

KULTURA BEZPIECZEŃSTWA
NR 40, 2021 (50–78)
ISSN 2299-4033 DOI: 10.5604/01.3001.0015.6971

ARCHITEKTURA I NARZĘDZIA
POLICYJNEJ WYMIANY INFORMACJI
KRYMINALNYCH. PERSPEKTYWA
KRAJOWA I MIĘDZYNARODOWA

ARCHITECTURE AND TOOLS OF THE POLICE
EXCHANGE OF CRIMINAL INFORMATION.
NATIONAL AND INTERNATIONAL PERSPECTIVE

Piotr Zalewski*

ABSTRACT

The article presents the national and international system of criminal information exchange, implemented at the operational and non-operational level, between the Polish Police and services, agencies and institutions of the European Union and third countries, in the area of prosecuting perpetrators of crimes and ensuring public order. Purpose of the publication is to verify the hypothesis that in the modern world, without effective, fast exchange of information of importance for security and public order, it is difficult to effectively recognize and neutralize emerging threats, and to prosecute perpetrators of crimes. In order to verify the adopted hypothesis, the most important national and international databases and instruments for the exchange of criminal information available to law enforcement authorities of the European Union (EU) and third countries, as well as EU agencies

* dr Piotr Zalewski, Uniwersytet Jana Kochanowskiego w Kielcach; correspondence address: Wydział Prawa i Nauk Społecznych Uniwersytetu Jana Kochanowskiego w Kielcach, ul. Uniwersytecka 15, 25-406 Kielce, Polska; e-mail: piotr.zalewski@ujk.edu.pl, ORCID: 0000-0002-0997-8561

and international organizations established to prevent, fight and detect crimes (INTERPOL, EUROPOL) and the prosecution of the perpetrators of these crimes. The subject matter has been presented in the perspective of the historical development of tools and instruments for gathering and exchanging criminal information in national databases in Poland as well as in EU countries and third countries. The presented review of the tools and instruments of the international exchange of criminal information made it possible to prove the adopted hypothesis.

KEYWORDS

Police, security, criminal information, international cooperation

ABSTRAKT

Artykuł stanowi próbę scharakteryzowania krajowego i międzynarodowego systemu wymiany informacji kryminalnych realizowanej na poziomie operacyjnym i pozaoperacyjnym, pomiędzy polską Policją a służbami, agencjami i instytucjami Unii Europejskiej i państw trzecich, w zakresie ścigania sprawców przestępstw i zapewnienia porządku publicznego. Celem publikacji jest weryfikacja hipotezy, że we współczesnym świecie, bez efektywnej, szybkiej wymiany informacji, mających znaczenie dla bezpieczeństwa i porządku publicznego, trudno skutecznie rozpoznawać i neutralizować pojawiające się zagrożenia, a także ścigać sprawców przestępstw. W celu weryfikacji przyjętej hipotezy dokonano przeglądu najważniejszych krajowych i międzynarodowych baz danych i instrumentów wymiany informacji kryminalnych dostępnych organom ścigania państw członkowskich Unii Europejskiej (dalej UE) i państw trzecich, a także agencjom UE oraz organizacjom międzynarodowym, powołanym do zapobiegania, zwalczania i wykrywania przestępstw (INTERPOL, EUROPOL) oraz ścigania sprawców tych przestępstw. Przedmiotowa problematyka pokazana została w perspektywie historycznego rozwoju narzędzi i instrumentów gromadzenia i wymiany informacji kryminalnych w krajowych bazach danych w Polsce oraz w państwach EU i państwach trzecich. Zaprezentowany przegląd narzędzi i instrumentów międzynarodowej wymiany informacji kryminalnych pozwolił udowodnić przyjętą hipotezę.

SŁOWA KLUCZOWE

Policja, bezpieczeństwo, informacja kryminalna, współpraca międzynarodowa

WPROWADZENIE

Procesy globalizacyjne, depresja barier granicznych oraz rozwijające się na różnych płaszczyznach i poziomach sieci nowych powiązań i relacji między jednostkami i całymi społeczeństwami, a także systemami technologicznymi i informacyjnymi, wymagają stałego poszerzania zdolności do rozpoznawania pojawiających się ryzyk i zagrożeń bezpieczeństwa, oraz doskonalenia metod ich zapobiegania i neutralizacji. Każde państwo, a w jego strukturach urzędy, instytucje, służby, organizacje, a nawet pojedynczy obywatele, podejmują różne działania na rzecz wypracowania rozwiązań i narzędzi do skutecznego rozpoznawania i identyfikacji pojawiających się zagrożeń, a także do minimalizowania ich skutków bądź całkowitej eliminacji.

Powszechnie przyjmuje się, że zapewnienie porządku publicznego i bezpieczeństwa obywateli należy do podstawowych obowiązków państwa, które tworzy w tym celu odpowiednie rozwiązania prawne i organizacyjne, a także ponosi związane z tym nakłady finansowe. Zadaniem państwa jest więc budowanie odpowiedniego potencjału infrastrukturalnego i organizacyjnego, który funkcjonalnie będzie służył instytucjom i organom państwa powołanym do zapewnienia porządku i bezpieczeństwa. Wyzwania, jakie stają przed państwami i ich strukturami w tych kwestiach, wymagają ciągłego doskonalenia struktur i poszukiwania nowych sposobów działania przy zaangażowaniu i wykorzystaniu zasobów organizacyjnych i technicznych. Rozwój technologiczny i globalizacja zagrożeń, z jakimi mamy do czynienia we współczesnym świecie w naturalny sposób wymuszają właściwe gromadzenie, przetwarzanie i wykorzystanie informacji dotyczących zagrożeń i efektów ich zwalczania. Zjawiska te determinują także lokalną (krajową) i międzynarodową współpracę między podmiotami odpowiedzialnymi za ochronę porządku i bezpieczeństwa państwa. Chcąc zapewnić porządek publiczny na terenie własnego terytorium, rządy zmuszone są do coraz efektywniejszej kooperacji w zakresie współpracy i wymiany informacji kryminalnych¹ na poziomie prowadzo-

¹ Informacje kryminalne to dane pobierane, uzyskiwane, gromadzone, przetwarzane i przekazywane przez uprawnione organy, takie jak: czas i miejsce popełnienia przestępstwa; rodzaj działalności przestępczej; informacje o osobach dokonujących przestępstw (dane personalne, wiek, pseudonim, adres miejsca pobytu); informacje o przedmiotach wykorzystanych do popełnienia przestępstw; informacje o przedsiębiorcach, fundacjach, stowarzyszeniach, co do których zachodzi uzasadnione podejrzenie, że zostały wykorzystane w celu popełnienia przestępstwa; informacje o numerach rachunków bankowych lub rachunków papierów wartościowych, co do których zachodzi uzasadnione podejrzenie, że zostały wykorzystane w celu popełnienia przestępstwa; informacje o *modus operandi* przestępców; *Vide* Art. 13 ustawy z dnia 6 lipca 2001 r.

nych registratur i baz danych poszczególnych służb. Ważny jest również udział ich przedstawicieli w pracach gremiów eksperckich, wspólne działania prewencyjne i operacyjne, szkolenia, współpraca sąsiadujących regionów przygranicznych, czy też operacje utrzymania porządku publicznego i pokoju².

Zapobieganie przestępczości, wykrywanie przestępstw popełnionych, a także podejmowanie adekwatnych działań na rzecz ochrony bezpieczeństwa i porządku publicznego przez służby policyjne zależy od poziomu wyszkolenia, zaangażowania i kreatywności policjantów. Równie ważne w tym procesie jest wykorzystanie możliwości, jakie daje rozwój nauki, zastosowanie nowych technologii badawczych, informatyzacja procesów gromadzenia, przetwarzania, analizy i rozpowszechniania informacji i danych (ważnych z punktu widzenia reakcji na zdarzenie), prawidłowego i efektywnego dyslokowania służb czy też efektywności procesu wykrywczego. Informacje i dane gromadzone i przetwarzane przez służby i organizacje policyjne na poziomie krajowym i międzynarodowym wykorzystywane w procesie zapewnienia porządku publicznego, mają wiele zastosowań. Łącznie z zasobami i bazami danych podmiotów administracji państwowej, samorządowej i sektora pozarządowego tworzą zaplecze, które ułatwia proces diagnozowania i rozpoznawania ryzyk i zagrożeń. Wspomaga to także działania wspomnianych podmiotów pozwalając na właściwe formułowanie zadań dla służb policyjnych, ułatwia poszukiwanie osób zaginionych i ukrywających się przed instytucjami wymiaru sprawiedliwości, pomaga weryfikować wiarygodność dokumentów oraz prowadzić czynności operacyjne i dochodzeniowe, a także wiele innych³.

o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych (tekst jedn. Dz. Urz. z 2010 r. Nr 29, poz. 153 z późn. zm.); T. Safjański, 'Administracyjne modele wymiany informacji kryminalnych z zagranicą na przykładzie polskiej Policji', *Research Gate*, January 2016, https://www.researchgate.net/publication/326539662_Administracyjne_modele_wymiany_informacji_kryminalnych_z_zagranica_na_przykladzie_polskiej_Policji_eng_Administrative_models_of_criminal_information_exchange_with_foreign_partners_on_the_example_of_th, (accessed 31 October 2021).

² P. Zalewski, 'Międzynarodowa współpraca polskiej Policji w świetle teorii dóbr publicznych', *Kultura Bezpieczeństwa*, no. 37, 2020, p. 86.

³ Możliwości gromadzenia, przetwarzania i wymiany informacji o osobach, podmiotach, zdarzeniach, rzeczach, zjawiskach, trendach, sposobie działania (*modus operandi*), planowanych lub dokonanych przestępstwach – ograniczenia w zakresie gromadzonych i przetwarzanych danych, wynikają z porządku prawnego poszczególnych państw, a ich katalog jest otwarty.

Rozwój technologiczny w zakresie możliwości gromadzenia, przetwarzania i wykorzystania danych i informacji ważnych z punktu widzenia szeroko rozumianego bezpieczeństwa spowodował tworzenie registratur manualnych, a następnie scentralizowanych, rozbudowywanych systemów informatycznych posiadających tematyczne bazy danych. Są to krajowe systemy i bazy danych tworzone specjalnie dla Policji, jak również systemy informatyczne o zasięgu międzynarodowym, tworzone dla potrzeb zwalczania międzynarodowej przestępczości zorganizowanej, a także kontroli przestępczości na terenie Unii Europejskiej i zabezpieczenia bezpieczeństwa państw strefy Schengen.

Przedmiotem artykułu jest próba refleksji nad problematyką zapewnienia bezpieczeństwa i porządku publicznego w Polsce w perspektywie działań podejmowanych przez służby do tego powołane – w tym wypadku przez Policję, która swoje ustawowe zadania realizuje przy wykorzystaniu instrumentów wymiany informacji kryminalnych na poziomie krajowym i międzynarodowym. Wymiana takich danych sprowadza się w praktyce do udostępniania, przekazywania, uzyskiwania lub otrzymywania informacji gromadzonych przez podmioty krajowe oraz organy ścigania poszczególnych państw lub inne uprawnione instytucje i agencje. Współpraca w tym zakresie realizowana jest na poziomie krajowym poprzez integrację zasobów informatycznych i baz danych poszczególnych instytucji. Międzynarodowa wymiana informacji kryminalnych odbywa się w ramach międzynarodowej współpracy operacyjnej i pozaoperacyjnej za pośrednictwem krajowego punktu kontaktowego (dalej KPK), Biura Międzynarodowej Współpracy Policji KGP (dalej BMWP KGP), przy użyciu trzech głównych kanałów wymiany informacji, tj. Międzynarodowej Organizacji Policji Kryminalnych INTERPOL⁴, Agencji Unii Europejskiej ds. Współpracy Organów Ścigania EUROPOL⁵, platformy wymiany infor-

⁴ Interpol (ang. *International Criminal Police Organization* – Międzynarodowa Organizacja Policji Kryminalnych) to policyjna organizacja międzynarodowa, założona w 1923 roku w Wiedniu jako Międzynarodowa Komisja Policji Kryminalnych. Od 1938 miała siedzibę w Berlinie, w 1946 wznowiła działalność, z siedzibą Sekretariatu Generalnego w Saint Cloud koło Paryża; od 1956 roku działa jako Międzynarodowa Organizacja Policji Kryminalnych. Należy do niej 187 państw. Celem Interpolu jest ułatwianie międzynarodowej współpracy policyjnej, nawet w przypadku braku więzi dyplomatycznych pomiędzy poszczególnymi członkami.

⁵ Europol (Agencja Unii Europejskiej ds. Współpracy Organów Ścigania) to unijna agencja egzekwowania prawa, której zadaniem jest zwiększanie poziomu bezpieczeństwa w Europie poprzez zapewnianie pomocy organom ścigania w państwach członkowskich

macji państw strefy Schengen – Systemu Informacji Schengen (dalej SIS, SIS II) za pośrednictwem biura SIRENE⁶. Dodatkowo wymiana informacji odbywa się za pośrednictwem Oficerów Łącznikowych Policji oraz Policyjno-Celnych Centrów Współpracy (dalej PCCC), których zadaniem jest bezpośrednia współpraca służb policyjnych, celnych i granicznych w ramach przygranicznej wymiany informacji⁷.

Artykuł zawiera przegląd najważniejszych krajowych i międzynarodowych baz danych i instrumentów wymiany informacji kryminalnych dostępnych organom ścigania państw członkowskich Unii Europejskiej (dalej UE) i państw trzecich, a także agencjom UE oraz organizacjom międzynarodowym powołanym do zapobiegania, zwalczania i wykrywania przestępstw (INTERPOL, EUROPOL) oraz ścigania sprawców tych przestępstw.

UE. Z racji tego, że zajmuje ona centralne miejsce w europejskiej strukturze bezpieczeństwa, Europol oferuje wsparcie w zakresie operacji egzekwowania prawa w terenie, platformę wymiany informacji na temat działalności przestępczej, ośrodek wiedzy specjalistycznej z zakresu ścigania oraz długoterminowe analizy dotyczące przestępczości i terroryzmu; *Vide* Unia Europejska, 'Europol', *Europa.eu*, https://europa.eu/european-union/about-eu/agencies/europol_pl, (accessed 31 October 2021).

⁶ SIRENE (ang. *S.I.Re.N.E – Supplementary Information Request At National Entries* – wniosek o informacje uzupełniające do wpisów krajowych); Organ wyznaczony przez każde państwo członkowskie, zgodnie z jego przepisami wewnętrznymi, na podstawie art. 92 ust. 4 Konwencji Wykonawczej do Układu Schengen (KWS), zastąpionego z dniem 9 kwietnia 2013 roku przepisami art. 7 ust. 2 Decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz. Urz. UE L 205 z 2007 r.) oraz Rozporządzenia (WE) 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz. Urz. UE L 381 z 2006 r.). Zadaniem biura SIRENE jest wymiana informacji uzupełniających niezbędnych przy wprowadzaniu wpisów i w celu umożliwienia podjęcia odpowiednich działań w przypadku trafienia w SIS, (czyli gdy w wyniku sprawdzenia w Systemie Informacyjnym Schengen (SIS) odnaleziono osoby lub przedmioty wprowadzone do systemu). *Vide* Policja, 'Co to jest biuro SIRENE', *Policja.pl*, <https://policja.pl/pol/sirene/biuro-sirene/7842,Co-to-jest-BIURO-SIRENE.html>, (accessed 31 October 2021).

⁷ Policyjno-Celne Centra Współpracy (ang. *Police and Customs Cooperation Center – PCCC*) funkcjonują w Polsce pod wspólną nazwą Centrum Współpracy Przygranicznej (dalej CWP). Na podstawie umów i porozumień bilateralnych w Polsce istnieje 6 PCCC, natomiast w całej Unii Europejskiej 60 PCCC.

KRAJOWE BAZY DANYCH I WYMIANA INFORMACJI KRYMINALNYCH W POLSCE

Przez ponad 100 lat swojego istnienia polska Policja, wzorem podobnych służb na świecie, podejmowała wysiłki tworzenia registratur zawierających informacje o przestępstwach i przestępcach, a także istotnych okolicznościach przydatnych w procesie wykrywania i zapobiegania przestępstwom. Registratury kryminalistyczne i wykorzystanie ich funkcji informacyjnej w praktyce służb policyjnych są swoistą pamięcią organów ścigania, w której zapisane są informacje o czynach przestępczych, sprawcach oraz przedmiotach związanych ze zdarzeniem⁸. J. Widacki zauważa, że w „registraturach przechowywane są informacje istotne przy działaniach wykrywczych, a niekiedy także dowodowych. W registraturach nie tylko gromadzone są informacje, ale są one także opracowywane (selekcjonowane, klasyfikowane). Przechowywane informacje, dzięki istniejącemu systemowi, mogą być wzajemnie kojarzone i uzupełniane”⁹.

Wraz z rozwojem technologii komputerowych i informatycznych, manualne registratury kryminalistyczne prowadzone przez służby policyjne poddawane były procesowi digitalizacji, a architektura tych systemów sprowadzała się do procesów automatycznego przetwarzania i przechowywania danych. Pozwoliło to nie tylko wykorzystywać informacje i dane na potrzeby służby państwa prowadzącego takie bazy, ale stało się też elementem współpracy i wymiany informacji między służbami krajowymi na poziomie międzynarodowym, w celu zapobiegania i zwalczania przestępstw transgranicznych.

W warunkach panujących w Polsce potrzeba stopniowej informatyzacji Policji definiowana była w latach 1970–1990 w kontekście informatyzacji wszystkich służb podlegających resortowi spraw wewnętrznych. W 1990 roku opracowany został program informatyzacji Policji, który stał się elementem szerszego procesu modernizacji organizacji i zarządzania Policją¹⁰. Prace modernizacyjne koncentrowały się głównie w obrębie wprowadzania narzędzi informatycznych do obsługi pracy biurowej, programów i aplikacji do analizy i przetwarzania danych, digitalizacji registratur manualnych i tworzenia elektronicznych kartotek i baz danych,

⁸ D. Wilk, *Kryminalistyka: Przewodnik*, Toruń, TNOiK, 2013, p. 186.

⁹ T. Widła, *Kryminalistyka*, J. Widacki (ed.), Kraków, C. H. Beck, 2018, p. 146.

¹⁰ Programy te stały się dokumentami cyklicznymi definiującymi podstawowe kierunki rozwoju łączności i informatyki policyjnej na poszczególne lata.

budowania systemów wymiany informacji między bazami danych, a także wprowadzania programów ilustracji i prezentacji danych oraz komunikacji elektronicznej i teletransmisji danych.

Ustawowe uprawnienie Policji do uzyskiwania informacji – w tym także niejawnych – gromadzenia ich, sprawdzania oraz przetwarzania w odpowiednio zaprojektowanych bazach danych jest jednym z zasadniczych narzędzi, które umożliwia reagowanie na przestępstwa i wykroczenia, a także podejmowanie działań administracyjnych, operacyjno-rozpoznawczych i zapobiegawczych¹¹. Procesy wsparcia działań Policji w latach 90. XX wieku, poprzez informatyzację poszczególnych jej obszarów, charakteryzowały się rozproszeniem baz danych oraz zastosowaniem w tych systemach różnych narzędzi informatycznych, które czyniły je niewydolnymi i nie gwarantowały sprawnego ich funkcjonowania.

Formująca się w 1990 roku Policja eksploatowała więc różne systemy informatyczne i bazy danych, które służyć miały komputerowemu wsparciu śledztw i pozyskiwaniu informacji przydatnych w prowadzonych czynnościach ze zbiorów pełniących funkcję banków informacji kryminalnej, takie jak np.:

- Terenowe Banki Informacji Kryminalnej (TBIK); opracowany w Komendzie Wojewódzkiej Policji (dalej KWP) we Wrocławiu system TBIK eksploatowany był w Wydziale I Biura Łączności i Informatyki Komendy Głównej Policji (dalej KGP) oraz w Komendzie Stołecznej Policji (dalej KSP) w Warszawie. W KWP w Bydgoszczy użytkowany był, opracowany we własnym zakresie, System Informacyjno-Rozpoznawczy Policji – SIRP. W pozostałych KWP w kraju eksploatowane były systemy ewidencji kryminalnej opracowane i wdrożone w oparciu o własne prace projektowe;
- we wszystkich KWP w kraju użytkowane były bazy danych takie jak Centralna Kartoteka Rzeczy Utraconych (dalej CKRU), Kartoteka Osób Poszukiwanych (dalej SEPO);
- w Centralnym Laboratorium Policji eksploatowane są systemy ewidencji utraconej broni, niezidentyfikowanych śladów daktyloskopijnych;

¹¹ Przepisy upoważniające do uzyskiwania, gromadzenia, przetwarzania i wykorzystania informacji zawarte są w art. 20. [Uzyskiwanie, sprawdzanie, przetwarzanie i wymiana informacji] Ustawy o Policji oraz innych przepisach rangi ustawowej (np. Kodeks Postępowania Karnego) i aktach wykonawczych; Ustawa z dnia 6 kwietnia 1990 r. o Policji, (Dz. Urz. 1990 Nr 30 poz. 179 z późn. zm.)

- współpraca z INTERPOLEM odbywała się poprzez tradycyjną wymianę zapytań i odpowiedzi krajowego biura INTERPOLU KGP i Sekretariatu Generalnego w Lyonie. Jeszcze w 1992 roku trwały przygotowania do integracji systemu komputerowego KGP i Interpolu;
- w zakresie współpracy w Europie w Biurze Informatyki KGP eksploatowany był teleks podłączony do systemu komputerowego Federalnego Urzędu Kryminalnego Niemiec w Wiesbaden. W Biurze Informatyki KGP oraz KWP w Poznaniu utworzono połączenie modemowe do komputera zawierającego dane o samochodach kradzionych w sześciu krajach Europy (Zachodniej);
- policyjna statystyka przestępczości przetwarzana była w systemie TEMIDA (jednolitej policyjno-prokuratorskiej statystyce przestępczości, samobójstw, utonięć i wyników pracy policji). Dane wprowadzane były w poszczególnych KWP i przetwarzane na komputerach w KWP i KGP;
- statystyka wykroczeń w ruchu drogowym prowadzona była w bazie o nazwie System Ewidencyjno Rozpoznawczy Wykroczeń (dalej SERW), który w KWP we Wrocławiu należał do systemu TBIK, a w KSP funkcjonował na komputerach Departamentu PESEL Ministerstwa Spraw Wewnętrznych (dalej MSW). W niektórych KWP system SERW wyposażony był w podsystem rejestrujący legitymowania osób, a niektóre KWP opracowywały i wdrażały autorskie programy obsługiwane przez komputery osobiste;
- na poziomie krajowym Policja korzystała z funkcjonujących w administracji publicznej pozapolicyjnych baz danych. W zasobach Departamentu PESEL MSW funkcjonował Centralny Bank Danych (dalej TBD) oraz Terenowe Banki Danych (dalej TBD), które podłączone były do specjalnie dedykowanych komputerów w niektórych jednostkach Policji. W jednostkach, gdzie istniało połączenie komputerowe z bazą danych PESEL (funkcjonowała równolegle do CBD i TBD), wśród danych znajdowały się informacje dotyczące np. rejestracji w Centralnym Rejestrze Skazanych MSW (podsystem SESTA) oraz informacje z Kartoteki Skazanych i Tymczasowo Aresztowanych (dalej KSiTA) prowadzonych przez Centralny zarząd Zakładów Karnych Ministerstwa Sprawiedliwości¹².

Prace nad opracowaniem nowego rozwiązania informatycznego służącego gromadzeniu danych policyjnych rozpoczęto w 1992 roku, kiedy

¹² Komenda Główna Policji, *Kierunki Informatyzacji Policji*, Warszawa, KGP, 1993, p. 5, (materiały w zbiorach autora).

to w Biurze Informatyki KGP powstał pierwszy kompleksowy program informatyzacji polskiej Policji. Jego realizacja umożliwiła wdrożenie Zintegrowanego Systemu Informacyjnego Policji (dalej ZSIP), a tym samym przeniesienie wszelkich zasobów z kartotek manualnych do pamięci komputerowej. W zasobach ZSIPu gromadzono i przetwarzano dane tekstowe i numeryczne (nie było dostępnej funkcji graficznego gromadzenia i przetwarzania danych) dotyczące osób, zdarzeń, postępowań przygotowawczych, rzeczy i obiektów. System posiadał następujące funkcjonalności:

- wprowadzania danych, które zasilają bazy danych ZSIP nowymi informacjami;
- sprawdzeń (zapytań), które wspomagają działania służb policyjnych poprzez umożliwienie dostępu do zgromadzonych i przetworzonych informacji o osobach, zdarzeniach, pojazdach, dokumentach oraz rzeczach;
- analiz, które umożliwiały dostęp do zgromadzonych i przetworzonych informacji poprzez możliwość m.in. wyszukiwania i typowania w bazie danych ZSIP osób lub zdarzeń według zadanych kryteriów.

Zintegrowany System Informacyjny Policji stanowił pewien przełom w gromadzeniu, przetwarzaniu i udostępnianiu danych dla potrzeb Policji, chociaż miał oczywiście swoje wady. Kontrola funkcjonowania ZSIPu przeprowadzona w 2002 roku przez Najwyższą Izbę Kontroli zakończyła się oceną negatywną w zakresie skutecznego wspomagania działań Policji w ochronie bezpieczeństwa publicznego. Kontrolerzy zarzucali, że ZSIP nie spełnia wymagań w zakresie współdziałania z innymi bazami danych. Rozproszenie baz danych oraz zastosowane w tych systemach narzędzia informatyczne czyniły je niewydolnymi i nie gwarantowały sprawnego ich funkcjonowania. Narzędzia informatyczne zastosowane w ZSIP nie pozwalały na sprawną obsługę baz danych systemu, których zawartość stale wzrastała. W ZSIP zapisywane były wyłącznie informacje tekstowe i numeryczne, podczas gdy system powinien umożliwiać gromadzenie i przetwarzanie także informacji graficznych. ZSIP nie umożliwiał bezpośrednio współpracy z innymi systemami funkcjonującymi w Policji oraz poza Policją. Utrudniało to sprawne korzystanie z baz danych tych systemów, a zatem wydłużało czas pozyskiwania informacji. Rozwiązania informatyczne zastosowane w ZSIP były przestarzałe i nie odpowiadały rozwiązaniom zastosowanym w krajach Unii Europejskiej i NATO, co miało szczególne znaczenie w związku z członkostwem Polski w NATO oraz przyszłą integracją z Unią Europejską. Stan techniczny wielu urządzeń funkcjonujących w ZSIP był zły, odnotowano także istotne trudności z rozbudową baz danych systemu, ochroną danych przetwarzanych w systemach oraz

dostępem osób nieuprawnionych¹³. W 2003 roku ZSIP został zastąpiony przez Krajowy System Informacyjny Policji (dalej KSIP).

KRAJOWE CENTRUM INFORMACJI KRYMINALNEJ

Krajowe Centrum Informacji Kryminalnej (dalej KCIK)¹⁴ to ogólnopolski system informacyjny, którego głównym zadaniem jest wspieranie instytucji i służb porządku publicznego, w skutecznym wykrywaniu i ściganiu sprawców przestępstw oraz w zapobieganiu przestępczości. Funkcję Szefa KCIK pełni Komendant Główny Policji, który realizuje swoje zadania przy pomocy Centrum będącego komórką organizacyjną KGP. Do zadań KCIK należy gromadzenie w jednym miejscu informacji kryminalnych znajdujących się w zasobach organów zajmujących się zwalczaniem przestępczości, które przetwarzane są w bazach danych, dzięki czemu zainteresowane podmioty mogą uzyskiwać informacje o przestępstwach, przestępcach, grupach przestępczych.

Zgodnie z treścią ustawy o Krajowym Centrum Informacji Kryminalnej, w KCIK gromadzone są informacje kryminalne o: przestępstwach; osobach, przeciwko którym prowadzone jest postępowanie karne, w tym w sprawach o przestępstwa skarbowe, lub w stosunku do których prowadzone są czynności operacyjno-rozpoznawcze; przedmiotach wykorzystanych do popełnienia przestępstwa, lub utraconych w związku z przestępstwem; przedsiębiorcach, spółkach cywilnych, fundacjach, stowarzyszeniach, co do których zachodzi podejrzenie, że zostały wykorzystane w celu popełnienia przestępstwa, zgromadzone w rejestrach prowadzonych na podstawie odrębnych przepisów; numerach rachunków bankowych lub rachunków papierów wartościowych, co do których zachodzi uzasadnione podejrzenie, że zostały wykorzystane w celu popełnienia przestępstwa lub że gromadzone są na nich środki pochodzące z przestępstwa; innych postępowaniach lub czynnościach prowadzonych na podstawie ustaw przez podmioty objęte niniejszą ustawą, istotnych z punktu widzenia czynności operacyjno-rozpoznawczych lub postępowania karnego, w tym postępowania w sprawach o przestępstwa skarbowe.

Funkcjonalność KCIK umożliwia gromadzenie informacji kryminalnych (funkcja ewidencyjna), które podmioty uprawnione przekazują nie-

¹³ Najwyższa Izba Kontroli, *Informacja o wynikach kontroli funkcjonowania policyjnych systemów informatycznych*, Nr ewid. 12/2002/P01076/KOB, Warszawa, NIK, 2002, p. 7.

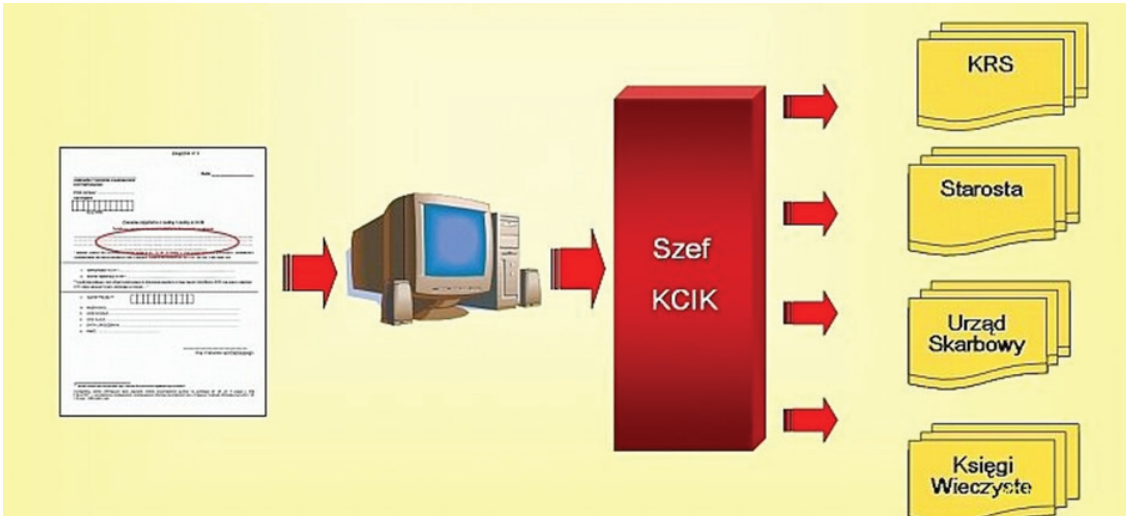
¹⁴ Krajowe Centrum Informacji Kryminalnej realizuje zadania określone w Ustawie z 6 lipca 2001 r., o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych, (Dz. Urz. z 2010 r., nr 29, poz. 153, z późn. zm.) KCIK utworzono 5 stycznia 2003 r.

zwłocznie po ich uzyskaniu do Szefa KCIK. Funkcja informacyjna KCIK realizowana jest poprzez obsługę zapytań kierowanych przez podmiot uprawniony do szefa KCIK. Istotnym uprawnieniem działań Szefa KCIK jest możliwość pozyskiwania i udzielania informacji kryminalnych przetwarzanych w bazach danych KCIK, a także zwracanie się do podmiotów uprawnionych i zobowiązanych do przekazywania wszelkich informacji jakie posiadają, istotnych z punktu widzenia postępowania karnego. Na wniosek podmiotu uprawnionego Szef KCIK kieruje zapytanie o uzupełnienie informacji kryminalnej do podmiotów biorących udział w wymianie informacji kryminalnych (podmiot uprawniony może wskazać jeden lub kilkadziesiąt podmiotów zobowiązanych, których dane chciałby uzyskać za pośrednictwem Szefa KCIK)¹⁵. Istotnym walorem tego rozwiązania jest to, że Szef KCIK zlecając podmiotom zobowiązanym przekazanie informacji kryminalnej, nie ujawnia podmiotu, który zlecił uzupełnienie informacji¹⁶.

¹⁵ Podmiotami biorącymi udział w wymianie informacji kryminalnej są m.in.: organy administracji rządowej lub organy samorządu terytorialnego właściwe w sprawach ewidencji ludności, Powszechnego Elektronicznego Systemu Ewidencji Ludności, ewidencji wojskowej osób podlegających obowiązkowi służby wojskowej, centralnej ewidencji pojazdów, centralnej ewidencji kierowców, rejestracji pojazdów, nadzoru geodezyjnego i kartograficznego, administracji geodezyjnej i kartograficznej, ewidencji gruntów i budynków lub rejestracji stanu cywilnego, sądy prowadzące Krajowy Rejestr Sądowy i księgi wieczyste, organy Inspekcji Ochrony Środowiska, organy Państwowej Straży Pożarnej, organy Zakładu Ubezpieczeń Społecznych, Komisja Nadzoru Bankowego, Państwowy Urząd Nadzoru Ubezpieczeń, Komisja Papierów Wartościowych i Giełd, Państwowa Straż Rybacka, nadleśniczkowie i dyrektorzy regionalnych dyrekcji Lasów Państwowych, Prezes Urzędu Ochrony Konkurencji i Konsumentów, Prezes GUS i dyrektorzy urzędów statystycznych w zakresie prowadzonych przez nich krajowych rejestrów urzędowych, dyrektor Biura Informacyjnego Krajowego Rejestru Karnego, dyrektorzy jednostek organizacyjnych Służby Więziennej, Główny Inspektor Inspekcji Handlowej, dyrektorzy parków narodowych, Państwowa Straż Łowiecka. Art. 19 i 20 ust. 1 Ustawy z 6 lipca 2010 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych.

¹⁶ Art. 13, Ustawy z 6 lipca 2010 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych.

RYSUNEK 1. KRAJOWE CENTRUM INFORMACJI KRYMINALNEJ



Źródło: Materiały z kursu specjalistycznego obsługi systemu KSIP w Szkole Policji w Pile, Szkoła Policji w Pile, <http://pila.szkolapolicji.gov.pl/spp/aktualnosci/2010-1/1479,W-wersji-K.html>, (dostęp 31.10.2021)

KRAJOWY SYSTEM INFORMACYJNY POLICJI

Krajowy System Informacyjny Policji (dalej KSIP)¹⁷ jest zestawem zbiorów danych, w którym przetwarza się informacje, w tym dane osobowe, w związku z realizacją zadań ustawowych Policji. Pierwotnie w zasobach KSIP gromadzone i przetwarzane są dane zawierające informacje o:

- wydarzeniach będących przestępstwami ściganymi z oskarżenia publicznego, wykroczeniami popełnianymi w ruchu drogowym, zdarzeniami podlegającymi określonemu w odrębnych przepisach Komendanta Głównego Policji obowiązkowi rejestracji w aplikacji o nazwie „Biuletyn KSIP”;
- osobach fizycznych podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego, nieletnich dopuszczających się czynów zabronionych przez ustawę jako przestępstwa ścigane z oskarżenia publicznego, osobach o nieustalonej tożsamości lub usiłujących ukryć swoją tożsamość, poszukiwanych;

¹⁷ Krajowy System Informacyjny Policji uruchomiono 1 stycznia 2003 r., na podstawie art. 21nb ust. 1 Ustawy o Policji. KSIP utworzył i prowadzi Komendant Główny Policji.

- rzeczach (przedmiotach) związanych z popełnianiem przestępstw i wykroczeń, a także osobach prawnych i jednostkach organizacyjnych nie posiadających osobowości prawnej, jeżeli ich funkcjonowanie ma związek z osobami pozostającymi w zainteresowaniu Policji¹⁸.

Wraz z rozwojem technologii internetowych i zmieniającym się katalogiem ustawowych zadań Policji, a także oczekiwań wobec funkcjonalności policyjnych baz danych, KSIP stał się scentralizowanym zestawem zbiorów danych prowadzonych w systemach teleinformatycznych KGP. Obejmuje on zakresem działania na terytorium całego kraju. Na funkcjonalność KSIP składają się zbiory danych: Osoba, Fakt (w tym z wykazu Biuletyn KSIP), Rzecz, Podmiot, Pokrzywdzeni oraz z rejestru wykroczeń, obejmującego swoim zakresem informacje, w tym dane osobowe, o osobach i wykroczeniach¹⁹.

Systemy teleinformatyczne KSIP umożliwiają dostęp oraz przetwarzanie informacji, w tym danych osobowych gromadzonych przez Policję i inne podmioty w następujących zbiorach danych: Policyjnym Rejestrze Imprez Masowych „PRIM”; Systemie Ewidencji Wypadków i Kolizji „SEWiK”; rejestrze „Broń” (w którym przetwarza się także informacje o broni utraconej); ewidencji kierowców naruszających przepisy ruchu drogowego; Centralnej Bazy Danych Osób Pozbawionych Wolności (prowadzonej na podstawie przepisów ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej, zwanej w KSIP „Noe.NET” lub „Osadzony”); centralnej ewidencji kierowców prowadzonej na podstawie przepisów ustawy – Prawo o ruchu drogowym; centralnej ewidencji pojazdów prowadzonej na podstawie przepisów ustawy – Prawo o ruchu drogowym; krajowego rejestru urzędowego podmiotów gospodarki narodowej (prowadzonego na podstawie ustawy o statystyce publicznej, zwanego w KSIP „REGON”); rejestrów prowadzonych na podstawie przepisów ustawy z dnia 24 września 2010 r. (o ewidencji ludności, w tym z rejestru PESEL i rejestru mieszkańców, zwanych w KSIP „PESEL”); Rejestru Dowodów Osobistych (prowadzonego na podstawie przepisów ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych, zwanego w KSIP „RDO”); centralnej ewidencji wydanych i unieważnionych paszportów (prowadzonej

¹⁸ Decyzja nr 726 Komendanta Głównego Policji z dnia 22 grudnia 2006 r. w sprawie funkcjonowania centralnych zbiorów danych tworzących Krajowy System Informacyjny Policji, (Dz. Urz. KGP.2006.17.106).

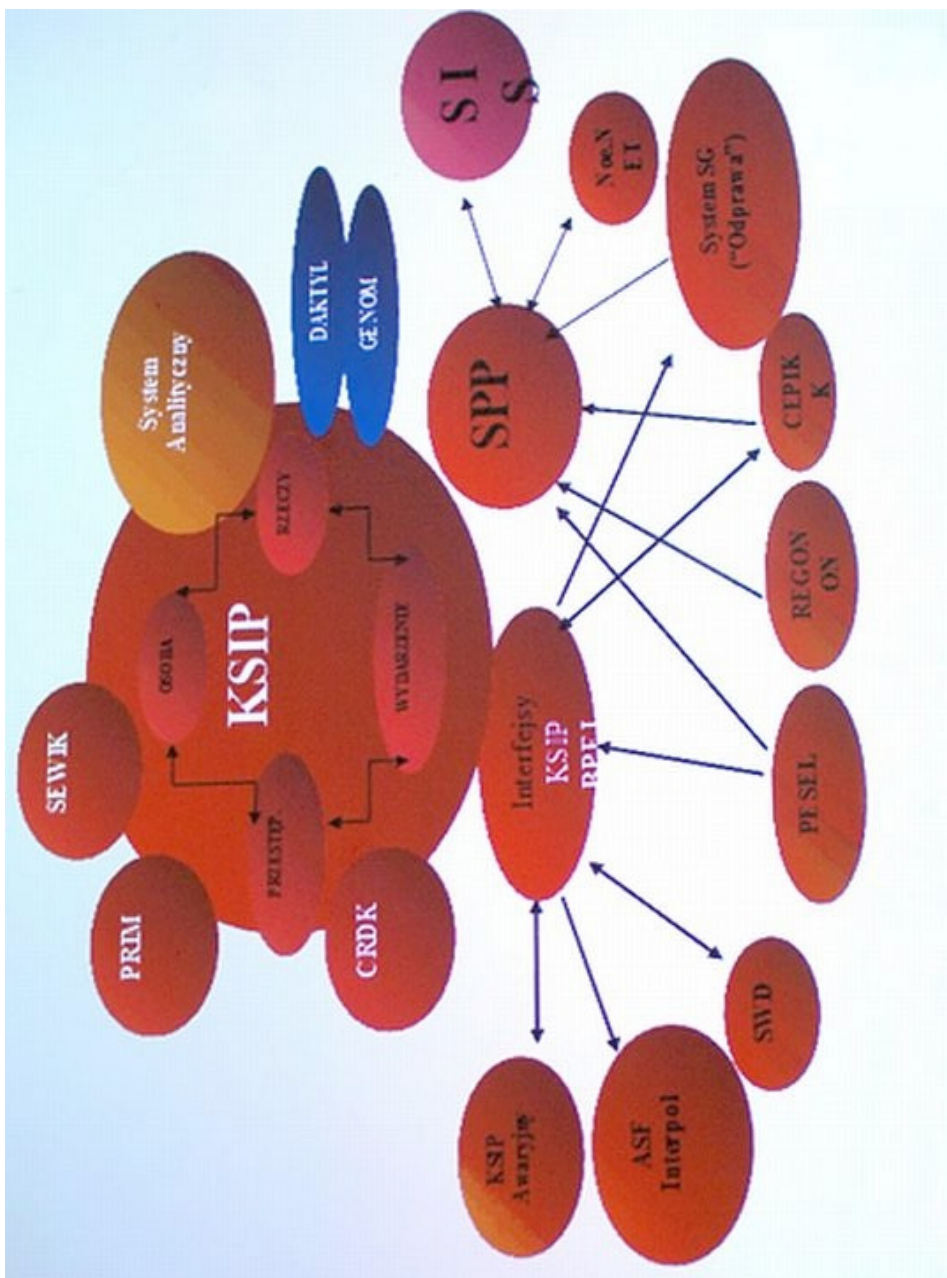
¹⁹ Zarządzenie nr 70 Komendanta Głównego Policji z dnia 2 grudnia 2019 r. w sprawie Krajowego Systemu Informacyjnego Policji, (Dz. Urz.KGP.2019.114).

na podstawie przepisów ustawy z dnia 13 lipca 2006 r. o dokumentach paszportowych, zwanej w KSIP „CEWiUP”); Systemu Informacyjnego Schengen (SIS, SIS II); Wizowego Systemu Informacyjnego (VIS); Zintegrowanego Systemu Ewidencji (administrowanego przez Straż Graniczną, zwanego w KSIP „ZSE SG”); Krajowego Rejestru Sądowego, zwanego w KSIP „KRS WWW”; krajowego zbioru rejestrów, ewidencji i wykazu w sprawach cudzoziemców o nazwie „System POBYT”; rejestrów w sprawach małego ruchu granicznego, zwanych w KSIP „MRG WWW”; Rejestru Sprawców Przepięstw na Tle Seksualnym, w tym Rejestru z dostępem ograniczonym, zwanego w KSIP „RSPTS”; baz danych Interpolu i Europolu²⁰.

Funkcjonalność KSIP umożliwia współdziałanie i integrację z innymi udostępnionymi policji bazami danych, które na podstawie obowiązujących przepisów prawa tworzone są przez podmioty administracji rządowej, samorządowej oraz przez agencje i instytucje międzynarodowe. Przykładowa architektura KSIP przedstawiona została na rysunku nr 2.

²⁰ §4 Zarządzenia nr 70 KGP w sprawie Krajowego Systemu Informacyjnego Policji.

RYSUNEK 2. KRAJOWY SYSTEM INFORMACYJNY POLICJI



Źródło: Materiały z kursu specjalistycznego obsługi systemu KSIP w Szkole Policji w Pile, Szkoła Policji w Pile, <http://pila.szkolapolicji.gov.pl/spp/aktualnosc/2010-1/1479,W-wersji-K.html>, (dostęp 31.10.2021)

BAZY DANYCH BADAŃ DNA I ODCISKÓW PALCÓW

Wyniki kryminalistycznych badań odcisków palców i profili DNA należą do najważniejszych dowodów w sprawach karnych²¹. Umożliwiają one jednoznaczne wskazanie zgodności śladu ujawnionego na miejscu zdarzenia z tożsamością osoby, która go zostawiła. Dane gromadzone są w systemach teleinformatycznych prowadzonych w Zakładzie Daktyloskopii Centralnego Laboratorium Kryminalistycznego Policji (dalej CLKP), gdzie znajduje się Centralna Registratura Daktyloskopijna (dalej CRD) i Automatyczny System Identyfikacji Daktyloskopijnej (dalej AFIS). W zbiorach daktyloskopijnych gromadzone są odfitki linii papilarnych osób oraz niezidentyfikowane ślady linii papilarnych, które następnie w ramach „wywiadów daktyloskopijnych” przeszukiwane są pod kątem zgodności ze śladami zabezpieczonymi na miejscach zdarzeń i udostępniane uprawnionym organom. Zbiory CRD i AFIS prowadzone są na podstawie art. 21 ustawy z dnia 6 kwietnia 1990 roku o Policji, a ich administratorem – w rozumieniu ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych – jest Komendant Główny Policji²².

Centralny zbiór danych zawierający informacje o wynikach analizy kwasu deoksyrybonukleinowego (dalej DNA) prowadzony jest na użytek organów ścigania i wymiaru sprawiedliwości, których zadaniem jest zapobieganie i zwalczanie przestępczości. Bazy DNA działają podobnie do systemów danych daktyloskopijnych. Do bazy danych wprowadzane są profile DNA podejrzanych oraz profile oznaczane na podstawie śladów biologicznych z miejsc zdarzeń. Ich automatyczne porównywanie daje możliwość ustalania tożsamości osób i zwłok, wykrywania sprawców przestępstw oraz kolarzenia zdarzeń, w których działali ci sami sprawcy.

W zbiorze danych DNA gromadzi się i przetwarza profile genetyczne: osób podejrzanych lub podejrzanych o popełnienie przestępstw ściganych z oskarżenia publicznego; nieletnich dopuszczających się czynów zabronionych przez ustawę jako przestępstwa ścigane z oskarżenia publicznego; osób stwarzających zagrożenie (o których mowa w ustawie z dnia 22 listo-

²¹ Praktyczna wartość dowodowa analizy DNA w postępowaniach sądowych i zasadność prowadzenia baz danych profili DNA skłoniły Komitet Ministrów Rady Europy do wydania w lutym 1992 roku Rekomendacji nr R (92), która dotyczyła wykorzystania analizy DNA w postępowaniu karnym, co zapoczątkowało tworzenie registratur danych DNA w Europie. Polska baza danych DNA została uruchomiona w roku 2007 w Laboratorium Kryminalistycznym Policji.

²² Ustawa z dnia 6 kwietnia 1990 r. o Policji.

pada 2013 r. o postępowaniu wobec osób z zaburzeniami psychicznymi stwarzających zagrożenie życia, zdrowia lub wolności seksualnej innych osób (Dz. U. z 2014 r. poz. 24, z 2015 r. poz. 396 oraz z 2016 r. poz. 2205)); osób, o których mowa w art. 10 ust. 1 ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (Dz. U. z 2018 r. poz. 452, 650 i 730); oskarżonych lub skazanych za popełnienie przestępstw ściganych z oskarżenia publicznego; osób o nieustalonej tożsamości oraz osób usiłujących ukryć swoją tożsamość; zwłok ludzkich o nieustalonej tożsamości; śladów nieznanymi sprawców przestępstw; osób zaginionych; osób, o których mowa w art. 15 ust. 1 pkt 3a lit. c ustawy o Policji; osób, o których mowa w art. 20 ust. 11 ustawy o Policji²³. Na mocy Decyzji Rady Europy w dniu 20 grudnia 2012 roku Polska otrzymała możliwość automatycznej wymiany danych DNA z państwami członkowskimi UE²⁴.

ELEKTRONICZNY REJESTR CZYNNOŚCI DOCHODZENIOWO-ŚLED CZYCH (ERCDS)

Elektroniczny Rejestr Czynności Dochodzeniowo-Śledczych jest aplikacją informatyczną przeznaczoną do przetwarzania danych w formie elektronicznej. Jej celem jest wykonywanie czynności dochodzeniowo-śledczych i techniczno-kryminalistycznych oraz realizacja wszelkich obowiązków ustawowych wynikających z przepisów ustaw wymienionych w § 1 pkt 1 Zarządzenia nr 25 Komendanta Głównego Policji z dnia 23 lipca 2015 r. w sprawie niektórych form organizacji i ewidencji czynności dochodzeniowo-śledczych policji oraz przechowywania przez policję dowodów rzeczowych uzyskanych w postępowaniu karnym²⁵.

ERCDS został wprowadzony 1 stycznia 2015 r. we wszystkich jednostkach organizacyjnych policji i Centralnym Biurze Śledczym Policji. W tej aplikacji ewidencjonowane są: czynności procesowe wykonywane

²³ Art. 20 ust. 1, Ustawa z dnia 6 kwietnia 1990 r. o Policji.

²⁴ Decyzja Rady Europy 2008/615/WSiSW z dn. 23 VI 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej, (Dz. Urz. UE L 210 z 6 VIII 2008 r.)

²⁵ Tj., ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego; ustawy z dnia 10 września 1999 r. Kodeks karny skarbowy; ustawy z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich. *Vide* Zarządzenie nr 25 Komendanta Głównego Policji z dnia 23 lipca 2015 r. w sprawie niektórych form organizacji i ewidencji czynności dochodzeniowo-śledczych policji oraz przechowywania przez policję dowodów rzeczowych uzyskanych w postępowaniu karnym, (Dz. Urz. KGP 2015, poz. 58).

przez funkcjonariuszy policji w ramach prowadzonych śledztw i dochodzeń – Elektroniczny Rejestr Śledztw i Dochodzeń (e-RCDS); prowadzone postępowania sprawdzające – Elektroniczny Rejestr Postępowań Sprawdzających (e-RPS); zabezpieczone w toku sprawy dowody rzeczowe – Elektroniczna Księga Dowodów Rzeczowych (e-KDRz); wydane postanowienia o powołaniu biegłego – Elektroniczny Rejestr wydanych Postanowień o dopuszczeniu dowodu z opinii biegłego (e-RPB); czynności techniczno-kryminalistyczne (zabezpieczone ślady i przedmioty na miejscu zdarzeń przestępczych) – Elektroniczny Rejestr Czynności Techniczno-Kryminalistycznych (e-RCTK)²⁶.

SYSTEM WSPOMAGANIA DOWODZENIA (SWD)

System Wspomagania Dowodzenia (dalej SWD) jest centralnym systemem informatycznym Policji przeznaczonym do wspierania zarządzania pracą Policji na etapie przyjmowania i obsługi zdarzeń przekazywanych przez Centra Powiadamiania Ratunkowego (dalej CPR) obsługujące zgłoszenia alarmowe oraz na etapie dyslokacji służb patroli pozostających w dyspozycji dyżurnego stanowiska dowodzenia jednostki.

System wdrażany był od 2013 roku i zastąpił Elektroniczną Książkę Służby Dyżurnego. Obejmuje on wszystkie szczeble dowodzenia w Policji i jest wykorzystywany w KGP oraz jednostkach poziomu komisariatu, komend miejskich, powiatowych, rejonowych i wojewódzkich Policji.

Do podstawowych funkcjonalności aplikacji należy: przyjmowanie, rejestracja i obsługa zgłoszeń przekazywanych za pomocą systemów teleinformatycznych z CPR i innych służb; zarządzanie zasobami i personelem pozostającym w dyspozycji dyżurnego; synchronizacja sprawdzeń w policyjnych bazach danych (KSIP) dokonywanych przez patrole w trakcie służby, realizowanych przy wykorzystaniu terminali mobilnych (poszukiwania osób, sprawdzenia przedmiotów, potwierdzanie danych, sprawdzanie uprawnień punktów karnych kierujących w ruchu drogowym i inne); wykorzystanie elektronicznego modułu mapowego do zarządzania zasobami; wizualizacja realizowanych czynności przez patrole w rejonie

²⁶ M. Białęcki, 'Kierunki rozwoju policyjnego systemu informatycznego wspierającego dokumentowanie czynności dochodzeniowo-śledczych i techniczno-kryminalistycznych', *Problemy Kryminalistyki*, no. 291 (1), 2016, p. 23.

służbowym; wspomaganie analizy zagrożeń i prawidłowego planowania służby poprzez moduł analityczny; raportowanie i statystyki zdarzeń²⁷.

MIĘDZYKARODOWA WYMIANA INFORMACJI KRYMINALNYCH

Globalizacja i likwidacja barier w kontaktach międzynarodowych w naturalny sposób wymusza współpracę między podmiotami odpowiedzialnymi za ochronę porządku i bezpieczeństwa publicznego w różnych państwach. Jest to szczególnie istotne ze względu na fakt, że świat przestępczy skutecznie korzysta ze wszelkich zdobyczy technologicznych, a granice nie stanowią w tym przypadku żadnych przeszkód. W tym kontekście każde z państw staje się kluczowym ogniwem środowiska bezpieczeństwa w wymiarze wewnętrznym i transgranicznym.

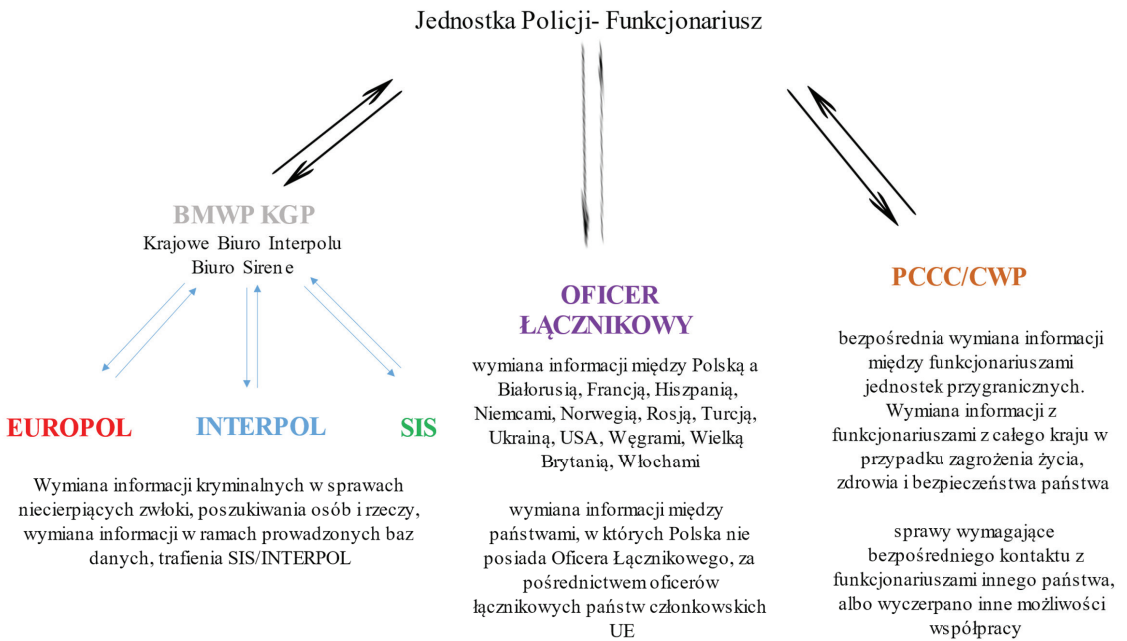
Międzynarodowa współpraca służb porządku publicznego i bezpieczeństwa w wymianie informacji kryminalnych w celu ścigania sprawców przestępstw i zapobieganiu przestępczości realizowana jest w Polsce poprzez kanały wymiany informacji i bazy administrowane przez Komendanta Głównego Policji. Ustawowe zadania realizuje on przy pomocy Komendy Głównej Policji i jednego z jej podmiotów, jakim jest Biuro Międzynarodowej Współpracy Policji (dalej BMWP)²⁸. BMWP KGP koordynuje, nadzoruje i przekazuje zainteresowanym podmiotom informacje w ramach współpracy operacyjnej i pozaoperacyjnej w systemie całodobowym przez cały rok.

Wymiana informacji kryminalnych realizowana przez służby policyjne państw członkowskich UE oraz państw trzecich odbywa się poprzez kanały komunikacyjne krajowego punktu kontaktowego (KPK) umiejscowionego w BMWP. Współpraca międzynarodowa w tym zakresie obejmuje bazy danych Interpolu, Europolu i Systemu Informacyjnego Schengen. Istnieją także możliwości wymiany informacji przez Oficerów Łącznikowych w krajach, z którymi Polska ma podpisane stosowne umowy dwustronne lub w krajach, które oddelegowały swoich Oficerów Łącznikowych do Polski oraz poprzez Policyjno-Celne Centra Współpracy (PCCC/CWP).

²⁷ Zarządzenie nr 12 Komendanta Głównego Policji z dnia 19 maja 2020 r. w sprawie Systemu Wspomagania Dowodzenia Policji, (Dz. Urz. KGP.202.23).

²⁸ Szczegółowe zadania BMWP KGP określone są w Zarządzeniu nr 2 Komendanta Głównego Policji z dnia 1 kwietnia 2016 r. w sprawie regulaminu Komendy Głównej Policji, (Dz. Urz. 2016.13).

RYSUNEK 3. MIĘDZYKRAJOWA WSPÓŁPRACA POLICJI, KANALEY WYMIANY INFORMACJI KRYMINALNYCH



Źródło: opracowanie własne na podstawie materiałów Biura Międzynarodowej Współpracy Policji, Warszawa 2021, materiały niepublikowane

EUROPOL

Europol prowadzi własne bazy danych oraz korzysta z zasobów głównych centralnych baz danych UE, które może przeglądać i przeszukiwać (np. SIS, VIS, Eurodac). Europol wspiera wymianę informacji między krajowymi organami policyjnymi jako centrum informacji o przestępstwach w UE. System informacyjny Europolu (EIS) jest bazą danych zawierającą informacje o popełnionych przestępstwach, które wykorzystywane są do celów prowadzenia dochodzeń oraz przeszukiwania danych dotyczących poważnej przestępczości i terroryzmu. Informacje przechowywane w systemie EIS obejmują dane dotyczące osób, dokumentów tożsamości, pojazdów, broni palnej, numerów telefonu, adresów e-mail, odcisków palców i DNA. Wymiana informacji na poziomie krajowym odbywa się w Polsce za pośrednictwem systemu informatycznego SWIzE, który zapewnia dostęp

do aplikacji SIENA będącej siecią bezpiecznej łączności elektronicznej między Europolem, biurami łącznikowymi i jednostkami krajowymi Europolu²⁹.

Informacje i dane przekazywane do systemów i baz Europolu podlegają gromadzeniu i przetwarzaniu na potrzeby rozpracowywania działalności przestępczej poprzez specjalną procedurę uzyskiwania, weryfikacji, gromadzenia i dystrybuowania informacji kryminalnych. Procedura ta realizowana jest przez zespoły analityków oraz specjalistów, którzy posiadają dostęp do wszystkich informacji gromadzonych przez Europol. Przy wykorzystaniu systemów analitycznych (ang. *Analysis Work Files*, dalej AWF) realizują oni projekty analityczne (ang. *Analytical Project* – AP, dalej AP), które koncentrują się wokół wszechstronnego, międzynarodowego rozpracowania konkretnego podmiotu zagrożenia związanego z osobą, środowiskiem lub zjawiskiem³⁰.

Analitycy badają powiązania spraw prowadzonych przez organy ścigania kilku państw członkowskich, które łączą się pod względem operacyjnym, a zainteresowane państwa uznają potrzebę ich zintegrowanego pilotowania. Ostatecznie przygotowują kierunkową analizę przydatności informacji w konkretnych rozpracowaniach analitycznych oraz w poszczególnych dochodzeniach krajowych i przekazują ustalenia zainteresowanym stronom³¹.

INTERPOL

Podstawowym celem istnienia Interpolu jest gromadzenie, przetwarzanie i udostępnianie informacji kryminalnych przetwarzanych w prowadzonych bazach danych na potrzeby państw członkowskich Interpolu. W wymiarze technicznym system Informacyjny Interpolu (ang. *Interpol Information System* – IIS, dalej SII) zintegrowany jest z sieciami teleinformatycznymi Krajowych Biur Interpolu (dalej KBI) państw członkowskich oraz

²⁹ Komisja Europejska, 'Komunikat Komisji do Parlamentu Europejskiego i Rady: Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa', *eur-lex.europa.eu*, Bruksela, 6 kwietnia 2016, <https://eur-lex.europa.eu/legalcontent/PL/TXT/PDF/?uri=CELEX:52016DC0205&from=NL>, (accessed 31 October 2021).

³⁰ Aktualnie w ramach Europolu funkcjonują 32 AP dotyczące m.in. przestępczości kryminalnej, przestępczości zorganizowanej, terroryzmu itp.

³¹ T. Safjański, 'Rozpracowywanie działalności terrorystycznej w ramach Europolu – uwarunkowania prawne i praktyczne', *Przegląd Bezpieczeństwa Wewnętrznego*, vol. 19, no. 10, 2018, p. 111.

z Sekretariatem Generalnym Interpolu w Lyonie – za pomocą specjalnego elektronicznego Systemu Globalnej Komunikacji Interpolu (ang. *Interpol Global Communication System*, dalej IGCS), zwanego I-24/7. SII umożliwia wymianę informacji z Sekretariatem Generalnym Interpolu oraz KBI, dostęp do not i dyfuzji, a także dostęp do tematycznych baz danych. Noty i dyfuzje to narzędzia współpracy międzynarodowej wykorzystywane do poszukiwań osób oraz do rozprzestrzeniania ostrzeżeń o osobach, wydarzeniach lub zachowaniach mogących stanowić zagrożenie dla państwa członkowskiego Interpolu³².

SII integruje w swoich zbiorach tematyczne bazy danych, które zawierają informacje kryminalne przekazywane przez KBI:

- Digital Interpol Alert Library – Document (DialDoc), informacje o nowo wykrytych sposobach podrabiania dokumentów podróży;
- Illicit Firearms Records and tracing Management System (iARMS), numery seryjne skradzionej, zagubionej lub przemyconej broni palnej;
- INTERPOL firearms Reference Table (IFRT), wzorce broni produkowanej seryjnie;
- INTERPOL Child Sexual Exploitation (ISCE), zdjęcia, filmy wideo dotyczące seksualnego wykorzystania dzieci oraz spraw, w których zidentyfikowano ofiarę albo sprawcę;
- Facial Recognition Database, zdjęcia twarzy z not i dyfuzji;
- INTERPOL'S Maritime Piracy Global Database, osoby, miejsca, sprawy dotyczące piractwa morskiego;
- RELIEF, baza znaków szczególnych i mikrośladów pozostawionych przez maszyny prasujące na opakowaniach narkotyków;
- GEIGER, informacje na temat zagrożenia promieniowaniem radioaktywnym i handlu materiałami promieniotwórczymi;
- Fingerprints, odciski linii papilarnych osób poszukiwanych, podejrzanych i skazanych;

³² Nota to wniosek o współpracę międzynarodową lub ostrzeżenie międzynarodowe, publikowane przez Interpol na wniosek KBI lub innego podmiotu międzynarodowego, przesyłany do wszystkich KBI państw członkowskich Interpoli, rejestrowany jednocześnie w bazie Interpolu. Dyfuzja to wniosek o współpracę międzynarodową lub ostrzeżenie międzynarodowe, przesyłane z KBI do innego KBI, rejestrowane jednocześnie w bazie Interpolu. Noty i dyfuzje oznaczane są kolorami, które odpowiadają akcji jaka ma zostać podjęta w stosunku do osoby poszukiwanej lub zgłaszanej sytuacji: nota czerwona, żółta, niebieska, zielona, czarna, pomarańczowa, fioletowa i srebrna. *Vide* Zarządzenie nr 5 Komendanta Głównego Policji z dnia 4 lutego 2021 r. w sprawie not i dyfuzji Międzynarodowej Policji Kryminalnej – Interpol, (Dz. Urz. KGP. 2021.9).

- DNA Database, profile DNA NN osób;
- I-Familia, profile DNA krewnych osób zaginionych;
- NOMINAL, osoby objęte czerwoną, żółtą, niebieską, zieloną i czarną notą Interpolu;
- STOLEN AND LOST TRAVEL DOCUMENTS (SLDT), skradzione, zagubione, odwołane i nieważne dokumenty podróży;
- Stolen Motor Vehicles (SMV), skradzione pojazdy silnikowe i części samochodowe;
- Stolen Administrative Documents (SAD), skradzione dokumenty administracyjne pojazdów i osób;
- Stolen Work of Art. (WoA), skradzione dzieła sztuki³³.

SYSTEM INFORMACYJNY SCHENGEN (SIS, SIS II)

System Informacyjny Schengen (SIS) – to największa w Europie baza danych. Przetwarzane są w niej określone przepisami kategorie danych osób, m.in.: poszukiwanych europejskimi nakazami aresztowania; zaginionych; niepożądanych na terytorium strefy Schengen; zarejestrowanych na potrzeby prowadzenia niejawnych kontroli lub w celu ustalenia miejsca pobytu oraz dotyczących przedmiotów; wprowadzanych do systemu przez państwa strefy Schengen. Przepisy dorobku prawnego Schengen i prawa wspólnotowego dotyczące SIS zostały wdrożone do polskiego porządku prawnego na mocy ustawy z dnia z 24 sierpnia 2007 roku *o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym*³⁴, która reguluje zasady i sposób realizacji udziału w SIS II³⁵.

³³ Interpol, 'The Stolen Works of Art database is our main tool to tackle the traffic in cultural property', <https://www.interpol.int/>, <https://www.interpol.int/en/Search-Page?search=Database> [dostęp 31.10.2021].

³⁴ Ustawa z dnia z 24 sierpnia 2007 roku o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, (Dz. Urz. Nr 165, poz.1170 z późn. zm.) Podstawę utworzenia Systemu Informacyjnego Schengen drugiej generacji (SIS II) stanowi Rozporządzenie (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 roku w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) oraz Decyzja Rady 2007/533/WSiSW z dnia 12 czerwca 2007 roku w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen Drugiej generacji (SISII).

³⁵ Rozszerzenie UE spowodowało, że infrastruktura techniczna SIS uniemożliwiła przyłączenie nowych państw do istniejącego systemu, wobec czego zdecydowano o zastąpieniu SIS nowym Systemem Informacyjnych Schengen drugiej generacji (SIS II). Docelowo wszystkie Państwa Członkowskie miały obowiązek wprowadzić SIS II, który

- Na podstawie obowiązujących przepisów wpisy do SIS II dotyczą m.in.³⁶:
- osób poszukiwanych w celu aresztowania ich i wydania lub ekstradycji na podstawie ENA, art. 26 Decyzji 533/2007;
 - obywateli państw trzecich, dokonywane w związku z odmową wjazdu lub pobytu w strefie Schengen, art. 24 Rozporządzenia 1987/2007;
 - osób zaginionych, art. 32 Decyzji 533/2007;
 - osób, których obecność jest wymagana do celów procedury sądowej, art. 34 Decyzji 533/2007;
 - osób lub przedmiotów (pojazdów), wprowadzane w celu przeprowadzenia kontroli niejawnych lub kontroli szczególnych, art. 36.2 i 3 Decyzji 533/2007;
 - przedmiotów przeznaczonych do zajęcia lub wykorzystania jako dowód w postępowaniu karnym, art. 38 Decyzji 533/2007.

W przypadku wprowadzania przez Policję do KSIP rejestracji dotyczących poszukiwania osób zaginionych oraz skradzionych przedmiotów, systemy teleinformatyczne automatycznie replikują te rekordy i wpis pojawia się w SIS II, w pozostałych przypadkach rejestracja odbywa się poprzez Biuro Wywiadu i Informacji Kryminalnych KGP.

INNE NARZĘDZIA I KANAŁY MIĘDZYNARODOWEJ WSPÓŁPRACY POLICYJNEJ

W ramach wymiany informacji kryminalnych z podmiotami, państwami i instytucjami uprawnionymi Policja posiada dostęp do różnych narzędzi i instrumentów współpracy międzynarodowej. Wymiana informacji w takiej sytuacji odbywa się w trybie automatycznym za pośrednictwem Oficera Kontaktowego do spraw międzynarodowej wymiany informacji kryminalnych (dalej OK ds. mwik), który pełni służbę lub jest zatrudniony w każdej Komendzie Wojewódzkiej Policji oraz poprzez punkty kontaktowe umiejscowione w BMWP KGP lub innych upoważnionych komórkach organizacyjnych KGP.

miał być systemem o dużo większej funkcjonalności. W dniu 1 stycznia 2021 r. od systemu SIS II odłączono Wielką Brytanię, stąd też współpraca z tym krajem odbywa się poprzez KBI Interpolu. SIS II działa obecnie w 25 państwach członkowskich UE oraz w czterech państwach niebędących członkami UE, które zostały włączone we współpracę Schengen: Norwegii, Islandii, Szwajcarii i Liechtensteinie.

³⁶ Decyzja Rady 2007/533/WSiSW z dnia 12 czerwca 2007 roku w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen Drugiej generacji (SISII).

Międzynarodowa współpraca policyjna realizowana jest m.in. w oparciu o wymianę informacji kryminalnych przetwarzanych w:

- PNR (*Passanger Name Record*), w zakresie danych przetwarzanych przez przewoźników lotniczych;
- EUCARIS PRÜM (*European Car and driving license Information System* – Europejskim Systemie Informacyjnym o Pojazdach i Prawach Jazdy), w zakresie danych osobowych posiadacza pojazdu, danych pojazdu, danych z polis ubezpieczeniowych;
- Inteligentnym Systemie Transportowym – ITS (*Inteligent Transportation System*), w zakresie danych pojazdów uczestniczących w transporcie drogowym, zarządzania ruchem pojazdów, danych z kontroli, zarejestrowanych przez systemy informatyczne. Integralną częścią systemu jest Automatyczny System Rozpoznawania Numerów Rejestracyjnych – ANPR, w zakresie automatycznego odczytu w czasie rzeczywistym tablic rejestracyjnych pojazdów.

PODSUMOWANIE

Rozwój nauki i nowych technologii informatycznych zasadniczo zmienił oblicze współczesnej kryminalistyki i praktyki działania instytucji porządku publicznego, stwarzając nowe możliwości wykrywcze i dowodowe. Niewątpliwie skuteczność działań służb porządku publicznego uzależniona jest od sprawnego korzystania z dostępnych informacji kryminalnych, a także nowoczesnych narzędzi ich gromadzenia, przetwarzania, analizowania i wykorzystania w prowadzonych czynnościach służbowych.

Wymiana informacji na poziomie krajowym i międzynarodowym stała się koniecznością i codziennością wielu służb w sytuacji pojawiających się nowych ryzyk i zagrożeń, których źródła i skutki występują na terenie różnych państw. Zastąpienie tradycyjnych form współpracy między jednostkami, instytucjami i służbami w zakresie wymiany informacji kryminalnych na rzecz rozwoju aplikacji, baz danych i systemów informatycznych przyczynia się do uporządkowania i usystematyzowania rozproszonych często informacji i danych, a także podnosi profesjonalizm i skuteczność współpracy w zapobieganiu i ściganiu sprawców przestępstw.

BIBLIOGRAFIA

- Białęcki, M., 'Kierunki rozwoju policyjnego systemu informatycznego wspierającego dokumentowanie czynności dochodzeniowo-śledczych i techniczno-kryminalistycznych', *Problemy Kryminalistyki*, no. 291 (1), 2016 r., pp. 21–28.
- Safjański, T., 'Rozpracowywanie działalności terrorystycznej w ramach Europolu – uwarunkowania prawne i praktyczne', *Przegląd Bezpieczeństwa Wewnętrznego*, vol. 19, no. 10, 2018, pp. 107–125.
- Widła, T., 'Kryminalistyka', J. Widacki (ed.), Kraków, C.H. Beck, 2018, pp. 145–155.
- Wilk, D., *Kryminalistyka: Przewodnik*, Toruń, TNOiK, 2013.
- Zalewski, P., 'Międzynarodowa współpraca polskiej Policji w świetle teorii dóbr publicznych', *Kultura Bezpieczeństwa*, no. 37, 2020, pp. 83–116, DOI:10.5604/01.3001.0014.2817.

AKTY PRAWNE

- Decyzja nr 726 Komendanta Głównego Policji z dnia 22 grudnia 2006 r. w sprawie funkcjonowania centralnych zbiorów danych tworzących Krajowy System Informacyjny Policji, Dz.Urz.KGP.2006.17.106.
- Decyzja Rady Europy 2008/615/WSiSW z dn. 23 VI 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej, Dz. Urz. UE L 210 z 6 VIII 2008 r.
- Ustawa z 6 lipca 2001 r., o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych, Dz. U. z 2010 r., nr 29, poz. 153, z późn. zm.
- Ustawa z dnia 6 kwietnia 1990 r. o Policji, Dz. U. z 1990 r. Nr 30, poz. 179 z późn. zm.
- Ustawa z dnia 6 lipca 2001 r. o gromadzeniu, przetwarzaniu i przekazywaniu informacji kryminalnych, Dz. U. z 2010 r. Nr 29 (tekst jedn.), poz. 153 z późn. zm.
- Ustawa z dnia z 24 sierpnia 2007 roku o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, Dz. U. Nr 165, poz.1170 z późn. zm.
- Zarządzenie nr 12 Komendanta Głównego Policji z dnia 19 maja 2020 r. w sprawie Systemu Wspomagania Dowodzenia Policji, Dz. Urz. KGP.2020.23.
- Zarządzenie nr 2 Komendanta Głównego Policji z dnia 1 kwietnia 2016 r. w sprawie regulaminu Komendy Głównej Policji, Dz. Urz.KGP.2016.13.
- Zarządzenie nr 25 Komendanta Głównego Policji z dnia 23 lipca 2015 r. w sprawie niektórych form organizacji i ewidencji czynności dochodze-

- niowo-śledczych policji oraz przechowywania przez policję dowodów rzeczowych uzyskanych w postępowaniu karnym, Dz. Urz. KGP.2015.58.
Zarządzenie nr 5 Komendanta Głównego Policji z dnia 4 lutego 2021 r. w sprawie not i dyfuzji Międzynarodowej Policji Kryminalnej – Interpol, Dz. Urz. KGP.2021.9.
Zarządzenie nr 70 Komendanta Głównego Policji z dnia 2 grudnia 2019 r. w sprawie Krajowego Systemu Informacyjnego Policji, Dz. Urz. KGP.2019.114.

RAPORTY

- Najwyższa Izba Kontroli, Informacja o wynikach kontroli funkcjonowania policyjnych systemów informatycznych, Nr ewid. 12/2002/P01076/KOB, Warszawa, 2002.

ZASOBY INTERNETOWE

- Safijański, T., 'Administracyjne modele wymiany informacji kryminalnych z zagranicą na przykładzie polskiej Policji', <https://www.researchgate.net/publication/326539662> - (poz. 7).
Interpol, <https://www.interpol.int/en/Search-Page?search=Database> [dostęp 31.10.2021].
Komisja Europejska, KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY, Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa, Bruksela, dnia 6.04.2016 r., COM (2016) 205 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52016DC0205&from=NL> [dostęp 31.10.2021].
Oficjalna strona internetowa Unii Europejskiej, https://europa.eu/european-union/about-eu/agencies/europol_pl [dostęp 31.10.2021].
Policja.pl, <https://policja.pl/pol/sirene/biuro-sirene/7842,Co-to-jest-BIURO-SIRENE.html> [dostęp 31.10.2021].
Safijański T., Administracyjne modele wymiany informacji kryminalnych z zagranicą na przykładzie polskiej Policji, https://www.researchgate.net/publication/326539662_

SPIS RYSUNKÓW

Rys. 1. Krajowe Centrum Informacji Kryminalnej

Rys. 2. Krajowy System Informacyjny Policji

Rys. 3. Międzynarodowa współpraca Policji – kanały wymiany informacji kryminalnych

CITE THIS ARTICLE AS:

P. Zalewski, 'Architektura i narzędzia policyjnej wymiany informacji kryminalnych. Perspektywa krajowa i międzynarodowa', *Kultura Bezpieczeństwa*, no. 40, 2021, pp. 50–78, DOI: 10.5604/01.3001.0015.6971.

Licence: This article is available in Open Access, under the terms of the Creative Commons License Attribution 4.0 International (CC BY 4.0; for details please see <https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided that the author and source are properly credited. Copyright © 2021 University of Public and Individual Security "Apeiron" in Cracow