla służb – od przyjęcia zgłoszenia po przygotowanie ekspertyzy dowodowej.
Typowy proces można opisać w czterech krokach.

1. **Zgłoszenie** – funkcjonariusz lub prokurator przekazuje posiadane informacje dotyczące celu i kontekstu sprawy oraz określa oczekiwany rezultat analizy, np. identyfikacja sprawcy, odtworzenie chronologii zdarzeń, ustalenie powiązań z innymi osobami.
2. **Weryfikacja możliwości** – eksperci Mediarecovery oceniają, jakie działania OSINT są możliwe w danej sprawie, w jakim horyzoncie czasowym oraz w jakiej formie można dostarczyć wyniki; na tym etapie doprecyzowywany jest zakres ekspertyzy.
3. **Analiza** – zespół przeprowadza właściwe działania: wykorzystuje najnowsze technologie i wiedzę ekspertów, aby wydobyć informacje z najgłębszych warstw sieci Internet i Darknet.
4. **Ekspertyza** – przygotowywany jest dokument zawierający opis przeprowadzonych czynności, pozyskane dane wraz z informacją o ich źródle, wyniki analizy, a także wnioski.

Ekspertyza może być następnie wykorzystana zarówno na etapie działań operacyjnych, jak i w postępowaniu sądowym.

Dyskretnie, ale profesjonalnie – rola Mediarecovery w śledztwach cyber

Mediarecovery od kilkunastu lat wspiera polskie służby w sprawach dotyczących cyberprzestępczości, oszustw internetowych, handlu ludźmi, zniknięć osób, a także przestępstw motywowanych nienawiścią – zarówno poprzez analizy OSINT, jak i usługi z zakresu informatyki śledczej oraz analizy transakcji kryptowalutowych.
Dzięki połączeniu kompetencji z obszaru białego wywiadu, analizy danych mobilnych i komputerowych oraz śledzenia przepływów kryptowalut możliwe jest zbudowanie pełnego obrazu sprawy. Dla służb oznacza to realne oszczędności czasu i zasobów: dobrze zaplanowana współpraca z zespołem OSINT redukuje liczbę fałszywych tropów i pozwala skupić się na najbardziej perspektywicznych wątkach.

Granice OSINT i znaczenie korelacji z innymi źródłami

Warto podkreślić, że sam OSINT rzadko daje stuprocentowe potwierdzenie tożsamości – najczęściej mówimy o hipotezach o wysokim prawdopodobieństwie, które wymagają weryfikacji poprzez dane niejawne, takie jak bilingi, dane abonenta czy logi operatorów telekomunikacyjnych i dostawców usług internetowych. Dlatego w dojrzałym podejściu śledczym OSINT traktowany jest jako element większej układanki, łączony z tradycyjnymi metodami operacyjnymi i procesowymi, a nie jako zamiennik klasycznego dochodzenia.
Z drugiej strony, dobrze przeprowadzona analiza OSINT może znacząco zawęzić krąg podejrzanych, wskazać nowe wątki, obalić alibi lub ujawnić powiązania między pozornie niezależnymi incydentami (np. seriami ataków phishingowych czy kampaniami mowy nienawiści prowadzonymi z różnych kont).
Tak rozumiany OSINT jest dziś jednym z kluczowych elementów w walce z przestępczością, cyberprzestępczością i przestępstwami motywowanymi nienawiścią – od pierwszego, pozornie anonimowego postu, aż po wyrok skazujący, oparty na solidnym, skorelowanym materiale dowodowym.

Summary

From nickname to verdict: de-anonymization cybercrime criminals using OSINT methods

The article presents the use of modern techniques for obtaining and analyzing information from widely available Internet sources. The Internet is a tool that, combined with traditional operational and procedural methods, is currently one of the key elements in the fight against crime, cybercrime, and hate crimes.

Tłumaczenie: Beata Pepłowska

JAKIE CYBERZAGROŻENIA CZYHAJĄ

na polskich użytkowników urządzeń mobilnych?

Łukasz Cepok

Incident Response Manager w Mediarecovery

Zdjęcia: Mediarecovery.

Łukasz Cepok – od początku ścieżki zawodowej związany z IT w organizacjach z sektora finansowego: od młodszego administratora IT i kierownika zespołu IT, przez analityka L1, do eksperta Incident Response. Od kilku lat zaangażowany w role Cyber Threat Intelligence. Uważa, że te dwa procesy nie mogą istnieć oddzielnie i muszą się wzajemnie uzupełniać. Analityk złośliwego oprogramowania na urządzenia mobilne. Lubi dzielić się wiedzą w rolach wykładowcy lub prelegenta. W życiu prywatnym również angażuje się w rozwiązywanie incydentów jako strażak ochotnik.

Polska przestrzeń cyfrowa nie jest bezpieczną przystanią, to front ciągłej walki o dane i pieniądze użytkowników. Na cyberzagrożenia narażone są także urządzenia mobilne – smartfony, które nosimy w kieszeniach i często uważamy je za bezpieczniejsze od komputerów. Wiele osób jest o tym przekonanych, ponieważ ataki na urządzenia mobilne nie są tak spektakularne i nie przebijają się do mediów głównego nurtu. A prawda jest zgoła inna.

Urządzenia mobilne już dawno zastąpiły nam komputery w większości czynności codziennych. Wykorzystujemy je do wielu aktywności: realizujemy przez nie zakupy, płacimy rachunki, obsługujemy pocztę elektroniczną oraz korespondencję z urzędami, wykorzystujemy do komunikacji z innymi użytkownikami. Okazuje się zatem, że telefony, zwane również smartfonami, czy szerzej – urządzenia mobilne – w obecnych czasach służą za banki informacji o nas, przechowujemy na nich informacje, dokumenty, zdjęcia i inne treści cyfrowe. Tymi wszystkimi danymi zainteresowane są różne grupy przestępcze, każda z nich będzie chciała wykorzystać je na swój sposób, ale cel jest jeden: monetyzacja ataku, czyli przestępcom atak musi się po prostu opłacać.

Co istotne z punktu widzenia cyberbezpieczeństwa, zagrożenia znane z komputerów można praktycznie w pełni odwzorować na urządzeniach mobilnych, a więc istnieją np. phishing, złośliwe oprogramowanie, oszustwa itp.

Warto zatem dowiedzieć się, jakie cyberzagrożenia czyhają na użytkowników. I tak, na przykład w ramach złośliwego oprogramowania możemy zetknąć się z nw. klasami zagrożeń.

Spyware/stealer

Oprogramowanie, które ma za zadanie wykradać informacje użytkownika i o użytkowniku, które następnie będą wykorzystywane w dalszych etapach ataków lub odsprzedawane innym grupom wyspecjalizowanym w konkretnych atakach i zainteresowanych tego typu danymi.

Adware

Jest oprogramowaniem, którego głównym celem jest monetyzowanie oszustw na sieciach reklamowych. Z pozoru niewinne aplikacje serwują użytkownikowi setki niewidocznych reklam, co powoduje zużycie zasobów baterii, sieć reklamowa odbiera informację o tym, że użytkownik zobaczył reklamy i wypłaca autorowi aplikacji prowizje i nagrody za wygenerowane obejrzenia.

Ransomware

To zagrożenie kojarzy nam się jednoznacznie z atakami na komputery i sieci firmowe. Jednak przestępcy od dawna już eksperymentują z tego typu oprogramowaniem w atakach na telefony. Co prawda nie jest ono jeszcze w pełni skuteczne, co wynika bezpośrednio z architektury systemów operacyjnych urządzeń mobilnych, ale to kwestia czasu, aż zostanie odpowiednio rozwinięte.

WebAPK

Technologia do instalowania plików do aplikacji internetowych wykorzystywana do przeprowadzania ataków phishingowych lub legendowania oszustw, zagrożenie to zostało odkryte w lipcu 2023 r. przez CSIRT KNF.

NFC Relay

Początkowo uznany za atak możliwy tylko w warunkach laboratoryjnych, pokazuje, że przestępcy potrafią zaadaptować skomplikowane mechanizmy sieci płatniczych do monetyzowania ataków.

Ostatnim wartym nadmienienia zagrożeniem są **trojany** – można je podzielić na kilka grup: bankowe, RAT i te najbardziej zaawansowane jak oprogramowanie klasy Pegasus.
To właśnie trojany bankowe były w Polsce wykorzystywane przez przestępców od 2017 r. i były najpopularniejszym zagrożeniem aż do 2022 r.
Warto zauważyć, że obecnie zagrożenia mobilne działają w modelu MaaS (*Malware as a Service*), czyli oprogramowanie do wynajęcia w modelu subskrypcji miesięcznej. Mamy tu zatem tak naprawdę dwie grupy przestępcze: developerów, którzy tworzą takie oprogramowanie, i operatorów, którzy je wynajmują. Ceny takiego oprogramowania na forach przestępczych wahają się od 1000 do 5000 $. Więc tak naprawdę udany atak na jedną lub dwie ofiary spłaca miesięczną inwestycję. Analizy kampanii wykazywały ponadto, że wśród operatorów znajdowały się osoby, których natywnym językiem był język polski, co sugeruje, że były to rodzime grupy przestępcze. Polska ze swoją wysoką adaptacją nowych technologii jako środków płatności, ale również ze społeczeństwem, które bardzo szybko przystosowuje się do rozwiązań fintechowych i jest coraz bardziej „smart", stanowi swego rodzaju poligon doświadczalny dla przestępców.
Można tutaj przytoczyć przykład, kiedy specjaliści od cyberbezpieczeństwa obserwowali ogłoszenia promujące nową rodzinę złośliwego oprogramowania i jeszcze tego samego lub następnego dnia kampania wykorzystująca tego trojana była dystrybuowana do polskich użytkowników. Schemat całego ataku był dosyć prosty, a w dodatku powtarzalny i mimo wysiłków zespołów bezpieczeństwa, czy to po stronie banków, czy CSIRT-ów poziomu krajowego i sektorowego włożonych w ostrzeganie użytkowników, zbierał on bardzo wysokie żniwo.
Jak to wyglądało? Zaczynało się od standardowego SMS-a z treścią dotyczącą codziennych spraw: *Twoja paczka nie mogła zostać dostarczona, uzupełnij adres dostawy w nowej aplikacji* (*link do nowej aplikacji*). Ale były również bardziej bezczelne, takie jak kampanie w czasie pandemii koronawirusa, kiedy promowano aplikację do sprawdzenia, czy jest się zakażonym, przez to, że było trzeba zakaszleć do mikrofonu urządzenia mobilnego. Następnie użytkownik pobierał „nową aplikację" i wtedy pojawiał się „problem w działaniu". Taki komunikat legendował żądania oprogramowania dotyczące wysokich uprawnień, które rzekomo były potrzebne do prawidłowego działania. Kluczowe dla pełnej realizacji tego ataku było jedno uprawnienie – **ułatwienie dostępu** (ang. *Accessibility Access*). To uprawnienie w telefonach z Androidem ma służyć do ułatwiania obsługi urządzenia osobom z dysfunkcjami. Przestępcy zauważyli, że można to uprawnienie wykorzystać do tego, by system/aplikacja same klikały po ekranie urządzenia (mechanizm miał ułatwić sterowanie urządzeniem osobom np. niewidomym). Dzięki temu mogli nadawać sobie wyższe uprawnienia i dostęp do kolejnych elementów systemu.
Kolejnym etapem ataku było poczekanie, aż użytkownik zaloguje się do bankowości elektronicznej, czasem starano się to przyśpieszyć poprzez wysłanie powiadomienia o treści, która powodowała, że użytkownik logował się

do aplikacji w celu zweryfikowania operacji na koncie (np. uznanie 10 000 zł na konto lub podobny, „kuszący" komunikat). Użytkownik, chcąc to zweryfikować, uruchamiał aplikację bankowości mobilnej. W tym momencie trojan przystępował do właściwego etapu ataku. W ułamku sekundy nad ekranem prawidłowej aplikacji bankowości rysowała się tzw. nakładka (nazywana również *overlay* lub *inject*), było to okienko imitujące ekran logowania do aplikacji bankowej. Użytkownik, działając w emocjach, nawet nie zauważał, że nagle system prosi o pełny login/hasło, a dotychczas był to zawsze PIN, odcisk palca czy inny mechanizm biometrii lub uwierzytelniania. Zmanipulowana ofiara wpisywała zatem swoje pełne poświadczenia. Te automatycznie były wysyłane do atakujących i od razu wykorzystywane w systemach bankowych do realizacji transakcji. Na telefon ofiary przychodził co prawda SMS z kodem lub powiadomienie informujące o nowym logowaniu i kod, który miał potwierdzić, że użytkownik świadomie autoryzuje transakcje. W tym momencie działał jednak już kolejny komponent złośliwego oprogramowania pozwalający przejąć atakującym pełną kontrolę nad wiadomościami i powiadomieniami. Powodowało to, że mimo iż powiadomienie dotarło do urządzenia ofiary, nie wyświetlało się ono użytkownikowi, a SMS-y z banku oznaczane były jako odczytane i przesłane do atakujących.

Co więcej, zależnie od użytej rodziny złośliwego oprogramowania przestępcy byli w stanie utrudnić korzystanie użytkownikowi z telefonu podczas kolejnych faz ataku. Polegało to np. na permanentnym blokowaniu i wygaszaniu ekranu urządzenia, co uniemożliwiało korzystanie z niego. W tym czasie atakujący wyprowadzali środki z konta ofiary do wysokości limitów dziennych lub wyżej, wcześniej modyfikując takie limity. Niejednokrotnie zdarzało się, że atakujący wykorzystywali również uproszczone wnioskowanie o produkty kredytowe w aplikacji i składali wniosek o dodatkowe środki. Bywały przypadki, gdy ofiary były nieświadome ataku przez kilkanaście dni. W końcu okazywało się, że nie są w stanie przeprowadzić operacji z wykorzystaniem karty bankowej i dopiero wtedy, po zalogowaniu do banku, uświadamiali sobie, że przez kilkanaście dni ktoś drenował ich środki finansowe.

Atakujący przeważnie przelewali środki na konta innych ofiar, robiąc z nich tzw. muły finansowe. Z kont tych osób środki były przelewane dalej na giełdy kryptowalutowe lub były wykorzystywane do płacenia za zakupy w sklepach internetowych z elektroniką, czasem w połączeniu z oszustwami, które nazywają się refundami. Polegało to na tym, że później były robione zwroty zakupionych rzeczy lub ich podróbek, co pozwalało odzyskać część zapłaconych pieniędzy za sprzęt. W ten sposób atak był monetyzowany więcej niż jeden raz.

Analiza kodu źródłowego takich aplikacji pozwala na wskazanie pełnych możliwości trojanów bankowych. Wykazała ona, że na celowniku przestępców były nie tylko aplikacje bankowe, ale również użytkowe, np. aplikacje zakupowe, pocztowe, obsługujące programy partnerskie. Powód jest prozaiczny, większość użytkowników wykorzystuje ten sam login, hasło do wielu aplikacji i systemów. Uzyskanie przez atakujących dostępu do mało znaczącej aplikacji mogło im dać znacznie więcej niż celowanie od razu w aplikację bankową.

Można sobie np. wyobrazić sytuację, kiedy atakujący przejąłby dostęp do poczty elektronicznej ofiary. W dzisiejszych czasach dostęp do poczty elektronicznej to jak dostęp do tożsamości cyfrowej. Są tam zapisane informacje nie tylko prywatne, ale również o tym, gdzie dane konto zostało wykorzystane do rejestracji. Znając takie informacje, atakujący może zażądać zmiany hasła i link do zmiany przyjdzie właśnie na tę skrzynkę, do której ma on dostęp. Było to wykorzystywane w scenariuszach z wyłudzeniami kodów BLIK na platformach społecznościowych.

Jakie zatem działania mogą podjąć osoby odpowiedzialne za cyberbezpieczeństwo?

Po pierwsze koniecznie należy zwrócić uwagę, że kluczowe w zachowaniu dowodów do analizy ataku jest nieusuwanie SMS-ów, aplikacji, nieresetowanie urządzenia do stanu fabrycznego. Takie działanie usunie co prawda zagrożenie z urządzenia, ale jednocześnie uniemożliwi analizę. Jednocześnie należy pamiętać o tym, że podjęcie powyższych kroków nie odbierze jednak dostępów do kont, do których atakujący uzyskali już dostęp.

Dokładna analiza kodu źródłowego przeprowadzana przez zespoły bezpieczeństwa lub laboratoria informatyki śledczej wraz z zestawieniem z logami z zainfekowanego urządzenia pozwala w pełni odbudować łańcuch zdarzeń w ataku. Dodatkowo właśnie analiza kodu wskaże pełne funkcjonalności złośliwego oprogramowania i pozwoli na wskazanie ofierze, do czego atakujący miał jeszcze dostęp.

Należy zauważyć, że ilość złośliwego oprogramowania znacząco zmalała w 2022 r., to dlatego że grupy, które zajmowały się jego tworzeniem, były pochodzenia rosyjsko-ukraińskiego i doszło do rozłamów pomiędzy nimi ze względu na toczącą się wojnę, a dodatkowo osoby te zostały zaangażowane w działania w ramach konfliktu zbrojnego.

Nie oznacza to jednak, że zagrożenie całkowicie zniknęło. Obecnie wytwarzanie złośliwego oprogramowania zostało przejęte przez grupy pochodzenia tureckiego i nadal się pojawia, a nowe rodzaje oprogramowania nadal są testowane w Polsce, przeciwko polskim użytkownikom.

Summary

What cyber threats are facing Polish mobile devices users?

The author of this article notes that mobile devices have long since replaced computers in most everyday activities and that a lot of information is stored on them. However, smartphone users are not always aware that various criminal groups are interested in all this data. The goal for criminals is, of course, financial benefit. This article presents the types and methods of operation of cybercriminals, and also provides concise information on how to protect yourself against these types of threats.

Tłumaczenie: Beata Pepłowska

PATOSTREAMING

jako zjawisko kryminogenne

Fot. 1.

Grafika wygenerowana z wykorzystaniem licencjonowanego programu Adobe Firefly.

asp. szt. Arkadiusz Paciorek

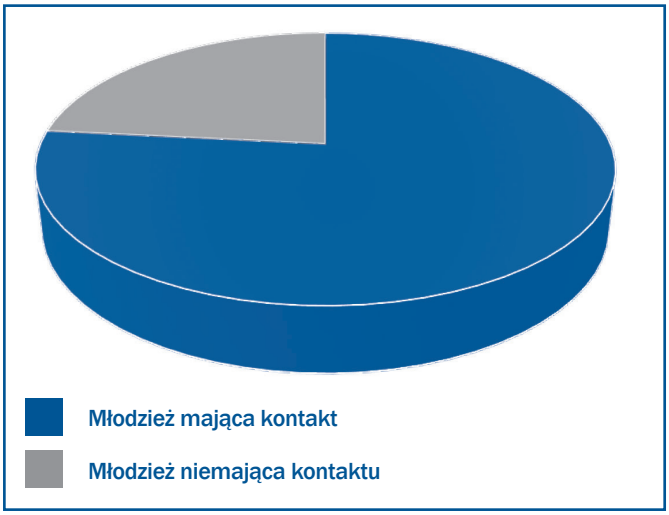
Zakład Techniki Operacyjnej CSP

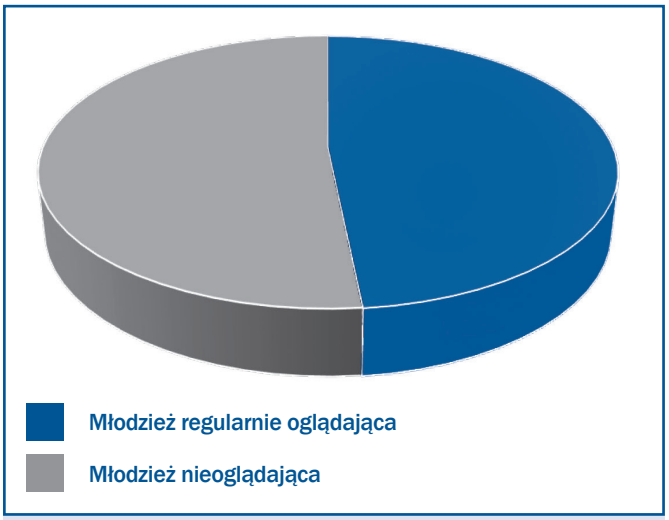
W niniejszym artykule zdefiniowano termin patostreamingu oraz zjawiska z tym związane. Celem artykułu jest uświadomienie jak największej liczby odbiorców skali zjawiska, a przede wszystkim na temat bardzo negatywnego wpływu treści płynących z patostreamingu na najmłodszą część naszego społeczeństwa. Jest to obecnie na tyle poważny problem, że ustawodawca rozważał nowelizację Kodeksu karnego w celu uwzględnienia tej patologii społecznej jako osobnego typu przestępstwa. Jest to ściśle związane z prezentowaniem treści o charakterze przemocowym, w szczególności dla małoletnich. W pierwszej części artykułu wskazano prace dotyczące penalizacji tego zjawiska, a następnie omówiono projekt zmiany ustawy – Kodeks karny oraz opinię wnioskodawców w przedmiotowej sprawie. Zaprezentowano również najbardziej jaskrawe przykłady patostreamingu. Nowelizacja została uchwalona w Sejmie i czeka na akceptację w Senacie oraz podpis prezydenta.

Samo słowo streaming wiąże się z pewnego rodzaju usługą internetową, która polega na transmitowaniu plików audio lub audiowizualnych bez konieczności ich pobierania. Na tej samej zasadzie działają radio i telewizje internetowe, takie jak Netflix czy HBO GO. Wśród odbiorców popularnego od 2005 r. YouTube'a dużym zainteresowaniem cieszą się transmisje streamingowe graczy komputerowych umożliwiające obserwowanie gry, a także jej komentowanie. Takie transmisje stały się inspiracją dla rozwoju wielu youtuberów. To z kolei zainicjowało trend polegający na pokazaniu swojego życia codziennego innym internautom przez osoby określane jako streamerzy. Część z nich nadawała transmisje zawierające zachowania naruszające normy społeczne i prawne, m.in. pokazujące libacje alkoholowe, zażywanie narkotyków, przemoc, zmuszanie, wulgarne treści, po to, by osiągać jak największą oglądalność i by obserwujący to w internecie dokonywali wpłat na rzecz nadawców. Tak powstało zjawisko zwane patostreamingiem[1].

„Patostreaming to słowo zapożyczone z języka angielskiego, *patological* oznaczające patologiczny oraz *stream*, które można zdefiniować jako strumień danych lub relacja na żywo. Tak więc patostreaming to internetowa transmisja w czasie rzeczywistym treści o charakterze wulgarnym, obscenicznym i przemocowym. Tego typu nagrania cieszą się dużą popularnością wśród internautów, w szczególności przedstawicieli młodego pokolenia"[2].

Patostreamerzy często nagrywają swoje libacje alkoholowe, wulgarne zachowania bądź odzywki, a nawet bójki po to, aby w zamian otrzymywać tzw. „donate", czyli wpłaty pieniężne dokonywane przez widzów[3]. Patostreamy podobne są do reality show lub seriali, ale bez reżysera, których twórcy w czasie swoich występów są bardzo często nietrzeźwi, palą marihuanę, upijają się na wizji, posługują się językiem pełnym przemocy i wulgaryzmów. Transmitują rozmowy z innymi użytkownikami sieci, komentują prywatne sprawy, opowiadają o przeszłości i planach na przyszłość. Podkreślenia wymaga występowanie zjawiska ich wzajemnej rywalizacji, która często przybiera postać bójek, w których niekiedy zwolennicy na hasło swojego lidera potrafią wypisywać nienawistne komentarze pod adresem rywali.
Jednym ze skrajnych przykładów takich zachowań jest sprawa patostreamera o pseudonimie „Kamerzysta", czyli Łukasza W., skazanego w 2022 r. na 6 miesięcy ograniczenia wolności, 30 godzin prac społecznych oraz grzywnę za uderzenie starszego mężczyzny w wieku 66 lat zupełnie bez powodu, tylko dla „podbicia" oglądalności. „Kamerzysta" zaczął nagrywać jeden ze swoich streamów w jednym ze szczecińskich sklepów. Kiedy ekspedientki wyraziły sprzeciw, zaczął się awanturować. Podczas sprzeczki, do której doszło w sklepie, Łukasz W. uderzył jednego z klientów robiących zakupy (który stanął w obronie ekspedientek)[4]. Niestety to nie jedyny wybryk „Kamerzysty". W kwietniu 2021 r. w internecie pojawił się film, w którym patostreamer wraz z innymi osobami zmuszali niepełnosprawnego intelektualnie do takich czynności, jak tarzanie się w błocie, jedzenie odchodów kota czy rozbijanie głową cegieł. Sprawa ta została zgłoszona przez opiekunkę niepełnosprawnej osoby oraz przez media, w wyniku czego YouTube usunął konto Łukasza W. oraz jego materiał. Ponadto „Kamerzysta" i pozostałe osoby biorące udział w znęcaniu się nad osobą niepełnosprawną usłyszeli zarzuty znęcania się nad osobą nieporadną (art. 207 § 1a Kodeksu karnego)[5].
Raport Państwowego Instytutu Badawczego Naukowej i Akademickiej Sieci Komputerowej NASK wskazuje, że 56,6% dorosłych i 76,6% polskiej młodzieży zna zjawisko patostreamingu, natomiast 29,4% dorosłych i 48,4% nastolatków ma regularny kontakt z tymi treściami. Fundacja Daje Dzieciom Siłę wskazuje, że największą grupę odbiorców patostreamingu stanowią nastolatkowie. 84% grupy wiekowej 13–15 lat zna zjawisko patostreamingu i aż 37% je ogląda[6].
Wykresy przedstawiają w sposób graficzny dane dotyczące młodzieży mającej kontakt z treściami patostreamingu i młodzieży regularnie oglądającej takie treści. Jak widać, zatrważająca liczba młodych osób poruszających się w świecie cyfrowym natrafia na takie treści, ale zjawiskiem jeszcze bardziej alarmującym jest liczba młodych ludzi, którzy fascynują się takimi treściami i regularnie je oglądają. Patostreaming nie jest prawnie zabroniony. Twórca takiego streamu może ponieść konsekwencje prawne dopiero wtedy, gdy transmitowany jest czyn zabroniony. Niestety, szukanie takich przestępców jest utrudnione ze względu na fakt, że jest to transmisja live, więc treści te (jeśli nikt ich nie zapisze) zaraz po emisji znikają.





Wykres 1. Młodzież mająca kontakt ze zjawiskiem patostreamingu. Źródło: opracowanie własne.

Eksperci zgodnie twierdzą, że zjawisko patostreamingu prowadzi do naruszenia praw i wolności jednostek, zwłaszcza prawa do ochrony godności człowieka oraz ochrony życia prywatnego. Poprzez nawoływanie do nienawiści narusza dobra osobiste, ale również zagraża dobrom ogólnospołecznym. Według licznej grupy znawców patostreaming wypełnia znamiona wielu przestępstw: art 216 Kodeksu karnego – przestępstwo znieważenia, art. 212 Kodeksu karnego – zniesławienie, art. 217 Kodeksu karnego – naruszenie nietykalności cielesnej czy chociażby art. 288 Kodeksu karnego – zniszczenie cudzej rzeczy. Wypełnia także znamiona wykroczeń, jak chociażby art. 52a Kodeksu wykroczeń – publiczne pochwalanie popełnienia przestępstwa, art. 141 Kodeksu wykroczeń – dopuszczanie się nieobyczajnego wybryku, zamieszczanie w miejscu publicznym nieprzyzwoitego ogłoszenia, napisu lub rysunku albo używanie słów nieprzyzwoitych[7]. To tylko przykłady, których jest znacznie więcej, co skłania do refleksji, czy jest to tylko subkultura czy może jednak zjawisko patologiczne zasługujące na wyodrębnienie w Kodeksie karnym.
Mając na uwadze charakter kryminogenny opisywanej patologii społecznej, Sejm Rzeczypospolitej IX kadencji zaproponował zmianę ustawy – Kodeks karny. Druk sejmo-

wy 3310 z dnia 24 maja 2023 r. zasugerował dodanie do Kodeksu karnego art. 255b uwzględniającego patostreaming jako przestępstwo[8]. Niecały miesiąc później, a dokładnie 14 czerwca 2023 r., pojawiło się pismo z Biura Analiz Sejmowych Kancelarii Sejmu oceniające skutki prawne poselskiego projektu ustawy. W projekcie tym zdefiniowano patostreaming jako udostępnianie treści przedstawiających dokonywanie czynów zabronionych, ale także pozorowanie przedstawiające czyn jako już popełniony. Poprzez udostępnianie należy rozumieć transmisję dźwięku lub obrazu albo udostępnianie za pośrednictwem sieci teleinformatycznej. Sankcje karne dotyczące zjawiska patostreamingu określone w pkt 5 Oceny skutków prawnych poselskiego projektu ustawy o zmianie ustawy – Kodeks karny (druk 3310) zakładają w typie podstawowym karę pozbawienia wolności od 6 miesięcy do 8 lat, natomiast w typie kwalifikowanym od 10 lat. Zgodnie z pkt 6 rozpowszechnianie treści przedstawiających pozorowane popełnienie czynu będzie cechować się niższym stopniem szkodliwości społecznej, w związku z czym ustawodawca zakłada ten czyn jako typ uprzywilejowany w stosunku do typu podstawowego[9].

Według projektu przestępstwo patostreamingu zostało podzielone na trzy główne kategorie: patologiczną – czyli umyślne przestępstwa określone w pkt 1, zwierzęcą – czyli szeroko rozumiane przestępstwa znęcania się nad zwierzętami i ich zabijanie, oraz przemocową – rozumianą jako przestępstwa cielesne prowadzące do poniżenia lub upokorzenia innej osoby. Grupa przemocowa związana jest ściśle z rosnącą liczbą materiałów związanych z poniżaniem i przemocą, natomiast grupa zwierzęca wynika bardziej z historycznego rysu przypadków patostreamingu.

Ponadto w § 4 proponowanej zmiany w projekcie uwzględniono wyłączenie z odpowiedzialności karnej grupy osób, które nie są pomocnikami do czynu zabronionego ani podżegaczami, działających w celu obrony interesu publicznego lub celu zasługującego na uwzględnienie interesu prywatnego[10].

Fot. 2. Zjawisko patostreamingu. Zdj. A. Paciorek.

Niestety, od czerwca 2023 r. prace w tym kierunku zostały zaniechane. Dopiero 23 czerwca 2025 r. do sejmu wpłynęła „Interpelacja nr 10457 do ministra sprawiedliwości w sprawie zjawiska patostreamingu i skuteczności działań organów państwa w jego zwalczaniu”[11]. Z treści tej interpelacji jasno wynika, że w ostatnich latach zjawisko patostreamingu stało się poważnym problemem prowadzącym do nagminnego łamania prawa poprzez prezentowanie przemocy, wulgarność czy demoralizujące zachowania. Zwrócono uwagę, że: „pomimo licznych apeli środowisk obywatelskich, rodziców, nauczycieli i ekspertów patostreaming wciąż jest dostępny na wielu popularnych platformach internetowych. Treści tego typu są często konsumowane przez osoby niepełnoletnie, co ma istotny negatywny wpływ na rozwój psychiczny i społeczny”[12].

Należy zaznaczyć, iż zignorowanie patostreamingu będzie miało swoje konsekwencje w wielu aspektach życia społecznego, a przede wszystkim w odniesieniu do kondycji psychicznej najmłodszej części naszego społeczeństwa. Jest to ogromne zagrożenie dla dzieci i młodzieży. W okresie dorastania bardzo ważne jest kształtowanie cech charakteru opartych na takich wartościach, jak: sprawiedliwość, szacunek, odpowiedzialność, empatia, tolerancja. Niestety, przez zjawiska patologiczne obecne w dzisiejszym świecie jest to trudne zadanie. Poprzez łatwy dostęp do Internetu młodzież jest narażona na kontakt z patostreamingiem. Fakt, że nasze pociechy są odbiorcami treści, które ewidentnie nie powinny do nich trafiać, sprawia, że niezwykle ważna wydaje się potrzeba regulacji prawnych w tym zakresie.

Aby skutecznie chronić młodzież przed patotreściami oraz zapewnić możliwość kształtowania wartości zgodnych z normami społecznymi i kulturowymi, należy uznać patostreaming za zjawisko kryminogenne. Oczywiście istnieje wiele innych równie groźnych subkultur czy zjawisk, natomiast patostreaming jest w Polsce najbardziej popularny. Bardzo niepokojąca jest skala tego zjawiska. Kontakt z tymi niebezpiecznymi zachowaniami mają dziś nie tylko młodzi ludzie wychowujący się w środowiskach patologicznych, lecz także wszyscy mający dostęp do YouTube’a. Według Alberta Bandury: „ludzie uczą się zachowań agresywnych, tak jak wszystkich innych sposobów postępowania – za pośrednictwem mechanizmów warunkowania oraz modelowania postaw. W pierwszym etapie jednostka rozszerza swój repertuar zachowań poprzez zapoznanie się z nieznanym dotychczas wzorcem – podkultura pełni rolę ich dostarczyciela. Następnie dochodzi do wyzwolenia i utrwalenia przez nią własnych zachowań agresywnych. W kontekście patostreamingu warte są podkreślenia przede wszystkim trzy kwestie: opłacalności zachowań agresywnych, kształtowania postaw widzów oraz zobojętnienia publiczności na przejawy przemocy”[13].

Zjawisko patostreamingu to bardzo niebezpieczny i niedostatecznie kontrolowany obszar internetu. Badania wyraźnie pokazują, że młodzież w bardzo dużym stopniu jest stale narażona na tego typu treści, a przerażające jest, jak duża część naszego społeczeństwa w młodzieńczym wieku ogląda je regularnie. Patostreaming normalizuje wulgaryzmy i patologię, ale również wpływa w znacznym stopniu

na powstawanie zaburzeń emocjonalnych oraz zniekształcenie postrzegania rzeczywistości. Zjawisko to jest na tyle niepokojące, że wymaga zdecydowanej reakcji zarówno ze strony rodziców i opiekunów, jak i instytucji publicznych, platform internetowych oraz szkół.

W ostatnim czasie walka z patostreamingiem przeniosła się realnie na grunt prawny. Wyczekiwany przełom nastąpił 11 czerwca 2026 r., kiedy Sejm prawie jednogłośnie uchwalił historyczną nowelizację Kodeksu karnego. Nowe przepisy kryminalizują publiczne rozpowszechnianie materiałów, które ukazują popełnianie przestępstwa, znęcanie się nad zwierzętami czy też skrajnie poniżające traktowanie drugiego człowieka. Karygodność czynu zachodzi również w sytuacji, gdy ofiara formalnie wyraziła na to zgodę. Ustawodawca położył nacisk na motyw finansowy. Twórcy, którzy z tego typu transmisji uczynili sobie źródło dochodu w postaci dobrowolnych wpłat od widzów, muszą liczyć się teraz z sankcjami karnymi. Za tego typu czyny grozi im od 3 miesięcy do 5 lat pozbawienia wolności. Odpowiedzialności nie unikną również osoby, które inscenizują tego typu patologiczne zachowania. Znowelizowana ustawa oczekuje obecnie na procedowanie w Senacie i podpis prezydenta. Jej wejście w życie wyposaży organy ścigania w konkretne narzędzia do szybkiej i bezwzględnej eliminacji patologicznych i niewłaściwych zachowań w przestrzeni cyfrowej[14].

[1] A. Stenzel, *Patostreaming*, „Gazeta Policyjna" 2026, nr 5, https://gazeta.policja.pl/997/aktualne-wydanie/277789,Patostreaming.html [dostęp: 7.06.2026 r.].

[2] A. Kmieciak-Goławska, *Patostreaming jako narzędzie popularyzacji podkultury przemocy*, „Biuletyn Polskiego Towarzystwa Kryminologicznego im. profesora Stanisława Batawii" 2019, nr 25, s. 171, https://czasopisma.inp.pan.pl/plugins/generic/pdfJsViewer/pdf.js/web/viewer.html?file=https%3A%2F%2Fczasopisma.inp.pan.pl%2Findex.php%2Fbk%2Fissue%2Fdownload%2F168%2F135 [dostęp: 28.05.2026 r.].

[3] Tamże, s. 172.

[4] Rzeczpospolita, *Patoyoutuber „Kamerzysta" usłyszał wyrok za pobicie seniora*, https://www.rp.pl/prawo-karne/art37199241-patoyoutuber-kamerzysta-uslyszal-wyrok-za-pobicie-seniora?utm_source=chatgpt.com [dostęp:13.07.2025 r.].

[5] W. Kazanecki, *„Kamerzysta" przed sądem. Proces patoyoutubera ruszył na nowo*, https://wydarzenia.interia.pl/kraj/news-kamerzysta-przed-sadem-proces-patoyoutubera-ruszyl-na-nowo,nId,6402839 [dostęp:13.07.2025 r.].

[6] K. Sobczak, *Patostreaming wciąż czeka na kary, jak za pornografię*, https://www.prawo.pl/prawnicy-sady/penalizacja-patostreamingu-a-kary-za-pornografie,530882.html [dostęp:10.07.2025 r.].

[7] Tamże.

[8] Poselski projekt ustawy o zmianie ustawy – Kodeks karny z dnia 23.05.2023 r., Druk Nr 3310.

[9] *Ocena skutków prawnych poselskiego projektu ustawy o zmianie ustawy – Kodeks karny*, Warszawa, 14 czerwca 2023 r., s. 2.

[10] Tamże, s. 3–4.

[11] Interpelacja nr 10457 do ministra sprawiedliwości w sprawie zjawiska patostreamingu i skuteczności działań organów państwa w jego zwalczaniu, https://sejm.gov.pl/Sejm10.nsf/InterpelacjaTresc.xsp?key=DHYB7B [dostęp:16.06.2026 r.].

[12] Tamże.

[13] A. Kmieciak-Goławska, *Patostreaming jako narzędzie popularyzacji podkultury przemoc*, s. 175.

[14] Sejm RP, *Zakaz patostreamingu oraz wybór sędziego TK. Podsumowanie 59. posiedzenia Sejmu*, https://www.sejm.gov.pl/Sejm10.nsf/komunikat.xsp?documentId=D8E1BD5CE3FF9BB-1C1258E1400336181 [dostęp:16.06.2026 r.].

Bibiliografia

Bek D., Popiołek M., *Patostreaming – charakterystyka i prawne konteksty zjawiska*, „Zarządzanie Mediami" 2019, t. 7, nr 4.

Interpelacja nr 10457 do ministra sprawiedliwości w sprawie zjawiska patostreamingu i skuteczności działań organów państwa w jego zwalczaniu, https://sejm.gov.pl/Sejm10.nsf/InterpelacjaTresc.xsp?key=DHYB7B.

Kazanecki W., *„Kamerzysta" przed sądem. Proces patoyoutubera ruszył na nowo*, https://wydarzenia.interia.pl/kraj/news-kamerzysta-przed-sadem-proces-patoyoutubera-ruszyl-na-nowo,nId,6402839.

Kmieciak-Goławska A., *Patostreaming jako narzędzie popularyzacji podkultury przemocy*, „Biuletyn Polskiego Towarzystwa Kryminologicznego im. profesora Stanisława Batawii" 2019, nr 25, https://czasopisma.inp.pan.pl/plugins/generic/pdfJsViewer/pdf.js/web/viewer.html?file=https%3A%2F%2Fczasopisma.inp.pan.pl%2Findex.php%2Fbk%2Fissue%2Fdownload%2F168%2F135.

Ocena skutków prawnych poselskiego projektu ustawy o zmianie ustawy – Kodeks karny, Warszawa, 14 czerwca 2023 r.

Poselski projekt ustawy o zmianie ustawy – Kodeks karny z dnia 23.05.2023 r., Druk Nr 3310.

Rosiak Ł., *Patostreaming – istota projektowanego art. 255b kodeksu karnego*, „Prokuratura i Prawo" 2024, nr 3.

Rzeczpospolita, *Patoyoutuber „Kamerzysta" usłyszał wyrok za pobicie seniora*, https://www.rp.pl/prawo-karne/art37199241-patoyoutuber-kamerzysta-uslyszal-wyrok-za-pobicie-seniora?utm_source=chatgpt.com.

Sobczak K., *Patostreaming wciąż czeka na kary, jak za pornografię*, https://www.prawo.pl/prawnicy-sady/penalizacja-patostreamingu-a-kary-za-pornografie,530882.html.

Stenzel A., *Patostreaming*, „Gazeta Policyjna" 2026, nr 5, https://gazeta.policja.pl/997/aktualne-wydanie/277789,Patostreaming.html.

Summary

Trash streaming as a criminogenic phenomenon

This article defines the term trash streaming and the phenomenon related to it. The aim of this article is to raise awareness among as many people as possible about the scale of this phenomenon, and above all, the very negative impact of trash streaming on the youngest segment of the society. Trash streaming is currently such a serious problem that the Lawmaker is considering amending the Penal Code in order to include this social deviance as a separate type of crime. Trash streaming is closely related to the presentation of violent content, especially for minors.

The article describes the work on penalizing this phenomenon, the draft amendment to the Penal Code and cites the opinion of the applicants on the matter. The most striking examples of trash streaming were also presented.

Tłumaczenie: Beata Pepłowska

NOWOCZESNE NARZĘDZIA, REALNE WSPARCIE

Jak powstają systemy sztucznej inteligencji dla Policji

mł. insp. Adam Bogucki
kom. Kamil Jurczyk
nadkom. Sławomir Sobolewski
Justyna Biegańska

Wydział Ochrony Systemów Informatycznych
Biura Łączności i Informatyki
Komendy Głównej Policji

W Biurze Łączności i Informatyki Komendy Głównej Policji realizowane jest przedsięwzięcie pod nazwą „Pilotażowe wdrożenie wielkoskalowego systemu sztucznej inteligencji do automatyzacji procesów operacyjnych i administracyjnych w Policji" (karta projektu nr 30/25). Jego celem jest stworzenie bezpiecznych, działających w środowisku *on-premise*, narzędzi wspierających policjantów i pracowników Policji w codziennej służbie oraz pracy.
Powstające rozwiązania są projektowane z myślą o rzeczywistych potrzebach formacji oraz rozwijane z uwzględnieniem opinii i doświadczeń przyszłych użytkowników.

Coraz więcej informacji, coraz większe wyzwania

Współczesna Policja funkcjonuje w środowisku, w którym ilość dostępnych informacji stale rośnie. Każdego dnia funkcjonariusze i pracownicy Policji mają do czynienia z dokumentami, analizami, materiałami spraw, informacjami pochodzącymi z różnych systemów teleinformatycznych oraz danymi wymagającymi szybkiego odnalezienia, uporządkowania i właściwej interpretacji.

Zmienia się również otoczenie informacyjne. Rozwój usług cyfrowych, powszechny dostęp do informacji oraz dynamiczny rozwój technologii powodują, że coraz większego znaczenia nabierają narzędzia wspierające wyszukiwanie wiedzy, analizę treści oraz pracę z dużymi zbiorami danych. Jedną z technologii, która w ostatnich latach rozwija się wyjątkowo dynamicznie, jest sztuczna inteligencja. Narzędzia wykorzystujące duże modele językowe, analizę treści, klasyfikację informacji czy rozpoznawanie tekstu coraz częściej znajdują zastosowanie w administracji publicznej, sektorze naukowym oraz biznesie. Obecnie

również w Policji prowadzone są działania mające na celu bezpieczne i odpowiedzialne wykorzystanie potencjału tych technologii.

Od zainteresowania technologią do przedsięwzięcia o zasięgu ogólnopolskim

Początki przedsięwzięcia sięgają analiz oraz prac koncepcyjnych prowadzonych przez osoby z Biura Łączności i Informatyki Komendy Głównej Policji zainteresowane rozwojem nowoczesnych technologii informatycznych oraz sztucznej inteligencji.
Obserwując dynamiczny rozwój tej dziedziny, zaczęto analizować, w jaki sposób podobne rozwiązania mogłyby zostać wykorzystane również w środowisku Policji. Pierwsze działania obejmowały rozpoznanie dostępnych technologii, ocenę ich przydatności, weryfikację potencjalnych zastosowań oraz identyfikację obszarów, w których sztuczna inteligencja mogłaby skutecznie wspierać realizację zadań formacji.
W miarę zdobywania doświadczeń stało się jasne, że największą wartość mogą przynieść rozwiązania tworzone z uwzględnieniem specyfiki służby i pracy w Policji. Szczególnego znaczenia nabrały zagadnienia związane z bezpieczeństwem informacji, ochroną danych, integracją z istniejącymi procesami oraz dostosowaniem funkcjonalności do rzeczywistych potrzeb użytkowników.
Kolejnym etapem były testy różnych modeli językowych, rozwiązań sprzętowych oraz architektur wdrożeniowych. Pozwoliły one określić kierunki dalszego rozwoju oraz wypracować założenia środowiska, które w przyszłości będzie mogło obsługiwać rozwiązania AI przeznaczone dla policjantów i pracowników Policji w całym kraju.
W ramach prowadzonych prac szybko zauważono również, że budowa narzędzi wykorzystujących sztuczną inteligencję to znacznie więcej niż samo uruchomienie modelu językowego. Równie istotne okazały się zagadnienia związane z oceną jakości działania systemów, walidacją wyników, bezpieczeństwem przetwarzanych informacji, skalowalnością infrastruktury oraz możliwością ciągłego rozwoju tworzonych usług.
Istotną rolę w rozwoju przedsięwzięcia odgrywają także przyszli użytkownicy. Rozwój funkcjonalności prowadzony jest w ścisłej współpracy z policjantami i pracownikami Policji zainteresowanymi wykorzystaniem sztucznej inteligencji w codziennej służbie i pracy. Zbierane są opinie dotyczące oczekiwanych funkcjonalności, potencjalnych zastosowań oraz obszarów, w których nowe technologie mogłyby stanowić realne wsparcie. Dzięki temu rozwijane rozwiązania odpowiadają na rzeczywiste potrzeby formacji, a nie wyłącznie na możliwości technologiczne.
Dziś przedsięwzięcie „Pilotażowe wdrożenie wielkoskalowego systemu sztucznej inteligencji do automatyzacji procesów operacyjnych i administracyjnych w Policji" obejmuje tworzenie wielu narzędzi wykorzystujących różne obszary sztucznej inteligencji. Część z nich znajduje się już na etapie zaawansowanych prototypów, które są testowane przez użytkowników i stale udoskonalane. Celem projektu jest dostarczenie funkcjonariuszom i pracownikom Policji bezpiecznych, praktycznych oraz użytecznych narzędzi wspierających realizację codziennych zadań.
Efektem prowadzonych prac są konkretne rozwiązania wykorzystujące różne obszary sztucznej inteligencji. Obejmują one między innymi cyfryzację dokumentów, wsparcie pracy z informacją i dokumentacją, analizę dużych zbiorów danych oraz ocenę wiarygodności treści.

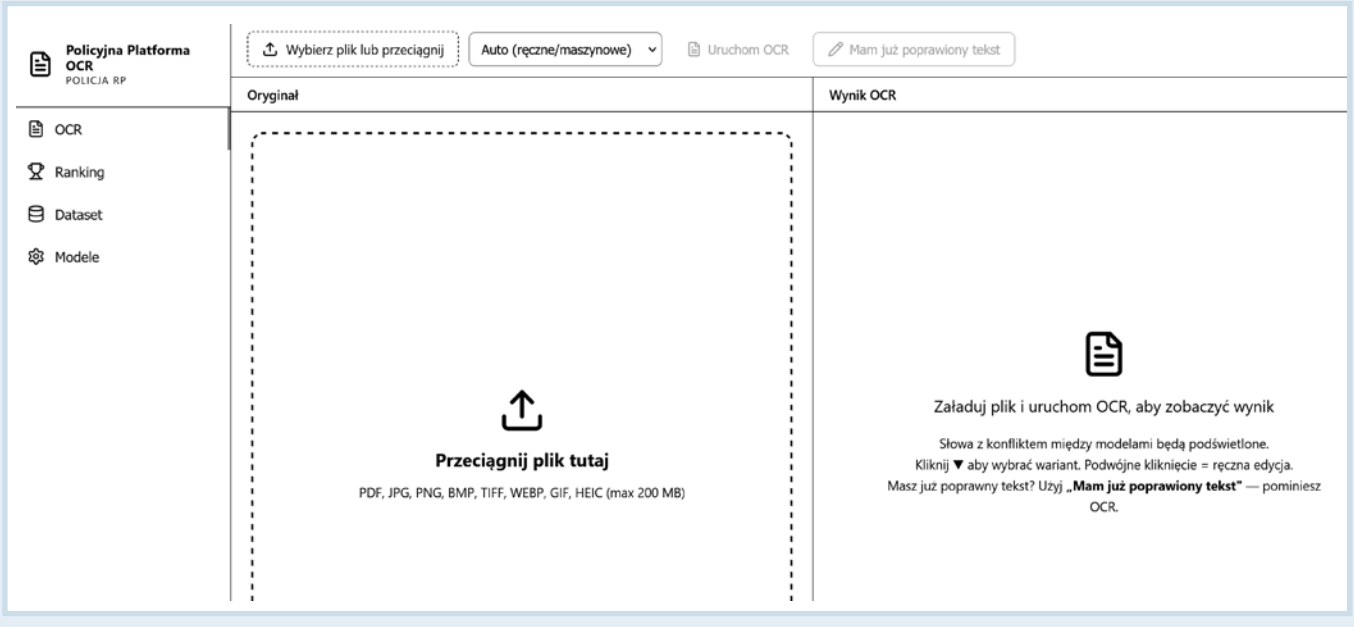
Od dokumentu papierowego do cyfrowej informacji

Jednym z pierwszych rozwijanych narzędzi jest system wykorzystujący technologię OCR (Optical Character Recognition), czyli optyczne rozpoznawanie znaków.
W praktyce rozwiązanie to umożliwia przekształcanie dokumentów występujących w postaci skanów, wydruków, maszynopisów oraz dokumentów zawierających pismo odręczne do postaci cyfrowej. Dzięki temu treść dokumentu staje się możliwa do wyszukiwania, kopiowania, analizowania oraz dalszego wykorzystania w innych systemach.
Znaczenie tego procesu wykracza jednak poza samo rozpoznanie tekstu. Dokument, który dotychczas był jedynie obrazem zapisanym w pliku, staje się źródłem informacji możliwym do wykorzystania podczas dalszej pracy analitycznej. W praktyce oznacza to szybszy dostęp do informacji oraz możliwość efektywniejszego wykorzystania wiedzy zawartej w dokumentach.

Policyjny Asystent AI – wsparcie codziennej pracy

Kolejnym rozwiązaniem rozwijanym w ramach przedsięwzięcia jest Policyjny Asystent AI (PAAI). Narzędzie zostało zaprojektowane jako uniwersalny asystent wspierający policjantów i pracowników Policji w codziennej pracy z informacją.
PAAI wykorzystuje możliwości dużych modeli językowych dostosowanych do pracy w języku polskim. Użytkownik może prowadzić z systemem konwersację w języku naturalnym, podobnie jak ma to miejsce w przypadku popularnych asystentów opartych na sztucznej inteligencji.
Możliwości PAAI obejmują między innymi wsparcie w przygotowywaniu dokumentów, opracowywaniu podsumowań, porządkowaniu informacji, analizie treści oraz wyszukiwaniu wiedzy. Narzędzie może również wspierać użytkownika podczas pracy z większymi zbiorami dokumentów, pomagając szybciej odnajdywać potrzebne informacje.
Istotnym założeniem PAAI jest zapewnienie prostego i intuicyjnego dostępu do możliwości oferowanych przez nowoczesne modele językowe. Dzięki temu użytkownik może korzystać z zaawansowanych funkcji sztucznej inteligencji bez konieczności posiadania specjalistycznej wiedzy technicznej.

NARZĘDZIE OCR



Jeszcze większe możliwości analityczne oferuje rozwijany równolegle Dochodzeniowy Asystent AI (DAAI), który został zaprojektowany z myślą o pracy ze złożonym materiałem spraw oraz z dużymi zbiorami dokumentów.

Dochodzeniowy Asystent AI – cyfrowe środowisko wspierające analizę spraw

Jednym z najbardziej zaawansowanych rozwiązań rozwijanych w ramach przedsięwzięcia jest Dochodzeniowy Asystent AI (DAAI).

Narzędzie zostało zaprojektowane z myślą o pracy z obszerną dokumentacją oraz materiałami gromadzonymi w toku prowadzonych spraw. W przeciwieństwie do uniwersalnych asystentów opartych na dużych modelach językowych, DAAI rozwijany jest jako wyspecjalizowane środowisko wspierające analizę informacji, dokumentów oraz zależności występujących pomiędzy osobami, zdarzeniami i innymi elementami sprawy.

Podstawą działania systemu jest możliwość tworzenia odrębnych przestrzeni roboczych odpowiadających konkretnym sprawom. W ramach każdej z nich użytkownik może gromadzić dokumenty, porządkować materiał oraz prowadzić analizy dotyczące wyłącznie wybranej sprawy.

Do systemu mogą być dodawane różnego rodzaju dokumenty, które następnie stają się częścią wspólnej bazy wiedzy dotyczącej prowadzonego postępowania. Dzięki temu informacje znajdujące się w różnych materiałach mogą być analizowane łącznie, niezależnie od miejsca ich pierwotnego występowania.

Jedną z kluczowych funkcjonalności DAAI jest możliwość zadawania pytań dotyczących treści dokumentów. Użytkownik może uzyskiwać informacje na podstawie pojedynczego dokumentu, wybranej grupy dokumentów lub całego materiału zgromadzonego w ramach sprawy.

W praktyce oznacza to możliwość zadawania pytań, takich jak:

- w których dokumentach pojawia się wskazana osoba,
- jakie numery telefonów występują w zgromadzonych materiałach,
- jakie zdarzenia miały miejsce w określonym przedziale czasu,
- jakie osoby pojawiają się w kontekście wskazanego zdarzenia,
- jakie zależności można odnaleźć pomiędzy wybranymi podmiotami.

W przypadku spraw obejmujących setki stron materiałów odnalezienie konkretnych informacji bywa czasochłonne. DAAI pozwala znacząco przyspieszyć ten proces poprzez analizę zgromadzonych dokumentów i wskazywanie miejsc, w których znajdują się informacje związane z zadanym pytaniem.

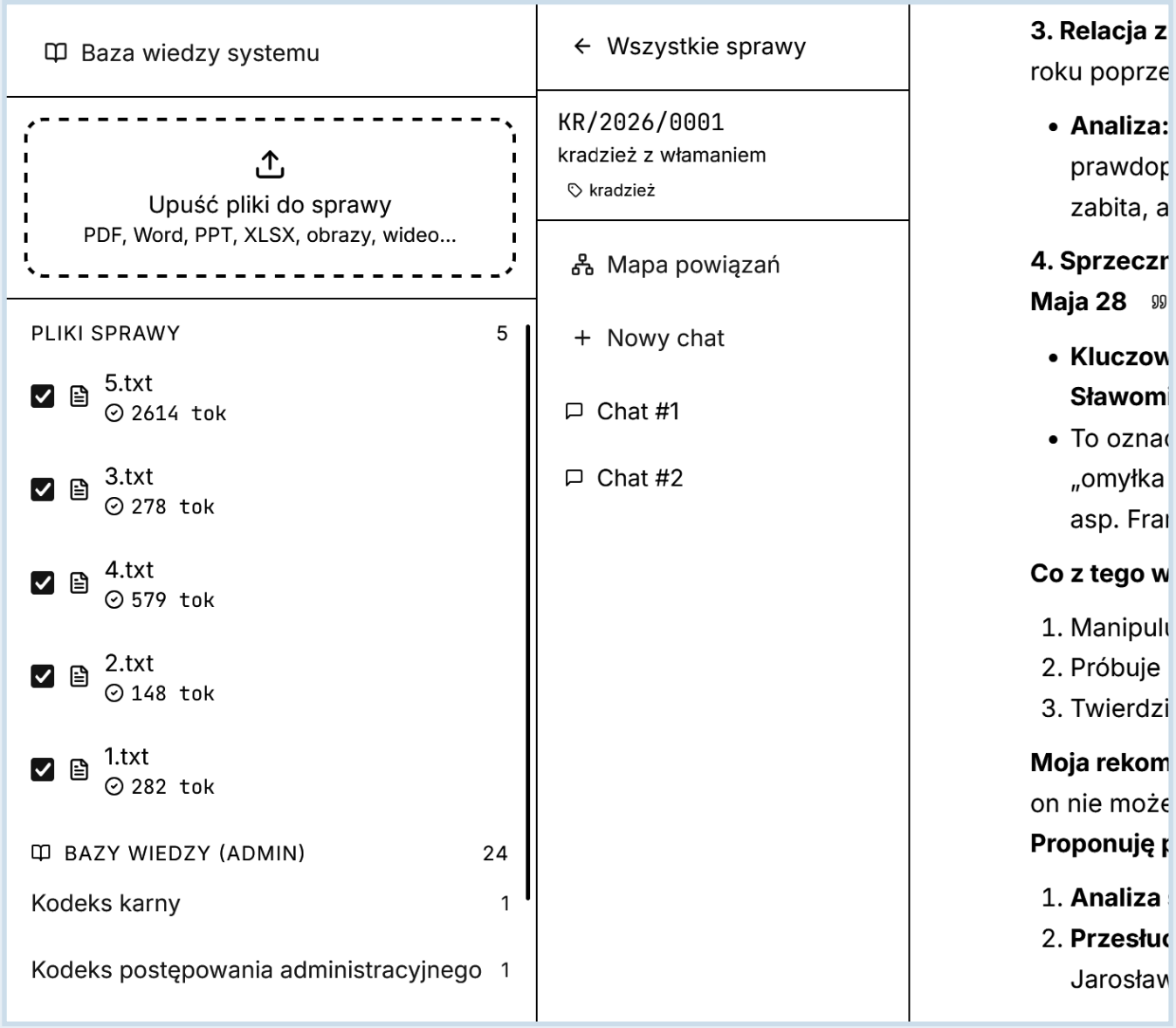
Istotnym elementem rozwijanego rozwiązania są również funkcje wizualizacji informacji. System może wspierać tworzenie grafów powiązań prezentujących relacje pomiędzy osobami, numerami telefonów, dokumentami, zdarzeniami lub innymi elementami występującymi w materiale sprawy.

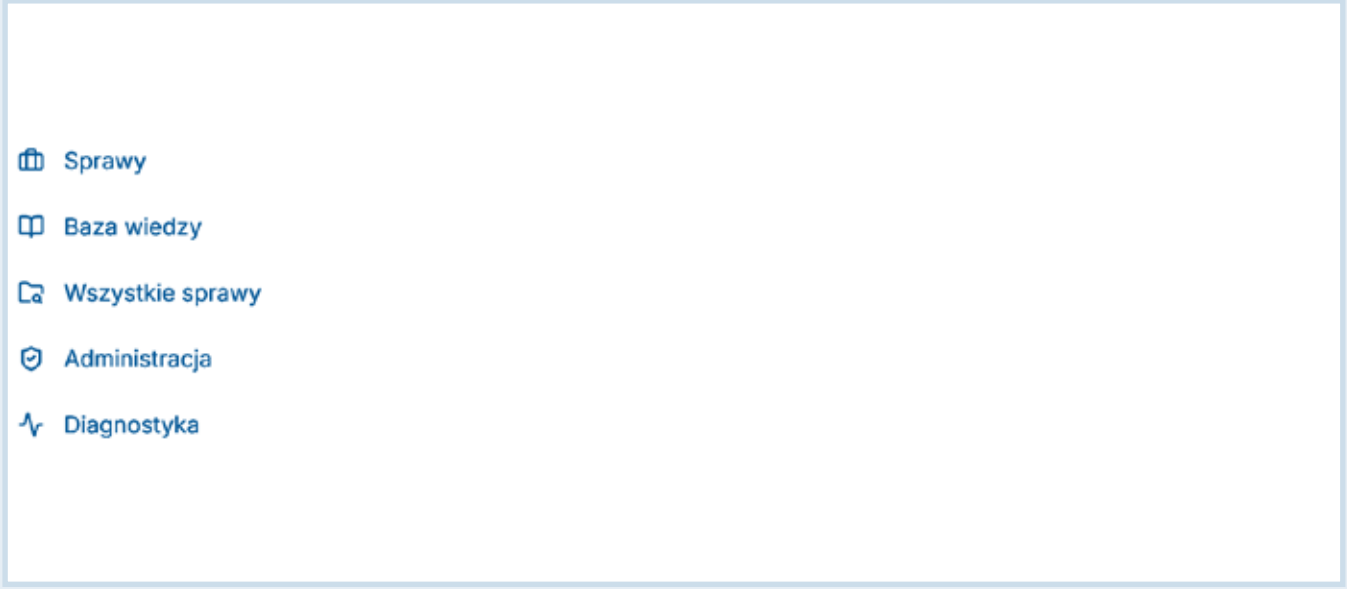
Grafy mogą być budowane zarówno automatycznie na podstawie informacji zawartych w dokumentach, jak również rozwijane przez użytkownika, który może uzupełniać je o własne ustalenia oraz dodatkowe zależności wynikające z prowadzonych czynności.

Takie podejście pozwala na połączenie możliwości analitycznych sztucznej inteligencji z wiedzą, doświadczeniem i oceną funkcjonariusza prowadzącego sprawę.

Warto podkreślić, że DAAI nie został zaprojektowany jako system podejmujący decyzje za użytkownika. Zadaniem narzędzia jest wspieranie procesu analizy informacji, porządkowanie wiedzy oraz ułatwianie odnajdywania danych zawartych w zgromadzonych materiałach.

NARZĘDZIE DAAI





Ocena materiału dowodowego, podejmowanie decyzji procesowych, planowanie czynności oraz formułowanie wniosków pozostają w kompetencji funkcjonariusza prowadzącego sprawę.
Rozwijane obecnie funkcjonalności są stale weryfikowane i udoskonalane. Szczególne znaczenie mają testy prowadzone z udziałem przyszłych użytkowników, których doświadczenia, potrzeby i sugestie stanowią ważny element dalszego rozwoju systemu.

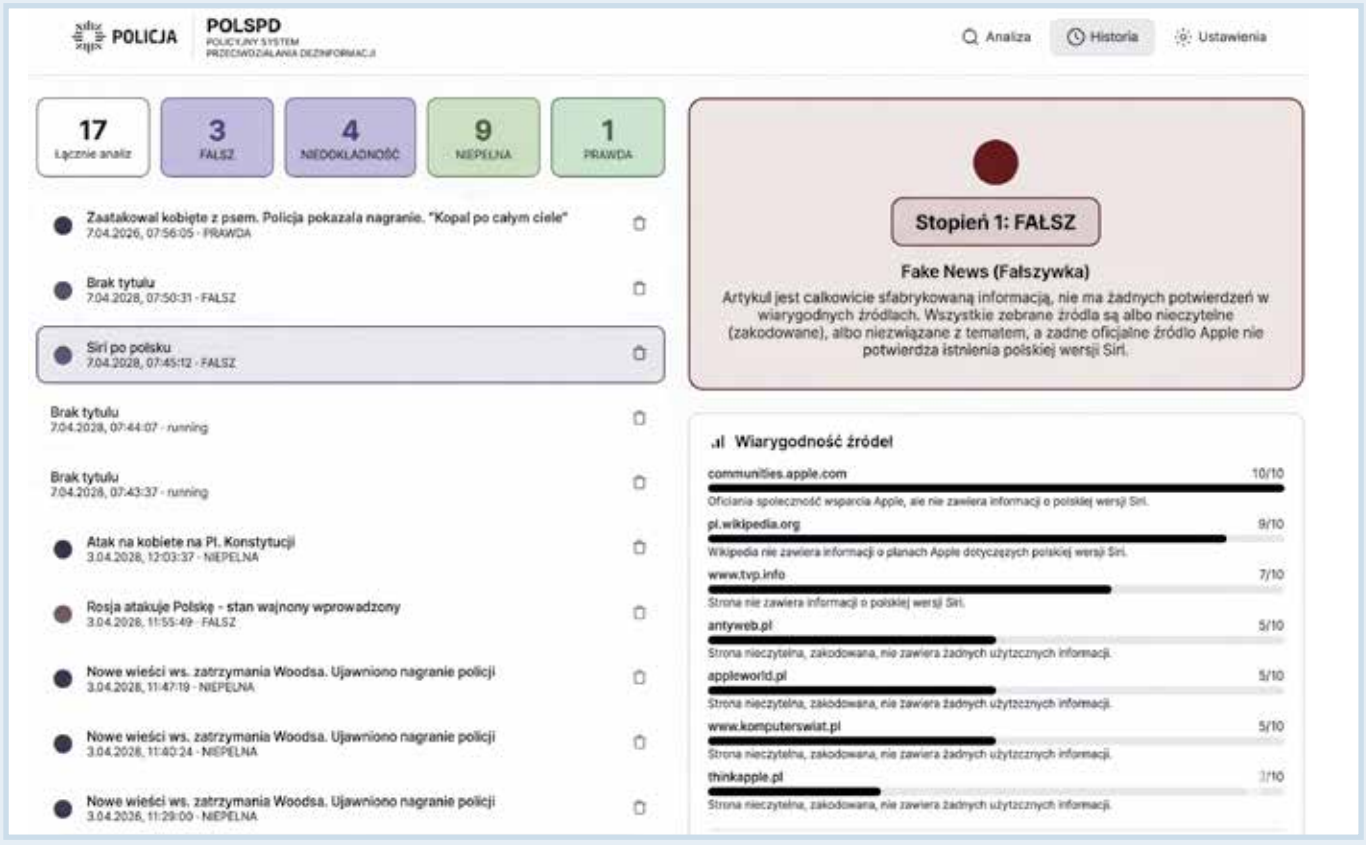
Sztuczna inteligencja w analizie informacji i przeciwdziałaniu dezinformacji

Obszarem, który w ostatnich latach zyskał szczególne znaczenie, jest również analiza wiarygodności informacji. Dynamiczny rozwój mediów społecznościowych, łatwość publikowania treści oraz szybkość ich rozpowszechniania powodują, że ocena jakości informacji staje się coraz większym wyzwaniem.
Z myślą o tym zagadnieniu rozwijany jest Policyjny System Przeciwdziałania Dezinformacji (POLSPD).
Celem rozwiązania jest wspieranie użytkownika podczas analizy treści pochodzących z różnych źródeł informacji. System wykorzystuje mechanizmy sztucznej inteligencji do oceny analizowanych materiałów oraz przygotowywania uzasadnienia przedstawionych wyników.
W zależności od charakteru analizowanej treści system może wskazywać, czy badany materiał nosi cechy informacji prawdziwej, manipulacji, informacji niepełnej lub dezinformacji. Szczególne znaczenie ma jednak sposób prezentowania wyników.
System wskazuje argumenty, źródła oraz przesłanki wykorzystane podczas analizy, umożliwiając użytkownikowi samodzielną ocenę przedstawionych informacji.
Podobnie jak w przypadku pozostałych rozwijanych narzędzi, ostateczna interpretacja wyników oraz podejmowanie decyzji pozostają po stronie człowieka. Zadaniem systemu jest wspieranie procesu analizy informacji oraz zwiększanie świadomości dotyczącej zjawiska dezinformacji.

Rozwój nie kończy się po wdrożeniu

Przedstawione rozwiązania stanowią jedynie część przedsięwzięć realizowanych obecnie w obszarze sztucznej inteligencji. Równolegle prowadzone są prace nad kolejnymi narzędziami znajdującymi się na różnych etapach rozwoju, od prac koncepcyjnych po zaawansowane prototypy poddawane testom.
Doświadczenia zdobywane podczas realizacji tych projektów pokazują jednak, że rozwój systemów sztucznej inteligencji znacząco różni się od wdrażania tradycyjnego oprogramowania.
W przypadku klasycznych systemów informatycznych moment uruchomienia rozwiązania często oznacza przejście do etapu utrzymania i dalszego rozwoju funkcjonalnego. W przypadku sztucznej inteligencji proces ten jest znacznie bardziej złożony.

NARZĘDZIE POLSPD



Modele AI wymagają stałego monitorowania jakości działania, regularnej oceny skuteczności oraz ciągłej weryfikacji poprawności generowanych wyników. Szczególnego znaczenia nabiera również analiza parametrów jakościowych, takich jak precyzja działania (precision) czy kompletność odnajdywania informacji (recall).
W praktyce oznacza to konieczność nieustannego doskonalenia narzędzi, testowania nowych modeli, oceny skuteczności wdrożonych rozwiązań oraz dostosowywania ich do zmieniających się potrzeb użytkowników.
Znaczną część prac realizowanych w ramach przedsięwzięcia stanowią właśnie działania związane z ewaluacją, walidacją i doskonaleniem rozwijanych systemów. Dzięki temu możliwe jest budowanie rozwiązań, które będą nie tylko nowoczesne, ale przede wszystkim użyteczne i wiarygodne z punktu widzenia przyszłych użytkowników.

Technologia wspierająca człowieka

Rozwój sztucznej inteligencji bardzo często wywołuje pytania dotyczące wpływu nowych technologii na sposób wykonywania pracy. Dotyczy to również Policji.
Doświadczenia zdobywane podczas realizacji przedsięwzięcia pokazują jednak, że największą wartością sztucznej inteligencji jest wspieranie użytkownika w realizacji zadań wymagających pracy z informacją, dokumentami oraz dużymi zbiorami danych.
Sztuczna inteligencja może pomagać w wyszukiwaniu informacji, analizie dokumentów, przygotowywaniu podsumowań czy porządkowaniu wiedzy zgromadzonej w różnych źródłach. Może również przyspieszać wykonywanie wielu czasochłonnych czynności związanych z pracą administracyjną i analityczną.
Jednocześnie istnieje wiele obszarów, w których kluczową rolę nadal odgrywa człowiek.
Kontakt z obywatelem, ocena sytuacji, prowadzenie czynności służbowych, podejmowanie decyzji, doświadczenie zawodowe, znajomość lokalnych uwarunkowań czy umiejętność rozmowy z drugim człowiekiem pozostają elementami, których nie można sprowadzić do działania algorytmu.
Sztuczna inteligencja nie posiada świadomości, nie rozumie rzeczywistości w sposób właściwy człowiekowi i może popełniać błędy. Dlatego rozwijane narzędzia traktowane są jako systemy wspierające użytkownika, a nie rozwiązania zastępujące jego wiedzę, doświadczenie czy odpowiedzialność.
Założenie to znajduje odzwierciedlenie we wszystkich rozwijanych rozwiązaniach. Zarówno Policyjny Asystent AI, Dochodzeniowy Asystent AI, system OCR, jak i Policyjny System Przeciwdziałania Dezinformacji zostały zaprojektowane jako narzędzia wspomagające realizację określonych zadań, pozostawiając użytkownikowi pełną kontrolę nad procesem podejmowania decyzji.
Historia rozwoju technologii pokazuje, że kolejne innowacje zmieniały sposób wykonywania pracy i zwiększały możliwości użytkowników. Pojawienie się komputerów, systemów teleinformatycznych, radiowozów wyposażonych w nowoczesne środki łączności czy mobilnego dostępu do informacji nie zastąpiło funkcjonariuszy, lecz usprawniło realizację ich zadań. Podobnie postrzegana jest obecnie sztuczna inteligencja – jako kolejne narzędzie wspierające policjantów i pracowników Policji w wykonywaniu obowiązków, ułatwiające pracę z informacją oraz pomagające efektywniej wykorzystywać dostępne dane i wiedzę.

Przygotowując się na przyszłość

Sztuczna inteligencja staje się jednym z narzędzi coraz powszechniej wykorzystywanych przez administrację publiczną, środowisko naukowe, przedsiębiorstwa oraz obywateli. Zmiany te wpływają również na sposób funkcjonowania instytucji odpowiedzialnych za bezpieczeństwo państwa.
Realizowane przedsięwzięcie stanowi element przygotowań Policji do funkcjonowania w rzeczywistości, w której rozwiązania oparte na sztucznej inteligencji będą stopniowo stawały się częścią codziennej pracy wielu organizacji. Wymaga to nie tylko budowy odpowiedniej infrastruktury technicznej, ale również rozwijania kompetencji, zdobywania doświadczeń oraz wypracowywania dobrych praktyk związanych z bezpiecznym wykorzystaniem nowych technologii.
Udoskonalane obecnie rozwiązania są opracowywane przez policjantów i pracowników Policji, którzy znają specyfikę służby i pracy w formacji oraz rozumieją wyzwania stojące przed jej użytkownikami. Dzięki temu możliwe jest tworzenie narzędzi odpowiadających na rzeczywiste potrzeby, a jednocześnie uwzględniających wymagania związane z bezpieczeństwem informacji oraz specyfiką policyjnego środowiska teleinformatycznego.
Prace prowadzone w ramach przedsięwzięcia będą kontynuowane, a rozwijane narzędzia będą podlegały dalszym testom, ocenie oraz doskonaleniu. Równolegle analizowane są kolejne obszary, w których sztuczna inteligencja może wspierać realizację zadań Policji.
Powstają konkretne rozwiązania, które w przyszłości będą wspierały codzienną pracę policjantów i pracowników Policji. Ich celem nie jest zastępowanie człowieka, lecz dostarczanie nowoczesnych narzędzi pomagających sprawniej wykorzystywać informacje, wiedzę i doświadczenie zgromadzone w organizacji.

Summary

Modern tools, real support. How the systems of AI for the Police are being developed

The article describes a project called: Pilot implementation of a large-scale AI system to automate operational and administrative processes in the Police (Polish: Pilotażowe wdrożenie wielkoskalowego systemu sztucznej inteligencji do automatyzacji procesów operacyjnych i administracyjnych w Policji), carried out at the IT Bureau of the National Police Headquarters.
The goal of this project is to create the safe tools using in everyday tasks, supporting police officers and police employees.
The emerging solutions are designed with the actual needs of the Police and developed, taking into account, the opinions and experiences of future users.

Tłumaczenie: Beata Pepłowska

ŁĄCZNOŚĆ RADIOWA W POLICJI

Podstawy, procedury i technologie

asp. Adam Bochenek
Zakład Prewencji CSP

asp. szt. Iwona Gierczak
Zakład Prewencji CSP

Łączność radiowa jest jednym z kluczowych elementów funkcjonowania polskiej Policji, wpływającym na skuteczność działań operacyjnych, koordynację jednostek w terenie oraz bezpieczeństwo funkcjonariuszy. Odpowiednie przeszkolenie policjantów w zakresie obsługi środków łączności radiowej oraz przestrzeganie określonych procedur są regulowane przepisami prawa i wewnętrznymi aktami normatywnymi Policji.

PODSTAWY PRAWNE SZKOLENIA I UŻYTKOWANIA ŚRODKÓW ŁĄCZNOŚCI RADIOWEJ

Szkolenie z zakresu łączności funkcjonariusze rozpoczynają już na szkoleniu zawodowym podstawowym, które obecnie prowadzone jest na podstawie decyzji nr 276 Komendanta Głównego Policji z dnia 25 sierpnia 2023 r. w sprawie programu szkolenia zawodowego podstawowego (Dz. Urz. KGP poz. 81, z późn. zm.). Zajęcia programowe obejmują naukę obsługi radiotelefonów, zasad prowadzenia korespondencji oraz procedur bezpieczeństwa w komunikacji.

Zasady organizacji i funkcjonowania systemu łączności w Policji reguluje zarządzenie nr 22 Komendanta Głównego Policji z dnia 14 lipca 2020 r. w sprawie określenia metod i form wykonywania zadań Policji z użyciem środków łączności radiowej (Dz. Urz. KGP poz. 38, z późn. zm.). Dokument ten określa m.in. strukturę sieci radiowych, sposób ich eksploatacji oraz standardy techniczne i proceduralne w zakresie prowadzenia korespondencji radiowej.

PODSTAWOWE DEFINICJE I SPOSÓB PRACY W ŁĄCZNOŚCI RADIOWEJ

W ramach policyjnej łączności radiowej stosuje się określoną terminologię oraz procedury zapewniające skuteczność i jednoznaczność przekazywanych informacji. Do podstawowych pojęć należą:

- **radiotelefon (RT)** – urządzenie elektroniczne składające się z nadajnika i odbiornika, przeznaczone do przekazywania komunikatów głosowych drogą radiową oraz opcjonalnie do transmisji danych[1];
- **łączność radiowa** – łączność między stacjami radiowymi realizowana w oparciu o przydzielony kanał radiowy[2];
- **sieć radiowa** – zespół stacji radiowych utrzymujących ze sobą łączność i pracujących według wspólnych danych radiowych[3];
- **kanał radiowy** – tor transmisyjny wykorzystywany do bezprzewodowego przesyłania informacji za pomocą fal elektromagnetycznych oraz stosowania kodów i sygnałów[4].

RODZAJE RADIOTELEFONÓW UŻYWANYCH W POLSKIEJ POLICJI

Polska Policja wykorzystuje różne typy radiotelefonów dostosowane do specyfiki wykonywanych zadań.

Standard cyfrowy DMR:

- radiotelefony noszone, np. Motorola DP4601, R7, Excera EP8100, Hytera PD785G,
- radiotelefony przewoźne (mobilne) lub biurkowe – montowane w pojazdach policyjnych lub w centrach dowodzenia i stanowiskach kierowania charakteryzujące się większym zasięgiem i mocą nadawczą, np. Motorola DM4601e, Excera EM8100, Hytera HM78X.

Fot. 1. Wybrane modele radiotelefonów firmy Sepura. Źródło: materiał własny firmy Sepura.

Standard cyfrowy TETRA:
– radiotelefony noszone – Sepura SC20/21, Motorola MTP3550,
– radiotelefony przewoźne/bazowe – Sepura SCG22, Motorola MTM5400.

SIECI RADIOWE W POLICJI

W Policji funkcjonują różne typy sieci radiowych dostosowane do potrzeb operacyjnych i organizacyjnych.

1. **Sieci dyspozytorskie** – wykorzystywane do koordynacji działań służb patrolowych przez stanowiska kierowania.
2. **Sieci operacyjne** – służące do bezpośredniej łączności pomiędzy jednostkami biorącymi udział w działaniach operacyjnych.
3. **Sieci taktyczne** – używane w ramach działań specjalnych np. przez jednostki antyterrorystyczne.
4. **Sieci alarmowe i kryzysowe** – aktywowane w sytuacjach zagrożenia o charakterze nadzwyczajnym.
5. **Sieci DMR (*Digital Mobile Radio*)** – nowoczesne sieci cyfrowe wykorzystywane m.in. na terenie Centrum Szkolenia Policji w Legionowie.
6. **Sieć TETRA** (***TEerrestial TRunked RAdio***) – system łączności trankingowej wdrażany obecnie w wielu rejonach Polski jako spójna sieć łączności Policji.

SZKOLENIE I ĆWICZENIA PRAKTYCZNE Z RADIOTELEFONAMI

Na terenie Centrum Szkolenia Policji w Legionowie w wyznaczonych rejonach służbowych podczas zajęć dydaktycznych słuchacze biorą udział w ćwiczeniach z wykorzystaniem radiotelefonów DMR. Podczas zajęć praktycznych funkcjonariusze:
– praktykują prawidłowe formy komunikacji radiowej zgodnie z obowiązującymi przepisami prawa,
– biorą udział w symulacjach,
– doskonalą umiejętność posługiwania się urządzeniami łączności w warunkach stresu i presji czasu,
– ćwiczą przekazywanie meldunków, komunikatów i sygnałów alarmowych,
– uczą się rozpoznawania i eliminowania zakłóceń w łączności,
– ćwiczą współpracę z innymi jednostkami poprzez sieć radiową.

ZNACZENIE ŁĄCZNOŚCI RADIOWEJ DLA BEZPIECZEŃSTWA I EFEKTYWNOŚCI POLICJI

Łączność radiowa w Policji jest kluczowa, ponieważ zapewnia skuteczną koordynację działań operacyjnych, szybkie reagowanie na zagrożenia oraz bezpieczeństwo funkcjonariuszy i obywateli. Umożliwia płynny przepływ informacji między jednostkami, co pozwala na efektywne zarządzanie akcjami, szczególnie w sytuacjach kryzysowych. Sprawna i niezawodna łączność radiowa pozwala funkcjonariuszom natychmiast przekazywać meldunki, uzyskiwać wsparcie, koordynować działania grup interwencyjnych czy reagować na dynamicznie zmieniające się sytuacje. W przypadku zdarzeń masowych, pościgów czy akcji ratowniczych to właśnie komunikacja radiowa decyduje o czasie reakcji, skuteczności interwencji i minimalizacji ryzyka dla osób zaangażowanych. Ponadto znajomość zasad właściwej korespondencji radiowej, w tym stosowanie odpowiednich kodów i procedur, jest niezbędna, by uniknąć nieporozumień, które w warunkach stresu mogłyby prowadzić do błędów operacyjnych. Współczesne wyzwania w obszarze bezpieczeństwa publicznego wymagają od funkcjonariuszy nie tylko umiejętności technicznej obsługi radiotelefonów, ale również wysokiego poziomu kompetencji komunikacyjnych oraz znajomości zasad obowiązujących w systemach łączności radiowej. Dlatego tak istotne jest systematyczne podnoszenie kwalifikacji również przez kadrę dydaktyczną. Właśnie w tym celu wykładowcy Centrum Szkolenia Policji w Legionowie aktywnie uczestniczą w szkoleniach i warsztatach, m.in. w szkoleniu doskonalącym z zakresu łączności radiowej, które odbyło się

w Uniejowie. Udział w tego typu przedsięwzięciach pozwala nie tylko poszerzać wiedzę teoretyczną, ale także zdobywać praktyczne doświadczenie, które następnie przekazujemy słuchaczom podczas szkoleń – zarówno specjalistycznych, jak i podstawowych dla nowo przyjętych funkcjonariuszy. Nasze zaangażowanie w rozwój kompetencji własnych przekłada się bezpośrednio na jakość prowadzonych zajęć oraz na przygotowanie słuchaczy do realnych wyzwań służby w terenie. Dzięki temu szkolenia w CSP w Legionowie odpowiadają na aktualne potrzeby Policji i służą budowaniu skutecznych i profesjonalnych kadr policyjnych.

NOWOCZESNA ŁĄCZNOŚĆ TETRA W SŁUŻBACH MUNDUROWYCH. KOMPLEKSOWY RAPORT Z WARSZTATÓW SEPURA W UNIEJOWIE

W dniach 4–6 marca 2025 r. w Uniejowie odbyły się warsztaty poświęcone obsłudze nowoczesnych radiotelefonów systemu TETRA, organizowane przez firmę Covertech, autoryzowanego dystrybutora firmy SEPURA w Polsce. W spotkaniu uczestniczyli przedstawiciele Policji oraz Straży Pożarnej z całego kraju, aby zapoznać się z najnowszymi rozwiązaniami technologicznymi. Artykuł stanowi szczegółową relację z wydarzenia, opisując zarówno aspekty merytoryczne, jak i prezentację różnorodnych modeli radiotelefonów oraz ich unikalne parametry techniczne.

Fot. 2 i 3. Uczestnicy szkolenia w Uniejowie podczas prezentacji i pokazu radiotelefonów. Źródło: materiał własny firmy Covertech.

Wprowadzenie i cele warsztatów

W dobie dynamicznych zmian technologicznych niezawodna łączność stanowi fundament działań operacyjnych. Warsztaty w Uniejowie zostały zorganizowane w celu podniesienia kwalifikacji służb mundurowych, które muszą sprostać coraz bardziej wymagającym warunkom pracy. Firma SEPURA, lider w dziedzinie terminali TETRA, zaprezentowała najnowsze modele radiotelefonów, w tym wielofunkcyjny terminal SEPURA SCL3 oraz urządzenia z serii SC20 i SC21, urządzenia przewoźne z serii SCG22 oraz urządzenie hybrydowe SCU3 (4G i TETRA). Prezentacje miały na celu ukazanie możliwości integracji sprzętu z systemami zarządzania operacyjnego, co w znaczący sposób wpływa na poprawę efektywności i koordynacji działań ratowniczych.

Zaawansowana technologia radiotelefonów SEPURA

Szczególne wrażenie na uczestnikach zrobił model SEPURA SCL3. To urządzenie wyróżnia się dzięki możliwościom, które integrują:

- **funkcje radiotelefonu TETRA** – gwarantujące niezawodną komunikację nawet w ekstremalnych warunkach,
- **telefon służbowy –** eliminując potrzebę korzystania z oddzielnych urządzeń komunikacyjnych,
- **mobilny terminal –** umożliwiający szybkie sprawdzenie informacji o pojazdach, osobach i rzeczach,
- **rejestrator interwencji –** który pozwala na nagrywanie obrazu i dźwięku podczas przeprowadzanej interwencji.

Ten przenośny terminal może być wykorzystywany wyłącznie w sieciach 4G/5G lub w trybie hybrydowym TETRA i 4G/5G, umożliwiając migrację do komunikacji o znaczeniu krytycznym[5].

Fot. 4. Terminal Sepura wykorzystywany w trybie SCL3 4G/5G lub hybrydowym. Źródło: Sepura, SCL3 One rugged device, two mission-critical options, https://sepura.com/devices/scl3-4g-radio/ [dostęp: 1.10.2025 r.].

Fot. 5. Prezentacja asortymentu radiotelefonów i akcesoriów firmy Sepura. Źródło: materiał własny firmy Covertech.

Oferuje wszystko, czego można oczekiwać od wytrzymałego urządzenia noszonego, wraz z systemem operacyjnym Android, 5-calowym wyświetlaczem, opcjonalnym modułem SC28 TETRA i bogatą gamą akcesoriów.
Ta wielofunkcyjność urządzenia może znacznie redukować ilość sprzętu, jaki mógłby być noszony przez funkcjonariusza Policji, zwiększając wygodę i efektywność działań służbowych. Urządzenie posiada odłączalny moduł TETRA, który umożliwia rozpoczęcie korzystania z niego jako terminala PoC lub zwykłego telefonu komórkowego i późniejsze rozszerzenie do funkcjonalności do urządzenia hybrydowego poprzez proste dołączenie modułu TETRA w miejsce baterii.
Takie rozwiązanie jest unikalne w skali światowej – jest to jedyne urządzenie z odłączalnym modułem TETRA.
Urządzenie otrzymało również prestiżowe wyróżnienie na konferencji CCW (Critical Communication World) w Brukseli jako zwycięzca konkursu na najlepszy produkt lub rozwiązanie TETRA roku 2025[6].

Rodzaje radiotelefonów i akcesoriów

Oprócz wspomnianego radiotelefonu SCL3 firma SEPURA zaprezentowała radiotelefony przenośne:
– seria SC20 – urządzenia wyposażone w złącze męski SMA[7], co umożliwia szeroką kompatybilność z akcesoriami audio oraz dodatkowymi modułami transmisyjnymi;

Fot. 6. Radiotelefon SC20 VHF. Źródło: Sepura, SC20 Powerful TETRA Hand-Portable Radio, https://sepura.com/devices/sc20-tetra-radio/[dostęp: 1.10.2025 r.].

Fot. 7. Radiotelefon SC21. Źródło: Sepura, SC21 Compact TETRA Hand-Held Radio, https://sepura.com/devices/sc21-tetra-radio/ [dostęp: 1.10.2025 r.].

– seria SC21 – wyróżnia się unikalnym systemem złącza (gwint M6[8]) i dedykowanym interfejsem dla zastosowań specjalistycznych, gdzie wymagana jest najwyższa precyzja połączeń oraz małe wymiary i waga radiotelefonu.

Każdy z tych modeli został zaprojektowany z myślą o specyfice pracy służb operacyjnych, oferując niezawodność, ergonomię oraz możliwość łatwej integracji z różnorodnymi akcesoriami – od anten o różnych częstotliwościach pracy, przez ładowarki wielostanowiskowe, po specjalistyczne zestawy audio. Oba modele współdzielą akcesoria oraz oprogramowanie, czyniąc zmianę użytkowania wyjątkowo prostą i tańszą.
Według dokumentacji termin „radiotelefony przenośne" odnosi się do urządzeń z serii SC – SC20 i SC21. Najważniejsze cechy tych modeli to:
– ergonomiczny design – pozwala łatwo je nosić i szybko używać w terenie;
– intuicyjny układ interfejsu użytkownika GUI (do wyboru 3 rodzaje interfejsu, w tym jeden typu „Motorola");
– dedykowane interfejsy – np. boczne złącze RAC[9], które chroni podłączone akcesoria audio przed przypadkowym odłączeniem, dolne złącze akcesoriów i programowania zabezpieczone elektrycznie przed słoną korozją;
– zintegrowane systemy ładowania i programowania – umożliwiają obsługę akcesoriów, takich jak ładowarki biurkowe i samochodowe, zwiększając tym samym niezawodność całego systemu;
– pełna kompatybilność ze wszystkimi funkcjonalnościami systemu TETRA produkcji Motorola;
– unikalne systemy aplikacji AppSpace, które automatyzują różne funkcje radiotelefonu i/lub zbierają dane i/lub raportują zdarzenia; aplikacje można instalować na radiotelefonie za pomocą oprogramowania RadioManager 2.

Wszystkie modele zostały zaprojektowane z myślą o pracy w trudnych warunkach operacyjnych, co potwierdza certyfikat ochrony IP68 i norma ETSI EN 300 019 5M3.

Radiotelefony samochodowe SCG22

Radiotelefon samochodowy SCG 22 to nowoczesne urządzenie przewoźne o funkcjonalnościach identycznych jak radiotelefony noszone. Urządzenie oferuje wiele możliwości montażu w pojazdach. Dostępna jest podstawowa wersja montażu rozłącznego z jedną konsolą zdalną i przewodami łączącymi o długości do 10 m, a także wersja dwukonsolowa – z montażem lokalnym i zdalnym lub z dwiema konsolami zdalnymi, przeznaczona do większych pojazdów. Istnieje również wersja konsoli wirtualnej, którą można zaimplementować na platformie Windows lub pojazdowych systemach Infotainment (np. pojazdów grupy VW). Wirtualna konsola umożliwia sterowanie radiotelefonem bez potrzeby instalacji fizycznej konsoli w pojeździe lub na komputerze Windows PC.
Wersja biurkowa radiotelefonu SCG22 oferuje zintegrowaną z głośnikiem obudowę oraz wygodnie zainstalowaną na niej zdalną konsolę umożliwiającą dostosowanie kąta widzenia do miejsca instalacji. Umożliwia podłączenie dodatkowych akcesoriów, takich jak słuchawka typu telefonicznego, mikrofon biurkowy i/lub mikrofon doręczny, nożny przycisk nadawania, i dostarczana jest z zasilaczem sieciowym.

Fot. 8. Radiotelefon samochodowy SCG22 oraz konsola SCC5. Źródło: Sepura, *Sepura Colour Console 3 (SCC3)*, https://sepura.com/accessories/sepura-colour-console-3/ [dostęp: 1.10.2025 r.].

Fot. 9. Przykład instalacji radiotelefonu w szwedzkiej Policji. Źródło: Sepura, https://polistidningen.se/2019/12/studie-det-behovs-mer-forskning-om-rakel/ [dostęp: 1.10.2025 r.]

Fot. 10. Radiotelefon samochodowy SCG22. Źródło: Sepura, *SCG22 TETRA Mobile Radio*, https://sepura.com/devices/scg22-tetra-radio/ [dostęp: 1.10.2025 r.].

Radiotelefony samochodowe SCG22 współdzielą oprogramowanie i interfejs użytkownika z radiotelefonami noszonymi serii SC, co czyni ich obsługę prostą i intuicyjną.

Testy ekstremalne i wyniki próby wytrzymałościowej

Praca w ekstremalnych temperaturach

Podczas warsztatów zaprezentowano szereg przeprowadzonych symulacji, które pokazały, że radiotelefony SEPURA działają bez zakłóceń nawet w bardzo niskich i bardzo wysokich temperaturach. Zakres temperatury pracy wynosi od -30ºC do +65ºC[10]. Urządzenia te sprawdzają się świetnie zarówno podczas zimowych operacji ratowniczych, jak i przy intensywnych upałach, co czyni je uniwersalnymi narzędziami operacyjnymi.

Odporność na wilgoć i zabrudzenia

Dzięki zastosowanym technologiom zabezpieczającym radiotelefony uzyskały certyfikat IP68[11], co gwarantuje ich odporność na wodę, kurz i inne zanieczyszczenia. Technologia *Water Porting* pozwala utrzymać wysoką jakość dźwięku nawet podczas deszczu, ponieważ oczyszcza z wody kanały dźwiękowe głośnika, zapobiegając ich zatykaniu przez wodę, co jest bardzo ważne podczas działań w mokrych lub wilgotnych warunkach.

Mechaniczne próby wytrzymałościowe

Urządzenia przeszły rygorystyczne testy mechaniczne obejmujące symulacje upadków i wstrząsów. Zostały zaprojektowane w taki sposób, aby akcesoria audio nie odłączały się przypadkowo, co gwarantuje ciągłość komunikacji podczas dynamicznych operacji. Takie testy potwierdzają, że radiotelefony są gotowe do pracy w najbardziej wymagających warunkach. Urządzenie spełnia normy MIL STD 810F oraz ETSI EN 300 019[12].

Wśród interesujących szczegółów technicznych warto wymienić:

- **anteny i ich kolory** – każda antena jest oznaczona kolorem, co wskazuje na pasmo częstotliwości, np. antena helikalna dla zakresu 300–344 MHz jest oznaczona kolorem brązowym, co ułatwia szybkie dopasowanie sprzętu do warunków pracy;
- **system zarządzania energią** – oparty na akumulatorach litowo-polimerowych o napięciu 7,4 V[13], które charakteryzują się długim czasem pracy oraz możliwością pracy w trybach intensywnych transmisji;
- **interfejsy i złącza** – boczne złącze RAC jest zabezpieczone mechanizmem blokującym, co zapobiega przypadkowemu odłączeniu akcesoriów audio; radiotelefony serii SC21 posiadają natomiast złącza gwintowane, zapewniające stabilne połączenia w najbardziej ekstremalnych warunkach;
- **ładowarki** – oferta obejmuje różne rodzaje ładowarek: osobiste szybkie ładowarki, ładowarki samochodowe oraz wielostanowiskowe systemy ładowania, co pozwala na nieprzerwaną pracę radiotelefonów w terenie; ładowarki wielostanowiskowe umożliwiają programowanie do 6 radiotelefonów jednocześnie, co znacznie skraca czas przygotowania floty radiotelefonów do działania;

– **akcesoria audio** – wśród nich znajdują się różne zestawy słuchawek, mikrofonogłośniki oraz zaawansowane systemy Ultra CSM/RSM z funkcją Water Porting, zapewniające doskonałą jakość dźwięku nawet w bardzo trudnych warunkach;
– **oprogramowanie** do konfiguracji sprzętu RadioManager 2 może być zainstalowane w wersji lokalnej lub sieciowej, umożliwiającej centralne zarządzanie flotą radiotelefonów z dowolnego miejsca poprzez sieć LAN/WAN bez konieczności przenoszenia plików konfiguracyjnych pomiędzy lokalizacjami; wszystkie dane znajdują się w centralnej bazie danych, do której mogą mieć dostęp poszczególne stanowiska programistyczne rozmieszczone w dowolnym miejscu z dostępem do sieci korporacyjnej; dostęp do centralnej bazy nie musi być stały, klient może pobrać dane z bazy i zapisać do niej wyniki w czasie krótkiego połączenia;
– **Radio Manager 2** w wersji sieciowej umożliwia programowanie jednocześnie (w tym samym czasie) do 32 radiotelefonów na jednym stanowisku programującym.

Przykładowe akcesoria

Dokumentacja produktowa Sepura prezentuje także liczne certyfikaty, m.in. CB, CE, UL, IRAM oraz CCC[14], które potwierdzają zgodność sprzętu z międzynarodowymi normami bezpieczeństwa i jakości.

Fot. 11. Ładowarka sześciostanowiskowa (6+6) programująca. Źródło: Sepura, *Biuletyn produktowy*, *„Akcesoria do serii STP i SC2”*, wydanie 1.4a, s. 16.

Fot. 12. Mikrofonogłośnik IP67. Źródło: Sepura, *IP67 Sepura Remote Speaker Microphone (sRSM)*, https://sepura.com/accessories/ip67-remote-speaker-microphone/ [dostęp: 1.10.2025 r.].

Fot. 13. Mikrofonogłośnik profesjonalny IP67 Ultra z możliwością konfiguracji różnych dodatkowych akcesoriów, zmianą grup rozmównych i regulacją głośności. Źródło: Sepura, *IP67 Ultra Controller Speaker Microphone (Ultra CSM)*, https://sepura.com/accessories/ip67-ultra-controller-speaker-microphone/ [dostęp: 1.10.2025 r.].

Praktyczne zastosowania w służbach mundurowych

Wsparcie operacyjne i szybka reakcja

Radiotelefony przenośne Sepura, dzięki swojej wielofunkcyjności i odporności na ekstremalne warunki, stanowią kluczowy element w operacjach ratowniczych. Funkcjonariusze wyposażeni w urządzenia serii SCG22, SC20 i SC21 mogą korzystać z natychmiastowego połączenia głosowego oraz transmisji danych.

Integracja systemów i akcesoriów

Kompleksowa oferta akcesoriów – od anten przez systemy ładowania po zaawansowane zestawy audio – umożliwia tworzenie spójnych sieci komunikacyjnych. Łatwość integracji z systemami zarządzania operacyjnego pozwala na bieżąco monitorować stan radiotelefonów oraz zarządzać zasobami w czasie rzeczywistym. Dzięki temu operacje służb mundurowych są nie tylko bardziej efektywne, ale także bezpieczniejsze.
W wielu testach potwierdzono pełną kompatybilność radiotelefonów SEPURA z używanym w polskiej Policji systemem TETRA oraz istniejącymi radiotelefonami, co czyni je ciekawą alternatywą dla obecnie użytkowanych urządzeń.

Szkolenia i wymiana doświadczeń

Warsztaty w Uniejowie nie tylko były okazją do zapoznania się z nowoczesnymi urządzeniami – stały się również miejscem, gdzie różne służby mogły podzielić się swoimi doświadczeniami. Podczas interaktywnych sesji szkoleniowych uczestnicy mieli szansę przetestować sprzęt w warunkach symulujących prawdziwe sytuacje, co pomogło im określić najlepsze sposoby działania. Profesjonalne prezentacje ekspertów firmy Sepura dostarczyły praktycznej wiedzy technicznej, którą można od razu wykorzystać w codziennej pracy funkcjonariuszy.

Perspektywy rozwoju technologicznego

Innowacje w radiokomunikacji

Prezentowane modele radiotelefonów są dowodem na dynamiczny rozwój technologii komunikacyjnych w sektorze bezpieczeństwa. Firma Sepura konsekwentnie inwestuje w rozwój urządzeń, które odpowiadają na rosnące potrzeby operacyjne służb mundurowych. Wielofunkcyjność urzą-

Fot. 15 Radiotelefon Sepura. Źródło: Sepura TETRA Hand-portable Radios Equipped By The Dutch Royal Military Police, https://sepura.com/case-studies/dutch-royal-military-police/ [dostęp: 1.10.2025 r.].

dzeń, możliwość integracji z najnowszymi akcesoriami oraz zastosowanie zaawansowanych technologii ochronnych (jak IP68 czy Water Porting) otwierają nowe perspektywy dla skutecznej komunikacji w sytuacjach kryzysowych.

Zastosowania w nowych scenariuszach operacyjnych

Wraz z rozwojem technologii radiotelefonów wzrasta także rola systemów łączności w nowoczesnych operacjach ratowniczych. Integracja radiotelefonów z systemami IT, zastosowanie zaawansowanych algorytmów do zarządzania siecią komunikacyjną oraz możliwość programowania funkcji urządzeń stwarzają nowe możliwości. Przyszłość radiokomunikacji opiera się na elastyczności i adaptacyjności systemów, co umożliwi jeszcze lepsze reagowanie na dynamiczne zagrożenia.

Wpływ na efektywność i bezpieczeństwo

Inwestycje w nowoczesne systemy komunikacyjne bezpośrednio przyczyniają się do zwiększenia efektywności operacyjnej. Umożliwiają one szybszą reakcję, lepszą koordynację działań oraz stały monitoring w czasie rzeczywistym, co ogranicza ryzyko wystąpienia błędów i podnosi poziom bezpieczeństwa zarówno funkcjonariuszy, jak i obywateli. Dzięki zaawansowanym radiotelefonom Sepura służby mundurowe dysponują narzędziami kluczowymi do skutecznego zarządzania sytuacjami kryzysowymi.

Podsumowanie i wnioski – kompleksowy obraz nowoczesnej łączności

Podsumowując, należy stwierdzić, że warsztaty w Uniejowie były doskonałą okazją do zapoznania się z szeroką gamą radiotelefonów przenośnych, w tym modeli SEPURA SCL3, a także urządzeń z serii STP, SC20 i SC21. Zaprezentowane modele wyróżniają się nie tylko funkcjonalnością, ale również zdolnością do pracy w ekstremalnych warunkach – od niskich temperatur po intensywne upały, od pyłu po wilgoć. Liczne nowoczesne rozwiązania techniczne, takie jak kolorowe oznaczenia anten, unikalne interfejsy złączy czy zaawansowane systemy ładowania, świadczą o wysokim stopniu zaawansowania technologicznego tych urządzeń.

Rozwój technologii radiokomunikacyjnych zapowiada kolejne innowacje, które jeszcze bardziej usprawnią pracę służb mundurowych. Inwestycje w nowoczesne systemy łączności to nie tylko kwestia techniczna, ale przede wszystkim strategiczny krok w kierunku zwiększenia sprawności przeprowadzania interwencji policyjnych i poprawy bezpieczeństwa publicznego.

Artykuł został opracowany na podstawie materiałów udostępnionych przez firmy Covertech i Sepura oraz dokumentacji technicznej akcesoriów do radiotelefonów serii STP/SC2.

[1] Zarządzenie nr 22 Komendanta Głównego Policji z dnia 14 lipca 2020 r. w sprawie określenia metod i form wykonywania zadań Policji z użyciem środków łączności radiowej § 1 (Dz. Urz. KGP poz. 38, z późn. zm.).
[2] Tamże, § 1.
[3] Tamże, § 1.
[4] Tamże, § 1.
[5] Sepura, *The next generation of mission-critical devices*, https://sepura.com/devices/scl3-4g-radio/ [dostęp: 1.10.2025 r.].
[6] Sepura, Sepura Celebrates Double Award Win ICCA Awards 2025 https://sepura.com/news/sepura-celebrates-double-award-win-at-the-icca-awards-2025/ [dostęp: 1.10.2025 r.].
[7] Sepura, *Biuletyn produktowy. Akcesoria do serii STP i SC2*, wydanie 1.4a, s. 9.
[8] Tamże, s. 9.
[9] Sepura, *Biuletyn produktowy. Akcesoria do serii STP i SC2*, wydanie 1.4a, s. 7.
[10] Sepura, SC20 HAND-POR TABLE RADIO https://sepura.com/wp-content/uploads/2024/06/0064_0622_V18-SC20-brochure_ONLINE.pdf [dostęp: 1.10.2025 r.].
[11] Sepura, TETRA, Hybrid and 4G/5G hand-portable radios https://sepura.com/hand-portable-radios/ [dostęp: 1.10.2025 r.].
[12] https://sepura.com/wp-content/uploads/2024/06/0064_0622_V18-SC20-brochure_ONLINE.pdf [dostęp: 1.10.2025 r.].
[13] Sepura, *Biuletyn produktowy. Akcesoria do serii STP i SC2*, wydanie 1.4a, s.13.
[14] Tamże, s. 12.

Summary

Radio communications in the Police. Basics, procedures, and technologies

The article highlights the fundamental role of radio communication in the Polish Police, essential for operational efficiency, coordination, and officer safety. It reviews the legal framework for training and procedures, including the use of DMR and TETRA radios, and explains the organization of different communication networks such as dispatch, operational, and tactical systems. Training at the Police Training Centre in Legionowo ensures that officers master standardized communication, message protocols, and cooperation under stress.

A key part of the article reports on the SEPURA workshops in Uniejów (March 2025), where Police and Fire Service representatives tested advanced TETRA devices such as the SEPURA SCL3, SC20/21, and SCG22. These radios combine reliability, multifunctionality, and extreme durability, with features like detachable TETRA modules, advanced audio technology, and full compatibility with existing systems. Practical exercises and stress tests confirmed their effectiveness in challenging conditions.

The article concludes that continuous investment in modern communication systems, together with systematic training, is vital for improving operational readiness and public safety.

Tłumaczenie: Autorzy

Przygotowanie i zlecenie

ZABÓJSTWA

podkom. Jarosław Bakuła

Zakład Kryminalny CSP

W polskim systemie karnym obowiązuje prawo stanowione. Kompetentne organy państwa tworzą prawo w określonej formie i trybie, a jego realizacja jest zabezpieczona sankcją przymusu państwowego. Podstawową zasadą jest, że akty normatywne muszą być zgodne z ustawą zasadniczą – Konstytucją Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. Na straży zgodności tworzonego prawa z ustawą zasadniczą stoi Trybunał Konstytucyjny.

Od 1 października 2023 r. w ustawie z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2025 r. poz. 383, z późn. zm.), zwanej dalej: „k.k.", obowiązują przepisy, które po raz pierwszy w historii tej kodyfikacji penalizują samo przygotowanie do zabójstwa (art. 148 § 5 k.k.) oraz przyjęcie zlecenia zabójstwa (148a § 1 k.k.). Wcześniej karalne było jedynie usiłowanie lub dokonanie zabójstwa, natomiast czynności przygotowawcze oraz przyjęcie zlecenia zabójstwa pozostawały bezkarne.

Jedną z podstawowych funkcji prawa karnego jest ochrona życia ludzkiego. W polskim systemie prawnym dobro to zostało objęte szczególną ochroną zarówno na gruncie Konstytucji Rzeczypospolitej Polskiej, jak i przepisów Kodeksu karnego. Zabójstwo, określone w art. 148 k.k., należy do najcięższych przestępstw przeciwko życiu i zdrowiu. Rozwój przestępczości zorganizowanej oraz coraz częstsze przypadki tzw. zabójstw na zlecenie doprowadziły jednak do potrzeby rozszerzenia zakresu odpowiedzialności karnej także na wcześniejsze stadia działalności przestępczej.

W odpowiedzi na te zagrożenia ustawodawca zdecydował się na penalizację przygotowania do zabójstwa oraz przyjęcia zlecenia zabójstwa. Zmiany te miały na celu umożliwienie organom ścigania skuteczniejszej reakcji jeszcze przed dokonaniem czynu lub wejściem sprawcy w fazę usiłowania.

Celem niniejszego artykułu jest analiza regulacji dotyczących odpowiedzialności za przygotowanie do zabójstwa oraz przyjęcie zlecenia zabójstwa, a także ocena ich znaczenia dla praktyki wymiaru sprawiedliwości.

W trakcie pełnienia służby jako policjant wydziału dochodzeniowo-śledczego przed wejściem w życie przepisów dotyczących odpowiedzialności karnej za przygotowanie do zabójstwa i za przyjęcie zlecenia zabójstwa uczestniczyłem w czynnościach służbowych w sprawie, gdzie – według ustaleń – dwóch sprawców przyjęło zlecenie pozbawienia życia ustalonego mężczyzny. Z uwagi na brak penalizacji przygotowania do zabójstwa i zlecenia zabójstwa, na podstawie art. 308 § 1 k.p.k.[1], wykonane zostały czynności procesowe mające na celu zatrzymanie nielegalnie posiadanej broni palnej, będącej w dyspozycji domniemanych współsprawców. Czynności niecierpiące zwłoki zostały wykonane, ponieważ istniało podejrzenia popełnienia przestępstwa stypizowanego w art. 263 § 2 k.k.

W art. 148 k.k., w rozdziale XIX, ustawodawca rodzajowym przedmiotem ochrony objął najcenniejsze dobro – życie i zdrowie.

Art. 148 § 1. Kto zabija człowieka, podlega karze pozbawienia wolności na czas nie krótszy od lat 10 albo karze dożywotniego pozbawienia wolności.

§ 2. Kto zabija człowieka:
1) ze szczególnym okrucieństwem,
2) w związku z wzięciem zakładnika, zgwałceniem albo rozbojem,
3) w wyniku motywacji zasługującej na szczególne potępienie,
4) z użyciem materiałów wybuchowych,

podlega karze pozbawienia wolności na czas nie krótszy od lat 15 albo karze dożywotniego pozbawienia wolności.

§ 3. Karze określonej w § 2 podlega, kto jednym czynem zabija więcej niż jedną osobę lub był wcześniej prawomocnie skazany za zabójstwo oraz sprawca zabójstwa funkcjonariusza publicznego popełnionego podczas lub w związku z pełnieniem przez niego obowiązków służbowych związanych z ochroną bezpieczeństwa ludzi lub ochroną bezpieczeństwa lub porządku publicznego.

§ 4. Kto zabija człowieka pod wpływem silnego wzburzenia usprawiedliwionego okolicznościami, podlega karze pozbawienia wolności od roku do lat 10.

§ 5. Kto czyni przygotowania do przestępstwa określonego w § 1, 2 lub 3, podlega karze pozbawienia wolności od lat 2 do 15.

Art. 148a § 1. Kto przyjmuje zlecenie zabójstwa człowieka w zamian za udzieloną lub obiecaną korzyść majątkową lub osobistą, podlega karze pozbawienia wolności od lat 2 do 15.

Zabójstwem jest umyślne pozbawienie człowieka życia. Zachowanie się sprawcy polega głównie na określonym działaniu (np. na zadaniu ciosu nożem, podaniu trucizny). Wyjątkowo można tej zbrodni dopuścić się przez zaniechanie, ale tylko wówczas, gdy na sprawcy ciąży prawny obowiązek określonego działania (np. matka umyślnie zaniechała karmienia noworodka, dotyczy to najbliższego członka rodziny, lekarza, ratownika). Obowiązek ten musi wynikać z uregulowań prawnych i nadto musi być szczególny. Nie jest nim obowiązek udzielenia pomocy, którego naruszenie jest zagrożone karą z art. 162 § 1 kk.

Zabójstwo jest przestępstwem skutkowym (materialnym) – do jego znamion należy skutek w postaci śmierci człowieka.

Zgon pokrzywdzonego (art. 49 § 1 k.p.k.[2]) nie musi nastąpić natychmiast po działaniu sprawcy, ale istotne jest ustalenie związku przyczynowo-skutkowego między zachowaniem a skutkiem.

Śmierć w art. 148 k.k. to według ekspertów prawa karnego śmierć mózgowa – nieodwracalne ustanie funkcji pnia mózgu. W przypadku gdy na przykład na skutek udzielonej pomocy pokrzywdzonemu nastąpi przywrócenie ofiary ze stanu śmierci klinicznej do życia, to sprawca może odpowiadać za usiłowanie zabójstwa.

Podmiotem przestępstwa zabójstwa może być każda osoba zdolna do ponoszenia odpowiedzialności karnej. Zdolność tę określa wiek sprawcy (określony w art. 10 § 1–4 k.k.) i poczytalność (art. 31 § 1–3 k.k.).

Przestępstwo zabójstwa można popełnić umyślnie w zamiarze bezpośrednim i ewentualnym (art. 9 § 1 k.k.).

Zachowania opisane w § 1, 2 i 3 art. 148 k.k. stanowią zbrodnię (art. 7 § 2 k.k.), a opisane w § 4 – stanowią występek (art. 7 § 3 k.k.) i wszystkie są ścigane z urzędu.

W art. 148 § 1 k.k. ustawodawca opisał typ podstawowy zabójstwa, w § 2 i § 3 – typy kwalifikowane, a w § 4 – typ uprzywilejowany – zabójstwo w afekcie.

Szczególne okrucieństwo oznacza, że sprawca nie ogranicza się do zadania śmiertelnego ciosu, lecz działa w sposób szczególnie drastyczny i brutalny, np. stosując wobec ofiary tortury, dręczenie, zadając dodatkowe cierpienia i upokorzenia, skazując na powolną śmierć.

Zabójstwo w związku z wzięciem zakładnika, zgwałceniem albo rozbojem jest środkiem do osiągnięcia celu, jakim jest np. wzięcie zakładnika albo rozbój. Popełnienie zabójstwa służy zatarciu śladów popełnionego wcześniej: rozboju, zgwałcenia, wzięcia zakładnika. Sprawca jednym czynem wyczerpuje znamiona zabójstwa i np. rozboju.

Motywacja zasługująca na szczególne potępienie to: niechęć do innego człowieka, nienawiść ze względów rasowych, narodowościowych, religijnych, chęć zysku, chęć zaspokojenia popędu płciowego, pobudki chuligańskie. Motyw zasługujący na szczególne potępienie dotyczy na przykład zabójstwa zaplanowanego, na zlecenie, z zemsty, w celu zagarnięcia majątku, dla zaspokojenia żądzy mordu.

Jeżeli do dokonania zabójstwa sprawca używa materiałów wybuchowych, to stanowią one narzędzie zbrodni. Według praktyków i orzeczników prawa poprzez użycie materiałów wybuchowych należy rozumieć posłużenie się nimi zgodnie z ich przeznaczeniem, choćby było ono nieskuteczne. Natomiast samo zademonstrowanie posiadanego przedmiotu w postaci materiałów wybuchowych nie będzie tożsame z ich użyciem.

Znamionami kwalifikującymi są również: zabicie jednym czynem więcej niż jednej osoby; fakt, iż sprawca był wcześniej prawomocnie skazany za zabójstwo; zabójstwo funkcjonariusza publicznego popełnionego podczas lub w związku z pełnieniem przez niego obowiązków służbowych związanych z ochroną bezpieczeństwa ludzi lub ochroną bezpieczeństwa lub porządku publicznego. Nowelizacja prawa karnego w zakresie karalności zabójstwa funkcjonariusza publicznego (typ kwalifikowany) weszła w życie 22 marca 2011 r. Nowy typ kwalifikowany – zabójstwo funkcjonariusza publicznego – został wprowadzony przez prawodawcę po zabójstwie podkomisarza Andrzeja Struja, polskiego policjanta z Wydziału Wywiadowczo-Patrolowego Komendy Stołecznej Policji (zabójstwa popełnionego w dniu 10 lutego 2010 r. w Warszawie).

Znamię „sprawca był wcześniej prawomocnie skazany za zabójstwo" dotyczy osoby, która kiedykolwiek w przeszłości została skazana prawomocnie za zabójstwo, ale nie nastąpiło jeszcze zatarcie skazania, np. sprawca w trakcie odbywania kary pozbawienia wolności za zabójstwo zabija współwięźnia lub dokonuje zabójstwa po opuszczeniu zakładu karnego.

Silne wzburzenie usprawiedliwione okolicznościami – chodzi w tym przypadku o stan psychiczny sprawcy, w którym jego przeżycia emocjonalne (silne, krótkotrwałe wzruszenie, np. gniew, przerażenie, odruch protestu, sprzeciw) górują nad sprawnością intelektualną. Stan silnego wzburzenia może być efektem długotrwałego narastania negatywnych emocji zakończonego nagłym wybuchem prowadzącym do zabójstwa, wywołanego nawet nieadekwatną, pozornie błahą przyczyną. Okolicznościami, które przyczyniają się do takiego wzburzenia, mogą być: ciężka obelga, znęcanie się, zdrada małżeńska. Dokonując oceny zachowania sprawcy jako przestępstwa zabójstwa w typie uprzywilejowanym, organ orzekający musi wykazać, że oba ww. warunki, tj. silne wzburzenie i szczególne okoliczności, wystąpiły łącznie.

Aby właściwie opisać ustawowe znamiona ujęte w nowym przepisie, tj. w art. 148 § 5 k.k., należy wskazać, że zgodnie z art. 16 § 1 k.k. przygotowanie zachodzi wtedy, gdy sprawca w celu popełnienia czynu zabronionego podejmuje czynności mające stworzyć warunki do jego dokonania, w szczególności wchodzi w porozumienie z inną osobą, uzyskuje środki, zbiera informacje lub sporządza plan działania. Przygotowanie jest więc najwcześniejszym stadium realizacji przestępstwa.

Polski ustawodawca przyjął zasadę, zgodnie z którą przygotowanie jest karalne jedynie wtedy, gdy ustawa wyraźnie tak stanowi (art. 16 § 2 k.k.). Wynika to z przekonania, że na tym etapie zagrożenie dla dobra prawnego ma jeszcze charakter potencjalny. Tradycyjnie karalność przygotowania przewidywano wyłącznie wobec szczególnie niebezpiecznych przestępstw, takich jak zamach stanu czy fałszowanie pieniędzy. Przygotowanie jest również karalne w odniesieniu do czynności poprzedzających handel ludźmi, podrabianie dokumentów lub posługiwanie się podrobionym dokumentem.

Przez wiele lat przygotowanie do zabójstwa nie było jednak odrębnie penalizowane. Odpowiedzialność karna mogła powstać dopiero na etapie usiłowania, a więc wtedy, gdy sprawca bezpośrednio zmierzał do dokonania czynu zabronionego. W praktyce prowadziło to do sytuacji, w których organy ścigania posiadały informacje o planowanym zabójstwie, lecz nie miały wystarczających podstaw prawnych do podjęcia działań represyjnych.

Żadna wcześniejsza polska kodyfikacja karna nie przewidywała karalności przygotowania do zabójstwa.

„Wśród powodów braku penalizacji przygotowania do zabójstwa zwraca się uwagę zwłaszcza na trudności natury dowodowej związane z bezspornym wykazaniem realizacji strony podmiotowej takiego czynu. Czynności przygotowawcze do zamachu na życie z reguły nie pozwalają na jednoznaczne i niewątpliwe ustalenie, że zostały podjęte z zamiarem bezpośrednim zorientowanym na skutek śmiertelny. W większości takich wypadków bardzo trudno wskazać – lub jest to niemożliwe – że osoba, podejmując określone działania, czyni przygotowanie do zbrodni zabójstwa. Jak dosadnie trudność tę ilustruje M. Małecki, chodzi o to, że z reguły niepodobna ustalić, czy sprawca »kupuje nóż po to, by pokroić chleb, czy po to, by pokroić sąsiada« (M. Małecki, *Przygotowanie*, s. 21–22)" (*Kodeks karny. Komentarz*, red. R.A. Stefański, Warszawa 2023, 6. wydanie, s. 977).

Według autorytetów prawa brak karalności przygotowania do zabójstwa ogranicza zakres ochrony najważniejszych dóbr przed zamachami na te dobra. Brak karalności przygotowania do zbrodni zabójstwa jest często interpretowana jako „swoista niekompetencja ustawodawcy", wynikająca jedynie z powodów trudności udowodnienia przygotowania do zbrodni zabójstwa.

W znowelizowanej ustawie karalne jest przygotowanie do zbrodni zabójstwa określonych w art. 148 § 1–3 k.k.

Dokonując analizy ustawowych znamion czynu zabronionego opisanego w art. 148 § 5 k.k., należy stwierdzić, że podmiot jest powszechny, to jest sprawcą może być każda osoba zdolna ponosić odpowiedzialność karną (osoba, która ukończyła 17 lat i jest poczytalna). Odpowiedzialności na podstawie art. 148 § 5 k.k. nie poniesie sprawca nieletni, o którym mowa w art. 10 § 2 k.k.[3]

Jeżeli chodzi o stronę podmiotową – stosunek sprawcy do czynu – to mamy do czynienia z zamiarem bezpośrednim kierunkowym (zamiar bezpośredni o szczególnym zabarwieniu – *dolus coloratus*). Sprawca – zgodnie z ogólną formułą art. 16 § 1 k.k. – „w celu popełnienia czynu zabronionego", w tym wypadku zabójstwa w jednej ze wskazanych w przepisie postaci, podejmuje czynności mające stworzyć warunki do przedsięwzięcia czynu zmierzającego bezpośrednio do jego dokonania[4].

Po stronie organów ścigania na etapie postępowania przygotowawczego oraz po stronie sądu na etapie postępowania jurysdykcyjnego leży obowiązek wykazania, że działania, które podjął sprawca, zmierzały do dokonania.

Do strony przedmiotowej zaliczamy każde zachowanie sprawcy stwarzające warunki do usiłowania popełnienia, a w szczególności, jak to wynika z art. 16 § 1 k.k., wejście w porozumienie z inną osobą lub osobami, mające na celu popełnienie zabójstwa, uzyskiwanie lub przysposabianie środków mających służyć jego popełnieniu oraz zbieranie informacji lub sporządzanie planu działania mające stworzyć warunki do wejścia w fazę usiłowania tego czynu.

Należy pamiętać, że niekaralnym etapem czynu zabronionego popełnionego umyślnie jest zamiar sprawcy. Nie ma mowy o odpowiedzialności karnej sprawcy w przypadku, gdy przygotowuje się on mentalnie lub fizycznie do zabójstwa. Ten etap nie wszedł faktycznie w etap przygotowania.

Przygotowanie zabójstwa jest przestępstwem publiczno-skargowym, ściganym z urzędu.

Na ogólnych zasadach wynikających z art. 17 § 1 k.k. nie podlega karze za przygotowanie do zabójstwa ten, kto dobrowolnie od niego odstąpił, a w szczególności zniszczył przygotowane środki lub zapobiegł skorzystaniu z nich w przyszłości, a w razie przygotowania w postaci wejścia w porozumienie z inną osobą w celu jego popełnienia, kto nadto podjął istotne starania zmierzające do zapobieżenia dokonaniu[5].

Przyjęcie zlecenia zabójstwa

Art. 148a k.k. [Przyjęcie zlecenia zabójstwa]
§ 1.
Kto przyjmuje zlecenie zabójstwa człowieka w zamian za udzieloną lub obiecaną korzyść majątkową lub osobistą, podlega karze pozbawienia wolności od lat 2 do 15.

§ 2.
Nie podlega karze za przestępstwo określone w § 1, kto przed wszczęciem postępowania karnego ujawnił wobec organu powołanego do ścigania przestępstw osobę lub osoby zlecające zabójstwo oraz istotne okoliczności popełnionego czynu.

Polskie prawo karne w sposób szczególny piętnuje zachowania godzące w ludzkie życie. Jedną z najbardziej drastycznych form przestępczości przeciwko życiu jest zabójstwo na zlecenie (tzw. morderstwo kontraktowe). W tradycyjnym ujęciu proces ten angażuje co najmniej dwa podmioty: zlecającego (mandanta) oraz wykonawcę (mandatariusza).
Samo dokonanie zabójstwa w wyniku motywacji zasługującej na szczególne potępienie – a za taką powszechnie uznaje się chęć osiągnięcia korzyści majątkowej (działanie „za pieniądze") – stanowi zbrodnię zagrożoną najsurowszymi karami[6]. Zgodnie z art. 148 § 2 pkt 3 k.k., kto zabija człowieka w wyniku motywacji zasługującej na szczególne potępienie, podlega karze pozbawienia wolności na czas nie krótszy od lat 15 albo karze dożywotniego pozbawienia wolności.
Dla bytu przestępstwa stypizowanego w art. 148a konieczne jest istnienie co najmniej dwóch sprawców (tzw. współsprawstwo konieczne).
Dokonując analizy strony podmiotowej, możemy wykazać zlecającego, który odpowiada za podżeganie do zabójstwa. Podżegaczem jest ten, kto chcąc, aby inna osoba dokonała czynu zabronionego, nakłania ją do tego (art. 18 § 2 k.k.)[7].
Przyjmujący zlecenie zabójstwa z chwilą faktycznego wykonania czynu staje się sprawcą (lub współsprawcą) zabójstwa kwalifikowanego[8].
Odpowiedzialność przyjmującego zlecenie na wczesnym etapie zależy od jego zachowania. Gdy po przyjęciu zlecenia sprawca podejmuje czynności przygotowawcze (np. kupuje broń, obserwuje ofiarę), odpowie za przygotowanie do zabójstwa (art. 148 § 5 k.k.).
W praktyce organów ścigania zdarzają się sytuacje, w których „zleceniobiorcą" okazuje się działający pod przykryciem funkcjonariusz Policji (operacja specjalna). W takim scenariuszu zlecający odpowiada w pełni za podżeganie, nawet jeśli realizacja zamachu od początku była niemożliwa ze względu na brak intencji ze strony policjanta[9]. Z kolei w sytuacji, gdy przestępca przyjmie zaliczkę, ale od początku zamierza jedynie oszukać zlecającego i nie ma zamiaru nikogo zabijać, jego czyn kwalifikuje się jako oszustwo (art. 286 k.k.), a nie przygotowanie do zabójstwa[10] lub przyjęcie jego zlecenia.
W przypadku gdy sprawca wcześniej przyjął zlecenie zabójstwa, a następnie zrealizował ustawowe znamiona czynów określonych w art. 148 § 1–3 k.k., będziemy mieli do czynienia z tzw. pozornym zbiegiem przestępstw, a sprawca odpowie za dokonanie zabójstwa. Należy pamiętać, że nie podlegają ukaraniu współukarane czyny uprzednie i następcze.
W art. 148a § 2 k.k. ustawodawca wprowadził klauzulę niekaralności. Przyjmujący zlecenie zabójstwa człowieka przed wszczęciem postępowania karnego może ujawnić wobec organu powołanego do ścigania przestępstw osobę lub osoby zlecające zabójstwo oraz istotne okoliczności popełnionego czynu. Spełnienie tych warunków sprawia, że zachowanie sprawcy, mimo że narusza normę sankcjonowaną w art. 148a § 1 k.k., nie aktualizuje normy sankcjonującej wynikającej z tego przepisu[11], gdyż wyklucza się on skutecznym czynnym żalem.
Podsumowując analizę zmian, które ustawodawca wprowadził do Kodeksu karnego poprzez dodanie art. 148 § 5 k.k. (przygotowanie do zabójstwa) oraz art. 148a § 1 k.k. (przyjęcie zlecenia zabójstwa) należy stwierdzić, że nowe przepisy przyczyniają się do zwiększenia ochrony życia i zdrowia ludzi. Organy powołane do ochrony bezpieczeństwa publicznego mogą zapobiegać popełnianiu zbrodni zabójstwa i ścigać sprawców opisanych czynów zabronionych już na etapie czynności poprzedzających skutek ww. czynu. Nadto trzeba zaznaczyć, że ostatecznej oceny prawnokarnej danego zdarzenia dokonuje sąd, który jest niezależny i niezawisły. Penalizacja przygotowania do zabójstwa i przyjęcia zlecenia zabójstwa uzupełniła istotny brak w zbiorze norm prawnych.

[1] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2026 r. poz. 490, z późn. zm.).
[2] Tamże.
[3] *Kodeks karny. Komentarz*, red. R.A. Stefański, Warszawa 2023, 6. wydanie, s. 978 (192).
[4] Tamże, s. 978 (193).
[5] Tamże, s. 980 (202).
[6] A. Marek, *Prawo karne. Zagadnienia teorii i praktyki*, Warszawa 2021, s. 342.
[7] Tamże.
[8] Wyrok Sądu Najwyższego z dnia 12 kwietnia 2018 r., sygn. akt II AKa 45/18, Biuletyn SN.
[9] Postanowienie Sądu Najwyższego z dnia 23 listopada 2022 r., sygn. akt V KK 112/22, LEX nr 351234.
[10] Wyrok Sądu Apelacyjnego w Katowicach z dnia 8 września 2016 r., sygn. akt II AKa 210/16, KZS 2017, z. 1, poz. 45.
[11] *Kodeks karny. Komentarz*, s. 989 (20).

Summary

Preparation for murder and contract killing

The article discusses the offence of murder under Article 148 of the Criminal Code of 6 June 1997 and examines the amendments introduced to this provision. Particular attention is paid to the changes that entered into force on 1 October 2023, introducing Article 148 § 5 on preparation for murder and Article 148a concerning contract killing. The author highlights how these new provisions strengthen the protection of human life and health by enabling law enforcement agencies to intervene at an earlier stage and prosecute offenders before a murder is committed.

Tłumaczenie: Joanna Łaszyn

ZGWAŁCENIE

jako przestępstwo implikujące konsekwencje na płaszczyźnie kryminologii, socjologii i psychologii

asp szt. Beata Spinek

Zakład Ruchu Drogowego CSP

Przestępstwo zgwałcenia pozostaje jednym z najpoważniejszych naruszeń wolności seksualnej człowieka oraz podstawowych praw jednostki. Jego konsekwencje wykraczają daleko poza wymiar prawny, obejmując długotrwałe skutki psychologiczne, społeczne oraz kryminologiczne. Zjawisko to stanowi istotny problem społeczny, który wymaga analizy w perspektywie interdyscyplinarnej. Niniejszy artykuł podejmuje próbę kompleksowego omówienia przestępstwa zgwałcenia w ujęciu kryminologicznym, socjologicznym i psychologicznym, ukazując jego definicję, uwarunkowania, skalę występowania oraz konsekwencje dla ofiar i funkcjonowania społeczeństwa.

DEFINICJA ZGWAŁCENIA

Terminy „gwałt", „zgwałcenie" od lat sprawiają niemałe problemy natury interpretacyjnej i semantycznej. Historycznie oba pojęcia zaczynają pojawiać się dopiero u schyłku I Rzeczypospolitej, kiedy to zmienia się rzeczywistość historyczna, a wraz z nią funkcjonowanie języka polskiego. Rozbiory wywołały całkowitą destrukcję administracyjną Polski, co wpłynęło również na system prawa, a także na terminologię prawniczą. Mimo funkcjonowania różnych określeń, typu: „usilstwo", „*violentia*", „*Oppresio feminae*", „*Stuprum*", „rapt" czy „raptus"[1], w aktach prawnych z tego okresu najczęściej napotykamy termin „zgwałcenie", chociaż oficjalne tłumaczenie, które odnajdujemy w dokumentach, prezentuje się odmiennie: „gwałtowne porubstwo" (austriacki Kodeks karny z 1787 r., tzw. Józefina – od cesarza Józefa II), „porubstwo" (Kodeks z 1803 r., tzw. Franciszkana – od cesarza Franciszka II)[2].

W powszechnym rozumieniu terminów „gwałt", „zgwałcenie" nie dostrzegamy wielkiej różnicy semantycznej. Synonimiczne stosowanie tych pojęć jest wynikiem oddziaływania mass mediów – telewizji, prasy czy internetu. W ten sposób traktujemy je mocno powierzchownie, mniej wnikliwie i przede wszystkim nienależycie, jedynie jako formę przestępczości seksualnej podlegającą określonej karze. Tymczasem język prawniczy przewiduje dla nich inne znaczenia, które należałoby wydobyć za pomocą metod historyczno-porównawczej oraz dogmatyczno-prawnej[3]. Jednakże nie jest moją intencją rozstrzyganie kwestii właściwego znaczenia konkretnych terminów, ale zwrócenie uwagi na implikacje przestępstwa zgwałcenia, które rozumiane jest następująco:

> Zgwałcenie jest najczęściej spotykaną formą przestępczości seksualnej podlegającej karze. W myśl art. 197 Kodeksu karnego, który charakteryzuje to przestępstwo jako doprowadzenie innej osoby do obcowania płciowego przemocą, groźbą bezprawną, podstępem lub w inny sposób mimo braku jej zgody, a także doprowadzenie innej osoby do poddania się innej czynności seksualnej albo wykonania takiej czynności.

Sama definicja ustawowa nie precyzuje w pełni zakresu pojęcia zgwałcenia ani nie rozstrzyga wszystkich wątpliwości interpretacyjnych związanych z kwalifikacją tego czynu. W związku z tym konieczne jest odwołanie się do dorobku doktryny prawa karnego oraz orzecznictwa sądowego, które doprecyzowują znaczenie użytych w przepisie terminów oraz określają granice odpowiedzialności karnej.
Zgwałcenie następuje, gdy (...) narządy płciowe jednego z uczestników aktu są wprowadzone do ciała innego uczestnika (kontakt genitalno-genitalny, genitalno-oralny, genitalno-analny). Za inne czynności seksualne natomiast uważa się każdą formę kontaktu cielesnego uczestników mającą charakter seksualny (obmacywanie ofiar, zmuszanie do masturbacji)[4].
Należy przy tym pamiętać, że termin ten nie obejmuje zachowań, które przebiegają bezdotykowo. Nie są one traktowane jako kategoria zgwałcenia. Natomiast każde działanie mające na celu zaspokojenie potrzeb seksualnych bez wyraźnej zgody drugiej osoby, obejmujące jakiekolwiek czynności bezpośredniego kontaktu, a więc dotykanie części intymnych, są interpretowane jako przestępstwo. W przypadku niepożądanych działań penetracyjnych (z wykorzystaniem ust i odbytu) mówimy o zgwałceniu odnoszącym się zarówno do kobiet, jak również mężczyzn[5].

ETIOLOGIA ZGWAŁCEŃ

Najpopularniejsza typologia zgwałceń, opierająca się w dużej mierze na motywacji przestępcy, została przygotowana przez J. Godlewskiego i prezentuje się następująco:
1. Gwałty motywowane potrzebą dominacji i kontroli:
   – władcze, gdzie sprawca oczekuje na okazanie uznania, szacunku przez ofiarę; celem gwałtu jest uspokojenie własnej niepewności, niezaradności;
   – gniewne, motywacją jest odwet za krzywdy doznane od innej kobiety;
   – represyjne, motywacją jest potrzeba ukarania ofiary.
2. Gwałty motywowane seksualnie, niespecyficzne bądź kombinowane, gdzie motywacją jest uzyskanie satysfakcji seksualnej.
3. Gwałty motywowane seksualnie:
   – sytuacyjne, motywacją jest zaspokojenie popędu seksualnego przy błędnej interpretacji zachowania ofiary;
   – instrumentalne, wiążące się z innymi dewiacjami;
   – sadystyczne, motywacją jest zaspokojenie potrzeby seksualnej, poczucie władania i dysponowania ciałem ofiary.
4. Gwałty dewiacyjne, aktywność seksualna sprawcy wynika z zaburzeń seksualności[6].

Typologia Godlewskiego z czasem wymagała znacznego poszerzenia o przestępstwa seksualne, które nie mieściły się w ramach usankcjonowanych w 1987 r. Szczególną uwagę zwróciły na siebie dwa przestępstwa seksualne: zgwałcenie pedofilskie i kazirodcze. Pojawienie się tych dwóch typów jest wynikiem oczywiście nowelizacji Kodeksu karnego z 5 listopada 2009 r., która poszerzyła krąg tematyczny o ofiary małoletnie poniżej 15. roku życia i najbliższe otoczenie osób pokrzywdzonych wskutek zgwałcenia[7]. Dokonane zmiany miały na celu rozszerzenie ochrony prawnokarnej osób małoletnich oraz tych, u których doszło do zakłócenia rozwoju psychofizycznego, i polegały one na zaostrzeniu odpowiedzialności sprawców przestępstw seksualnych.
Wyjaśnienia etiologii zgwałceń należy dopatrywać się w teoriach Zygmunta Freuda, a dokładnie w teoriach dotyczących nerwic, które zwróciły uwagę naukowców w kontekście pochodzenia przestępstw seksualnych. W tym ujęciu nerwica jest rozumiana jako negatyw perwersji, a więc rodzi się ze stłumienia. W perwersjach infantylnych seksualność pojawia się świadomie: „Kto doznaje rozkoszy w sytuacji, gdy w stosunku seksualnym przysparza bólu drugiej osobie, ten jest też zdolny samemu smakować ból jako rozkosz – ból zrodzony w relacji seksualnej”[8].
Podobne podejście do przestępstwa seksualnego ma Erich Fromm w *Anatomii ludzkiej destrukcyjności*. Zwraca on uwagę na agresję pozytywną (stanowi napędową rozwoju) oraz negatywną (destrukcyjną). Innymi teoriami odnoszącymi się do tego zagadnienia mogą być: psychologia ego, podejście psychodynamiczne, behawioralne czy wreszcie opierające się na kognitywistyce. Ostatnia z wymienionych teorii opiera się na mitach występujących w kulturze: o męskiej aktywności i pasywności kobiety, wyższej pozycji mężczyzn nad kobietami czy przynależności kobiety do mężczyzny. Do tego dochodzą jeszcze inne, znane nam ze społecznego obiegu, stereotypy dotyczące zarówno sprawcy, jak również ofiary przestępstw na tle seksualnym[9].
Jednym z głównych czynników popychających do przestępstw na tle seksualnym, które są atakiem na wolność jednostki, jest oczywiście alkohol. Motorem działania sprawcy jest zaspokojenie popędu płciowego bez akceptacji ofiary.

MODUS OPERANDI PRZESTĘPSTWA ZGWAŁCENIA

Naukowcy zwracają uwagę na trzy różne sposoby działania sprawcy.
1. Przemoc, przez którą rozumiemy stosowanie czynnej siły fizycznej dla przełamania oporu ofiary. Chodzi tu o przemożną siłę fizyczną. Sprawca może ogłuszyć ofiarę, tym samym z góry udaremnić wszelki opór, a następnie odbyć stosunek cielesny. Może również siłą, przy ciągłym oporze ofiary, doprowadzić do obcowania płciowego. Zatem przemoc może być stosowana różnorakimi środkami i sposobami.
2. Groźba bezprawna, która polega na tym, iż sprawca stawia kobiecie alternatywę, albo się mu odda, albo ją zabije, podpali dom, zrobi krzywdę dziecku czy zawiadomi organy śledcze np. o popełnieniu przez nią przestępstwa (…).
3. Podstęp – najczęściej stosowane formy podstępu to doprowadzenie kobiety do stanu uległości poprzez wprawienie w stan hipnozy, podawanie narkotyków, środków farmakologicznych, ale również wsypywanie środków nasennych np. do herbaty, wlanie alkoholu do kawy. W rezultacie tych i podobnych zabiegów kobieta traci odporność psychiczną i poczucie rzeczywistości (…)[10].

Socjologiczne ujęcie problemu przestępstw seksualnych pozwala chociaż częściowo zwrócić uwagę, kto przyczynia się do podjęcia tak karygodnego czynu i z jaką grupą społeczną jest związany. Wśród sprawców gwałtów dominują osoby z wykształceniem podstawowym (ok. 70%), w wieku od 20–40 lat (ok. 70%), bezrobotni

lub pracujący incydentalnie (63%), stanu wolnego (50%), uprzednio karani (58%) – w tym za przestępstwa seksualne (30%), z problemem alkoholowym lub innymi uzależnieniami (60%) oraz z zaburzeniami osobowości (77%)[11].

ZNAMIONA PRZESTĘPSTWA ZGWAŁCENIA

Po wstępnym zwróceniu uwagi na charakterystykę zjawiska przestępczego, jakim jest zgwałcenie, przejdę do kolejnych zagadnień. Pierwszym z nich jest analiza artykułu 197 Kodeksu karnego na płaszczyźnie prawnokarnej.

Poddając analizie problematykę przestępstwa zgwałcenia sformułowanego przez ustawodawcę w art. 197 k.k., nie sposób pominąć swoistej kwestii osobowej owego czynu. Podmiot przestępstwa stanowi osoba fizyczna, która w chwili dopuszczenia się określonego zachowania ma ukończone 17 lat oraz jest poczytalna, przynajmniej w stopniu ograniczonym[12].

Warto zwrócić uwagę na szczególne odstępstwo od powyżej przedstawionej granicy wieku, które zostało wyrażone w art. 10 § 2 k.k., stanowiącym o możliwości pociągnięcia osoby nieletniej, która ukończyła 15. rok życia, do odpowiedzialności karnej za zgwałcenie:

- w typie podstawowym (art. 197 § 1 k.k.);
- z wykorzystaniem braku możliwości rozpoznania przez ofiarę znaczenia czynu lub pokierowania swoim postępowaniem (art. 197 § 1a k.k.);
- wspólnie z inną osobą, zgwałcenie kazirodcze tudzież zgwałcenie z użyciem broni palnej, noża, innego podobnie niebezpiecznego przedmiotu lub środka obezwładniającego, a także w inny sposób, który bezpośrednio zagraża życiu człowieka, zgwałcenie kobiety ciężarnej, zgwałcenie z utrwaleniem obrazu lub dźwięku z przebiegu czynu (art. 197 § 3 pkt 5 i 6 k.k.);
- osoby małoletniej, osoby dorosłej ze szczególnym okrucieństwem lub zgwałcenie, którego następstwem jest ciężki uszczerbek na zdrowiu (art. 197 § 4 k.k.);
- którego konsekwencję stanowi śmierć ofiary (art. 197 § 5 k.k.)[13].

Przestępstwo zgwałcenia występuje w typie powszechnym, co oznacza, iż każda jednostka zdolna do poniesienia winy za swoje zachowanie, może je popełnić[14]. Wyrażenie *Kto* występujące na początku tejże regulacji prawnej determinuje wyżej wskazany typ czynu zabronionego z art. 197 k.k.

Zdaje się, że ustalenie podmiotu przestępstwa zgwałcenia ma niebotyczne znaczenie w kontekście kwalifikacji prawnej czynu, a zidentyfikowanie sprawcy oraz pociągnięcie go do odpowiedzialności karnej umożliwi ofierze odzyskanie poczucia bezpieczeństwa i stabilizacji egzystencjalnej zszarganych niegodziwym czynem sprawcy.

Poprzez określenie strony podmiotowej należy rozumieć podejście i stosunek sprawcy do czynu w obrębie jego psychiki. Zatem kwalifikując przestępstwo z art. 197 k.k. na kanwie psychicznych powiązań podmiotu z czynem zabronionym, dopuszczenie się zgwałcenia możliwe jest jedynie w wariancie zachowania umyślnego. Oznacza to, że sprawca ma zarówno świadomość, jak i wolę popełnienia czynu, a ustawodawca ogranicza postać zamiaru do jego bezpośredniej wersji[15]. Wydaje się to całkowicie zasadne, gdyż niemożliwe jest jedynie przewidywanie i godzenie się na wykorzystanie jednego z wymienionych w przepisie środków działania oraz doprowadzenie tym samym ofiary do obcowania płciowego – co następuje wedle rozwiązań nakreślonych przez ramy zamiaru ewentualnego.

Ze względu na specyficzne ugruntowanie elementów strony podmiotowej w indywidualnej percepcji sprawcy jej ustalenie zdaje się sprawiać największe problemy interpretacyjne w perspektywie kwalifikacji czynu.

Przedmiotem ochrony jest dobro w wymiarze materialnym lub też niematerialnym pozostające w swoistym zabezpieczeniu, które zostało wytworzone przez przepisy prawne ustanowione przez ustawodawcę[16]. Zatem jest to wartość, której zagrożenie lub naruszenie implikuje konsekwencje przewidziane przez prawo.

Biorąc pod uwagę specyfikę czynu określonego w art. 197 k.k., przedmiotem przestępstwa jest wolność seksualna[17]. Dookreślając – ochronie przez wyżej przytoczony przepis podlega autonomia decydowania o własnym aspekcie seksualnym. Niektóre ze składowych paragrafów art. 197 k.k. stoją również na straży obyczajności[18]. Przypuszczalnie dla większości gorszący będzie akt seksualny wobec osoby spokrewnionej czy też dokonany w stosunku do małoletniego, gdyż wykracza to poza społecznie przyjęte normy moralne, ze względu na dewiacyjny charakter tych czynów. A więc wysoce prawdopodobny pozostaje odbiór przestępstwa zgwałcenia jako nieobyczajny ze względu na obciążoną kontrowersją problematykę samego w sobie czynu zabronionego, jak i na gorszącą okoliczność ugruntowaną w osobie pokrzywdzonego.

Pod pojęciem strony przedmiotowej przestępstwa rozumie się elementy składowe, jakimi są:

- pojęcie czynu, a więc zachowanie sprawcy;
- warunki w jakich dopuszczono się tego zachowania;
- związek przyczynowy między tym zachowaniem a konsekwencją przez nie wywołaną[19].

Konieczne dla poniesienia przez sprawcę konsekwencji prawnych przewidzianych za czyn przez niego popełniony jest doprowadzenie innej osoby do obcowania płciowego bez jej zgody albo do poddania się innej czynności seksualnej bądź wykonania takiej czynności bez jej zgody. Zgodnie z aktualnym brzmieniem art. 197 k.k., podstawową przesłanką odpowiedzialności jest brak dobrowolnej i świadomej zgody osoby pokrzywdzonej, przy czym użycie przemocy, groźby bezprawnej, podstępu lub wykorzystanie bezradności może stanowić okoliczność wpływającą na ocenę stopnia społecznej szkodliwości czynu oraz jego kwalifikację prawną.

Pojęcie przemocy opiera się na podjęciu pewnych działań, które unieszkodliwią opór ofiary, co uniemożliwi powstanie bądź wykonanie decyzji będącej wyrazem jej woli lub też dzięki czemu sprawca uzyska pożądane przez siebie na-

stawienie ofiary. Przemoc może być ukierunkowana bezpośrednio na osobę lub też oddziaływać na ważny dla niej element rzeczywistości, co pośrednio będzie jak gdyby obligowało ją do poddania się woli sprawcy[20]. Przypuszczalnie kwalifikowana będzie przemoc natury fizycznej, jak i ta oddziałująca na psychiczną sferę ofiary.

Definicja groźby bezprawnej znajduje się w art. 115 § 12 k.k., wedle którego stanowi ona:

- groźbę karalną z art. 190 k.k. – tj. groźbę popełnienia przestępstwa na szkodę ofiary lub osoby dla niej najbliższej, jeżeli groźba wzbudza w osobie, do której została skierowana lub której dotyczy, uzasadnioną obawę, że będzie spełniona; w kontekście przestępstwa groźba bezprawna może zatem polegać na zapowiedzi użycia przemocy fizycznej, popełnienia innego przestępstwa (np. uszkodzenia ciała);
- groźbę spowodowania postępowania karnego lub innego postępowania;
- groźbę rozgłoszenia informacji, która godzi w cześć ofiary lub osób jej najbliższych.

Podstęp natomiast nie opiera się na swoistym przymuszeniu, ale polega na wprowadzeniu ofiary w błąd lub też wykorzystaniu błędnego przeświadczenia, w jakim ona już się znajdowała. W konsekwencji sprawca doprowadza do obcowania płciowego bądź innej czynności seksualnej, co nie miałoby miejsca w relewantnej sytuacji motywacyjnej z prawidłowym odbiorem rzeczywistości przez ofiarę[21].
Literatura przedmiotu dotycząca przestępstwa zgwałcenia zwraca uwagę na jego poważne konsekwencje psychologiczne i fizyczne dla ofiary. Wiktymolodzy, psycholodzy, a także naukowcy społeczni jednogłośnie podkreślają fakt upokorzenia i zdegradowania drugiego człowieka, przez co przez długi czas boryka się z ogromnymi problemami egzystencjalnymi.

FAZY REAKCJI OFIAR PO PRZESTĘPSTWIE ZGWAŁCENIA

W relacjach ofiar zgwałcenia na plan pierwszy wysuwa się szok i odrętwienie, jest to pierwsza z trzech faz syndromu traumy po zgwałceniu.

Faza pierwsza

Bezpośrednio po ataku występuje pierwsza faza – szok i odrętwienie. Może ona trwać od kilku godzin do dwóch tygodni. Ofiara gwałtu jest przerażona, nie może uwierzyć w to, co się stało, odczuwa strach przed sprawcą. Zazwyczaj boi się zwierzyć komuś bliskiemu, gdyż obawia się reakcji ze strony otoczenia. Obawia się słów typu: sama sobie jesteś winna, mogłaś nie prowokować, mogłaś tam nie iść itp. (...) W tej fazie ofiary zmagają się z poczuciem własnej bezradności, winy, lęku, odczuwają wstyd, głębokie upokorzenie[22].
Psycholodzy zajmujący się tego typu zagadnieniami zwracają uwagę, że niektóre ofiary są niezwykle spokojne, są w szoku, który powoduje, że zachowują się jakby nic się nie stało. W tym wypadku możemy mówić o mechanizmie obronnym, wyparciu, co ma zminimalizować konsekwencje bolesnych wydarzeń[23]. Wielu badaczy zwraca uwagę, że ofiara doznaje dodatkowych szkód wynikających z reakcji społecznych. Mam tu na myśli przede wszystkim najbliższe otoczenie czy instytucje udzielające wsparcia, pierwszej pomocy emocjonalnej. Może to wynikać z nadmiernej ciekawości, oburzenia czy potępienia środowiska, co w konsekwencji wywołuje efekt stygmatyzacji i znacznie odwleka powrót do stanu sprzed popełnienia przestępstwa[24]. Jest to tak zwana wtórna wiktymizacja, na którą może mieć również wpływ wymiar sprawiedliwości. Prowadzenie działań zmierzających do wyjaśnienia zjawiska przywołuje w pamięci krzywdę wyrządzoną ofierze[25]. Dodatkowo przestępstwo zgwałcenia jest mocno obarczone oddziaływaniami medialnymi, szczególnie jeżeli weźmiemy pod uwagę przekazywanie informacji. Oczywiście, w obu wymienionych przypadkach nie jest to zamierzone czy świadome ze strony otoczenia.
Wiktymizacja ofiar przemocy seksualnej wiąże się z wieloma stereotypami, które zakłócają powrót do normalnego funkcjonowania. Na reakcję ofiar przemocy stereotyp może oddziaływać dwutorowo. Po pierwsze, sam może stać się źródłem kryzysu – dotyczy to przede wszystkim szeroko rozpowszechnionych stereotypów przekazywanych kulturowo, które zgodnie z modelem Hoffa, uwzględniającym kulturowe źródła kryzysów, same mogą kryzys wywoływać lub go pogłębiać. Z drugiej strony definiowanie swojej sytuacji przez ofiarę gwałtu zgodnie z utrwalonym stereotypem może prowadzić do pogłębienia stanu stresowego – przykładowo, jeżeli ofiara pokrzywdzona tym przestępstwem myśli według stereotypu, że ofiara gwałtu to osoba niemoralna, będzie to pogłębiać jej stres poprzez większe zagrożenie *Ja* niż w sytuacji, gdyby nie podzielała takiego przekonania[26].
Stereotypy dotyczące przestępstwa seksualnego w znaczny sposób mogą pogłębiać stan zagubienia ofiary gwałtu. W dużej mierze jest to zależne od reakcji emocjonalnej na zaistniałą sytuację. Mogą one wywoływać u ofiary głębokie poczucie zagubienia i wstydu. W ten sposób osoba pokrzywdzona może całkowicie samoczynnie wykluczać się z otaczającego społeczeństwa, a więc pozostawać wyalienowana. Taka sytuacja potęguje stres. Stereotypy mogą również spowodować, że ofiara jest nieświadoma sytuacji, w jakiej się znajduje. Znakomity przykład podaje Irena Pospiszyl w książce *Przemoc domowa*:
„(...) wiele kobiet nie zdaje sobie sprawy z bycia ofiarami niejednokrotnie okrutnego gwałtu ze strony męża. Uświadamiają to sobie dopiero w gabinecie specjalistów próbujących ratować rozpadające się małżeństwo, udzielając psychologicznej pomocy kobiecie, która utraciła kontrolę nad własnym życiem, albo po obejrzeniu programu telewizyjnego na ten temat. Wypowiedź jednej z pacjentek poradni psychologicznej jest charakterystyczna (...) Do tej pory nie zdawałam sobie sprawy, że to był gwałt. Jestem przecież z nim tyle lat, znam go nie od dziś. Gwałt to zawsze było dla mnie coś, co może zdarzyć się na ulicy. No i oczywiście to musiałby być ktoś obcy”[27].
Oczywiście o problemie koegzystencji stereotypów i przestępstw seksualnych można byłoby napisać co najmniej obszerną dysertację, jednak ze względu na ograniczenie objętości artykułu, konieczne jest przejście do następnych kwestii.

Faza druga

Kolejną ważną implikacją przestępstwa seksualnego jest dezorientacja. To druga faza, w której dominują stany lękowe, depresje i niepewność. Wymienione elementy w znaczny sposób wpływają na dezorganizację normalnej egzystencji, co prowadzi do alienacji i wykluczenia z najbliższego środowiska. Osoby pokrzywdzone zadają sobie często pytanie dotyczące dalszego życia, które staje się dla nich czymś nierealnym, oddalonym, a nawet nieuchwytnym. Niestety długość trwania tego stanu jest czymś niedefiniowalnym, mogą to być całe miesiące, co w konsekwencji może prowadzić do autodestrukcji. Ofiary przemocy seksualnej w tej fazie są skłonne do nadużywania alkoholu, brania leków, a nawet prób samobójczych, które w ostatnim czasie stają się czymś nagminnym.

Faza trzecia

Kolejną fazą jest faza reorganizacji. Następuje w niej stopniowy powrót do równowagi, a proces ten może trwać nawet latami. Osoba pokrzywdzona próbuje powrócić do swojego normalnego życia, zaczyna snuć plany, jednak zazwyczaj pozostaje nieufna wobec innych.

Zespół stresu pourazowego (PTSD)

Jak wynika z przeprowadzonych badań, 80% ofiar przestępstw na tle seksualnym[28] boryka się z zespołem stresu pourazowego (post-traumatic stress disorder – PTSD). Mają one wyraźne objawy klasyfikacji DSM-III-R, a więc wykraczające poza zakres zwykłych ludzkich doświadczeń. Możemy tutaj wykazać szczególnie natarczywe powroty wspomnień, występujące również w sennych koszmarach. Pacjenci z PTSD wspominają również o uczuciach ogniskujących się na wspomnieniu wydarzenia, a nawet przedmiotach, które mogą mieć związek z doznanym aktem. PTSD można zdiagnozować, gdy objawy trwają przynajmniej miesiąc. W pierwszej kolejności należy zwrócić uwagę na trudności z zasypianiem, wybuchy gniewu, nadmierną czujność i trudności z koncentracją[29]. Oczywiście, przy tego typu objawach zaleca się krótkotrwałą i intensywną terapię maksymalnie skoncentrowaną na traumatycznej sytuacji, tak aby jak najszybciej doprowadzić ofiarę do stanu, w którym będzie mogła sprawnie funkcjonować.

ZAKOŃCZENIE

Nie sposób jest omówić całokształtu zarówno semantyki samego przestępstwa, jak i jego etiologii i implikacji. Zaprezentowane przeze mnie treści stanowią jedynie syntetyczne ujęcie tego tematu, który wymaga głębszych analiz, badań i diagnoz, tak aby poszerzyć naszą wiedzę na temat tego zjawiska.

[1] A. Wrzyszcz, *Karalność zgwałcenia na ziemiach polskich do pierwszych lat II Rzeczypospolitej*, w: *Przestępstwo zgwałcenia*, red. M. Mozgawa, Warszawa 2012, s. 9–10.
[2] P. Theuss, *Gwałt a zgwałcenie w polskim prawie karnym*, w: „Problemy Prawa Karnego" 2022, t. 6, 2, s. 1.
[3] Zob. tamże, s. 2.
[4] Tamże.
[5] Por. J. Godlewski, *Typologia zgwałceń*, w: „Psychiatria Polska" 1987, nr 4, s. 298.
[6] Tamże, s. 230.
[7] Por. H. Myśliwiec, *Zgwałcenie pedofilskie i kazirodcze – charakterystyka nowych kwalifikowanych typów zgwałcenia*, w: „Czasopismo Prawa Karnego i Nauk Penalnych" 2010, rok XIV, z. 3, s. 73–74.
[8] J. Warylewski, *Przestępstwa seksualne*, Gdańsk 2001.
[9] Tamże.
[10] L. Lernell, *Przestępczość seksualna. Zagadnienia prawne i kryminologiczne*, w: K. Imieliński, *Seksuologia społeczna*, Warszawa 1984, s. 478, 486.
[11] Cyt. za: R. Kowalczyk i in., *Gwałt – tło psychospołeczne zjawiska oraz ujęcie prawne przestępstwa*, https://www.researchgate.net/profile/Katarzyna-Waszynska/publication/287252609_Rape_-_A_psychosocial_background_and_the_legal_definition_of_the_offence/links/5a350c8e0f7e9b10d84504e3/Rape-A-psychosocial-background-and-the-legal-definition-of-the-offence.pdf [dostęp: 15.05.2025 r.].
[12] T. Bojarski, *Polskie prawo karne. Zarys części ogólnej*, Warszawa 2008, s. 138–139.
[13] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2025 r. poz. 383).
[14] A. Więcek-Durańska, M. Durański, *Zgwałcenie ze szczególnym okrucieństwem (art. 197 §4 k.k.) – analiza kryminologiczna*, „Prawo w Działaniu. Sprawy Karne", nr 19, 2014, s. 165.
[15] H. Myśliwiec, *Zgwałcenie pedofilskie i kazirodcze – charakterystyka nowych kwalifikowanych typów zgwałcenia*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2010, nr 3, s. 93–94.
[16] T. Bojarski, *Polskie prawo karne. Zarys części ogólnej*, s. 114.
[17] H. Myśliwiec, *Zgwałcenie pedofilskie i kazirodcze – charakterystyka nowych kwalifikowanych typów zgwałcenia*, s. 75–76.
[18] Tamże.
[19] T. Bojarski, *Polskie prawo karne. Zarys części ogólnej*, s. 120.
[20] T. Hanausek, *Przemoc jako forma działania przestępnego*, Kraków 1966, s. 65.
[21] H. Myśliwiec, *Zgwałcenie pedofilskie i kazirodcze – charakterystyka nowych kwalifikowanych typów zgwałcenia*, s. 87.
[22] S. Kluczyńska, *Psychologiczne konsekwencje gwałtu*, w: „Czasopismo Niebieska Linia" 2002, nr 1, s. 23.
[23] Por. tamże.
[24] M. Wysocka-Pleczyk, P. Passowicz, *Jawne i ukryte aspekty postawy wobec ofiar gwałtu*, w: *Psychologiczny wymiar zdrowia, kryzysu i choroby*, Kraków 2005, s. 130.
[25] Por. J.L. Herman, *Przemoc. Uraz psychiczny i powrót do równowagi*, Gdańskie Wydawnictwo Psychologiczne, Gdańsk 1998, s. 16.
[26] D. Doliński, *Przypisywanie moralnej odpowiedzialności*, Warszawa 1992, s. 78.
[27] I. Pospiszyl, *Przemoc w rodzinie*, Warszawa 1994, s. 74–75.
[28] Por. S. Kluczyńska, *Psychologiczne konsekwencje gwałtu*, w: „Czasopismo Niebieska Linia" 2002, nr 1, s. 24.
[29] Por. tamże.

Summary

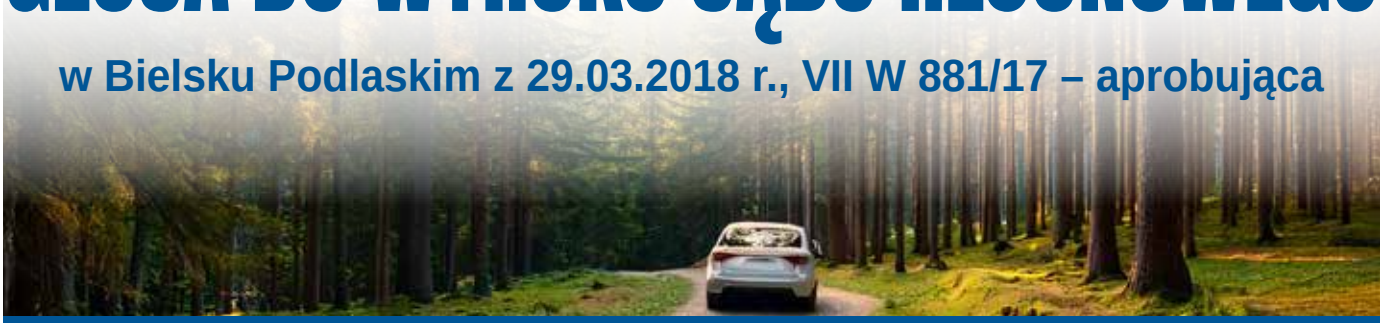
The criminological, sociological and psychological implications of rape

Rape remains one of the most severe violations of sexual autonomy and fundamental human rights. Its impact extends far beyond the legal sphere, having long-term psychological, social and criminological effects. As a major social issue, this phenomenon demands an interdisciplinary approach. This article provides a comprehensive analysis of rape through criminological, sociological, and psychological lenses, examining its definition, underlying causes, prevalence, and its impact on both individual victims and society as a whole.

Tłumaczenie: Joanna Łaszyn

GLOSA DO WYROKU SĄDU REJONOWEGO

w Bielsku Podlaskim z 29.03.2018 r., VII W 881/17 – aprobująca



Grafika wygenerowana z wykorzystaniem licencjonowanego programu Adobe Firefly.

Karol Józef Rosik

VIII LO im. Władysława IV w Warszawie

Glosa do wyroku Sądu Rejonowego w Bielsku Podlaskim z 29.03.2018 r., VII W 881/17 – aprobująca, podejmuje analizę sprawy R.G., obwinionego o wykroczenie z art. 161 k.w. polegające na pozostawieniu pojazdu w lesie w miejscu do tego nieprzeznaczonym. Artykuł wykorzystuje metodę dogmatyczno-prawną, analizując art. 161 k.w., art. 29 ustawy o lasach, orzecznictwo oraz doktrynę, w tym definicję „pozostawienia pojazdu" i jego społecznej szkodliwości. Autor zwraca uwagę, że wyrok ma istotne znaczenie dla wykładni art. 161 k.w., bowiem akcentuje rolę zamiaru sprawcy i kontekstu zdarzenia w ocenie odpowiedzialności wykroczeniowej. Wskazuje również potrzebę doprecyzowania przepisów prawa, aby jednoznacznie określały sytuacje, w których pozostawienie pojazdu w lesie stanowi wykroczenie.

Wprowadzenie

Motywacją do sporządzenia niniejszej glosy był interesujący stan faktyczny sprawy oraz sposób wykładni przepisów art. 161 kodeksu wykroczeń[1] (dalej k.w.) dokonany przez sąd. W analizowanym orzeczeniu widoczne jest zderzenie literalnego brzmienia przepisów, które kwalifikują każdy wjazd pojazdem silnikowym do lasu bez wymaganego zezwolenia jako wykroczenie, z zasadami logiki oraz podejściem uwzględniającym nadrzędność rzeczywistych potrzeb człowieka nad sztywnym formalizmem prawnym.
W artykule zastosowano metodę dogmatyczno-prawną, polegającą na analizie obowiązujących przepisów prawa, w szczególności art. 161 k.w. oraz art. 29 ustawy z dnia 28 września 1991 r. o lasach[2] (dalej: ustawa o lasach) oraz przepisów kodeksu postępowania w sprawach o wykroczenia[3] (dalej: k.p.s.w.), a także na analizie orzecznictwa sądowego i poglądów doktryny.

Stan faktyczny

Przedmiotem rozstrzygnięcia Sądu Rejonowego w Bielsku Podlaskim, Zamiejscowego VII Wydziału Karnego w Hajnówce, była sprawa dotycząca odpowiedzialności wykroczeniowej R.G., obwinionego o naruszenie art. 161 k.w., polegające na pozostawieniu pojazdu mechanicznego[4] w lesie w miejscu do tego nieprzeznaczonym. Jak ustalił sąd, w dniu 25 maja 2017 r. R.G. poruszał się samochodem osobowym po drodze leśnej znajdującej się na terenie Nadleśnictwa B., przy czym ruch pojazdów na tej drodze był dopuszczony[5]. W pojeździe, oprócz obwinionego, znajdowały się również inne osoby. W trakcie przejazdu jedna z pasażerek zgłosiła konieczność niezwłocznego załatwienia potrzeby fizjologicznej, co skłoniło kierującego do zatrzymania pojazdu na poboczu drogi leśnej. Zatrzymanie miało charakter incydentalny i krótkotrwały, było podyktowane wyłącznie zaistniałą sytuacją życiową, a nie zamiarem postoju w lesie. Zarówno obwiniony, jak i pozostali pasażerowie opuścili pojazd, nie oddalając się jednak od niego i przez cały czas zachowując możliwość natychmiastowego przestawienia samochodu lub odjazdu. Pojazd pozostawał pod stałym nadzorem użytkowników i nie został porzucony ani pozostawiony bez kontroli. W czasie tego zatrzymania na miejsce przybył patrol Straży Leśnej[6], który uznał, że doszło do pozostawienia pojazdu mechanicznego w miejscu nieprzeznaczonym do postoju i zaproponował obwinionemu przyjęcie mandatu karnego. Po odmowie jego przyjęcia sporządzony został

wniosek o ukaranie, w którym zachowanie R.G. zakwalifikowano jako wykroczenie z art. 161 k.w.
Sąd, opierając się na zgromadzonym materiale dowodowym, w tym zeznaniach funkcjonariuszy Straży Leśnej oraz dokumentacji urzędowej, nie zakwestionował samego faktu zatrzymania pojazdu, lecz poddał ocenie charakter tego zatrzymania oraz jego znaczenie w kontekście znamion czynu zabronionego. Okoliczności sprawy stały się podstawą do rozważań nad zakresem pojęcia „pozostawienia pojazdu" w rozumieniu art. 161 k.w., co w konsekwencji doprowadziło do uniewinnienia obwinionego.

Stan prawny

Sąd podkreślił na początku, że nie można zgodzić się z zarzutem obrony, jakoby sąd był związany szczegółowym opisem czynu przedstawionym we wniosku o ukaranie, w tym przede wszystkim datą jego popełnienia. Konstrukcja polskiego procesu karnego opiera się na zasadzie skargowości[7], która nie oznacza związania sądu literalnym opisem oskarżenia, lecz wyznacza tylko ramy zdarzenia historycznego, które podlega wyjaśnieniu w toku postępowania. Opis czynu przedstawiony przez oskarżyciela jest jedynie procesową hipotezą, którą sąd weryfikuje na podstawie zgromadzonych dowodów i własnej oceny. W ostatecznym rozstrzygnięciu to sąd konstruuje opis czynu przypisany obwinionemu, a nie bierze automatycznie opisu zawartego we wniosku o ukaranie (takie stanowisko zostało potwierdzone przez Sąd Najwyższy w postanowieniu z 25 października 2017 r., sygn. IV KK 85/17[8]).
W świetle sięgniętych dowodów sąd uznał, że choć we wniosku o ukaranie podana była data 30 maja 2017 r., faktyczne wydarzenie miało miejsce 25 maja 2017 r., co nie wpłynęło na zasadniczy charakter zdarzenia ani na jego ocenę prawną. Takie różnice co do daty, pozostające wewnątrz jednego zdarzenia historycznego, nie naruszają zasady skargowości i nie wymagają ponownego aktu oskarżenia (analogiczne podejście pojawia się w orzecznictwie sądów powszechnych, np. w sprawach sygn. II AKa 271/16[9] oraz II AKa 24/15[10], gdzie zmiany szczegółowych elementów opisu czynu nie przekraczały granic pierwotnego zdarzenia).
Przy ocenie materiału dowodowego sąd sięgnął następnie do zasad wykładni norm materialnych. Z analizy porządku prawnego wynika, że ustawa o lasach określa ogólne zasady ruchu i postoju pojazdów leśnych – wskazując, że są one dozwolone jedynie na drogach publicznych lub na drogach leśnych, które są odpowiednio oznakowane, a postój pojazdów dopuszczalny jest tylko w wyznaczonych miejscach. Przepis karny zawarty w kodeksie wykroczeń stanowi natomiast sankcję za „pozostawienie" pojazdu w lesie w miejscu do tego nieprzeznaczonym.
Sąd dostrzegł, że oba unormowania posługują się odmienną terminologią: regulacja porządkowa operuje pojęciem „postoju pojazdu", natomiast norma karna mówi o jego „pozostawieniu". W ocenie sądu, to właśnie interpretacja tego ostatniego pojęcia musi być kluczowa dla oceny przesłanek odpowiedzialności wykroczeniowej. Do wykładni tego pojęcia sąd zastosował przede wszystkim analizę językową, według której „pozostawienie" oznacza sytuację, w której następuje zerwanie bezpośredniej więzi z pojazdem – innymi słowy, brak faktycznego nadzoru nad pojazdem i brak możliwości jego niezwłocznego przestawienia, co prowadzi do zagrożenia dóbr prawnych, których ochrona jest celem przepisu wykroczeniowego. Takie rozumienie znamienia „pozostawienia" znajduje uzasadnienie w systemowym celu normy – ochrona lasu i zasobów leśnych przed skutkami niekontrolowanego ruchu i postoju pojazdów, w szczególności w kontekście bezpieczeństwa przeciwpożarowego oraz drożności dróg leśnych. W przeciwieństwie do regulacji o charakterze porządkowym, norma karna pełni funkcję ochronną i dlatego musi być interpretowana w świetle jej społecznego celu.
Przyjęte przez sąd rozumienie znamienia „pozostawienia" oznacza, że krótkotrwałe zatrzymanie pojazdu podyktowane nagłą potrzebą życiową – umożliwienie pasażerce zaspokojenia potrzeby fizjologicznej – nie stanowi „pozostawienia" w rozumieniu wykroczenia, dopóki kierujący pozostaje w bezpośrednim sąsiedztwie pojazdu i może go niezwłocznie usunąć. Taki stan faktyczny nie stwarza realnego zagrożenia chronionego prawem dobra, co w ocenie sądu wyklucza odpowiedzialność wykroczeniową.
W konsekwencji, wobec braku znamion czynu zabronionego, sąd uznał, że zachowanie obwinionego nie może być uznane za wykroczenie z art. 161 kodeksu wykroczeń i orzekł jego uniewinnienie.

Komentarz

Początkowo, aby mówić o wykroczeniach na terenach leśnych, należy określić, czym jest „las". Kwestię tę reguluje ustawa z dnia 28 września 1991 r. o lasach, która w art. 3 określa legalną definicję lasu. Zgodnie z treścią tego przepisu pojęcie lasu obejmuje dwa rodzaje gruntów. Po pierwsze, są to grunty o zwartej powierzchni co najmniej 0,10 ha, pokryte roślinnością leśną – drzewami, krzewami oraz runem leśnym – bądź przejściowo jej pozbawione, jeżeli są przeznaczone do produkcji leśnej, stanowią rezerwat przyrody, wchodzą w skład parku narodowego albo zostały wpisane do rejestru zabytków. Po drugie, za las uznaje się również grunty związane z gospodarką leśną, zajęte pod obiekty i urządzenia służące tej gospodarce, w szczególności budynki i budowle, urządzenia melioracji wodnych, linie podziału przestrzennego lasu, drogi leśne, tereny pod liniami energetycznymi, szkółki leśne, miejsca składowania drewna, a także tereny wykorzystywane jako parkingi leśne oraz pod urządzenia turystyczne.
W celu dokładnej analizy przedstawionego wyżej stanu faktycznego należy wpierw odwołać się do definicji szkodnictwa leśnego. Szkodnictwo leśne stanowi ogół zachowań naruszających przepisy prawa dotyczące ochrony lasów oraz zasad racjonalnego gospodarowania ich zasobami. W literaturze pojawia się definicja szkodnictwa leśnego jako wszelkiego rodzaju czyny niedozwolone polegające bądź na bezprawnym korzystaniu z lasu i produktów leśnych, bądź na naruszaniu przepisów dotyczących ochrony lasów lub z tą ochroną związanych[11]. Wykroczenie nieuprawnionego wjazdu do lasu zostało zdefiniowane w art. 161 kodeksu wykroczeń, który wskazuje, że „kto, nie będąc do tego uprawniony albo bez zgody właściciela lub posiadacza lasu, wjeżdża pojazdem silnikowym, zaprzęgowym lub motorowerem do nienależącego do niego lasu w miejscu, w którym jest to niedozwolone, albo pozostawia taki pojazd w lesie w miejscu do tego nieprzeznaczonym, podlega karze grzywny". Kluczowe w tym kon-

tekście jest pojęcie „pojazdu silnikowego", które należy rozumieć zgodnie z definicjami zawartymi w ustawie – Prawo o ruchu drogowym[12] (art. 2 pkt 32 tej ustawy). Zgodnie z definicją ustawową pojazd silnikowy jest to „pojazd wyposażony w silnik, z wyjątkiem motoroweru, pojazdu szynowego, roweru, wózka rowerowego, hulajnogi elektrycznej, urządzenia transportu osobistego i wózka inwalidzkiego;". Dyspozycja art. 161 k.w. reguluje sankcję za przewinienia, które swoje źródło mają w art. 29 ustawy o lasach. Przepis ten ustanawia normatywny porządek, którego zasadniczym celem jest ograniczenie i reglamentacja ruchu pojazdów mechanicznych w przestrzeni leśnej, z uwagi na potrzebę zapewnienia trwałości funkcji ekologicznych, ochronnych i gospodarczych lasu jako dobra wspólnego oraz komponentu środowiska naturalnego o szczególnej wrażliwości. Zgodnie z brzmieniem art. 29 ust. 1 ustawy, ruch pojazdem silnikowym, zaprzęgowym oraz motorowerem w lesie jest dozwolony wyłącznie drogami leśnymi, chyba że zachodzą szczególne przypadki wskazane w ustępie 2 lub gdy właściciel lasu wyrazi na to zgodę w trybie ustępu 3. Już na poziomie wykładni literalnej przepis ten ustanawia zakaz generalny, przy czym określa on jedynie wąski zakres dopuszczalnych wyjątków. Kluczowym pojęciem, którego interpretacja ma decydujące znaczenie dla stosowania przepisu, jest „droga leśna". Ustawodawca nie zawarł w ustawie o lasach definicji legalnej tego terminu, co powoduje konieczność odwołania się do wykładni funkcjonalnej i orzecznictwa administracyjnego oraz cywilnego. Zgodnie z art. 8 ust 1 u.d.p.[13]: „Drogi niezaliczone do żadnej kategorii dróg publicznych, w szczególności drogi w osiedlach mieszkaniowych, dojazdowe do gruntów rolnych i leśnych, dojazdowe do obiektów użytkowanych przez przedsiębiorców, place przed dworcami kolejowymi, autobusowymi i portami oraz pętle autobusowe, są drogami wewnętrznymi". Droga leśna stanowi bez wątpienia rodzaj drogi wewnętrznej, przy czym, aby mogła być zakwalifikowana jako droga leśna, musi przebiegać w obrębie obszaru leśnego[14]. Przyjmuje się, że drogą leśną jest droga, która nie wchodzi w skład systemu dróg publicznych i została wybudowana bądź jest utrzymywana w celu prowadzenia gospodarki leśnej, w tym udostępniania lasów dla służb leśnych i podmiotów uprawnionych do wykonywania zadań związanych z ochroną i użytkowaniem zasobów leśnych. W świetle ustępu 2 art. 29 ustawy o lasach, możliwy jest ruch pojazdów poza drogami leśnymi wyłącznie w ściśle określonych przypadkach, tj. gdy czynność ta związana jest bezpośrednio z prowadzeniem gospodarki leśnej, łowieckiej, rolniczej lub ochrony przyrody, a także w przypadku realizacji zadań z zakresu obronności, bezpieczeństwa publicznego lub ratownictwa[15].

Warto odwołać się do art. 1 kodeksu wykroczeń, który wskazuje, że za wykroczenie odpowiada wyłącznie ten, kto popełnia czyn społecznie szkodliwy. „Czyn wyczerpujący znamiona wykroczenia o subminimalnym stopniu społecznej szkodliwości nie traci cech wykroczenia. Ustalenie, że stopień społecznej szkodliwości wykroczenia jest znikomy, rzutuje co najwyżej na rodzaj i rozmiar reakcji organu orzekającego w stosunku do obwinionego (postanowienie Sądu Najwyższego z dnia 10 czerwca 2003 r., II KK 87/03). Innymi słowy, jedynie przy wykazaniu w ogóle braku szkodliwości danego zachowania w określonych okolicznościach, można mówić o niezaistnieniu samego wykroczenia mimo naruszenia określonego przepisu tej dziedziny prawa. Przy niewielkiej (nikłej) szkodliwości czynu możliwe jest zaś ograniczenie reakcji prawnej do środków oddziaływania wychowawczego (art. 41 k.w.), a w postępowaniu przed sądem do odstąpienia od ukarania i zastosowania jedynie środków oddziaływania społecznego (art. 39 k.w.) (por. *Komentarz do art. 1 Kodeksu wykroczeń* pod red. Tomasza Grzegorczyka)"[16].

W analizowanej sprawie warto najpierw ustalić, czy opisany czyn wyczerpał znamiona wykroczenia. Sąd w swoim orzeczeniu uniewinnił obwinionego, wskazując, że kierował się zasadą racjonalnego postępowania i zjechał z drogi udostępnionej do ruchu kołowego jedynie po to, aby pasażerka mogła skorzystać z potrzeby fizjologicznej. Możliwość swobodnego zaspokojenia podstawowych potrzeb biologicznych należy uznać za element godności człowieka, która zgodnie z art. 30 Konstytucji RP[17] stanowi źródło wolności i praw jednostki, a organy władzy publicznej są zobowiązane do jej poszanowania i ochrony. W tym kontekście prawo do korzystania z urządzeń sanitarnych, w tym toalet, zostało również uznane za prawo człowieka (por. Rezolucja Rady Praw Człowieka A/HRC/15/L.14[18]).

Zgodnie z przepisami i orzecznictwem, udowodnienie winy obwinionemu musi być całkowite, pewne i wolne od wątpliwości (wyrok Sądu Najwyższego z dnia 24 lutego 1999 r., sygn. akt V KKN 362/97[19]). Jest to zgodne z łacińską sentencją *in dubio pro reo*, która wskazuje, że wszelkie wątpliwości winny być rozstrzygane na korzyść oskarżonego. Wyraża to również art. 5 § 2 k.p.k.[20] (stosowane w sprawach o wykroczenia – art. 8)[21].

Straż Leśna w ocenie stanu faktycznego winna się oprzeć na wszelkich okolicznościach zdarzenia. Zgodnie z art. 7 k.p.k.[22] w zw. z art. 8 k.p.s.w. w ocenie sprawy należy kierować się zasadą „swobodnej oceny dowodów", która zobowiązuje organy ścigania do rzetelnego i obiektywnego zbadania sprawy. Należy odróżnić pozostawienie samochodu i pilnowanie go od celowego działania mającego na celu niszczenie środowiska. Przykładowo Sąd Rejonowy w Jeleniej Górze (sygn. II W 821/19)[23] skazał obwinionego, który poruszał się motocyklem krosowym po lesie, świadomie łamiąc przepisy mimo uprzedzenia przez leśniczego i znajomości prawa. Czyn został uznany przez sąd za społecznie szkodliwy, ponieważ nie miał uzasadnionego celu i negatywnie wpływał na środowisko.

W przedmiotowej sprawie mieliśmy do czynienia z nietypowym oskarżycielem publicznym – strażnikiem Straży Leśnej. Członkiem formacji, która działa w ramach Lasów Państwowych w oparciu o ustawę o lasach. Celem Straży Leśnej jest przede wszystkim ochrona zasobów leśnych, zapobieganie nielegalnemu wykorzystaniu lasów oraz zwalczanie szkodnictwa leśnego, w tym m.in. kradzieży drewna, kłusownictwa, nielegalnego pozyskiwania roślinności leśnej czy nieuprawnionego wjazdu do lasów. Straż Leśna stanowi integralną część struktur Lasów Państwowych, a jej działalność nadzoruje Dyrekcja Generalna Lasów Państwowych, która koordynuje pracę jednostek straży w całym kraju. Funkcjonowanie Straży Leśnej opiera się na regulacjach ustawowych, a jej zadania są szczegółowo określone w przepisach

wewnętrznych Lasów Państwowych oraz innych aktach prawnych związanych z ochroną środowiska i porządku w lasach.
W opisywanej sprawie Straż Leśna zdecydowała się ukarać kierującego pojazdem karą grzywny w drodze mandatu karnego (por. art. 97 k.p.s.w). Ma ona do tego prawo, ponieważ wynika to z art. 47 ust. 2 pkt 2 ustawy o lasach. Kierowca zdecydował się jednak skorzystać z uprawnienia, które przysługuje mu na podstawie art. 97 § 2 k.p.s.w., czyli odmówił przyjęcia mandatu karnego. Skutkowało to skierowaniem przez funkcjonariuszy wniosku o ukaranie do sądu. W ocenie autora Straż Leśna, nawet jeżeli uznałaby działanie kierowcy za wykroczenie, winna skorzystać ze środków pozapenalnych, czyli pouczenia (zob. art. 41 k.w.). Środek ten byłby zdecydowanie adekwatny, jeśli weźmiemy pod uwagę okoliczności sprawy, takie jak cel postoju oraz pozostawanie przy samochodzie.
Na tle art. 5 § 1 pkt 2 k.p.w. w doktrynie i praktyce pojawiają się wątpliwości, czy w sytuacji, gdy po wniesieniu wniosku o ukaranie sąd stwierdza, że czyn przypisany obwinionemu nie zawiera znamion wykroczenia, właściwą formą rozstrzygnięcia jest umorzenie postępowania. Wątpliwości te wynikają z literalnego brzmienia wskazanego przepisu, który przewiduje umorzenie postępowania w razie braku znamion czynu zabronionego.
Należy jednak podkreślić, że po merytorycznym rozpoznaniu sprawy sąd dokonuje oceny materialnoprawnej czynu, a nie jedynie kontroli istnienia przesłanek procesowych. Stwierdzenie, iż czyn nie stanowi wykroczenia, oznacza negatywną ocenę zasadności oskarżenia, co powinno prowadzić do wydania wyroku uniewinniającego. Umorzenie postępowania zachowuje natomiast właściwy charakter w przypadku wystąpienia przeszkód procesowych o charakterze formalnym, a nie w razie braku realizacji znamion wykroczenia ujawnionego na etapie merytorycznego rozpoznania sprawy. Zgodnie z literaturą i orzecznictwem k.p.w. art. 62 reguluje sytuację ujawnienia „okoliczności wyłączających orzekanie" po wszczęciu postępowania. Według art. 62 § 2 sąd ma obowiązek zamknąć postępowanie poprzez umorzenie, jeżeli dana okoliczność wystąpi przed rozpoczęciem przewodu sądowego. Natomiast art. 62 § 3 wprowadza wyjątek od tej reguły – jeżeli po rozpoczęciu przewodu sądowego stwierdzony zostanie brak znamion czynu zabronionego w rozumieniu art. 5 § 1 pkt 1 i 2 k.p.w., sąd wydaje wyrok uniewinniający, chyba że obwiniony był niepoczytalny w chwili czynu. Taka konstrukcja ustawowa oznacza, że brak znamion wykroczenia ujawniony merytorycznie nie prowadzi do umorzenia, lecz do najdalej idącego rozstrzygnięcia procesowego – uniewinnienia, które stanowi odpowiedź na zasadność oskarżenia, a nie przeszkodę formalną w postępowaniu. Omawiany przepis został potwierdzony w orzecznictwie sądowym. Przykładowo Sąd Okręgowy w Gliwicach w sprawie VI Ka 1305/16[24] uznał, że sąd pierwszej instancji błędnie umorzył postępowanie po stwierdzeniu, iż czyn nie zawiera znamion wykroczenia, zamiast wydać wyrok uniewinniający na podstawie art. 62 § 3 k.p.w. Wyrok ten podkreślił imperatywny charakter uniewinnienia w sytuacji, gdy analizowany czyn nie spełnia znamion wykroczenia, nawet jeżeli organ początkowo błędnie zakwalifikował go jako wykroczenie.
Niniejsza sprawa unaocznia potrzebę doprecyzowania pojęcia „pozostawienia pojazdu w lesie" oraz określenia, w jakich sytuacjach takie zachowanie rzeczywiście wyczerpuje znamiona wykroczenia. *De lege ferenda* należałoby jednoznacznie wskazać, że odpowiedzialność wykroczeniowa w takich sytuacjach powinna obejmować wyłącznie działania o charakterze celowym i umyślnym, tj. takie, w których sprawca ma świadomość pozostawienia pojazdu w miejscu do tego niedozwolonym.
W niniejszej sprawie kierowca nie naruszył przepisów w sposób zamierzony, albowiem poruszał się drogą prawidłowo oznaczoną jako udostępnioną do ruchu kołowego – drogą publiczną. Zjazd z niej był podyktowany wyłącznie koniecznością umożliwienia pasażerce zaspokojenia potrzeb fizjologicznych. Należy przy tym zauważyć, że zatrzymanie pojazdu na drodze mogłoby skutkować blokowaniem ruchu kołowego, co samo w sobie stanowiłoby wykroczenie na podstawie art. 90 k.w. W świetle powyższej analizy widoczna jest potrzeba indywidualnej oceny każdego zachowania w kontekście jego celowości i rzeczywistej szkodliwości dla lasu.

Podsumowanie

Wyrok Sądu Rejonowego w Bielsku Podlaskim z dnia 29.03.2018 r., VII W 881/17, w ocenie autora, stanowi orzeczenie słuszne i sprawiedliwe. Działanie obwinionego mogłoby potencjalnie stanowić wykroczenie, ale jedynie w sytuacji, gdyby pozostawił pojazd w lesie – w miejscu niedozwolonym – i następnie oddalił się z tego miejsca, na przykład w celach rekreacyjnych. Sąd prawidłowo ocenił stan faktyczny i, stosując przepisy k.p.s.w., uniewinnił obwinionego, stwierdzając, że jego czyn nie wyczerpał znamion wykroczenia. W tej sprawie rozsądkowe podejście oraz doświadczenie życiowe sędziego referenta pozwoliły na właściwą ocenę zarówno stanu faktycznego, jak i prawnego.
Warto podkreślić, że przedmiotowa sprawa ma istotne znaczenie dla wykładni art. 161 k.w., gdyż wskazuje, że nie każde pozostawienie pojazdu silnikowego w lesie automatycznie skutkuje odpowiedzialnością wykroczeniową. Wyrok uwypukla znaczenie zamiaru sprawcy oraz kontekstu sytuacji, w której doszło do zdarzenia, podkreślając zasadę proporcjonalności w stosowaniu prawa. W związku z tym, dla większej pewności prawnej i eliminacji wątpliwości interpretacyjnych, wskazane byłoby doprecyzowanie tej normy prawnej, tak aby jednoznacznie określała, kiedy pozostawienie pojazdu w lesie stanowi wykroczenie, a kiedy może być uznane za działanie usprawiedliwione okolicznościami.

[1] Ustawa z dnia 20 maja 1971 r. – Kodeks wykroczeń (Dz. U. z 2025 r. poz. 734, z późn. zm.).
[2] Ustawa z dnia 28 września 1991 r. o lasach (Dz. U. z 2025 r. poz. 567, z późn. zm.).
[3] Ustawa z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2025 r. poz. 860, z późn. zm.).
[4] Dokładnie: samochód osobowy.
[5] Zob. zarządzenie nr 54 Dyrektora Generalnego Lasów Państwowych z dnia 8 października 2019 r. w sprawie wprowadzenia wytycznych dotyczących korzystania z dróg leśnych, a także ich oznakowania i udostępniania dla ruchu pojazdami silnikowymi, zaprzęgowymi i motorowerami (B. I. LP z 2019 r. Nr 11, poz. 123).
[6] Zob. art. 47 ustawy o lasach.

[7] M. Kurowski, w: *Kodeks postępowania karnego. Tom I. Komentarz aktualizowany*, red. D. Świecki, LEX/el. 2025, art. 14.
[8] Postanowienie SN z 25.10.2017 r., IV KK 85/17, LEX nr 2427177.
[9] Wyrok SA w Gdańsku z 4.10.2016 r., II AKa 271/16, LEX nr 2157811.
[10] Wyrok SA we Wrocławiu z 5.03.2015 r., II AKa 24/15, LEX nr 1661279.
[11] L. Jastrzębski, E. Stankiewicz, *Ochrona lasów przed szkodnictwem*, Wydawnictwo Prawnicze, Warszawa 1997, s. 51.
[12] Ustawa z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. 2024 poz. 1251, z późn. zm.).
[13] Ustawa z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2025 r. poz. 889).
[14] B. Rakoczy, w: *Ustawa o lasach. Komentarz*, Warszawa 2011, art. 29.
[15] D. Danecka, W. Radecki [w:] D. Danecka, W. Radecki, Ustawa o lasach. Komentarz, wyd. IV, LEX/el. 2024, art. 29.
[16] Wyrok Sądu Okręgowego w Toruniu z 10.09.2013 r., IX Ka 406/13, LEX nr 1869633.
[17] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78, poz. 483, z późn. zm.).
[18] Rada Praw Człowieka ONZ, *Rezolucja A/HRC/15/L.14 – Prawa człowieka a dostęp do bezpiecznej wody pitnej i kanalizacji*, 15. sesja, Genewa, 24 września 2010 r., par. 1–3, https://undocs.org/A/HRC/15/L.14 (dostęp: 11 lutego 2026 r.).
[19] Wyrok SN z 24.02.1999 r., V KKN 362/97, LEX nr 564945.
[20] Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2025 r. poz. 46, z późn. zm.).
[21] Ustawa z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia.
[22] Tamże.
[23] Wyrok SR w Jeleniej Górze z 10.09.2019 r., II W 821/19, LEX nr 3008798.
[24] Wyrok Sądu Okręgowego w Gliwicach z 13.01.2017 r., VI Ka 1305/16, LEX nr 2266355.

Bibiliografia

Danecka D., Radecki W, w: *Ustawa o lasach. Komentarz*, wyd. IV, LEX/el. 2024.
Jastrzębski L., Stankiewicz E., *Ochrona Lasów przed szkodnictwem*, Wydawnictwo Prawnicze, Warszawa 1997.
Kowalska M., *Koncepcja ochrony przyrody w lasach publicznych w Polsce*, „Kwartalnik Prawa Publicznego", 2015, nr 2, s. 67–82, https://kwartalnik.csp.edu.pl/kp/archiwum-1/2015/nr-22015/2679,dok.html [dostęp: 11 lutego 2026 r.].
Kurowski M., w: *Kodeks postępowania karnego. Tom I. Komentarz aktualizowany*, red. D. Świecki, LEX/el. 2025.
Rakoczy B., w: *Ustawa o lasach. Komentarz*, Warszawa 2011.
Rada Praw Człowieka ONZ, *Rezolucja A/HRC/15/L.14 – Prawa człowieka a dostęp do bezpiecznej wody pitnej i kanalizacji*, 15. sesja, Genewa, 24 września 2010 r., https://undocs.org/A/HRC/15/L.14 [dostęp: 11 lutego 2026 r.].
Ustawa z dnia 20 maja 1971 r. – Kodeks wykroczeń (Dz. U. z 2025 r. poz. 734, z późn. zm.).
Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 2025 r. poz. 46, z późn. zm.).
Ustawa z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z 2024 r. poz. 1251, z późn. zm.).
Ustawa z dnia 21 marca 1985 r. o drogach publicznych (Dz. U. z 2025 r. poz. 889).
Ustawa z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2025 r. poz. 860, z późn. zm.).
Ustawa z dnia 28 września 1991 r. o lasach (Dz. U. z 2025 r. poz. 567, z późn. zm.).
Zarządzenie nr 54 Dyrektora Generalnego Lasów Państwowych z dnia 8 października 2019 r. w sprawie wprowadzenia wytycznych dotyczących korzystania z dróg leśnych, a także ich oznakowania i udostępniania dla ruchu pojazdami silnikowymi, zaprzęgowymi i motorowerami (B. I. LP z 2019 r. Nr 11, poz. 123).
Wyrok Sądu Apelacyjnego w Gdańsku z 4.10.2016 r., II AKa 271/16, LEX nr 2157811.
Wyrok Sądu Apelacyjnego we Wrocławiu z 5.03.2015 r., II AKa 24/15, LEX nr 1661279.
Wyrok Sądu Najwyższego z 24.02.1999 r., V KKN 362/97, LEX nr 564945.
Wyrok Sądu Najwyższego z 25.10.2017 r., IV KK 85/17, LEX nr 2427177.
Wyroku Sądu Rejonowego w Bielsku Podlaskim z 29.03.2018 r., VII W 881/17.
Wyrok Sądu Rejonowego w Jeleniej Górze z 10.09.2019 r., II W 821/19, LEX nr 3008798.
Wyrok Sądu Okręgowego w Gliwicach z 13.01.2017 r., VI Ka 1305/16, LEX nr 2266355.
Wyrok Sądu Okręgowego w Toruniu z 10.09.2013 r., IX Ka 406/13, LEX nr 1869633.

Słowa kluczowe: glosa aprobująca, Sąd Rejonowy w Bielsku Podlaskim, art. 161 k.w., las, pozostawienie pojazdu, wykroczenie, uniewinnienie, Straż Leśna.

Summary

Commentary on the Judgment of the District Court in Bielsk Podlaski of 29 March 2018, VII W 881/17 – Approving

Commentary on the judgment of the District Court in Bielsk Podlaski of 29 March 2018, VII W 881/17 – approving analyzes the case of R. G., accused of an offense under Article 161 of the Code of Petty Offenses for leaving a vehicle in a forest in a location not designated for parking. The factual circumstances showed that the driver briefly stopped the vehicle to allow a passenger to relieve herself, remained near the vehicle, and retained the ability to immediately move it if necessary. The commentary applies a doctrinal-legal method, examining Article 161 of the Code of Petty Offenses, Article 29 of the Forest Act, judicial precedent, and legal doctrine, including interpretations of the term "leaving a vehicle" and its social harmfulness. The court emphasized that such conduct does not meet the elements of an offense, as there was no loss of actual control over the vehicle and no real threat to legally protected goods. Human needs and the principle of proportionality were taken into account. The analysis concludes that the judgment is significant for interpreting Article 161 of the Code of Petty Offenses, highlighting the importance of the offender's intent and the context of the action in assessing liability. The commentary also underscores the need to clarify legal provisions to explicitly define situations in which leaving a vehicle in a forest constitutes an offense.

Keywords: Approving commentary, District Court in Bielsk Podlaski, Article 161 of the Code of Petty Offenses, forest, leaving a vehicle, offense, acquittal, Forest Guard.

Tłumaczenie: Autor

POŻAR

METODY ZABEZPIECZANIA ŚLADÓW KRYMINALISTYCZNYCH W TRAKCIE OGLĘDZIN MIEJSCA POŻARU

Zdj. 1. K. Poloczek

asp. szt. Marek Wrzosek
Zakład Szkoleń Specjalnych CSP

podkom. Kamila Poloczek
Zakład Szkoleń Specjalnych CSP

Ogień, który daje ciepło,
w jednej chwili może odebrać wszystko.
(autor nieznany)

Od tysiącleci ogień stanowi nieodłączny element egzystencji ludzkości. Dzięki swoim właściwościom fizycznym i chemicznym odgrywał oraz nadal odgrywa istotną rolę zarówno w życiu codziennym, jak i w działalności zawodowej człowieka. Jednakże w warunkach niekontrolowanych ogień może przekształcić się w pożar, wywołując poważne i destrukcyjne skutki.

W ujęciu ogólnym, pożarem nazywa się te procesy spalania, które są niekontrolowane i zachodzą w przestrzeni do tego nieprzeznaczonej. Cechą pożaru jest jego gwałtowny i niekontrolowany sposób rozprzestrzeniania się, co powoduje ogromne straty materialne, a przede wszystkim stwarza bezpośrednie zagrożenie dla zdrowia i życia ludzi oraz zwierząt[1].

Natomiast w nomenklaturze Państwowej Straży Pożarnej pożar to: „niekontrolowany proces spalania, występujący w miejscu do tego nieprzeznaczonym, rozprzestrzeniający się w sposób niekontrolowany, powodujący zagrożenie dla zdrowia i życia ludzi i zwierząt oraz straty materialne, a także charakteryzujący się emisją energii cieplnej, której towarzyszy wydzielanie dymu i zazwyczaj płomieni”[2].

Z kolei zgodnie z art. 163 § 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny: kto sprowadza zdarzenie, które zagraża życiu lub zdrowiu wielu osób albo mieniu w wielkich rozmiarach, mające postać m.in. pożaru, podlega karze pozbawienia wolności od roku do lat 10. W § 2 wskazano natomiast, iż odpowiedzialności karnej podlega również sprawca, który dopuszcza się tego czynu nieumyślnie[3].

W kryminalistyce zatem pożarem nazwiemy wszelkie umyślne lub nieumyślne działania albo też ich zaniechanie, powodujące niekontrolowane spalanie w miejscu do tego nieprzeznaczonym, w wyniku którego powstało zagrożenie dla życia lub zdrowia ludzkiego oraz zwierząt, a także pociągające za sobą straty materialne, o których mowa w art. 115 kk[4].

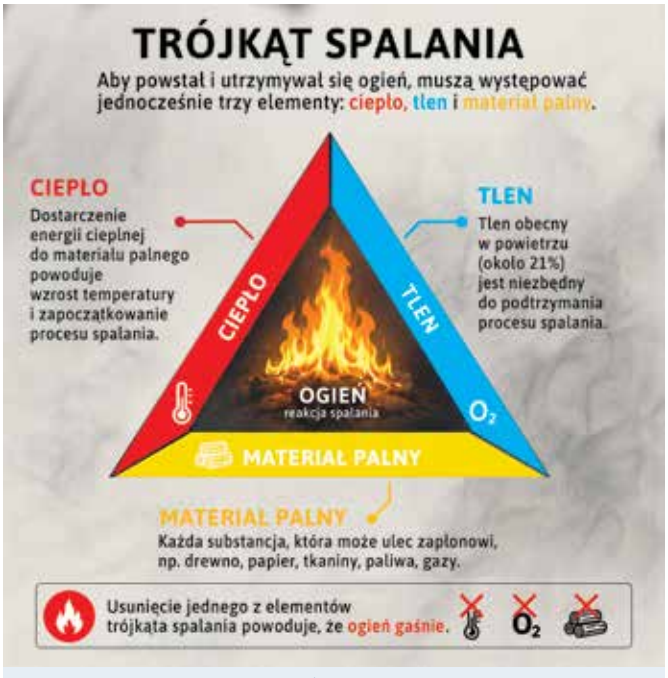
W latach 2020–2023 Państwowa Straż Pożarna odnotowała 470,6 tys. pożarów[5], natomiast w tym okresie Policja wszczęła 7513 postępowań z art. 163 kk, które w 1727 przypadkach zakończyły się stwierdzeniem popełnienia tego czynu[6]. Obecnie nie jest prowadzona statystyka związana z wywołaniem pożaru spenalizowanym w artykule 163 kk. Należy jednak zauważyć, że art. 163 kk obejmuje nie tylko zja-

Fot. 2. Miejsce pożaru.

wisko, jakim jest pożar, ale również inne zdarzenia o charakterze destrukcyjnym, takie jak eksplozje, zawalenie się budowli oraz podobne.

TEORETYCZNE ASPEKTY ZABEZPIECZANIA ŚLADÓW KRYMINALISTYCZNYCH PODCZAS OGLĘDZIN MIEJSCA POŻARU

Ogień, a co za tym idzie – powstanie pożaru, uwarunkowany jest jednak pewnymi elementami, a mianowicie musi wystąpić tzw. trójkąt spalania. Trójkąt spalania to model ilustrujący trzy kluczowe składniki niezbędne do powstania i podtrzymania ognia: materiał palny, utleniacz oraz źródło ciepła. Usunięcie jednego z tych elementów przerywa proces spalania i gasi pożar, co jest podstawą metod gaśniczych[7].



Ryc. 1. Tzw. trójkąt spalania. Źródło: opracowanie własne.

Zjawiska towarzyszące pożarowi, takie jak płomień (strefa spalania), gorące gazy (strefa oddziaływania termicznego) oraz toksyczne produkty spalania (strefa zadymienia), pozostawiają po sobie ślady popożarowe, które najczęściej mają charakter trwałych uszkodzeń. Są to przede wszystkim substancjalne ślady cieplne, obejmujące m.in. stopienia, wytopienia, nadtopienia, wypalenia, zwęglenia czy przebarwienia różnego rodzaju przedmiotów i materiałów. Podstawowe ślady popożarowe powstają jednak głównie w wyniku oddziaływania strefy spalania[8]. Na powyższe czynniki będziemy zwracać uwagę w trakcie oględzin, które są elementem kryminalistycznego badania miejsca zdarzenia.

Podczas oględzin miejsca pożaru lub pogorzeliska należy pamiętać o:

- przestrzeganiu zasad bezpieczeństwa, w tym dbaniu o bezpieczeństwo własne oraz innych uczestników czynności;
- zabezpieczeniu miejsca pożaru przed osobami postronnymi oraz przed spowodowaniem przez osoby zmian na tym miejscu;
- przeprowadzeniu oględzin w jak najkrótszym czasie od ugaszenia pożaru;
- sporządzeniu obszernej dokumentacji fotograficznej.

Podczas oględzin będziemy poszukiwać części składowych, które miały wpływ lub przyczyniły się do powstania pożaru. Części te nazwiemy śladami kryminalistycznymi, którymi będą „wszelkie zmiany w obiektywnej rzeczywistości, które jako postrzegalne znamiona po zdarzeniach będących przedmiotem postępowania stanowią podstawę do odtworzenia przebiegu tych zdarzeń zgodnie z rzeczywistością”[9].

W celu prawidłowego ujawnienia i zachowania wartości dowodowej śladów kryminalistycznych zabezpieczonych w trakcie oględzin miejsca pożaru powinniśmy, w miarę możliwości, odpowiedzieć sobie na tzw. siedem złotych pytań kryminalistki:

1) CO się zdarzyło (to znaczy czy badane zdarzenie jest w ogóle przestępstwem, czy też zdarzeniem innego rodzaju)?
2) GDZIE zdarzenie nastąpiło?
3) KIEDY (w jakim czasie)?
4) JAK (tzn. jaki był jego przebieg i sposób spowodowania)?
5) CZYM go spowodowano (patrząc od strony technicznej – czego używano)?
6) DLACZEGO zdarzenie zaistniało (motyw, pobudka, przyczyna)?

7) KTO uczestniczył w zdarzeniu i w jakiej roli (sprawca główny, pomocnicy, pokrzywdzeni, świadkowie itd.)?

Ponadto należy dążyć do uzyskania odpowiedzi na kilka innych, równie istotnych pytań, a mianowicie:

1) w jakich okolicznościach doszło do pożaru?
2) w którym miejscu doszło do zarzewia ognia?
3) czy ktoś przyczynił się do pożaru?
4) dlaczego doszło do pożaru?
5) jakiego rodzaju ślady zabezpieczyć?
6) do jakich badań będą wysyłane ślady?

Pod pojęciem prawidłowej ochrony i zachowania wartości dowodowej śladów kryminalistycznych ujawnionych na miejscu zdarzenia rozumiemy ich zabezpieczenie procesowe i techniczne.

W skład procesowego zabezpieczania śladu wchodzi:

1) opis śladu w protokole oględzin, który powinien zawierać:
   – dokładny opis miejsca ujawnienia śladu,
   – dokładne zwymiarowanie śladu od stałych odniesienia,
   – dokładny opis charakterystyki śladu wraz z jego wymiarami;
2) wykonanie metryczki śladowej, która powinna zawierać:
   – opis, miejsce i datę czynności,
   – sposób ujawnienia śladu,
   – sposób zabezpieczenia śladu,
   – podpis osoby ujawniającej i zabezpieczającej ślad oraz nazwę jednostki organizacyjnej;
3) wykonanie dokumentacji fotograficznej, która powinna pokazywać przestrzenne relacje pomiędzy śladem a jego otoczeniem;
4) zaznaczenie na szkicu miejsca ujawnienia śladu[10].

W zależności od rodzaju śladu, do jego technicznego zabezpieczenia można zastosować jedną lub więcej z poniższych metod:

1) zabezpieczenie śladu w całości;
2) zabezpieczenie śladu wraz z podłożem;
3) zabezpieczenie śladu przez pobranie próbki;
4) zabezpieczenie śladu przez wykonanie odwzorowania w postaci:
   – zabezpieczenia śladu na folię daktyloskopijną lub żelatynową,
   – wykonania odlewu gipsowego lub sylikonowego,
   – wykonania repliki sylikonowej;
5) wykonanie fotografii śladu, która powinna zawierać następujące elementy:
   – linia odniesienia obiektywu powinna być ustawiona prostopadle do płaszczyzny śladu oraz wycentrowana względem jego środka,
   – ślad powinien wypełniać większą część kadru, a dzięki odpowiednio dobranej ekspozycji przekazywać maksymalną ilość informacji,
   – przy śladzie powinna znajdować się skalówka ułożona równoległe do jego dłuższej krawędzi, natomiast oznaczenie śladu (numerek) powinno być ustawione przy skalówce i na wysokości śladu.

Fot. 3. Protokół oględzin i metryczka śladowa.

Zabezpieczenie śladów kryminalistycznych nie może opierać się wyłącznie na jednej z powyższych form. Aby było skuteczne, konieczne jest jednoczesne zastosowanie zabezpieczenia procesowego i technicznego, które wzajemnie się uzupełniają i warunkują prawidłową wartość dowodową śladów. Ślady ujawniane na miejscu pożaru, a w szczególności ich wygląd, często są niejasne dla osób prowadzących oględziny. Dlatego czynności oględzin, a co za tym idzie i ujawnianie śladów, powinny odbywać się w porze dziennej oraz w obecności biegłego z zakresu pożarnictwa.

Na miejscu zdarzenia związanego z pożarem do najczęściej identyfikowanych śladów sugerujących umyślne wzniecenie pożaru należą:

- obecność wielu niezależnych ognisk pożaru,
- nietypowe wypalenia oraz deformacje materiałów świadczące o gwałtownym działaniu wysokiej temperatury,
- pęknięcia i rozwarstwienia betonu, powstałe w wyniku kontaktu z cieczą palną i jej intensywnego spalania,
- dynamiczny rozwój pożaru, wskazujący na użycie substancji łatwopalnych,
- charakterystyczne wypalenia na podłodze, odzwierciedlające kształt rozlanej cieczy palnej,

Fot. 4. Miejsce pożaru.

- na podłożu drewnianym: naprzemienne strefy spalonych i niespalonych fragmentów, zlokalizowane poniżej powierzchni, typowe dla miejscowego rozlewu i zapłonu cieczy,
- w korytarzach: stożkowate opalenia na przeciwległych ścianach, będące efektem rozlania i zapalenia cieczy palnej,
- na ścianach: wypalenia o szerokości odpowiadającej plamie cieczy palnej znajdującej się u ich podstawy,
- wyczuwalny zapach cieczy palnej, utrzymujący się nawet w pogorzelisku,
- fragmenty nadpalonych tkanin o zapachu mieszanin węglowodorowych,
- pojemniki (często bez nakrętki) noszące ślady cieczy palnej,
- puszki lub inne naczynia, które mogły służyć do umieszczenia świec inicjujących zapłon,
- ślady włamania mogące wskazywać na motyw kryminalny,
- obecność elementów urządzeń, które nie powinny znajdować się w danym pomieszczeniu (np. baterii, mechanizmów zegarowych, układów elektronicznych),
- ślady ingerencji w instalacje gazowe lub elektryczne.

Do charakterystycznych śladów mogących wskazywać na elektryczną genezę pożaru zalicza się:

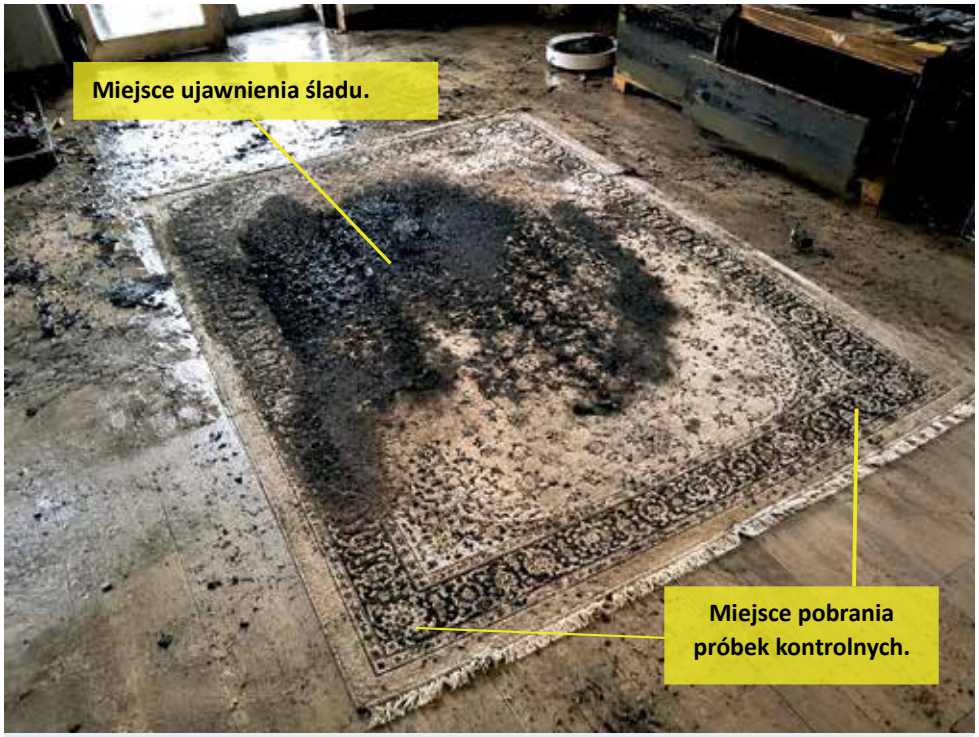
- stopienia i wytopienia typowe dla zwarcia lub działania łuku elektrycznego, ujawniane na przewodach, elementach sprzętu elektrotechnicznego oraz metalowych częściach konstrukcyjnych,
- ślady iskrzenia, przegrzania i wysokiej oporności stykowej na zaciskach oraz elementach stykowych urządzeń,
- uszkodzenia bezpieczników, w tym nadtopione ziarna piasku gasikowego, świadczące o przepływie prądu przekraczającego wartość znamionową,
- głębokie, miejscowe zwęglenia materiałów palnych, mogące wskazywać na pozostawienie rozgrzanego urządzenia grzejnego,
- charakterystyczne stopienia przewodów powstałe w wyniku zwarcia, które mogą zostać laboratoryjnie zweryfikowane pod kątem czasu ich powstania (przed pożarem lub w jego trakcie)[11].

NAJCZĘSTSZE NIEPRAWIDŁOWOŚCI PODCZAS ZABEZPIECZANIA ŚLADÓW Z MIEJSCA POŻARU

Nieprawidłowe zabezpieczenie śladów pochodzących z pożarów stanowi istotny problem w praktyce kryminalistycznej, wpływający bezpośrednio na wartość dowodową zgromadzonego materiału oraz możliwość prawidłowej rekonstrukcji przebiegu zdarzenia. Analiza praktyki oraz literatury przedmiotu wskazuje, iż uchybienia w tym zakresie wynikają z wielu czynników o charakterze organizacyjnym, proceduralnym oraz ludzkim.

Do najistotniejszych przyczyn należy zaliczyć brak współpracy oraz właściwej komunikacji pomiędzy służbami obecnymi na miejscu zdarzenia, co może prowadzić do utraty ważkich informacji dotyczących przebiegu pożaru oraz lokalizacji jego ogniska[12]. Równie istotnym proble-

Fot. 5. Instalacja elektryczna.



Fot. 6. Miejsce pożaru. Zdj. 2–6. M. Wrzosek.

mem jest niewłaściwe zabezpieczenie miejsca zdarzenia do czasu przeprowadzenia oględzin, w szczególności brak ewidencji osób przemieszczających się po tym obszarze, co powoduje zanieczyszczenie lub zatarcie śladów[13].

W praktyce odnotowuje się również przypadki nieprzestrzegania zasad prowadzenia oględzin, w tym niewyznaczenia lub nieprawidłowego wyznaczenia granic terenu oględzin. Uchybienia te mogą skutkować pominięciem ważnych obszarów lub naruszeniem integralności miejsca zdarzenia[14]. Mankamentem pozostaje także niewłaściwa dokumentacja procesowa lub jej brak, co uniemożliwia odtworzenie pierwotnego stanu pogorzeliska oraz kontekstu ujawnionych śladów[15].

Kolejną grupę czynników stanowią niedostatki w zakresie przygotowania merytorycznego osób uczestniczących w oględzinach, w tym brak odpowiedniego przeszkolenia techników kryminalistyki. W połączeniu z użyciem nieodpowiednich narzędzi lub technik zabezpieczania śladów może to prowadzić do ich uszkodzenia, utraty bądź kontaminacji[16]. Negatywny wpływ na jakość prowadzonych czynności wywierają również pośpiech oraz presja czasu, a także niewłaściwe pakowanie i przechowywanie materiału dowodowego, zwłaszcza w przypadku śladów zawierających substancje lotne[17].

Nie bez znaczenia pozostają także czynniki techniczne i środowiskowe, takie jak nieodpowiednie wyposażenie technika kryminalistyki czy niekorzystne warunki atmosferyczne, które mogą utrudniać prawidłowe ujawnianie i zabezpieczanie śladów. Ponadto w literaturze wskazuje się na błędy wynikające ze zmęczenia lub nieuwagi osób przeprowadzających oględziny, co zwiększa ryzyko popełnienia uchybień. Za poważne naruszenie metodyki należy również uznać prowadzenie czynności na miejscu pożaru bez udziału biegłego z zakresu pożarnictwa, którego wiedza specjalistyczna jest kluczowa dla prawidłowej interpretacji śladów pożarowych[18].

Wśród najczęściej występujących uchybień praktycznych należy wskazać zanieczyszczenie materiału dowodowego, wynikające z nieprzestrzegania podstawowych zasad higieny pracy, takich jak stosowanie jednorazowych rękawic ochronnych czy unikanie kontaktu krzyżowego między próbkami. Tego rodzaju zaniedbania mogą prowadzić do przeniesienia substancji łatwopalnych pomiędzy próbkami, co znacząco utrudnia ich późniejszą analizę laboratoryjną[19].

Do poważnych uchybień należy również zaliczyć niedostateczną dokumentację procesową miejsca zdarzenia. Brak szczegółowej dokumentacji fotograficznej oraz opisowej przed przystąpieniem do zabezpieczania śladów uniemożliwia odtworzenie ich pierwotnego rozmieszczenia i kontekstu przestrzennego, mające kluczowe znaczenie dla rekonstrukcji przebiegu pożaru. W praktyce spotyka się także przypadki nieprzestrzegania przyjętej metodyki prowadzenia oględzin pogorzeliska, w tym chaotycznego pobierania próbek bez uwzględnienia stref intensywności spalania[20].

Równie istotnym błędem popełnianym podczas oględzin miejsca pożaru jest niepobieranie próbek kontrolnych, które odgrywają kluczową rolę w procesie analizy kryminalistycznej. Próbki kontrolne stanowią materiał porównawczy, umożliwiający odróżnienie substancji naturalnie występujących w środowisku pogorzeliska od tych, które mogły zostać użyte celowo, np. jako przyspieszacze spalania. Ich brak znacząco utrudnia interpretację wyników badań laboratoryjnych oraz może prowadzić do błędnych wniosków dotyczących przyczyn powstania pożaru. Niepobranie próbek kontrolnych ogranicza możliwość weryfikacji, czy wykryte związki chemiczne są efektem procesów spalania materiałów znajdujących się w obiekcie, czy też stanowią ślad użycia substancji łatwopalnych. W konsekwencji może dojść zarówno do fałszywie pozytywnej identyfikacji przyspieszaczy spalania, jak i do ich błędnego wykluczenia. Tego rodzaju nieprawidłowość ma szczególne znaczenie w sprawach o charakterze przestępczym, gdzie prawidłowa kwalifikacja zdarzenia zależy od rzetelnej analizy śladów chemicznych.

Z punktu widzenia metodyki oględzin miejsca pożaru pobieranie próbek kontrolnych powinno stanowić standardową procedurę, realizowaną równolegle z zabezpieczaniem właściwego materiału dowodowego. Ich brak należy zatem uznać za poważne naruszenie zasad postępowania kryminalistycznego, mogące prowadzić do obniżenia wartości dowodowej zgromadzonego materiału oraz utrudnienia lub uniemożliwienia prawidłowej rekonstrukcji przebiegu zdarzenia[21].

Mając powyższe na uwadze, możemy wywnioskować, że nieprawidłowości w zabezpieczaniu śladów pożarowych mają charakter wieloczynnikowy i wynikają zarówno z niedoskonałości organizacyjnych, jak i błędów osób obecnych na miejscu zdarzenia oraz prowadzących oględziny. Ich konsekwencją może być obniżenie wartości dowodowej materiału, a w skrajnych przypadkach – błędne ustalenia faktyczne w toku postępowania karnego.

ZAKOŃCZENIE

Założeniem niniejszego artykułu było przybliżenie czytelnikowi problematyki pożaru w ujęciu kryminalistycznym oraz znaczenia prawidłowego zabezpieczania śladów podczas oględzin miejsca pożaru. Omówiona w nim definicja pożaru, zarówno w znaczeniu ogólnym, jak i prawnym, wskazała na istotę powstającego zagrożenia dla życia, zdrowia oraz mienia, wynikającego z niekontrolowanego procesu spalania. Przedstawione podstawowe zasady prowadzenia oględzin pogorzeliska, rodzaje śladów pożarowych oraz sposoby ich procesowego i technicznego zabezpieczania miały za zadanie przybliżyć prawidłowe ich wykonanie oraz wskazać najczęściej pojawiające się błędy. Szczególną uwagę należało zwrócić na ślady mogące świadczyć o umyślnym podpaleniu lub elektrycznej genezie pożaru, a także na znaczenie dokumentacji fotograficznej i udziału biegłego z zakresu pożarnictwa podczas oględzin. Omówione w artykule najczęściej występujące nieprawidłowości związane z zabezpieczaniem materiału dowodowego, takie jak zanieczyszczenie próbek, błędy w dokumentacji czy niepobranie próbek kontrolnych miały na celu ich wyeliminowanie. Na podstawie przedstawionych informacji wskazano, że nieprawidłowości w zabezpieczaniu śladów mogą utrudnić ustalenie przyczyn pożaru oraz obniżyć wartość dowodową zgromadzonego materiału.

[1] Rządowe Centrum Bezpieczeństwa, *Pożar – bądź bezpieczny*, https://www.gov.pl/web/rcb/pozar=--badz-bezpieczn6y#:~:text-Po%C5%BCar%20%20to%20niekontrolowany%20proces%20spalania,nie%20jest%20do%20tego%20przeznaczone [dostęp: 24.03.2026 r.].

[2] M. Pupek, *Pożar i jego rozwój*, https://www.gov.pl/attachment/dce442bf-7980-4b1b-9a2a-76d3ee4aaaf8 [dostęp: 24.03.2026 r.].

[3] Dz. U. z 2025 r. poz. 383, z późn. zm.

[4] Art. 115 § 5 kk. Mieniem znacznej wartości jest mienie, którego wartość w czasie popełnienia czynu zabronionego przekracza 200 000 złotych.
§ 6. Mieniem wielkiej wartości jest mienie, którego wartość w czasie popełnienia czynu zabronionego przekracza 1 000 000 złotych.
§ 7. Przepis § 5 stosuje się odpowiednio do określenia „znaczna szkoda" oraz określenia „wartość lub łączna wartość jest znaczna".
§ 7a. Przepis § 6 stosuje się odpowiednio do określenia „szkoda w wielkich rozmiarach".

[5] Główny Urząd Statystyczny, *Działalność służb ratowniczych*, https://stat.gov.pl/wyszukiwarka/szukaj.html [dostęp: 26.03.2026 r.].

[6] Policja, Statystyka, *Przestępstwa przeciwko bezpieczeństwu powszechnemu (163–172)*, https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-1/63441,Sprowadzenie-zdarzenia-powszechnie-niebezpiecznego-art-163.html [dostęp: 19.05.2026 r.].

[7] Konspoż, *Trójkąt spalania*, https://konspoz.pl/trojkat-spalania/#:~:text=Tr%C3%B3jk%C4%85t%20spalania%20to%20model%2C%20kt%C3%B3ry%20wyja%C5%9Bnia%2C%20jak,co%20stanowi%20podstaw%C4%99%20dzia%C5%82a%C5%84%20prewencyjnych%20i%20ga%C5%9Bniczych [dostęp: 24.03.2026 r.].

[8] T. Sawicki, *Ślady popożarowe*, https://www.ppoz.pl/czytelnia/rozpoznawanie-zagrozen/Slady-popozarowe/idn:1621 [dostęp: 7.04.2026 r.].

[9] I. Bogusz, M. Bogusz, *Ślady kryminalistyczne dla słuchaczy szkolenia zawodowego podstawowego*, CSP, Legionowo 2015, s. 7.

[10] Tamże, s. 37.

[11] T. Sawicki, *Pożary, przyczyny, metodyka, przykłady (wybrane zagadnienia*, Lublin 2021, s. 54–111.

[12] Tamże, s. 113–114.

[13] M. Kulicki, V. Kwiatkowska-Wójcikiewicz, *Kryminalistyka. Wybrane zagadnienia teorii i praktyki*, Toruń 2020, s. 419–420.

[14] E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka – czyli rzecz o metodach śledczych*, Warszawa 2021, s. 203.

[15] K. Witkowska, *Oględziny. Aspekty procesowe i kryminalistyczne*, Warszawa 2013, s. 36–45.

[16] Kontaminacja (zanieczyszczenie materiału dowodowego) to niepożądane wprowadzenie do śladu kryminalistycznego obcych substancji, cząstek lub informacji, które nie są związane z badanym zdarzeniem, a które mogą zmienić jego właściwości, skład lub wartość dowodową, prowadząc do błędnych wyników analizy lub nieprawidłowych wniosków. B. Hołyst, *Kryminalistyka*, Warszawa 2018, s. 188.

[17] B. Hołyst, *Kryminalistyka*, Warszawa 2018, s. 478–480.

[18] *Psychologia w kryminalistyce*, red. E. Gruza, Warszawa 2020, s. 300.

[19] B. Hołyst, *Kryminalistyka*, s. 500.

[20] E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka – czyli o współczesnych metodach dowodzenia przestępstw*, Warszawa 2020, s. 664.

[21] Tamże.

Summary

Fire – theoretical and practical methods of securing forensic evidence during a fire scene examination

The article discusses the issue of fire from a forensic perspective, focusing on the importance of properly securing evidence during the examination of the fire scene. The article points out that fire is an uncontrolled combustion process that poses a threat to life, health, and property, and its analysis requires both theoretical knowledge and practical skills.
The basics of fire formation mechanism are discussed, including the combustion triangle concept, and fire traces resulting from the impact of high temperature and combustion products are characterized. It was emphasized that the inspection of the fire scene should be conducted in accordance with specific principles, maintaining safety, proper securing of the area and reliable photographic documentation.
Special attention was paid to forensic evidence that enable the fire scene reconstruction. The need to use both procedural and technical methods of securing evidence was indicated, as well as to strive to answer key forensic questions. Characteristic evidence that may indicate arson or an electrical failure cause of the fire were also presented.
An important part of the article is the analysis of the most common errors committed during examination, such as improper securing of the fire scene, gaps in documentation, lack of cooperation between services, contamination of evidence, and failure to collect control samples.
It was emphasized that these errors could significantly reduce the probative value of the collected evidence and make it difficult to determine the cause of the fire.
The conclusion from the article is that there is a need to maintain high standards in securing evidence and strictly adhere to the examination methodology, which is crucial for the proper conduct of criminal proceedings and determining the fire scene reconstruction.

Tłumaczenie: Beata Pepłowska

HULAJNOGA ELEKTRYCZNA W EDUKACJI KOMUNIKACYJNEJ UCZNIA

Praktyczne wnioski z projektu edukacyjnego realizowanego w Rzeszowie

Grafika wygenerowana z wykorzystaniem licencjonowanego programu Adobe Firefly.

Mateusz Szarek

Prezes Polskiego Stowarzyszenia Lekkiej Elektromobilności

Artykuł przedstawia doświadczenia projektu edukacyjnego realizowanego w Rzeszowie, którego celem było praktyczne wsparcie dzieci, rodziców, nauczycieli oraz instytucji odpowiedzialnych za bezpieczeństwo ruchu drogowego. Programem objęto pięć szkół podstawowych i około 400 uczniów, a działania obejmowały zarówno część teoretyczną, jak i praktyczną naukę korzystania z hulajnogi elektrycznej w kontrolowanych warunkach. Szczególne znaczenie miało także pierwsze w Polsce uzupełnienie egzaminu na kartę rowerową w WORD Rzeszów o elementy teoretyczne i praktyczne dotyczące hulajnogi elektrycznej.

W artykule wskazano, że skuteczna profilaktyka powinna obejmować nie tylko zasady poruszania się po drodze, lecz także warunki techniczne pojazdu, odpowiedzialność rodzica przy zakupie hulajnogi oraz ryzyka związane z nabywaniem pojazdów niespełniających wymogów obowiązujących w Polsce. Karta rowerowa została przedstawiona jako wartościowe i istniejące już narzędzie edukacji komunikacyjnej, które nie powinno być marginalizowane, lecz rozwijane i dostosowywane do współczesnych realiów mobilności. Wnioski z projektu wskazują, że bezpieczeństwo dzieci korzystających z hulajnóg elektrycznych wymaga połączenia regulacji prawnych, edukacji praktycznej, odpowiedzialności rodziców oraz współpracy szkół, Policji, WORD, straży miejskich, samorządów i organizacji branżowych.

Wprowadzenie

Rozwój hulajnóg elektrycznych jako jednej z najpopularniejszych nowych form mobilności ostatnich lat wymaga spojrzenia wykraczającego poza samą kontrolę i sankcje. Szczególnego znaczenia nabiera to w odniesieniu do dzieci i młodzieży, ponieważ korzystanie z hulajnogi elektrycznej w ruchu drogowym wymaga nie tylko umiejętności technicznego prowadzenia pojazdu, lecz także znajomości przepisów, odpowiedniego wieku, wymaganych uprawnień oraz świadomości zagrożeń. Od 3 marca 2026 r. obowiązuje zakaz dopuszczania dziecka w wieku do 13 lat do kierowania hulajnogą elektryczną lub urządzeniem transportu osobistego na drodze[1]. Osoby niepełnoletnie, które ukończyły 13 lat, powinny posiadać odpowiednie uprawnienia, w praktyce najczęściej kartę rowerową[2]. Od 3 czerwca 2026 r. dodatkowo zacznie obowiązywać nakaz używania kasku ochronnego przez osoby poniżej 16. roku życia kierujące m.in. hulajnogą elektryczną[3].

Fot. 1. Szkolenie dla nauczycieli w WORD Rzeszów w zakresie prowadzenia zajęć oraz egzaminowania uczniów ubiegających się o kartę rowerową.

Hulajnoga elektryczna w ciągu kilku lat stała się jednym z najbardziej rozpoznawalnych symboli nowych form mobilności. Dla dorosłych bywa sposobem na szybkie przemieszczanie się po mieście. Dla dzieci i młodzieży często jest natomiast atrakcyjnym urządzeniem kojarzonym z niezależnością, nowoczesnością i zabawą. Problem polega na tym, że w sensie prawnym hulajnoga elektryczna jest pojazdem, którego użytkowanie w ruchu drogowym wymaga znajomości przepisów, odpowiedniego wieku, a w przypadku osób niepełnoletnich także określonych uprawnień.

W praktyce społecznej ta świadomość nie zawsze jest wystarczająca. Wielu rodziców kupuje hulajnogę elektryczną przede wszystkim przez pryzmat ceny, wyglądu, zasięgu lub deklarowanej prędkości. Rzadziej analizowane są parametry techniczne, wymagania prawne, dokumentacja pojazdu, obecność podmiotu odpowiedzialnego za produkt na rynku europejskim czy faktyczna możliwość bezpiecznego serwisowania urządzenia. W efekcie dziecko może otrzymać pojazd, którego nie powinno używać w ruchu drogowym albo którego parametry nie odpowiadają obowiązującym ograniczeniom.

Z punktu widzenia bezpieczeństwa ruchu drogowego problem nie zaczyna się więc dopiero na drodze. Bardzo często zaczyna się wcześniej, czyli w sklepie internetowym, na platformie marketplace, podczas rodzinnej decyzji zakupowej lub w momencie, gdy dorosły dopuszcza dziecko do korzystania z pojazdu bez pełnej wiedzy o przepisach.

Dlatego edukacja dotycząca hulajnóg elektrycznych powinna być rozumiana szerzej niż tylko przypomnienie kilku zasad ruchu drogowego. Powinna obejmować dziecko jako przyszłego uczestnika ruchu, rodzica jako osobę podejmującą decyzję zakupową i wychowawczą, nauczyciela jako osobę wspierającą edukację komunikacyjną oraz instytucje publiczne, które odpowiadają za profilaktykę, egzaminowanie, organizację ruchu i bezpieczeństwo lokalne.

Założenia projektu edukacyjnego w Rzeszowie

Projekt edukacyjny „Edukacja bezpieczeństwa ruchu drogowego dzieci i młodzieży w zakresie nowych form mobilności, w tym hulajnóg elektrycznych" został zainicjowany przez Polskie Stowarzyszenie Lekkiej Elektromobilności jako odpowiedź na rosnącą potrzebę praktycznego wsparcia dzieci, rodziców, nauczycieli i instytucji w zakresie bezpiecznego korzystania z nowych form mobilności[4].

Programem objęto pięć szkół podstawowych z terenu Rzeszowa: Szkołę Podstawową nr 6, Szkołę Podstawową nr 19, Szkołę Podstawową nr 24, Szkołę Podstawową nr 25 oraz Szkołę Podstawową nr 29. Łącznie w działaniach uczestniczyło około 400 uczniów, przede wszystkim z klas IV, czyli z grupy wiekowej przygotowującej się do uzyskania karty rowerowej[5].

Założenie projektu było proste: dzieciom nie wystarczy powiedzieć, że mają przestrzegać przepisów. Trzeba im pokazać, które zasady mają znaczenie w codziennych sytuacjach, dlaczego istnieją i w jaki sposób wpływają na ich bezpieczeństwo. W przypadku hulajnogi elektrycznej szczególnie ważne jest używanie jej w przestrzeni publicznej, co wiąże się z konkretnymi obowiązkami.

Projekt był realizowany przy współpracy instytucji odpowiedzialnych za bezpieczeństwo i edukację komunikacyjną. W działania zaangażowane były m.in. Komenda Miejska Policji w Rzeszowie, Wydział Ruchu Drogowego KMP w Rzeszowie, Wojewódzki Ośrodek Ruchu Drogowego w Rzeszowie, Straż Miejska w Rzeszowie, Wydział Edukacji Urzędu Miasta Rzeszowa, Rzeszowski Ruch Miejski oraz szkoły podstawowe uczestniczące w projekcie.

Wybór klas IV nie był przypadkowy. To właśnie na tym etapie uczniowie przygotowują się do uzyskania karty rowerowej, zaczynają samodzielniej poruszać się w przestrzeni publicznej i coraz częściej spotykają się z hulajnogami elektrycznymi – jako użytkownicy, uczestnicy ruchu albo obserwatorzy zachowań dorosłych i rówieśników. Dlatego projekt nie miał charakteru jednorazowej pogadanki, lecz był próbą praktycznego uzupełnienia edukacji komunikacyjnej o temat, który już realnie funkcjonuje w życiu dzieci.

Zakres działań obejmował część teoretyczną, materiały edukacyjne, spotkania informacyjne oraz elementy praktyczne. Istotnym założeniem projektu było połączenie rozmowy o przepisach z praktyczną nauką korzystania z hulajnogi elektrycznej w kontrolowanych warunkach. Uczniowie mogli zapoznać się z podstawami prowadzenia pojazdu, hamowania, utrzymywania toru jazdy, zachowania ostrożności oraz reagowania na sytuacje, które mogą wystąpić w ruchu drogowym.

Nowy kontekst prawny

Zmiany obowiązujące od 2026 r. wzmacniają znaczenie edukacji komunikacyjnej. Od 3 marca 2026 r. w ustawie – Prawo o ruchu drogowym obowiązuje zakaz dopuszczania dziecka w wieku do 13 lat do kierowania hulajnogą elektryczną lub urządzeniem transportu osobistego na drodze[6]. Ustawodawca przewidział jednak wyjątek odnoszący się do strefy zamieszkania. W tym przypadku dziecko poniżej 13. roku życia może kierować hulajnogą elektryczną lub urządzeniem transportu osobistego wyłącznie pod opieką osoby dorosłej[7].

W przypadku osób, które ukończyły 13 lat, ale nie są jeszcze pełnoletnie, samo osiągnięcie wymaganego wieku nie jest wystarczające. Do kierowania hulajnogą elektryczną przez osobę niepełnoletnią wymagane jest posiadanie od-


2


3


4

Fot. 2. Zajęcia teoretyczne dotyczące uprawnień do kierowania hulajnogą elektryczną w klasie IV Szkoły Podstawowej nr 25 w Rzeszowie.

Fot. 3. Spotkanie z rodzicami uczniów klas IV–VIII w Szkole Podstawowej nr 24 w Rzeszowie, poświęcone bezpiecznemu zakupowi oraz korzystaniu z hulajnóg elektrycznych.

Fot. 4. Zajęcia praktyczne z jazdy na hulajnodze elektrycznej dla uczniów klasy IV Szkoły Podstawowej nr 24 w Rzeszowie.

powiednich uprawnień. W praktyce najczęściej będzie to karta rowerowa, choć przepisy dopuszczają również określone kategorie prawa jazdy, tj. AM, A1, B1, B lub T[8].

Osoby pełnoletnie mogą kierować hulajnogą elektryczną bez dodatkowych uprawnień. Nie oznacza to jednak dowolności w wyborze miejsca jazdy. Kierujący hulajnogą elektryczną jest obowiązany korzystać z drogi dla rowerów, drogi dla pieszych i rowerów albo pasa ruchu dla rowerów, jeżeli są one wyznaczone dla kierunku, w którym się porusza lub zamierza skręcić[9]. W przypadku braku takiej infrastruktury może korzystać z jezdni, ale tylko wtedy, gdy ruch pojazdów na tej jezdni jest dozwolony z prędkością nie większą niż 30 km/h[10]. Korzystanie z drogi dla pieszych ma charakter wyjątkowy i jest dopuszczalne jedynie wtedy, gdy droga dla pieszych jest usytuowana wzdłuż jezdni, po której ruch pojazdów jest dozwolony z prędkością większą niż 30 km/h, a jednocześnie brakuje drogi dla rowerów, drogi dla pieszych i rowerów oraz pasa ruchu dla rowerów[11].

W praktyce oznacza to, że użytkownik hulajnogi elektrycznej powinien każdorazowo ocenić nie tylko własny wiek i posiadane uprawnienia, ale również rodzaj drogi, po której zamierza się poruszać. Jeżeli korzysta z drogi dla pieszych, ma obowiązek jechać z prędkością zbliżoną do prędkości pieszego, zachować szczególną ostrożność, ustępować pierwszeństwa pieszemu oraz nie utrudniać jego ruchu[12]. Przepisy zabraniają również przewożenia hulajnogą elektryczną innej osoby, zwierzęcia lub ładunku, ciągnięcia albo holowania innego pojazdu oraz jazdy po jezdni poza przypadkami wyraźnie dopuszczonymi w ustawie[13].

Odrębnym zagadnieniem są warunki techniczne samego pojazdu. Hulajnoga elektryczna, aby mogła być traktowana jako pojazd zgodny z obowiązującymi wymaganiami, powinna spełniać kryteria wynikające z przepisów technicznych, w tym ograniczenie prędkości konstrukcyjnej do 20 km/h[14]. Jej masa własna nie może przekraczać 30 kg[15]. Pojazd powinien być wyposażony m.in. w co najmniej jedno światło pozycyjne barwy białej albo żółtej selektywnej z przodu, co najmniej jedno światło pozycyjne barwy czerwonej oraz czerwony odblask z tyłu, elementy odblaskowe po bokach, co najmniej jeden skutecznie działający hamulec oraz dzwonek albo inny sygnał ostrzegawczy o nieprzeraźliwym dźwięku[16]. Ponadto hulajnoga elektryczna powinna być wyposażona w numer rozpoznawczy nadany i umieszczony przez producenta w sposób trwały na ramie lub innym podobnym podstawowym elemencie konstrukcyjnym, a także w podpórkę lub podpórki zapewniające stabilne ustawienie hulajnogi elektrycznej na podłożu[17].

Kolejna istotna zmiana została przewidziana od 3 czerwca 2026 r. Od tego dnia osoby poniżej 16. roku życia będą obowiązane do używania kasku ochronnego podczas kierowania rowerem, hulajnogą elektryczną lub urządzeniem transportu osobistego[18]. Przepis ten wzmacnia profilaktyczny charakter nowych regulacji, ponieważ odnosi się bezpośrednio do ograniczenia skutków ewentualnych upadków i zdarzeń drogowych z udziałem najmłodszych uczestników ruchu[19].

Zmiany te pokazują, że ustawodawca coraz wyraźniej dostrzega potrzebę ochrony najmłodszych uczestników ruchu. Sam przepis nie jest jednak wystarczający, jeżeli nie zostanie zrozumiany przez tych, których dotyczy. Dziecko musi wiedzieć, dlaczego nie może jechać określoną drogą. Rodzic musi wiedzieć, kiedy może dopuścić dziecko do korzystania z hulajnogi. Nauczyciel powinien mieć możliwość omówienia tego zagadnienia w sposób prosty i zgodny z prawem. Policjant prowadzący działania profilaktyczne powinien dysponować materiałem, który nie tylko wskazuje zakazy, ale wyjaśnia ich sens.

Hulajnoga elektryczna jako temat edukacyjny, techniczny i wychowawczy

W mediach hulajnoga elektryczna bywa przedstawiana głównie w kontekście wypadków, nieprawidłowego parkowania, jazdy po drogach dla pieszych lub zachowań niezgodnych z przepisami. Taka perspektywa jest zrozumiała, ponieważ to właśnie zdarzenia niebezpieczne najczęściej przyciągają uwagę opinii publicznej. Nie wyczerpuje ona jednak problemu. Nadmierne uproszczenie tej narracji

może prowadzić do wniosku, że podstawową odpowiedzią na rozwój nowych form mobilności powinny być wyłącznie zakazy, kontrole i sankcje.
W przypadku dzieci i młodzieży hulajnoga elektryczna powinna być traktowana równocześnie jako temat edukacyjny, techniczny i wychowawczy. Edukacyjny, ponieważ jej użytkowanie wymaga znajomości zasad ruchu drogowego. Techniczny, ponieważ nie każdy pojazd oferowany w sprzedaży spełnia wymagania, które pozwalają na bezpieczne i legalne korzystanie z niego w Polsce. Wychowawczy, ponieważ decyzja o dopuszczeniu dziecka do jazdy należy w dużej mierze do osoby dorosłej.
W praktyce szkolnej naturalnym punktem odniesienia pozostaje karta rowerowa. Jej uzyskanie jest uregulowane odrębnymi przepisami, które określają m.in. wymagania oraz sposób organizacji zajęć, a także tryb i warunki przeprowadzania egzaminu w zakresie karty rowerowej[20]. W tym sensie karta rowerowa pozostaje podstawowym formalnym narzędziem przygotowania dzieci do samodzielnego uczestnictwa w ruchu drogowym.
Znaczenie tego narzędzia potwierdzają dane zebrane w Rzeszowie w ramach działań Polskiego Stowarzyszenia Lekkiej Elektromobilności. Badaniem objęto szkoły podstawowe z terenu miasta Rzeszowa, pozostające w obszarze właściwości Wydziału Edukacji Urzędu Miasta Rzeszowa. Z informacji przekazanych przez szkoły wynika, że spośród 9986 uczniów klas IV–VIII kartę rowerową posiada 7144 uczniów, co stanowi około 72% badanej grupy. Karty rowerowej nie posiada 2506 uczniów, natomiast w przypadku 336 uczniów szkoły nie posiadały danych[21].

Tabela 1. Status uczniów klas IV–VIII w zakresie posiadania karty rowerowej w Rzeszowie.

STATUS UCZNIÓW KLAS IV–VIII W ZAKRESIE POSIADANIA KARTY ROWEROWEJ	LICZBA UCZNIÓW	UDZIAŁ W BADANEJ GRUPIE
Uczniowie posiadający kartę rowerową	7144	72%
Uczniowie nieposiadający karty rowerowej	2506	25%
Brak danych uczniów	336	3%
Łącznie	9986	100%

Źródło: dane zebrane przez Polskie Stowarzyszenie Lekkiej Elektromobilności w ramach projektu edukacyjnego „Edukacja bezpieczeństwa ruchu drogowego dzieci i młodzieży w zakresie nowych form mobilności, w tym hulajnóg elektrycznych", na podstawie informacji przekazanych przez szkoły podstawowe z terenu miasta Rzeszowa w roku szkolnym 2025/2026.

Dane te prowadzą do dwóch istotnych wniosków. Po pierwsze, karta rowerowa jest realnie obecna w systemie edukacji komunikacyjnej dzieci i młodzieży, dlatego może stanowić naturalny punkt wyjścia do rozmowy o hulajnogach elektrycznych. Po drugie, sama informacja o posiadaniu karty rowerowej nie rozwiązuje wszystkich problemów praktycznych. Obecnie brakuje jednolitego, łatwego i szybkiego sposobu weryfikacji uprawnień dziecka w codziennych sytuacjach, poza fizycznym posiadaniem dokumentu przy sobie.
Z tego względu interesującym kierunkiem są prowadzone w Rzeszowie prace nad możliwością powiązania informacji o posiadaniu karty rowerowej z Kartą Mieszkańca. Takie rozwiązanie mogłoby w przyszłości ułatwić potwierdzanie uprawnień bez konieczności każdorazowego posiadania przy sobie tradycyjnego dokumentu. Wymaga to jednak dalszych analiz organizacyjnych, prawnych i technicznych, w szczególności w zakresie ochrony danych, sposobu potwierdzania informacji oraz dostępu do niej przez uprawnione podmioty[22].
Nowe formy mobilności nie powinny zastępować dotychczasowego systemu edukacji komunikacyjnej, lecz go uzupełniać. Dziecko, które uczy się zasad pierwszeństwa, znaków drogowych, zachowania wobec pieszych czy obowiązków na przejazdach dla rowerów, powinno równocześnie rozumieć, że te same zasady mają znaczenie również wtedy, gdy korzysta z hulajnogi elektrycznej. Szczególnie ważne jest pokazanie, że hulajnoga elektryczna nie jest wyłącznie urządzeniem rekreacyjnym, ale pojazdem, którego używanie w przestrzeni publicznej wiąże się z obowiązkami.
Nie chodzi zatem o tworzenie odrębnego, skomplikowanego systemu edukacji dla hulajnóg elektrycznych. Chodzi o praktyczne rozszerzenie już istniejącej edukacji komunikacyjnej o pojazd, który realnie pojawił się w życiu dzieci i młodzieży. Karta rowerowa może pozostać podstawowym narzędziem formalnym, ale powinna być uzupełniana o zagadnienia wynikające z nowych form mobilności, w tym o zasady korzystania z hulajnogi elektrycznej, warunki techniczne pojazdu, obowiązki rodzica oraz odpowiedzialność za zachowania w ruchu drogowym.

Rodzic, zakup pojazdu i pozorne bezpieczeństwo platform sprzedażowych

Jednym z najważniejszych wniosków płynących z projektu edukacyjnego realizowanego w Rzeszowie jest potrzeba objęcia profilaktyką nie tylko dzieci, lecz także rodziców. To rodzic najczęściej podejmuje decyzję o zakupie hulajnogi elektrycznej, wybiera model, ocenia ofertę i dopuszcza dziecko do korzystania z pojazdu. Dlatego w ramach projektu szczególny nacisk położono na wyjaśnienie rodzicom, czym w świetle przepisów jest hulajnoga elektryczna i dlaczego nie każdy pojazd sprzedawany pod taką nazwą może być legalnie używany w ruchu drogowym. Przekaz edukacyjny objął ponad 3000 rodziców[23].
Zagadnienie to ma szczególne znaczenie w przypadku zakupów dokonywanych za pośrednictwem platform sprzedażowych działających na rynku polskim. Taka platforma często wzbudza większe zaufanie rodzica, ponieważ w razie problemów to ona pomaga klientowi w kontakcie z producentem lub dystrybutorem, dodatkowo oferta jest łatwo dostępna, a cena bywa niższa niż w tradycyjnej dystrybucji. Nie zawsze oznacza to jednak, że pojazd spełnia wymagania techniczne i formalne pozwalające na jego bezpieczne oraz legalne używanie w ruchu drogowym.
W praktyce konsument może mieć trudność z oceną, czy pojazd oferowany za pośrednictwem platformy internetowej spełnia wymagania obowiązujące w Polsce. Problem

jest szczególnie istotny wtedy, gdy w ofercie brakuje jednoznacznych danych producenta, importera albo innego podmiotu odpowiedzialnego za produkt na rynku Unii Europejskiej[24]. Znaczenie ma również dostępność dokumentacji, instrukcji, informacji o parametrach technicznych oraz ostrzeżeń dotyczących bezpiecznego użytkowania produktu[25].

Z punktu widzenia bezpieczeństwa dzieci jest to problem poważny. Rodzic może być przekonany, że kupuje „hulajnogę dla dziecka", podczas gdy w rzeczywistości nabywa pojazd, który nie powinien być używany przez dziecko w ruchu drogowym. Może to dotyczyć zarówno zbyt dużej prędkości lub masy, braku właściwego wyposażenia, jak i braku dokumentów pozwalających ocenić zgodność produktu z wymaganiami obowiązującymi w Polsce. Dlatego działania edukacyjne powinny obejmować także pytanie, jak kupować bezpiecznie i odpowiedzialnie. W przypadku hulajnóg elektrycznych profilaktyka nie zaczyna się dopiero od założenia kasku albo przypomnienia zasad jazdy. Zaczyna się już na etapie wyboru pojazdu.

Fot. 5. St. asp. Małgorzata Dencikowska oraz asp. Martyna Osowska, koordynatorki działań profilaktycznych z ramienia WRD KMP w Rzeszowie w projekcie edukacyjnym realizowanym w Rzeszowie.

Praktyczne uzupełnienie edukacji do karty rowerowej

Jednym z najważniejszych elementów projektu było sprawdzenie, czy edukację związaną z kartą rowerową można praktycznie uzupełnić o zagadnienia dotyczące hulajnóg elektrycznych. We współpracy z Wojewódzkim Ośrodkiem Ruchu Drogowego w Rzeszowie oraz Wydziałem Ruchu Drogowego Komendy Miejskiej Policji w Rzeszowie przeprowadzono egzamin na kartę rowerową z udziałem hulajnogi elektrycznej jako elementu edukacyjnego i praktycznego[26].

Do egzaminu w WORD Rzeszów przystąpiło blisko 20 uczniów. Było to pierwsze tego typu działanie w Polsce, w którym standardowe przygotowanie do karty rowerowej zostało uzupełnione o temat hulajnóg elektrycznych. Do części teoretycznej dotyczącej roweru dodano zagadnienia związane z zasadami korzystania z hulajnogi elektrycznej, natomiast część praktyczna została rozszerzona o jazdę hulajnogą w kontrolowanych warunkach na placu manewrowym WORD.

Należy podkreślić, że celem nie było zastąpienie obowiązującego modelu egzaminu na kartę rowerową. Egzamin zachował swój podstawowy charakter wynikający z obowiązujących zasad. Hulajnoga elektryczna została potraktowana jako praktyczne uzupełnienie, pozwalające odnieść wiedzę uczniów do pojazdu, który realnie funkcjonuje w przestrzeni publicznej i który, zgodnie z przepisami, wymaga od osoby niepełnoletniej posiadania odpowiednich uprawnień.

Takie podejście pozwoliło połączyć trzy elementy: znajomość przepisów, praktyczne zachowanie na placu manewrowym oraz rozmowę o odpowiedzialności. Uczniowie mogli zobaczyć, że hulajnoga elektryczna wymaga innego sposobu prowadzenia niż rower, inaczej reaguje podczas hamowania, ma inną stabilność i może sprawiać wrażenie prostszej w obsłudze, niż jest w rzeczywistości.

Z punktu widzenia edukacji komunikacyjnej szczególnie ważne było pokazanie, że sama umiejętność uruchomienia pojazdu i utrzymania równowagi nie oznacza jeszcze gotowości do samodzielnego udziału w ruchu drogowym. Dziecko może technicznie potrafić jechać hulajnogą, ale nie rozumieć zasad pierwszeństwa, obowiązków wobec pieszych, znaczenia ograniczenia prędkości czy konsekwencji jazdy po niewłaściwej części drogi.

W tym sensie hulajnoga elektryczna stała się narzędziem edukacyjnym. Pozwoliła przełożyć przepisy na sytuacje praktyczne i pokazać, że bezpieczeństwo nie wynika wyłącznie z zakazów, lecz z rozumienia własnej roli w ruchu drogowym.

Materiały edukacyjne jako narzędzie pracy

W projekcie przygotowano materiały edukacyjne dostępne za pośrednictwem QR kodu. Ich celem było stworzenie prostego i łatwo dostępnego narzędzia, które może zostać wykorzystane przez różne grupy odbiorców: dzieci, rodziców, nauczycieli, policjantów prowadzących działania profilaktyczne, strażników miejskich, instruktorów oraz przedstawicieli samorządów[27].

Ich zadaniem jest uporządkowanie podstawowych informacji dotyczących hulajnóg elektrycznych: wieku użytkownika, wymaganych uprawnień, zasad poruszania się, obowiązkowego wyposażenia, bezpieczeństwa technicznego, kasków oraz odpowiedzialności rodzica.

Z punktu widzenia praktyki ważne jest, aby takie materiały były krótkie, czytelne i możliwe do wykorzystania bez konieczności prowadzenia specjalistycznego szkolenia. Policjant prowadzący spotkanie profilaktyczne w szkole, nauczyciel przygotowujący uczniów do karty rowerowej czy rodzic chcący sprawdzić podstawowe zasady przed zakupem pojazdu powinni otrzymać informacje w formie, która pozwala szybko przejść od przepisu do praktycznego wniosku.

Od kontroli do profilaktyki

W przypadku dzieci i młodzieży działania kontrolne powinny być poprzedzone możliwie szeroką profilaktyką. Dziecko, które nie zna zasad korzystania z hulajnogi elektrycznej, nie zawsze działa z lekceważenia prawa. Często powiela zachowania dorosłych, obserwuje rówieśników albo korzysta z pojazdu kupionego przez rodzica bez pełnej świadomości ograniczeń prawnych i technicznych.

Nie oznacza to rezygnacji z egzekwowania przepisów. Oznacza natomiast, że w przypadku nowych form mobilności szczególnie ważne jest wcześniejsze wyjaśnienie zasad. Przepis, którego dziecko i rodzic nie rozumieją,

będzie traktowany jako formalny zakaz. Przepis, który zostanie powiązany z konkretną sytuacją drogową, może stać się elementem codziennego bezpieczeństwa.
Dobrym przykładem jest obowiązek używania kasku ochronnego przez osoby poniżej 16. roku życia. Można go przedstawić wyłącznie jako nakaz. Można jednak wyjaśnić, że dziecko korzystające z hulajnogi elektrycznej lub roweru porusza się pojazdem, który przy upadku nie chroni głowy, nie posiada pasów bezpieczeństwa, karoserii ani stref zgniotu, a nawet niewielka prędkość może prowadzić do poważnych obrażeń. Takie wyjaśnienie nie osłabia przepisu. Przeciwnie, zwiększa szansę, że zostanie przyjęty jako racjonalny element ochrony zdrowia.

Wnioski praktyczne

Doświadczenia projektu edukacyjnego realizowanego w Rzeszowie pozwalają sformułować kilka wniosków praktycznych.
Po pierwsze, hulajnoga elektryczna powinna być omawiana w edukacji nie jako dodatek, lecz jako realny pojazd używany przez dzieci, młodzież i dorosłych. Jej obecność w przestrzeni publicznej wymaga uwzględnienia w działaniach profilaktycznych.

Fot. 6. Egzamin teoretyczny i praktyczny na kartę rowerową w WORD Rzeszów, uzupełniony o segment dotyczący hulajnóg elektrycznych.

Po drugie, rodzic powinien być jednym z głównych adresatów edukacji. To on najczęściej decyduje o zakupie pojazdu, dopuszczeniu dziecka do jazdy, wyborze kasku, sprawdzeniu stanu technicznego i reakcji na zachowania ryzykowne.
Po trzecie, karta rowerowa może stanowić naturalny punkt wyjścia do edukacji o hulajnogach elektrycznych oraz innych nowych formach mobilności. Nie ma potrzeby budowania odrębnego systemu od podstaw, ale konieczne jest praktyczne uzupełnienie istniejących treści o zagadnienia, które realnie pojawiły się w codziennym uczestnictwie dzieci i młodzieży w ruchu drogowym. W tym kontekście szczególnej ostrożności wymaga dyskusja o ewentualnym fakultatywnym charakterze karty rowerowej. Ograniczenie jej znaczenia mogłoby w praktyce osłabić jeden z niewielu powszechnych mechanizmów przygotowania dzieci do samodzielnego uczestnictwa w ruchu drogowym. Lepszym kierunkiem wydaje się nie rezygnacja z karty rowerowej, lecz jej dostosowanie do współczesnych realiów mobilności. Obecny model ma dużą wartość edukacyjną, ponieważ łączy szkołę, przepisy, odpowiedzialność rodzica oraz praktyczne przygotowanie dziecka do poruszania się w przestrzeni publicznej. Właśnie dlatego karta rowerowa powinna zostać zachowana i rozwijana jako istotny element edukacji komunikacyjnej, a nie traktowana wyłącznie jako formalny dodatek do programu nauczania.
Po czwarte, część praktyczna ma szczególne znaczenie. Sama znajomość przepisu nie oznacza, że dziecko potrafi prawidłowo zachować się na drodze. Ćwiczenia praktyczne pozwalają szybciej zauważyć błędne nawyki, brak kontroli nad pojazdem, zbyt dużą pewność siebie albo niezrozumienie relacji z pieszymi.
Po piąte, edukacja powinna obejmować także wybór pojazdu. Pojazd niespełniający wymagań technicznych, zbyt szybki, zbyt ciężki lub pozbawiony właściwej dokumentacji może zwiększać ryzyko już na etapie zakupu.
Po szóste, współpraca Policji, WORD, szkoły, samorządu, straży miejskiej i organizacji branżowej pozwala połą-

Fot. 7. Przygotowanie toru egzaminacyjnego w WORD Rzeszów przez st. asp. Małgorzatę Sanecką-Kuźniar z Wydziału Ruchu Drogowego Komendy Miejskiej Policji w Rzeszowie.

Fot. 8–9. Dodatkowa część egzaminu praktycznego na kartę rowerową z uwzględnieniem jazdy na hulajnodze elektrycznej, prowadzona przez sierż. szt. Kingę Żuławską.

czyć kompetencje, których nie posiada samodzielnie żaden z tych podmiotów. Taki model współpracy może być możliwy do odtworzenia w innych miastach.
Po siódme, materiały edukacyjne powinny być dostępne, proste i możliwe do wykorzystania przez różne instytucje. Kod QR prowadzący do materiałów może wspierać kontynuację edukacji po zakończeniu spotkania lub zajęć.
Po ósme, regulacja prawna bez edukacji praktycznej może nie przynieść oczekiwanego efektu. Bezpieczeństwo dzieci korzystających z hulajnóg elektrycznych wymaga połączenia prawa, profilaktyki, odpowiedzialności rodziców i realnych ćwiczeń.

Podsumowanie

Hulajnoga elektryczna stała się trwałym elementem współczesnej mobilności miejskiej. W przypadku dzieci i młodzieży jej obecność wymaga jednak szczególnej ostrożności. Nie wystarczy przyjąć, że skoro dziecko potrafi utrzymać równowagę i uruchomić pojazd, jest gotowe do samodzielnego udziału w ruchu drogowym. Gotowość ta wymaga znajomości przepisów, dojrzałości, praktycznych umiejętności, odpowiedniego pojazdu i wsparcia dorosłych.
Projekt edukacyjny realizowany w Rzeszowie pokazał, że temat hulajnóg elektrycznych można włączyć do edukacji komunikacyjnej w sposób praktyczny, spokojny i oparty na współpracy instytucjonalnej. Szczególnie ważne okazało się połączenie perspektywy Policji, WORD, szkoły, samorządu, straży miejskiej oraz organizacji branżowej. Dzięki temu możliwe było pokazanie hulajnogi elektrycznej nie tylko jako potencjalnego źródła zagrożenia, ale także jako tematu, który można uporządkować przez edukację.
Wnioski z projektu wskazują, że skuteczna profilaktyka powinna zaczynać się przed wykroczeniem, przed wypadkiem i często także przed zakupem pojazdu. Rodzic, który wie, jaki pojazd kupuje, nauczyciel, który potrafi omówić podstawowe zasady, policjant, który dysponuje praktycznym materiałem profilaktycznym, oraz dziecko, które rozumie swoją rolę w ruchu drogowym, tworzą wspólnie warunki do realnej poprawy bezpieczeństwa.
Hulajnoga elektryczna nie powinna być traktowana wyłącznie jako problem kontrolny. Jest również tematem edukacyjnym, technicznym i wychowawczym. Dlatego odpowiedzią na nowe formy mobilności powinno być nie tylko stanowienie kolejnych przepisów, lecz także tworzenie praktycznych narzędzi, które pozwolą te przepisy zrozumieć i stosować w codziennym życiu.

[1] Art. 33d ust. 1 ustawy z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z 2024 r. poz. 1251, z późn. zm.; dalej: p.r.d.), w brzmieniu nadanym ustawą z dnia 17 października 2025 r. o zmianie ustawy – Prawo o ruchu drogowym oraz niektórych innych ustaw (Dz. U. poz. 1676).
[2] Art. 7 ust. 1 pkt 2 ustawy z dnia 5 stycznia 2011 r. o kierujących pojazdami (Dz. U. z 2025 r. poz. 1226, z późn. zm.; dalej: u.k.p.).
[3] Art. 33 ust. 1b p.r.d., w brzmieniu nadanym ustawą z dnia 17 października 2025 r. o zmianie ustawy – Prawo o ruchu drogowym oraz niektórych innych ustaw.
[4] Dokumentacja projektowa Polskiego Stowarzyszenia Lekkiej Elektromobilności dotycząca projektu „Edukacja bezpieczeństwa ruchu drogowego dzieci i młodzieży w zakresie nowych form mobilności, w tym hulajnóg elektrycznych", Rzeszów 2026.
[5] Dokumentacja projektowa PSLE, WORD Rzeszów oraz Komendy Miejskiej Policji w Rzeszowie dotycząca działań edukacyjnych i praktycznych z udziałem hulajnogi elektrycznej w ramach przygotowania uczniów do bezpiecznego uczestnictwa w ruchu drogowym, Rzeszów 2026.
[6] Art. 33d ust. 1 p.r.d.
[7] Art. 33d ust. 2 p.r.d.
[8] Art. 7 ust. 1 pkt 2 u.k.p.
[9] Art. 33 ust. 1 p.r.d.
[10] Art. 33a ust. 1 p.r.d.
[11] Art. 33a ust. 2 p.r.d.
[12] Art. 33c p.r.d.
[13] Art. 33a ust. 3 p.r.d.
[14] § 55d rozporządzenia Ministra Infrastruktury z dnia 31 grudnia 2002 r. w sprawie warunków technicznych pojazdów oraz zakresu ich niezbędnego wyposażenia (Dz. U. z 2024 r. poz. 502; dalej: rozporządzenie w sprawie warunków technicznych pojazdów).
[15] § 3 ust. 13a rozporządzenia w sprawie warunków technicznych pojazdów.
[16] § 55a ust. 1 pkt 1–5 rozporządzenia w sprawie warunków technicznych pojazdów.
[17] § 55a ust. 4 pkt 1–2 rozporządzenia w sprawie warunków technicznych pojazdów.
[18] Art. 33 ust. 1b p.r.d., w brzmieniu nadanym ustawą z dnia 17 października 2025 r. o zmianie ustawy – Prawo o ruchu drogowym oraz niektórych innych ustaw.
[19] Por. Ministerstwo Infrastruktury, *Obowiązek jazdy w kasku do 16. roku życia – rekomendacje po posiedzeniu KRBRD*, 14.07.2025 r.
[20] Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 12 kwietnia 2013 r. w sprawie uzyskiwania karty rowerowej (Dz. U. poz. 512).
[21] Dane zebrane przez Polskie Stowarzyszenie Lekkiej Elektromobilności w ramach projektu edukacyjnego „Edukacja bezpieczeństwa ruchu drogowego dzieci i młodzieży w zakresie nowych form mobilności, w tym hulajnóg elektrycznych", na podstawie informacji przekazanych przez szkoły podstawowe z terenu miasta Rzeszowa, Rzeszów 2026.
[22] Materiały robocze dotyczące możliwości powiązania informacji o posiadaniu karty rowerowej z Kartą Mieszkańca w Rzeszowie, opracowywane w ramach działań związanych z projektem edukacyjnym PSLE, Rzeszów 2026.
[23] Dane własne Polskiego Stowarzyszenia Lekkiej Elektromobilności z realizacji projektu „Edukacja bezpieczeństwa ruchu drogowego dzieci i młodzieży w zakresie nowych form mobilności, w tym hulajnóg elektrycznych", obejmujące działania informacyjne skierowane do rodziców uczniów rzeszowskich szkół podstawowych, Rzeszów 2026.
[24] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/988 z dnia 10 maja 2023 r. w sprawie ogólnego bezpieczeństwa produktów, zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 i dyrektywę Parlamentu Europejskiego i Rady (UE) 2020/1828 oraz uchylające dyrektywę 2001/95/WE i dyrektywę Rady 87/357/EWG, Dz. Urz. UE L 135 z 23.05.2023.
[25] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE i rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011, Dz. Urz. UE L 169 z 25.06.2019.
[26] Dokumentacja projektowa PSLE, WORD Rzeszów oraz Komendy Miejskiej Policji w Rzeszowie dotycząca egzaminu na kartę rowerową z elementem teoretycznym i praktycznym obejmującym hulajnogę elektryczną, Rzeszów 2026.
[27] Polskie Stowarzyszenie Lekkiej Elektromobilności, *Materiały edukacyjne dla dzieci, rodziców, nauczycieli i instytucji dotyczące hulajnóg elektrycznych*, https://psle.org.pl/projekt-edukacja/ [dostęp: 18.05.2026 r.].

Bibliografia

Akty prawne krajowe:

Ustawa z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym (Dz. U. z 2024 r. poz. 1251, z późn. zm.).

Ustawa z dnia 5 stycznia 2011 r. o kierujących pojazdami (Dz. U. z 2025 r. poz. 1226, z późn. zm.).

Rozporządzenie Ministra Infrastruktury z dnia 31 grudnia 2002 r. w sprawie warunków technicznych pojazdów oraz zakresu ich niezbędnego wyposażenia (Dz. U. z 2024 r. poz. 502).

Rozporządzenie Ministra Transportu, Budownictwa i Gospodarki Morskiej z dnia 12 kwietnia 2013 r. w sprawie uzyskiwania karty rowerowej (Dz. U. poz. 512).

Akty prawne Unii Europejskiej:

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1020 z dnia 20 czerwca 2019 r. w sprawie nadzoru rynku i zgodności produktów oraz zmieniające dyrektywę 2004/42/WE i rozporządzenia (WE) nr 765/2008 i (UE) nr 305/2011, Dz. Urz. UE L 169 z 25.06.2019.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/988 z dnia 10 maja 2023 r. w sprawie ogólnego bezpieczeństwa produktów, zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1025/2012 i dyrektywę Parlamentu Europejskiego i Rady (UE) 2020/1828 oraz uchylające dyrektywę 2001/95/WE i dyrektywę Rady 87/357/EWG, Dz. Urz. UE L 135 z 23.05.2023.

Źródła internetowe i komunikaty instytucjonalne:

Ministerstwo Infrastruktury, *Obowiązek jazdy w kasku do 16. roku życia – rekomendacje po posiedzeniu KRBRD*, 14.07.2025 r., https://www.gov.pl/web/infrastruktura/obowiazek-jazdy-w-kasku-do-16-roku-zycia--rekomendacje-po-posiedzeniu-krbrd [dostęp: 14.05.2026 r.].

Polskie Stowarzyszenie Lekkiej Elektromobilności, *Materiały edukacyjne dla dzieci, rodziców, nauczycieli i instytucji dotyczące hulajnóg elektrycznych*, https://psle.org.pl/projekt-edukacja/ [dostęp: 14.05.2026 r.].

Dokumentacja projektowa i materiały własne:

Dokumentacja projektowa Polskiego Stowarzyszenia Lekkiej Elektromobilności dotycząca projektu „Edukacja bezpieczeństwa ruchu drogowego dzieci i młodzieży w zakresie nowych form mobilności, w tym hulajnóg elektrycznych", Rzeszów 2026.

Dokumentacja projektowa PSLE, WORD Rzeszów oraz Komendy Miejskiej Policji w Rzeszowie dotycząca działań edukacyjnych i praktycznych z udziałem hulajnogi elektrycznej w ramach przygotowania uczniów do bezpiecznego uczestnictwa w ruchu drogowym, Rzeszów 2026.

Dokumentacja projektowa PSLE, WORD Rzeszów oraz Komendy Miejskiej Policji w Rzeszowie dotycząca egzaminu na kartę rowerową z elementem teoretycznym i praktycznym obejmującym hulajnogę elektryczną, Rzeszów 2026.

Dane zebrane przez Polskie Stowarzyszenie Lekkiej Elektromobilności w ramach projektu „Edukacja bezpieczeństwa ruchu drogowego dzieci i młodzieży w zakresie nowych form mobilności, w tym hulajnóg elektrycznych", na podstawie informacji przekazanych przez szkoły podstawowe z terenu miasta Rzeszowa, Rzeszów 2026.

Dane własne Polskiego Stowarzyszenia Lekkiej Elektromobilności z realizacji projektu „Edukacja bezpieczeństwa ruchu drogowego dzieci i młodzieży w zakresie nowych form mobilności, w tym hulajnóg elektrycznych", obejmujące działania informacyjne skierowane do rodziców uczniów rzeszowskich szkół podstawowych, Rzeszów 2026.

Materiały robocze dotyczące możliwości powiązania informacji o posiadaniu karty rowerowej z Kartą Mieszkańca w Rzeszowie, opracowywane w ramach działań związanych z projektem edukacyjnym PSLE, Rzeszów 2026.

Summary

Electric scooters in traffic education for kids. Practical conclusions from an educational project implemented in Rzeszów

Electric scooters have become one of the most visible forms of modern urban mobility. For children and young people, their use should not be seen only as individual behaviour, but also as part of road safety education, parental responsibility, technical requirements for vehicles and prevention. This article discusses an educational project implemented in Rzeszów, showing how electric scooters can be included in practical traffic education for kids.

The project covered five primary schools in Rzeszów: Primary School No. 6, Primary School No. 19, Primary School No. 24, Primary School No. 25 and Primary School No. 29. About 400 children, mainly from fourth grades, took part in the activities. The project combined theory with practical exercises in controlled conditions. Children learned the basic principles of riding an electric scooter, braking, keeping the correct path of travel and reacting to situations that may occur in road traffic. The educational activities also reached more than 3,000 parents, with particular emphasis on explaining that not every vehicle sold as an electric scooter may be legally and safely used on public roads.

An important part of the project was checking whether the existing bicycle card education system could be supplemented with topics related to electric scooters. In cooperation with the Regional Road Traffic Centre in Rzeszów and the Traffic Department of the Municipal Police Headquarters in Rzeszów, nearly 20 children took part in a bicycle card examination extended with theoretical and practical elements concerning electric scooters. This was the first activity of this kind in Poland. The experience showed that the bicycle card can remain a valuable tool for preparing children for independent participation in road traffic, provided that it is developed and adapted to new forms of mobility.

The article also refers to data collected in Rzeszów on bicycle card possession among children in grades IV–VIII. Out of 9,986 children covered by the survey, 7,144 had a bicycle card, which is about 72% of the group. At the same time, 2,506 children did not have such a document, and in the case of 336 children no data were available. These figures show that the bicycle card is still an important element of traffic education, but they also point to the need for better practical use of this tool.

The conclusions from the Rzeszów project show that legal regulations alone are not enough to improve the safety of children using electric scooters. Effective prevention requires practical education, clear materials for schools and parents, awareness of technical requirements, responsible purchasing decisions and cooperation between the Police, road traffic education centres, schools, municipal guards, local authorities and industry experts. Electric scooters should therefore be treated not only as a legal challenge, but also as an educational, technical and preventive issue directly connected with the safety of children and young people in road traffic.

Tłumaczenie: Autor

Komisariat Młodego Policjanta w Rzeszowie

Pionierska przestrzeń edukacji na rzecz bezpieczeństwa, która zmienia podejście do profilaktyki w Policji

st. asp. Małgorzata Dencikowska

Wydział Ruchu Drogowego Komendy Miejskiej Policji w Rzeszowie

W marcu 2025 r. w strukturach Wydziału Ruchu Drogowego Komendy Miejskiej Policji w Rzeszowie, w siedzibie Komisariatu Policji II przy ul. Wołyńskiej 1, uruchomiono Komisariat Młodego Policjanta – wyjątkową, interaktywną przestrzeń edukacyjną skierowaną do dzieci i młodzieży. Projekt od samego początku wyróżnia się na tle inicjatyw profilaktycznych realizowanych w Polsce, stanowiąc jeden z najbardziej rozbudowanych i nowoczesnych modeli edukacji bezpieczeństwa w strukturach Policji.

Edukacja, która angażuje – nowoczesna profilaktyka w praktyce

Komisariat Młodego Policjanta został zaprojektowany jako kompleksowa, interaktywna przestrzeń edukacyjna, której fundamentem jest nauka poprzez doświadczenie. To odejście od tradycyjnych form przekazu na rzecz aktywnego uczestnictwa dzieci w procesie edukacyjnym.

Sala profilaktyczna została wyposażona w nowoczesne narzędzia dydaktyczne. Jednym z nich jest podłoga interaktywna FunFloor z pakietem „Karta Rowerowa", dzięki której poprzez gry i quizy dzieci uczą się zasad ruchu drogowego, znaków drogowych oraz prawidłowych zachowań na drodze. Drugim filarem jest tablica multimedialna z programem „Bezpieczeństwo w ruchu drogowym", obejmującym zarówno część teoretyczną, jak i praktyczną – od zasad poruszania się pieszych i rowerzystów, przez pierwszą pomoc, aż po symulacje skrzyżowań i zadania edukacyjne.

Fot. 1. Pokój profilaktyczny „Komisariat Młodego Policjanta w Rzeszowie".

Całość uzupełniają minimundurki policyjne, które dzieci mogą zakładać podczas zajęć, oraz spójna, przyjazna przestrzeń edukacyjna w stylistyce policyjnej – z elementami wizualnymi, znakami drogowymi, oświetleniem LED i modelem radiowozu, który stał się jednym z najbardziej rozpoznawalnych elementów sali.

Zajęcia prowadzone są w formie warsztatowej i trwają około trzech godzin, a ich główną grupą odbiorców są uczniowie klas 1–3 szkół podstawowych.

Projekt, który wyrósł z realnej potrzeby

Pomysł stworzenia Komisariatu Młodego Policjanta dojrzewał we mnie przez wiele lat służby i obserwacji pracy profilaktycznej w terenie. Już kilka lat przed przeprowadzką Wydziału Ruchu Drogowego do nowej siedziby wiedziałam, że jeśli tylko pojawi się odpowiednia przestrzeń, chciałabym stworzyć miejsce zupełnie inne niż standardowe działania profilaktyczne – miejsce stworzone specjalnie dla dzieci.

KOMISARIAT MŁODEGO POLICJANTA

Fot. 2. Minimundurki policyjne.

Fot. 5. Tablica multimedialna dotykowa z programem „Bezpieczeństwo w ruchu drogowym". Gra zadaniowa pod nazwą „Obowiązkowe wyposażenie roweru".

Fot. 3. Wyposażenie sali edukacyjnej.

Fot. 6. Postacie służb mundurowych do wykonywania pamiątkowych fotografii.

Fot. 4. Podłoga interaktywna FunFloor z pakietem „Karta Rowerowa". Nowoczesne urządzenie multimedialne, które wyświetla obraz na podłożu, reagując na ruch i dotyk.

Fot. 7. Kurteczki i czapki policyjne dla dzieci oraz tarcze stop.

Fot. 8. St. asp. Małgorzata Dencikowska z uczennicami szkół podstawowych z Rzeszowa.
Zdj. 1–7: M. Dencikowska, zdj. 8: zbiory KMP Rzeszów.

Przez lata pełnienia służby realizowałam zajęcia profilaktyczne w szkołach i placówkach edukacyjnych. Widziałam ogromne zainteresowanie dzieci, ale jednocześnie miałam poczucie, że krótkie spotkania nie pozwalają w pełni przekazać najważniejszych treści dotyczących bezpieczeństwa. Potrzebna była przestrzeń, która pozwoli dzieciom doświadczać, uczestniczyć i uczyć się poprzez praktykę.
Projekt powstał również z obserwacji realnych potrzeb szkół i ograniczeń dotychczasowych form współpracy. Szkoły od lat chciały odwiedzać Policję i organizować dzieciom wycieczki do komendy. Problem polegał na tym, że wcześniej nie mieliśmy miejsca przygotowanego z myślą o najmłodszych. Wizyty ograniczały się głównie do krótkiego zwiedzania budynku czy prezentacji sprzętu.

Od inspiracji do autorskiego projektu

Inspiracją były dla mnie zarówno pojedyncze sale profilaktyczne funkcjonujące w różnych częściach Polski, tworzone przez funkcjonariuszy z ogromną pasją do edukacji, jak również nowoczesne sale edukacyjne „Ognik" realizowane przez Państwową Straż Pożarną. Pokazywały one, jak ogromny potencjał ma edukacja oparta na doświadczeniu i jak bardzo dzieci potrzebują takich miejsc.
Od początku miałam w głowie bardzo konkretną wizję tego miejsca – nowoczesnej, interaktywnej przestrzeni, która będzie przyjazna dzieciom, angażująca i jednocześnie niosąca realną wartość edukacyjną.

Zespół realizujący zajęcia edukacyjne dla dzieci

St. asp. Małgorzata Dencikowska – specjalista Wydziału Ruchu Drogowego Komendy Miejskiej Policji w Rzeszowie z 15-letnim doświadczeniem w służbie, od początku związana z pionem ruchu drogowego. Inicjatorka i autorka projektu „Komisariat Młodego Policjanta w Rzeszowie", współtwórczyni jego koncepcji i przestrzeni edukacyjnej opartej na nauce poprzez doświadczenie.
Asp. Martyna Osowska – kontroler Wydziału Ruchu Drogowego Komendy Miejskiej Policji w Rzeszowie z 17-letnim doświadczeniem w służbie. Współprowadzi zajęcia edukacyjne w Komisariacie Młodego Policjanta, przekazując dzieciom praktyczną wiedzę z zakresu bezpieczeństwa w ruchu drogowym. Zainicjowała współpracę z Polskim Stowarzyszeniem Lekkiej Elektromobilności, realizując działania edukacyjne dotyczące bezpiecznego korzystania z hulajnóg elektrycznych przez dzieci oraz budowania świadomości zagrożeń wynikających z ich niewłaściwego użytkowania.
Od momentu otwarcia Komisariatu Młodego Policjanta funkcjonariuszki Wydziału Ruchu Drogowego przeprowadziły 124 warsztaty edukacyjne, w których uczestniczyło blisko 3720 uczniów. Zajęcia spotkały się z bardzo dużym zainteresowaniem szkół i placówek oświatowych, stając się miejscem, w którym dzieci nie tylko uczą się zasad bezpieczeństwa w ruchu drogowym, ale również poznają – w formie praktycznego doświadczenia – codzienną pracę policjantów.

Przestrzeń, która powstała dzięki współpracy i wizji

Realizacja projektu była możliwa dzięki zaangażowaniu wielu osób i wsparciu przełożonych, którzy dostrzegli potencjał edukacyjny inicjatywy, uwierzyli w ten pomysł i pomogli przekuć tę wizję w rzeczywistość.
Szczególne podziękowania należą się ówczesnemu i obecnemu kierownictwu, które od samego początku wspierało i nieustannie rozwija ideę tej nowoczesnej przestrzeni edukacyjnej dla dzieci i młodzieży.

Projekt o znaczeniu ogólnopolskim

Komisariat Młodego Policjanta pokazuje, jak ogromne jest zainteresowanie tego typu edukacją – zarówno ze strony dzieci, jak i szkół. Mam nadzieję, że Komisariat Młodego Policjanta stanie się inspiracją również dla innych jednostek Policji w Polsce. Takie miejsca mają realny wpływ na edukację i bezpieczeństwo dzieci. Projekt z Rzeszowa mógłby tym samym nie tylko stanowić lokalną inicjatywę, ale także wyznaczyć potencjalny kierunek rozwoju policyjnej profilaktyki w całej Polsce – opartej na doświadczeniu, interakcji i realnym zaangażowaniu najmłodszych uczestników ruchu drogowego.

Summary

Police Station of the Young Officer in Rzeszów. A pioneering space for safety education that is changing the approach to prevention in the Police

The author of this article describes the genesis, implementation and functioning of an innovative project called Police Station of the Young Officer. This project was launched in March 2025 within the Traffic Police Department of the Municipal Police Headquarters in Rzeszów, at Police Station II at Wołyńska Street 1.
Police Station of the Young Officer, of which the author of this article is a co-creator, is a unique, interactive educational space aimed at children and youth. This project stands out amid preventive initiatives implemented in Poland, constituting one of the most extensive and modern models of safety education within the Police.

Tłumaczenie: Beata Pepłowska

AR-15 BEZ TAJEMNIC

10 krytycznych błędów, których musi unikać każdy użytkownik

mł. asp. Krystian Chudziński

Zakład Interwencji Policyjnych CSP

Platforma AR-15, znana ze swojej modułowości i wszechstronności, oferuje użytkownikom niemal nieograniczone możliwości konfiguracji. Jednak ta elastyczność ma swoją cenę: niezawodność, bezpieczeństwo i celność broni są nierozerwalnie związane z prawidłowym montażem, doborem komponentów i regularną konserwacją. Każdy błąd, nawet pozornie drobny, może prowadzić do kosztownych uszkodzeń lub, co gorsza, do niebezpiecznych awarii. Niniejszy przewodnik opiera się na sprawdzonych wojskowych procedurach konserwacyjnych, zawartych w *Instrukcji technicznej TM 9-1005-319-23&P*, które pomogą uniknąć najczęstszych pułapek i zapewnić, że karabinek będzie działać zgodnie z przeznaczeniem – bezpiecznie i niezawodnie.

1. FUNDAMENTALNE BŁĘDY DOTYCZĄCE BEZPIECZEŃSTWA I PROCEDUR

Zanim zagłębimy się w techniczne aspekty montażu poszczególnych komponentów, kluczowe jest omówienie błędów proceduralnych. Zaniedbania w tym obszarze stanowią bezpośrednie zagrożenie dla bezpieczeństwa użytkownika i osób postronnych, a także podważają podstawową funkcjonalność broni. Poniższe zasady to absolutny fundament, bez którego dalsze rozważania o konfiguracji tracą sens.

BŁĄD 1:

Ignorowanie podstawowych protokołów bezpieczeństwa

Najpoważniejszym i niestety wciąż popełnianym błędem jest praca przy broni bez jej uprzedniego, dokładnego sprawdzenia i rozładowania. Wojskowa instrukcja techniczna jest w tej kwestii jednoznaczna:

> „Przed rozpoczęciem inspekcji upewnić się, że karabin jest rozładowany. […] Sprawdzić komorę, aby upewnić się, że jest pusta" [tłum. własne].
>
> Źródło: *TM 9-1005-319-23&P, Technical Manual.* [*Instrukcja techniczna*].

Każda czynność konserwacyjna lub modyfikacja musi być poprzedzona fizycznym i wizualnym sprawdzeniem komory nabojowej oraz gniazda magazynka. Instrukcja kategorycznie zabrania także trzymania amunicji w pobliżu miejsca pracy, co minimalizuje ryzyko przypadkowego załadowania broni.

BŁĄD 2:

Wymiana krytycznych komponentów między różnymi egzemplarzami broni

Modułowość platformy AR-15 może skłaniać do swobodnego wymieniania części między różnymi karabinkami. Instrukcja techniczna surowo tego zabrania w odniesieniu

do kluczowych elementów, takich jak kompletne zespoły zamka (*bolt assemblies*), na poziomie niższym niż specjalistyczny serwis. Ostrzeżenie jest jednoznaczne:

> „Może to skutkować obrażeniami lub śmiercią użytkownika" [tłum. własne].
> Źródło: TM 9-1005-319-23&P, *Technical Manual.*

Chociaż komponenty zdają się wyglądać identycznie, minimalne różnice w tolerancjach produkcyjnych między egzemplarzami mogą prowadzić do niebezpiecznych problemów z luzem zamkowym (*headspace*). Niewłaściwy luz zamkowy zagraża integralności strukturalnej broni podczas strzału i stanowi bezpośrednie zagrożenie dla strzelca.

2. SERCE KARABINKA: BŁĘDY DOTYCZĄCE ZESPOŁU SUWADŁA Z ZAMKIEM (BCG) I UKŁADU POWROTNEGO

Zespół suwadła z zamkiem (BCG) i układ powrotny działają w precyzyjnej harmonii; pierwszy jest silnikiem napędzanym gazem, a drugi hamulcem i mechanizmem resetującym. Błędy w którymkolwiek z tych obszarów zakłócają ten cykl, prowadząc bezpośrednio do najczęstszych zacięć i awarii.

BŁĄD 3:

Nieprawidłowy montaż zespołu suwadła z zamkiem (BCG)

Jednym z najniebezpieczniejszych błędów montażowych jest pominięcie obsady rygla (*bolt cam pin*). Instrukcja wojskowa zawiera jedno z najsurowszych ostrzeżeń w całym dokumencie:

> „Obsada rygla musi być zainstalowana,
> w przeciwnym razie karabin/karabinek eksploduje
> podczas oddawania pierwszego strzału. […]
> Może to spowodować obrażenia lub śmierć personelu" [tłum. własne].
> Źródło: *TM 9-1005-319-23&P, Technical Manual.*

Równie istotne jest prawidłowe zamontowanie iglicy i jej kołka ustalającego (*firing pin, retaining pin*). Instrukcja wyraźnie ostrzega, aby nie modyfikować tych elementów. Jakakolwiek ingerencja może prowadzić do ich uszkodzenia, wypadnięcia i w konsekwencji do zablokowania mechanizmów wewnętrznych broni.

BŁĄD 4:

Zaniedbywanie stanu technicznego zamka i pierścieni uszczelniających

Pierścienie uszczelniające zamek (*bolt rings*) odgrywają kluczową rolę w utrzymaniu odpowiedniego ciśnienia gazów napędzających suwadło. Instrukcja TM 9-1005-319-23&P podaje prostą procedurę diagnostyczną:

> „Włóż zespół zamka do klucza i nośnika zamka.
> Odwróć zespół klucza i nośnika zamka tak,
> aby zespół zamka był skierowany w dół.
> Zespół zamka nie może wypaść" [tłum. własne].
> Źródło: *TM 9-1005-319-23&P, Technical Manual.*

Jeśli zamek wypadnie z suwadła pod własnym ciężarem, pierścienie są zużyte i wymagają natychmiastowej wymiany – brak szczelności skutkuje utratą ciśnienia gazu i niewystarczającą energią do pełnego cyklu przeładowania. W praktyce oznacza to, że karabinek może działać wyłącznie jako broń powtarzalna, wymagająca ręcznego przeładowania po każdym strzale. Podczas instalacji przerwy w pierścieniach powinny być rozstawione względem siebie o około 1/3 obrotu, co zapobiega tworzeniu się kanału przepływu gazów.

BŁĄD 5:

Niedopasowane lub zużyte elementy układu powrotnego

Sprężyna powrotna (*action spring*) musi być dopasowana do systemu, w którym pracuje (karabin z kolbą stałą lub karabinek z kolbą teleskopową). Użycie niewłaściwej sprężyny jest poważnym błędem konfiguracyjnym, który zakłóca cykl pracy broni. Instrukcja podaje następujące graniczne wymiary obu typów:

TYP BRONI	MIN. DŁUGOŚĆ SPRĘŻYNY	MAKS. DŁUGOŚĆ SPRĘŻYNY
Karabin (Rifle)	11 3/4 cala (29,85 cm)	13 1/2 cala (34,29 cm)
Karabinek (Carbine)	10 1/16 cala (25,56 cm)	11 1/4 cala (28,58 cm)

Instalacja sprężyny karabinowej w karabinku (lub odwrotnie) prowadzi do problemów z przeładowaniem lub nadmiernego zużycia komponentów. Jeśli sprężyna jest zużyta i jej długość spada poniżej wartości minimalnej, należy ją wymienić. Instrukcja kategorycznie zabrania próby regulacji długości sprężyny przez jej rozciąganie.

3. PUŁAPKI ZWIĄZANE Z SYSTEMEM GAZOWYM I ZESPOŁEM LUFY

System gazowy jest silnikiem karabinka napędzającym cały cykl automatyki. Zespół lufy odpowiada za balistykę i celność. Błędy w konfiguracji lub konserwacji tych

dwóch obszarów mają bezpośredni wpływ na niezawodność przeładowania oraz zdolność broni do precyzyjnego trafienia w cel.

BŁĄD 6:

Nieprawidłowe ustawienie i konserwacja systemu gazowego

Główną przyczyną tzw. krótkiego odrzutu (*short recoil*), czyli niepełnego cyklu przeładowania, są problemy z systemem gazowym. Sekcja rozwiązywania problemów w instrukcji wojskowej wskazuje na następujące przyczyny:

- nagromadzenie nagaru: nagar węglowy gromadzący się w kluczu gazowym suwadła (*bolt carrier key*) lub w porcie gazowym lufy może z czasem ograniczyć lub całkowicie zablokować przepływ gazów;
- nieszczelności przy bloku gazowym: nieszczelność na połączeniu rurki gazowej z blokiem gazowym powoduje utratę ciśnienia i niewystarczającą siłę do napędzenia zespołu suwadła, problem wymaga interwencji rusznikarskiej;
- zgięta lub niewłaściwa rurka gazowa: nawet niewielkie odkształcenie może powodować tarcie o klucz gazowy i prowadzić do niepełnego cyklu, instrukcja zaleca próbę delikatnego prostowania, zaznaczając, że niepowodzenie kwalifikuje broń do serwisu rusznikarskiego.

BŁĄD 7:

Nieprawidłowy montaż kompensatora i ignorowanie zużycia lufy

Prawidłowe ustawienie urządzenia wylotowego jest kluczowe dla kontroli odrzutu i podrzutu lufy. Instrukcja precyzuje, że w przypadku standardowego kompensatora trzeci (środkowy) otwór musi być skierowany idealnie pionowo w górę – w górnym martwym punkcie (TDC, od ang. *Top Dead Center*). Nieprawidłowe ustawienie sprawi, że gazy wylotowe nie będą kierowane w optymalny sposób, co negatywnie wpłynie na stabilność broni podczas strzału.
Instrukcja jasno określa również granicę zużycia lufy: wżery w komorze nabojowej o długości przekraczającej 1/8 cala (0,32 cm) kwalifikują ją do wymiany, ponieważ mogą powodować problemy z ekstrakcją łusek. Drobne, powierzchowne wżery są dopuszczalne.

4. BŁĘDY DOTYCZĄCE KOMORY SPUSTOWEJ I MECHANIZMU SPUSTOWEGO

Komora spustowa (*lower receiver*), chociaż pozornie prostsza w budowie niż komora zamkowa, zawiera kluczowe mechanizmy kontroli ognia. Błędy w jej montażu lub zaniedbania konserwacyjne mogą prowadzić do niebezpiecznych awarii: strzałów dubletowych, niemożności zabezpieczenia broni czy problemów z przeładowaniem.

BŁĄD 8:

Nieprawidłowy montaż mechanizmu spustowego

Najczęstszym błędem podczas montażu mechanizmu spustowego jest odwrotne założenie sprężyny kurka (*hammer spring*). Instrukcja precyzuje prawidłowe ułożenie:

> „Końce sprężyny kurka muszą być zainstalowane za kołkiem spustu, spoczywając w rowku na jego górnej powierzchni" [tłum. własne].
>
> Źródło: *TM 9-1005-319-23&P, Technical Manual.*

Odwrotny montaż znacząco zmniejsza siłę uderzenia kurka w iglicy, co prowadzi do słabych zbić spłonki i licznych niewypałów.

BŁĄD 9:

Ignorowanie zużycia kolby i prowadnicy sprężyny powrotnej

W przypadku karabinów z kolbą stałą (typu M16A2) instrukcja określa szczegółowe kryteria oceny pęknięć. Dopuszczalne są wyłącznie:

- Jedno włoskowate pęknięcie na stronę, nieprzekraczające 1 cala (2,54 cm) długości, wychodzące od stopki kolby.
- Dwa dodatkowe włoskowate pęknięcia o długości do 0,25 cala (0,64 cm) na stronę.
- Pęknięcia w „obszarze krytycznym" z przodu kolby – w miejscu jej połączenia z komorą spustową – są niedopuszczalne.

Jeśli prowadnica sprężyny powrotnej (*lower receiver extension*) jest luźna, broń wymaga interwencji rusznikarskiej: grozi to uszkodzeniem gwintu w komorze spustowej.

5. SMAROWANIE, CZYSZCZENIE I WYKOŃCZENIE

Nawet najlepiej skonfigurowany karabinek zawiedzie, jeśli będzie zaniedbany. Prawidłowe czyszczenie i smarowanie mają bezpośredni wpływ na żywotność kluczowych części, płynność działania mechanizmów i ogólną niezawodność broni.

BŁĄD 10:

Niewłaściwe czyszczenie i smarowanie

Instrukcja techniczna zaleca stosowanie rękawic gumowych przy kontakcie z rozpuszczalnikiem do czyszczenia na sucho (*dry cleaning solvent*) oraz środkiem do usuwania nagaru (*carbon removing compound*) ze względu na ich toksyczność.
Kluczowym błędem, który może bezpośrednio prowadzić do awarii, jest niewłaściwe stosowanie smaru stałofilnowego (*Solid Film Lubricant, SFL*). Ten rodzaj powłoki jest przeznaczony wyłącznie do ochrony zewnętrznych powierzchni metalowych przed korozją i zużyciem. Instrukcja zawiera w tym zakresie jednoznaczne ostrzeżenie:

Fot. 1. Podstawowe rozłożenie karabinka AR. Zdj. K. Chudziński.

„Jeśli smar stałofilnowy wejdzie w kontakt z ruchomymi częściami lub powierzchniami roboczymi karabinu, należy go natychmiast usunąć" [tłum. własne].

Źródło: *Fostech AR-15 Operator Manual.*

SFL nie jest smarem do mechanizmów wewnętrznych. Jego gęsta, sucha konsystencja powoduje zwiększone tarcie i może prowadzić do zacięć suwadła, zamka lub mechanizmu spustowego. Powierzchnie robocze należy smarować wyłącznie odpowiednimi olejami do broni.

ZAKOŃCZENIE

Omawiane błędy, zidentyfikowane na podstawie rygorystycznych wojskowych standardów konserwacji, stanowią fundament wiedzy niezbędnej każdemu właścicielowi platformy AR-15. Unikanie tych pułapek jest warunkiem posiadania broni celnej, bezpiecznej i niezawodnej. Właściciele powinni traktować regularną inspekcję i konserwację nie jako opcję, lecz jako element stałej procedury eksploatacyjnej. W przypadku wątpliwości technicznych – zwłaszcza przy wymianie komponentów krytycznych – każdorazowo należy konsultować się z wykwalifikowanym rusznikarzem.

Literatura

Departments Of The Army And Air Force, *TM 9-1005-319-23&P, Technical Manual*: *Unit and Direct Support Maintenance Manual for Rifle*, *5.56mm*, *M16A2; Carbine*, *5.56mm, M4*; *Carbine, 5.56mm*, *M4A1*, May 1991.

SOG AR-15 – Instrukcja obsługi/bezpieczeństwa. Standard Mfg. Co., New Britain, CT.

Fostech AR-15 Operator Manual.

Real Avid – Instrukcja modyfikacji karabinka AR-15 (*AVTOPMODS*).

Summary

AR-15 uncovered: 10 critical mistakes every user must avoid

The AR-15 platform is valued for its modularity and flexibility, giving users almost endless configuration options. However, this flexibility comes with responsibility – the rifle's reliability, safety, and accuracy all depend on proper assembly, compatible components, and regular maintenance. Even a minor mistake can lead to costly damage or, worse, dangerous malfunction. Based on proven military protocols outlined in technical manual TM 9-1005-319-23&P, this guide helps users avoid the most common pitfalls and ensure their rifle operates safely and reliably, as intended.

Tłumaczenie: Joanna Łaszyn

SIŁA FIZYCZNA JAKO ŚRODEK PRZYMUSU BEZPOŚREDNIEGO

Obezwładnienie osoby agresywnej za pomocą obalenia z uchwytu za nogi

kom. Adam Kryszajtys

Zakład Interwencji Policyjnych CSP

W artykule zaprezentowano propozycje obezwładnienia osoby za pomocą obalenia z uchwytu za nogi z podejścia z przodu oraz z podejścia z tyłu. Omówiono samo pojęcie techniki obalenia, a także za pomocą zdjęć i opisu zilustrowano prawidłowe jej wykonanie.

Funkcjonariusz Policji, już podczas szkolenia zawodowego podstawowego, a następnie w trakcie kursów specjalistycznych oraz doskonalenia lokalnego, jest przygotowywany do podejmowania interwencji oraz wykonywania czynności służbowych m.in. wobec osób agresywnych, pod wpływem środków odurzających, nietrzeźwych, z zaburzeniami psychicznymi.

Interwencje wobec takich osób wymagają od funkcjonariusza dużej sprawności fizycznej oraz umiejętności technicznych. Wiążą się również z możliwością obezwładnienia osoby agresywnej i użycia środków przymusu bezpośredniego lub broni palnej. Oczywiście, odpowiedni dobór środka przymusu bezpośredniego w takich interwencjach jest kluczowy, a funkcjonariusz musi postępować zgodnie z prawem, zasadami oraz warunkami wynikającymi z ustawy z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2026 r. poz. 244) oraz działać w sposób bezpieczny z poszanowaniem godności ludzkiej.

Zgodnie z ww. ustawą jednym z podstawowych i najczęściej stosowanych przez policjantów środków przymusu bezpośredniego jest siła fizyczna. Podzielona jest na techniki: transportowe, obrony, ataku, obezwładnienia.

Samo obezwładnianie polega na pozbawieniu swobody ruchów lub spowodowaniu odwracalnej, krótkotrwałej dysfunkcji kończyn lub zmysłów w celu wyeliminowania zagrożenia ze strony osoby lub przełamania oporu osoby niepodporządkowującej się poleceniom wydanym na podstawie prawa. Funkcjonariusz Policji może stosować obezwładnienie w postaci różnorodnych technik, takich jak np.: podcięcie zewnętrzne, obalenie za głowę, obchwyt szyi z uciskiem, obalenie za nogi itd.

W poniższym artykule chciałbym przedstawić jedną z możliwości zastosowania obezwładnienia agresywnej osoby poprzez obalenie za pomocą uchwytu za nogi z podejścia z przodu lub z tyłu.

Pod pojęciem obalenia z uchwytu za nogi należy rozumieć kontrolowane zblokowanie nóg z jednoczesnym przeniesieniem środka ciężkości człowieka, co powoduje utratę przez niego równowagi, a tym samym pozbawia go swobody wykonywania ruchów.

Obezwładnienie osoby do pozycji do założenia kajdanek poprzez obalenie z uchwytu za nogi z podejścia z przodu

Fot. 1. Przyjęcie postawy walki frontem do osoby obezwładnianej.

Fot. 2. Wejście w zwarcie, klincz oraz kontrola osoby.

Fot. 3. Wybranie ręki napastnika.

Fot. 4. Obniżenie środka ciężkości z jednoczesnym ustawieniem głowy przy biodrze napastnika oraz chwytem oburącz jego nóg.

Fot. 5. Pchanie napastnika z jednoczesnym blokowaniem jego nóg (do obalenia).

Fot. 6. Ustawienie się w pozycji dominującej „bocznej”.

Fot. 7. Zastosowanie dźwigni na dalszą rękę napastnika – „kimura”.

OBALENIE Z UCHWYTU ZA NOGI

Fot. 8. Przetoczenie napastnika na brzuch.

Fot. 9. Dosiad boczny z jednoczesnym zabezpieczeniem ręki dźwignią łokciowo-barkowo-nadgarstkową.

Obezwładnienie osoby z przetoczeniem do pozycji do założenia kajdanek z uchwytu za nogi z podejścia z tyłu

Fot. 10. Przyjęcie postawy walki za plecami osoby obezwładnianej.

Fot. 11. Obniżenie środka ciężkości z jednoczesnym ustawieniem barku w okolicach pośladków i chwytem nóg napastnika na wysokości kolan.

Fot. 12. Pchnięcie barkiem w przód z jednoczesnym blokowaniem nóg.

Fot. 13. Przewrócenie napastnika na brzuch.

Fot. 14. Wybranie ręki napastnika.

Fot. 15. Kontrolowany ucisk stawu barkowego napastnika kolanem.

Fot. 16. Dosiad boczny z jednoczesnym zabezpieczeniem ręki dźwignią łokciowo-barkowo-nadgarstkową. Zdj. 1–16: B. Stępak.

Bibliografia

Ustawa z dnia 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej (Dz. U. z 2026 r. poz. 244).

Bartnicki D., *Stosowanie siły fizycznej jako środka przymusu bezpośredniego. Część II. Obezwładnienie agresywnej osoby poprzez sprowadzenie do parteru*, Słupsk 2014.

Kryszajtys A., *Siła fizyczna jako środek przymusu bezpośredniego. Obezwładnienie osoby agresywnej za pomocą obalenia z uchwytu za głowę,* „Kwartalnik Policyjny" 2022, nr 3.

Summary

Use of force. Neutralising aggressive subjects via leg-grab takedowns

The article explores tactical methods for subduing aggressive individuals using leg-grabs takedowns from both frontal and rear approaches. It discusses the concept of the takedown technique itself and illustrates its correct execution through photographs and descriptions.

Tłumaczenie: Joanna Łaszyn

CZAPKA ZIMOWA POLICYJNA

podkom. Wojciech Pudło

Wydział Dowodzenia CSP

Czapka zimowa służbowa jest istotną częścią munduru policjanta. Funkcjonariusze zakładają zimową czapkę, uwzględniając rodzaje służb w Policji, okres zimowy trwający w Policji od 1 listopada do 30 kwietnia[1] i rodzaj umundurowania. W niniejszym artykule opisano czapkę zimową służbową, wyjaśniono, jakie standardy powinny być zachowane, aby spełniała wymogi przepisów, oraz omówiono zasady dotyczące jej noszenia.

W okresie zimowym, podczas służby, policjanci noszą do munduru służbowego i ćwiczebnego ciemnogranatową czapkę zimową.

Czapka zimowa służbowa typu sportowego jest wykonana z dzianiny w kolorze ciemnogranatowym, z wykończeniem z polaru w tym samym kolorze. Do czapki zimowej jest doszyty nausznik z polaru, który w zależności od warunków atmosferycznych może być wysunięty lub schowany do wewnątrz. Czapkę zimową nosi się prosto nałożoną na głowę. Dolna krawędź czapki zimowej powinna znajdować się na wysokości około 3 cm nad linią brwi[2]. Na przodzie czapki zimowej służbowej znajduje się wizerunek orła mechanicznie haftowany ustalony dla godła Rzeczypospolitej Polskiej z napisem „POLICJA", w kolorze srebrnym, umieszczony na wstędze w kolorze ciemnoniebieskim. Wzór wizerunku orła z napisem „POLICJA" jest określony w załączniku nr 6 do rozporządzenia[3].

Dzięki temu, że ma ona formę zbliżoną do standardowej czapki beanie, model ten dobrze układa się na głowie i świetnie zabezpiecza przed chłodem – nawet przy niesprzyjającej aurze.

Fot. 1. Wzór wizerunku orła z napisem „POLICJA". Źródło: rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 20 maja 2009 r. w sprawie umundurowania policjantów (Dz. U. Nr 90, poz. 738, z późn. zm.).

Fot. 2. Sposób noszenia nausznika z polaru schowany do wewnątrz lub wysunięty. Zdj. W. Pudło.

Fot. 3. Sposób noszenia czapki zimowej z mundurem służbowym i ćwiczebnym[4]. Źródło: rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 20 maja 2009 r. w sprawie umundurowania policjantów (Dz. U. Nr 90, poz. 738, z późn. zm.).

[1] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 20 maja 2009 r. w sprawie umundurowania policjantów (Dz. U. Nr 90, poz. 738, z późn. zm.). § 34 nin. rozporządzenia wskazujący okres letni i okres zimowy został zmieniony przez § 1 pkt 1 rozporządzenia z dnia 28 marca 2011 r. (Dz. U. Nr 70, poz. 372) zmieniającego nin. rozporządzenie z dniem 1 kwietnia 2011 r.

[2] Tamże, § 5 ust. 4 został zmieniony przez:
- § 1 pkt 2 lit. d rozporządzenia z dnia 27 września 2017 r. (Dz. U. poz. 1879) zmieniającego nin. rozporządzenie z dniem 11 października 2017 r.
- § 1 pkt 4 lit. b rozporządzenia z dnia 18 maja 2022 r. (Dz. U. poz. 1176) zmieniającego nin. rozporządzenie z dniem 3 czerwca 2022 r.
- § 1 pkt 1 rozporządzenia z dnia 19 grudnia 2024 r. (Dz. U. poz. 1953) zmieniającego nin. rozporządzenie z dniem 31 grudnia 2024 r.

[3] Tamże, § 27 został zmieniony przez:
- § 1 pkt 12 rozporządzenia z dnia 27 września 2017 r. zmieniającego nin. rozporządzenie z dniem 11 października 2017 r.
- § 1 pkt 14 rozporządzenia z dnia 18 maja 2022 r. zmieniającego nin. rozporządzenie z dniem 3 czerwca 2022 r.

[4] Tamże, zał. nr 1 zmieniony przez § 1 pkt 16 rozporządzenia z dnia 19 grudnia 2024 r. zmieniającego nin. rozporządzenie z dniem 31 grudnia 2024 r. (mundur służbowy); zał. nr 4 zmieniony przez:
- § 1 pkt 21 rozporządzenia z dnia 27 września 2017 r. zmieniającego nin. rozporządzenie z dniem 11 października 2017 r.
- § 1 pkt 17 rozporządzenia z dnia 19 grudnia 2024 r. zmieniającego nin. rozporządzenie z dniem 31 grudnia 2024 r. (mundur ćwiczebny).

Bibliografia

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 20 maja 2009 r. w sprawie umundurowania policjantów (Dz. U. Nr 90, poz. 738).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 28 marca 2011 r. zmieniające rozporządzenie w sprawie umundurowania policjantów (Dz. U. Nr 70, poz. 372).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 27 września 2017 r. zmieniające rozporządzenie w sprawie umundurowania policjantów (Dz. U. poz. 1879).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 18 maja 2022 r. zmieniające rozporządzenie w sprawie umundurowania policjantów (Dz. U. poz. 1176).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 19 grudnia 2024 r. zmieniające rozporządzenie w sprawie umundurowania policjantów (Dz. U. poz. 1953).

Summary

Police winter cap

The police winter cap is an essential part of a police officer's uniform. Its use depends on the duties performed, the type of uniform worn, and the official winter uniform period, which runs from November 1st to April 30th. This article describes the police winter cap, explains the standards it must meet under applicable regulations, and outlines the rules governing its wear.

Tłumaczenie: Joanna Łaszyn

ZASADY PUBLIKOWANIA
w „Kwartalniku Policyjnym”

Informacje dla autorów

1. Redakcja przyjmuje teksty dotąd niepublikowane, dotyczące zagadnień związanych z funkcjonowaniem Policji i z szeroko rozumianym bezpieczeństwem, a także z praktyką policyjną i współpracą formacji z innymi instytucjami ochrony porządku prawnego oraz z samorządem lokalnym.
2. Materiały do publikacji należy przesyłać pocztą elektroniczną na adres: kwartalnik@csp.edu.pl lub składać w sekretariacie Wydziału Wydawnictw i Poligrafii Centrum Szkolenia Policji w Legionowie (ul. Zegrzyńska 121, 05-119 Legionowo, tel. 47 725 58 81 lub 47 725 52 70).
3. Prace są kwalifikowane do druku przez zespół redakcyjny czasopisma. Redakcja zastrzega sobie prawo dokonywania skrótów i adiustacji tekstów oraz zmiany tytułów i śródtytułów.
4. Artykuły mogą być kierowane do recenzji. Recenzja ma formę pisemną. Zawiera syntetyczną charakterystykę artykułu, część analityczną, ocenę ogólną i kończy się jednoznaczną konkluzją, tj. jest pozytywna, negatywna lub warunkowo pozytywna, jeśli recenzent wskazuje na konieczność wprowadzenia poprawek. Autorzy artykułów są zobowiązani do ustosunkowania się do uwag i uwzględnienia sugerowanych zmian.
5. W celu zapobiegania wszelkim przejawom nierzetelności, w tym zjawisku *ghostwriting* i *guest authorship*, redakcja wymaga ujawnienia przez autorów wkładu w powstanie publikacji.
6. Materiały mogą być weryfikowane w systemie antyplagiatowym, zgodnie z procedurą obowiązującą w Centrum Szkolenia Policji w Legionowie.
7. Materiały są publikowane w „Kwartalniku Policyjnym” nieodpłatnie, po złożeniu przez autora pisemnego oświadczenia, zgodnie z otrzymanym od redakcji wzorem.
8. Nadesłanych materiałów do publikacji redakcja nie zwraca.
9. Wersją pierwotną (referencyjną) czasopisma jest wydanie papierowe. Ponadto poszczególne numery są również dostępne w wersji elektronicznej na stronie internetowej: www.kwartalnik.csp.edu.pl.
10. Wskazówki edytorskie dotyczące przygotowania materiału przez autorów:

- format A4, czcionka Times New Roman, wielkość 12 punktów, interlinia 1,5 wiersza, marginesy – 2,5 cm;
- na pierwszej stronie należy podać imię i nazwisko autora materiału, stopień (lub tytuł) naukowy (tytuł zawodowy), nazwę instytucji, w której autor jest zatrudniony, nr telefonu, adres e-mailowy;
- do tekstu należy dołączyć streszczenie oraz tytuł pracy w języku angielskim;
- materiał ilustracyjny powinien być dostarczony w oddzielnych plikach (rysunki lub fotografie w formacie jpg, rozdzielczość 300 dpi, minimalna wielkość 1,5 MB);
- schematy i wykresy muszą być edytowalne, tak aby można było nanieść korektę;
- przypisy należy umieścić na dole strony lub na końcu pracy; przypisy wstawia się automatycznie i oznacza się cyframi arabskimi;
- zgodnie z normami wydawniczymi przypis bibliograficzny powinien zawierać:
  - imię i nazwisko autora, tytuł, wydawcę, miejsce i rok wydania, numer strony:

    M. Olbrycht, J. Rutkowski, *Taktyka minersko-pirotechniczna w działaniach antyterrorystycznych*, Centrum Szkolenia Policji, Legionowo 2003, s. 35–36;
  - jeżeli dzieło jest pracą zbiorową:

    Nowy leksykon PWN, red. A. Dyczkowski, Warszawa 1998, s. 684;
  - jeżeli jest to artykuł w pracy zbiorowej:

    J. Szreniawski, *Prawo do dobrej administracji prawem podmiotowym obywatela*, w: *Dobra administracja. Teoria i praktyka*, red. J. Łukasiewicz, S. Wrzosek, Radom 2007, s. 256;
  - jeżeli jest to artykuł w czasopiśmie:

    B. Jankowska, *Odpowiedzialność karna osób prawnych*, „Państwo i Prawo” 1996, nr 7, s. 46;
  - jeżeli jest to akt prawny (należy wskazać publikator):

    Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2025 r. poz. 636, z późn. zm.);
  - jeżeli jest to tekst opublikowany w Internecie:

    J. Kowalski, *Edukacja online*, www.gazeta.pl/forum?forumedukacyjne5645 [dostęp: 12.03.2004 r.].

100-LECIE

SPORT w POLICJI

1926–2026