

Interoperacyjność unijnych systemów informacyjnych – narzędzie wykorzystywane w zwalczaniu terroryzmu i poważnej przestępczości transgranicznej (część I)

mł. insp. dr Edyta Kot¹

¹ Centralne Laboratorium Kryminalistyczne Policji, edyta.kot@policja.gov.pl

Streszczenie

Terroryzm i przestępstwa transgraniczne są problemami złożonymi i zróżnicowanymi. Są one jednymi z najważniejszych zagrożeń współczesnego świata, zarówno na płaszczyźnie krajowej, jak i międzynarodowej. W Ustawie o Policji¹ ujęte zostały główne zadania tej formacji, a mianowicie: „współdziałanie z policjami innych państw oraz ich organizacjami międzynarodowymi, a także z organami i instytucjami Unii Europejskiej na podstawie umów i porozumień międzynarodowych oraz odrębnych przepisów” oraz „Policja realizuje także zadania wynikające z przepisów prawa Unii Europejskiej oraz umów i porozumień międzynarodowych na zasadach i w zakresie w nich określonych”. W celu realizacji ustawowych zadań, policjanci w kraju i na świecie pracują w oparciu o informacje, które są gromadzone i przetwarzane w różnego rodzaju kartotekach, rejestrach, zbiorach czy bazach. Informacje te podlegają wymianie pomiędzy uprawnionymi organami w kraju i na świecie. Przedmiotowa współpraca ma na celu zapobieganie, wykrywanie i zwalczanie najgroźniejszej przestępczości, w szczególności terroryzmu i zorganizowanej przestępczości transgranicznej. Te ostatnie stały się bardzo realne w chwili zniesienia kontroli na granicach wewnętrznych Unii Europejskiej, poprzez utworzenie strefy Schengen. Od początku uruchomienia obszaru Schengen zdawano sobie sprawę, że bezpieczeństwo wewnątrz strefy oraz zarządzanie granicami zewnętrznymi będzie wiązało się z koniecznością stworzenia i wdrożenia systemów informatycznych, których zadaniem będzie wspieranie powyższych działań. Zniesienie kontroli na granicach oraz wzmożone ruchy migracyjne w Europie sprzyjają rozwojowi przestępczości o charakterze transgranicznym i terrorystycznym. Świadomość oraz doświadczenia związane z materializacją powyższych zagrożeń zainicjowały zacieśnienie współpracy pomiędzy poszczególnymi państwami globu. Zacieśnienie współpracy stało się możliwe po utworzeniu i uruchomieniu wielkoskalowych systemów informacyjnych, a mianowicie: Systemu Informacyjnego Schengen (SIS), Eurodac, Wizowego Systemu Informacyjnego (VIS), Systemu Wjazdu/Wyjazdu (EES) i europejskiego systemu przekazywania informacji z rejestrów karnych o obywatelach państw trzecich (ECRIS-TCN). W niniejszej części publikacji, z uwagi na obszerność zagadnienia, opisano tylko systemy SIS, VIS, jednakże zachęcam do zgłębienia wiedzy o pozostałych systemach wielkoskalowych, tj. Eurodac, Entry/Exit, ECRIS-TCN oraz o zagadnieniu związanym z ich interoperacyjnością.

Słowa kluczowe: SIS, VIS, terroryzm, przestępczość transgraniczna, eu-LISA

Wstęp

Zamachy bombowe, mające miejsce w Hiszpanii (2004 r.), w Londynie (2005 r.), a także narastająca fala nielegalnej migracji w roku 2015, wywołały szereg problemów związanych z zarządzaniem granicami zewnętrznymi Unii Europejskiej oraz zapewnieniem bezpieczeństwa na jej terytorium (Jaroszevska-Choraś 2016). W odpowiedzi na powyższe problemy państwa członkowskie UE rozpoczęły prace nad udoskonalaniem informacyjnych systemów wielkoskalowych, przechowujących dane osobowe obywateli państw trzecich próbujących przedostać się do strefy Schengen, które umożliwiają dostęp uprawnionym organom

państw członkowskich UE do zgromadzonych w nich informacji, w celu zapobiegania poważnym przestępstwom, ich wykrywania i prowadzenia dochodzeń w ramach przydzielonych kompetencji [Gajda, 2019]. Obecnie funkcjonuje sześć głównych unijnych systemów, z których w pięciu przetwarzane są dane biometryczne w postaci danych daktyloskopijnych. Są to: System Informacyjny Schengen (SIS), Eurodac, Wizowy System Informacyjny (VIS), System Wjazdu/Wyjazdu (EES) i europejski system przekazywania informacji z rejestrów karnych o obywatelach państw trzecich (ECRIS-TCN). W przyszłości planowane jest rozszerzenie przeszukań o wizerunek twarzy. W szóstym europejskim systemie informacji o podróży oraz zezwolenia na podróż (ETIAS) nie przetwarza się danych biometrycznych.

¹ Ustawa z dnia 6 kwietnia 1990 roku o Policji, (Dz. U. 1990 Nr 30 poz. 179).

Za rozwój i zarządzanie operacyjne wielkoskalowymi systemami informatycznymi odpowiada agencja unijna ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA). Agencja ta została ustanowiona Rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 1077/2011 z dnia 25 października 2011 r.² Swoją działalność rozpoczęła 1 grudnia 2012 r. Agencja jest organem Unii, posiadającym autonomię prawną, administracyjną i finansową. Akt prawny, na mocy którego powołano Agencję, został zastąpiony nowym rozporządzeniem (UE) nr 2018/1726 z dnia 14 listopada 2018 r.³

Eu-LISA odpowiada za rozwój i zarządzanie operacyjne wielkoskalowymi systemami informacyjnymi, które są niezbędnymi instrumentami wdrażania polityki azylowej, zarządzania granicami UE i migracji. Wśród tych systemów znajdują się System Informacyjny Schengen drugiej generacji – SIS II, Wizowy System Informacyjny – VIS, System Eurodac, System Wjazdu/Wyjazdu – Entry/Exit System (EES) oraz europejski system informacji o podróżach oraz zezwoleń na podróże – European Travel Information and Authorisation System (ETIAS). Agencja ściśle współpracuje z państwami członkowskimi, instytucjami UE i agencjami UE działającymi w obszarze sprawiedliwości i spraw wewnętrznych. Zapewnia rozwój wielkoskalowych systemów informatycznych, a co za tym idzie – wsparcie techniczne. Przyczynia się do tego, aby Europejczycy mogli swobodnie podróżować na terytorium Unii Europejskiej bez zagrożenia ich bezpieczeństwa. Wdraża nowe technologie, dzięki którym zarządzanie granicami UE staje się bardziej nowoczesne, efektywne i bezpieczne.

System Informacyjny Schengen – SIS

Współpraca policyjna zajmuje kluczowe miejsce w polityce Unii Europejskiej. Jej umocnienie na terenie UE nastąpiło w latach 80 XX wieku, a za główny cel przyjęto wówczas utrzymanie wewnętrznego bezpieczeństwa w obszarze Wspólnot Europejskich (Banach-Gutierrez, 2008). Rozwój współpracy policyjnej na terenie Unii Europejskiej zainicjowało zawarcie w dniu 14 czerwca 1985 r. Układu z Schengen,

zwanego Schengen I, który został podpisany przez pięć państw członkowskich Wspólnot Europejskich (Belgia, Francja, Niemcy, Luksemburg i Holandia) w luksemburskiej miejscowości Schengen, położonej na pograniczu Luksemburga, Niemiec i Francji. Obecnie Układ zrzesza 26 państw. Miał on charakter porozumienia politycznego pomiędzy państwami członkowskimi i zakładał stopniowe znoszenie kontroli na jego wewnętrznych granicach. Znoszenie kontroli granicznej wymusiło zintensyfikowanie współpracy służb policyjnych PC UE, mającej na celu nieustanną walkę z przestępczością, w tym z transgraniczną przestępczością zorganizowaną.

Baza SIS zbudowana jest z systemu centralnego, zwanego systemem centralnym SIS (CS SIS), jednolitego interfejsu krajowego (NI-SIS) oraz infrastruktury łączności pomiędzy CS-SIS a NI-SIS, która zapewnia przekazywanie danych przez zaszyfowaną wirtualną sieć na potrzeby SIS oraz wymiany danych pomiędzy biurami SIRENE. System SIS, jako najważniejsze narzędzie wymiany informacji w Europie służące do zapewnienia bezpieczeństwa i skutecznego zarządzania granicami, musi dbać o ciągłość funkcjonowania systemu na szczeblach centralnym i krajowym. System centralny SIS i infrastruktura łączności umożliwiają użytkownikom dostęp do danych przez 24 godziny na dobę, 7 dni w tygodniu. Dane wprowadzone do systemu przez jedno państwo członkowskie dostępne są dla służb i organów pozostałych państw, odpowiedzialnych za ochronę granic, wydawanie wiz i bezpieczeństwo publiczne. Podczas przekraczania granic zewnętrznych lub standardowej kontroli policyjnej dokonuje się sprawdzenia przy użyciu SIS, czy dany przedmiot (np. samochód) lub osoba figurują we wspólnej bazie danych. Do danych zgromadzonych w SIS II mają dostęp np.: Policja, organy kontroli skarbowej, Straż Graniczna, Agencja Bezpieczeństwa Wewnętrznego, Żandarmeria Wojskowa, Centralne Biuro Antykorupcyjne, Służba Kontrwywiadu Wojskowego, Służba Wywiadu Wojskowego i inne⁴.

Dane wprowadzane do SIS dotyczące osób zawierają: imiona, nazwiska, imiona i nazwiska nadane przy urodzeniu, poprzednio używane imiona i nazwiska, pseudonimy, datę i miejsce urodzenia, płeć, wszelkie posiadane obywatelstwa, oznaczenie „uzbrojony”, „groźny”, podstawę wpisu i inne informacje. Do SIS wprowadza się również przedmioty w następujących kategoriach⁵: pojazdy silnikowe, przyczepy o masie własnej przekraczającej 750 kg, przyczepy turystyczne, urządzenia przemysłowe, jednostki pływające, silniki jednostek pływających, kontenery, statki powietrzne i ich silniki, sprzęt informatyczny, blankiety

² Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1077/2011 z dnia 25 października 2011 r. *ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości*, (Dz. Urz. UE L 286 z 01.11.2011 r.).

³ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1726 z dnia 14 listopada 2018 r. *w sprawie Agencji Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA), zmiany rozporządzenia (WE) nr 1987/2006 i decyzji Rady 2007/533/WSiSW oraz uchylecia rozporządzenia (UE) nr 1077/2011*, (Dz. Urz. UE L 295 z 21.11.2018 r.).

⁴ Ustawa z dnia 24 sierpnia 2007 roku *o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym*, (Dz. U. z 2007, nr 165, poz. 117).

⁵ Ibidem.

dokumentów urzędowych, które zostały skradzione, przywłaszczone, utracone, wydane dokumenty tożsamości (np. paszporty, dowody tożsamości, dokumenty pobytowe, dokumenty podróży, prawa jazdy), które zostały skradzione, przywłaszczone, utracone lub unieważnione, dowody rejestracyjne pojazdów i tablice rejestracyjne pojazdów, które zostały skradzione, przywłaszczone, utracone lub unieważnione, inne, które mają charakter wymienionych powyżej dokumentów lub tablic rejestracyjnych, jednakże są fałszywe, oraz inne przedmioty.

W celu jednoznacznej identyfikacji osób system SIS umożliwia przetwarzanie danych biometrycznych, które dotyczą cech fizycznych lub fizjologicznych osoby oraz umożliwiają jej jednoznaczną identyfikację. Są to: fotografie, wizerunki twarzy, dane daktyloskopijne i profile DNA. Dane daktyloskopijne w SIS oznaczają „dane dotyczące odbitek linii papilarnych palców i odbitek linii papilarnych dłoni, które z powodu ich niepowtarzalnego charakteru i układu cech szczególnych umożliwiają przeprowadzenie dokładnych i dających jednoznaczne wyniki porównań odnośnie do tożsamości danej osoby”⁶. Oznacza to, że do SIS wprowadza się od jednej do dziesięciu płaskich i przetoczonych odbitek linii papilarnych palców. Mogą one również zawierać do dwóch odbitek linii papilarnych dłoni⁷. Dane daktyloskopijne i profile DNA wykorzystuje się w każdym przypadku w celu identyfikacji lub potwierdzenia tożsamości osoby, która została ustalona w wyniku wyszukiwania alfanumerycznego przeprowadzonego w SIS. Jeżeli tożsamości osoby nie można ustalić w żaden sposób, to przeprowadza się wyszukiwanie biometryczne w systemie SIS posiadającym Automatyczny System Identyfikacji Daktyloskopijnej (tzw. SIS w AFIS). Do SIS wprowadzane są dane daktyloskopijne na wniosek organu wymiaru sprawiedliwości państwa członkowskiego, które dokonuje wpisu. Wpisy te dotyczą⁸:

- a) osób poszukiwanych w celu aresztowania i wydania na podstawie europejskiego nakazu aresztowania (ENA) lub aresztowania i ekstradycji,
- b) osób zaginionych lub osób narażonych na niebezpieczeństwo, którym należy uniemożliwić podróżowanie, w celu zapewnienia im ochrony lub wy-

eliminowania zagrożenia dla bezpieczeństwa lub porządku publicznego,

- c) dzieci zagrożonych uprowadzeniem przez rodzica, członka rodziny lub opiekuna,
- d) dzieci, którym należy uniemożliwić podróżowanie ze względu na konkretne i realne zagrożenie związane z wywiezieniem ich z terytorium państwa członkowskiego,
- e) dzieci, które mogą stać się ofiarami handlu ludźmi, przymusowego małżeństwa, okaleczenia żeńskich narządów płciowych lub innych form przemocy warunkowanej płcią,
- f) dzieci, które mogą się stać ofiarami przestępstw terrorystycznych lub wziąć udział w popełnianiu takich przestępstw, lub mogą zostać zwerbowane, zaciągnięte do ugrupowań zbrojnych.

Ponadto istnieje możliwość wprowadzenia do SIS wpisów⁹:

- a) dotyczących nieznanymi osób, które są poszukiwane,
- b) zawierających jedynie dane daktyloskopijne, które stanowią ślady linii papilarnych palców lub dłoni zabezpieczonych na miejscach popełnienia przestępstw terrorystycznych lub innych poważnych przestępstw,
- c) będących przedmiotem postępowania przygotowawczego.

Dane te wprowadza się do SIS wyłącznie wtedy, gdy istnieje bardzo duże prawdopodobieństwo, że należą one do sprawcy danego przestępstwa lub aktu terrorystycznego. W szczególności dotyczy to sytuacji, w której dane daktyloskopijne ujawniono i zabezpieczono na broni lub innym przedmiocie użytym do popełnienia przestępstwa oraz przeszukano w dostępnych krajowych, unijnych lub międzynarodowych bazach danych z wynikiem negatywnym.

Dostęp do danych wprowadzonych do SIS oraz prawo do bezpośredniego wyszukiwania takich danych mają krajowe organy wymiaru sprawiedliwości, w tym organy odpowiedzialne za wszczynanie postępowań karnych z oskarżenia publicznego, a także wprowadzenie postępowań przygotowawczych przed wniesieniem aktu oskarżenia, w ramach wykonywania swoich ustawowych zadań.

Usługa automatycznej identyfikacji daktyloskopijnej wprowadzona w ramach SIS stanowi uzupełnienie istniejącego mechanizmu Prüm, dotyczącego wzajemnego transgranicznego dostępu on-line do wyznaczonych krajowych baz zawierających dane DNA

⁶ Ustawa z dnia 24 sierpnia 2007 roku o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, (Dz. U. z 2007, nr 165, poz. 117).

⁷ Ibidem.

⁸ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylecia decyzji Rady 2007/533/WSiSW oraz uchylecia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE, (Dz. Urz. UE L 312 z 7.12.2018 r.).

⁹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylecia decyzji Rady 2007/533/WSiSW oraz uchylecia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE, (Dz. Urz. UE L 312 z 7.12.2018 r.).

i daktyloskopijne, przewidziane w decyzjach Rady 2008/615/WSiSW¹⁰ i 2008/616/WSiSW¹¹. Dzięki wyszukiwaniu danych daktyloskopijnych w SIS możliwe jest aktywne poszukiwanie sprawcy. Jeżeli w wyniku przeszukania danych daktyloskopijnych nastąpi dopasowanie, państwo członkowskie przeprowadza weryfikację z udziałem ekspertów w celu ustalenia, czy istnieje zgodność pomiędzy danymi daktyloskopijnymi poddawanymi przeszukaniu a danymi przechowywanymi w SIS. Tego typu identyfikacja ma na celu pomoc w postępowaniu przygotowawczym i doprowadzenie do aresztowania osoby podejrzanej.

Każde państwo członkowskie dokonuje tylko jednego wpisu do SIS II dotyczącego danej osoby lub przedmiotu. Drugie i kolejne wpisy dotyczące danej osoby lub przedmiotu przechowuje się na szczeblu krajowym, aby po usunięciu pierwszego wpisu z systemu można było wprowadzić je ze szczebla krajowego. Przed dokonaniem wpisu do SIS II konieczne jest sprawdzenie, czy dana osoba lub przedmiot figurują już w systemie. W przypadku osoby, sprawdzanie występowania wielokrotnych wpisów wiąże się z obowiązkowym porównaniem nazwiska, imienia, daty urodzenia, płci, danych daktyloskopijnych. Wprowadzenie do systemu SIS II możliwości sprawdzenia osoby na podstawie danych daktyloskopijnych zwiększyło prawdopodobieństwo zidentyfikowania istniejących już wpisów dotyczących tej samej osoby posługującej się różnymi tożsamościami¹². W SIS II „trafienie” i „dopasowanie” mają różne definicje. O trafieniu w SIS II można mówić, gdy w wyniku sprawdzenia użytkownik otrzymuje informację o zagranicznym wpisie do systemu, a dane dotyczące wpisu do SIS II pasują do danych wprowadzonych na potrzeby sprawdzenia. Są to dane alfanumeryczne. Dopasowanie ma miejsce, jeżeli użytkownik przeprowadza wyszukiwanie odbitek linii papilarnych palców spośród danych zgromadzonych w systemie SIS-AFIS. Użytkownik otrzymuje powiadomienie z SIS II o możliwości dopasowania i w dalszym kroku zobowiązany jest przeprowadzić procedurę weryfikacji pod kątem zgodności odbitek linii papilarnych. W Polsce weryfikację prowadzi Wydział Badań Daktyloskopijnych i Traseologicznych CLKP, do którego

przesyłane są obrazy odbitek linii papilarnych palców, celem ich porównania¹³.

W sytuacji, gdy dane daktyloskopijne nie będą dostępne, państwo członkowskie powinno zamieszczać w SIS II wpisy o profilu DNA. Profile te powinny ułatwiać identyfikację zaginionych osób potrzebujących ochrony, a w szczególności zaginionych dzieci, m.in. w sytuacji, gdy dozwolone będzie korzystanie z profili DNA bliskich krewnych w celu przeprowadzenia identyfikacji. Dane DNA powinny zawierać wyłącznie minimalne informacje niezbędne do identyfikacji osoby zaginionej. Profile DNA nie powinny być przetwarzane w innym celu niż ten, w którym zostały wprowadzone do SIS¹⁴.

Polska z chwilą przystąpienia do UE w dniu 1 maja 2004 roku stała się odpowiedzialna za zabezpieczenie jednego z najdłuższych odcinków wspólnej lądowej granicy zewnętrznej na wschodzie kraju. Mając powyższe na uwadze, w sierpniu 2007 r. Sejm Rzeczypospolitej Polskiej przyjął ustawę *o udziale RP w Systemie Informacyjnym Schengen (SIS) i Systemie Informacji Wizowej (VIS)*. Ustawa ta określa zasady i tryb udziału Rzeczypospolitej Polskiej w tych systemach, w tym obowiązki organów dokonujących wpisów oraz organów uprawnionych do dostępu do danych poprzez Krajowy System Informatyczny.

Rozporządzenie Rady (WE) nr 871/2004 z dnia 29 kwietnia 2004 r., *dotyczące wprowadzenia niektórych nowych funkcji Systemu Informacyjnego Schengen*¹⁵, rozszerzyło krąg podmiotów uprawnionych do korzystania z danych SIS do celów zwalczania terroryzmu. Rozporządzenie to zostało zmienione rozporządzeniem (WE) nr 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)*¹⁶. System SIS II funkcjonuje jako jednolity system informacyjny, pomimo iż bazuje na dwóch podstawach prawnych, a mianowicie na rozporządzeniu (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. oraz decyzji Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r.¹⁷ System ten funkcjonuje od 9 kwietnia 2013 roku i umożliwia przetwarzanie większej liczby danych oraz korzystanie z nowoczesnych funkcjonalności¹⁸.

¹⁰ Decyzja Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. *w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej*, (Dz. Urz. UE L 210 z 06.08.2008 r.).

¹¹ Decyzja Rady 2008/616/WSiSW z dnia 23 czerwca 2008 r. *w sprawie wdrożenia decyzji 2008/615/WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej*, (Dz. Urz. UE L 210/12 z 06.08.2008 r.).

¹² Decyzja Wykonawcza Komisji (UE) 2017/1528 z dnia 31.08.2017 r. *zastępująca załącznik do decyzji wykonawczej Komisji 2013/115/UE w sprawie przyjęcia podręcznika SIRENE i innych środków wykonawczych dla systemu informacyjnego Schengen drugiej generacji (SIS II)*, (Dz. Urz. UE L 231 z 07.09.2017 r.).

¹³ Ibidem.

¹⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. *w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylenia decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE*, (Dz. Urz. UE L 312 z 7.12.2018 r.).

¹⁵ Dz. Urz. UE, L 162 z 30.04.2004 r.

¹⁶ Dz. Urz. UE L 381 z 28.12.2006 r.

¹⁷ Dz. Urz. UE L 205 z 7.8.2007 r.

¹⁸ Decyzja Rady z dnia 7 marca 2013 r. *ustalająca datę rozpoczęcia stosowania rozporządzenia (WE) nr 1987/2006*

Organami uprawnionymi do dostępu i bezpośredniego przeszukiwania danych wprowadzonych do SIS II są „krajowe organy sądownicze, w tym odpowiedzialne za wszczynanie dochodzeń z oskarżenia publicznego w postępowaniu karnym i dochodzeń sądowych przed wniesieniem aktu oskarżenia, w ramach wykonywania zadań określonych przez ustawodawstwo krajowe, a także przez organy pełniące wobec nich funkcję koordynującą” oraz organy odpowiedzialne za ustalanie tożsamości obywateli państw trzecich do celów kontroli granicznej, jak również kontroli policyjnych i celnych¹⁹. Zgodnie z założeniami, istotną zaletą Systemu Informacyjnego Schengen drugiej generacji jest poprawa jakości danych i zdolności identyfikacji osób. Nowoczesne technologie informatyczne umożliwiają przetwarzanie w SIS II danych alfanumerycznych oraz danych biometrycznych, takich jak wizerunek twarzy, DNA czy odfitki linii papilarnych. Skutkuje to sprawniejszą i dokładniejszą identyfikacją osób²⁰. Obrazy linii papilarnych palców są wykorzystywane jedynie do celów potwierdzania tożsamości obywatela państwa trzeciego, który został znaleziony w SIS II w trakcie wyszukiwania po danych alfanumerycznych²¹.

W dniu 19 listopada 2018 r. Rada przyjęła trzy rozporządzenia, zwane w skrócie „SIS Recast”, dotyczące użytkowania systemu informacyjnego Schengen, które będą stopniowo zastępowały obecnie obowiązujące unijne rozporządzenie i decyzję. Są to²²:

- a) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1860 z dnia 28 listopada 2018 r. w sprawie użytkowania Systemu Informacyjnego Schengen do celów powrotu nielegalnie przebywających obywateli państw trzecich,
- b) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1861 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmiany konwencji wykonawczej do układu z Schengen oraz zmiany i uchylecia rozporządzenia (WE) nr 1987/2006,

Parlamentu Europejskiego i Rady w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) oraz Decyzja Rady z dnia 7 marca 2013 r. ustalająca datę rozpoczęcia stosowania decyzji 2007/533/WSiSW w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), (Dz. Urz. UE L. 2013.87.8 oraz Dz. Urz. UE L. 2013. 87.10).

¹⁹ Ibidem, artykuł 27, ust. 1 i 2.

²⁰ <https://www.policja.pl/pol/sirene/sis/12473,Co-to-jest-System-Informacyjny-Schengen-SIS.html>.

²¹ Rozporządzenie (WE) nr 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), artykuł 22, (Dz. Urz. UE L 381 z 28.12.2006 r.).

²² Dz. Urz. UE L 312 z 7.12.2018 r.

- c) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylecia decyzji Rady 2007/533/WSiSW oraz uchylecia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. stanowi podstawę do przeszukiwania danych biometrycznych, w tym danych daktyloskopijnych, do celów identyfikacyjnych i wykrywczych. Zautomatyzowana identyfikacja daktyloskopijna realizowana w ramach SIS stanowi uzupełnienie mechanizmu Prüm, jako wzajemnego transgranicznego dostępu online do odpowiednich krajowych baz danych daktyloskopijnych. Nowością jest gromadzenie i przeszukiwanie w bazach SIS niezidentyfikowanych śladów linii papilarnych palców rąk lub dłoni, które zostały ujawnione i zabezpieczone na miejscu poważnego przestępstwa lub przestępstwa terrorystycznego. W rozporządzeniu są one zdefiniowane jako dane daktyloskopijne, czyli „dane dotyczące odbitek linii papilarnych palców rąk i odbitek linii papilarnych dłoni, które z powodu ich niepowtarzalnego charakteru i układu cech szczególnych umożliwiają przeprowadzenie dokładnych i dających jednoznaczne wyniki porównań odnośnie tożsamości danej osoby”²³.

Na podstawie powyższego rozporządzenia możliwe będzie również przetwarzanie profili DNA w celu identyfikacji osób zaginionych, a w szczególności zaginionych dzieci²⁴. Pozostałe dwa rozporządzenia stanowią podstawę do przetwarzania danych daktyloskopijnych w celach identyfikacyjnych.

Wdrożenie rozporządzeń unijnych wymusiło konieczność dostosowania zapisów obowiązującej ustawy z dnia 24 sierpnia 2007 r. o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, która zawiera przepisy umożliwiające udział Polski w SIS i VIS.

Wizowy System Informacyjny (VIS)

Wizowy System Informacyjny (VIS) umożliwia państwu członkowskiemu Schengen wymianę danych wizowych. W celu identyfikacji osób i weryfikacji tożsamości przeprowadza się w systemie identyfikację

²³ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylecia decyzji Rady 2007/533/WSiSW oraz uchylecia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE, art. 3 pkt 13, (Dz. Urz. UE, L 312 z 7.12.2018 r.).

²⁴ Ibidem, pkt 26.

biometryczną, głównie na podstawie odbitek linii papilarnych palców²⁵.

System VIS ustanowiony został na mocy decyzji Rady 2004/512/WE z dnia 8 czerwca 2004 r. *ustanawiającej Wizowy System Informacyjny (VIS) jako system wymiany danych dotyczących wiz pomiędzy państwami członkowskimi*. Z kolei Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. *w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych* (zwany w skrócie rozporządzeniem w sprawie VIS) określa cel Wizowego Systemu Informacyjnego²⁶.

W Polsce system VIS został uruchomiony w dniu 11 października 2011 r. Zgodnie z Ustawą z dnia 24.08.2007 r. *o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym* umożliwia wskazanym użytkownikom indywidualnym i instytucjom korzystanie z aplikacji „VIS”, „www VIS”, „VISMail”²⁷. Wizowy System Informacyjny oparty jest na architekturze scentralizowanej. Składa się z centralnego systemu informacyjnego, zwanego „Centralnym Wizowym Systemem Informacyjnym” (CS-VIS), interfejsu zlokalizowanego w każdym państwie członkowskim, zwanego „interfejsem krajowym” (NI-VIS). Elementem składowym systemu jest również infrastruktura łączności umożliwiająca komunikację pomiędzy Centralnym Wizowym Systemem Informacyjnym a interfejsami krajowymi²⁸. Centralny Wizowy System Informacyjny (CS-VIS) otrzymuje obrazy odbitek płaskich dziesięciu palców o rozdzielczości 500 dpi (dopuszczalne odchylenie +/- 5 dpi) w 256 odcieniach szarości²⁹.

Celem Wizowego Systemu Informacyjnego jest poprawa współpracy konsularnej i wymiany informacji pomiędzy państwami należącymi do strefy Schengen, dotyczącej wydanych wiz oraz osób starających się o ich wydanie. System usprawnia współpracę pomiędzy państwami członkowskimi, m.in. w zakresie wspólnej polityki wizowej, w tym uproszczenia procedury składania wniosków wizowych, zapobiegania handlu wizami oraz identyfikacji osób, które mogą nie spełniać warunków wjazdu, pobytu lub zamieszkania na terytorium Unii Europejskiej. Wykorzystanie technologii biometrycznej umożliwia wykrywanie osób posługujących się dokumentami podróży innej osoby, co chroni podróżnych przed kradzieżą tożsamości oraz

umożliwia prowadzenie szybszych, dokładniejszych i bezpieczniejszych kontroli. System ułatwia również proces wydawania wiz, co ma istotne znaczenie dla osób często podróżujących, a także umożliwia ustalenie, które państwo UE jest odpowiedzialne za rozpatrzenie wniosku o ochronę międzynarodową. Ponadto system VIS wpływa na zwiększenie bezpieczeństwa, ponieważ wspomaga organy w zapobieganiu, wykrywaniu i dochodzeniu przestępstw terrorystycznych i innych poważnych przestępstw.

W systemie VIS zarejestrowane i przetwarzane są dane alfanumeryczne dotyczące osoby ubiegającej się o wizę oraz informacje dotyczące wiz ze złożonym wnioskiem, wiz wydanych, unieważnionych, cofniętych, przedłużonych oraz wiz, w stosunku do których odmówiono ich wydania. Oprócz danych alfanumerycznych w przedmiotowym systemie przetwarzane są fotografie, odbitki linii papilarnych palców, odesyłacze do wcześniejszych wniosków o wydanie wizy oraz plików z wnioskami utworzonych dla osób podróżujących wspólnie. Wprowadzanie danych do systemu VIS odbywa się za pośrednictwem organów wizowych. Po akceptacji wniosku, odpowiedni organ tworzy plik danych zawierający informacje, np. dane osobowe, szczegóły dotyczące podróży osoby ubiegającej się o wizę z formularza wniosku, zdjęcia i odbitki linii papilarnych palców. W przypadku podjęcia decyzji o wydaniu wizy, organ wizowy dodaje do pliku danych dotyczących wniosku dodatkowe istotne informacje, w tym rodzaj wizy, terytorium, na którym posiadacz wizy ma prawo podróżować, okres ważności wizy, liczbę wjazdów na terytorium, na którym jest ona ważna, a także długość pobytu. Konieczne jest również dodanie danych uzupełniających, w przypadku gdy organ wizowy z innego kraju UE zaprzestanie rozpatrywania wniosku lub gdy podejmie decyzję o odmowie, unieważnieniu lub cofnięciu wizy, a także w przypadku przedłużenia okresu ważności wizy³⁰.

Od osób ubiegających się o wydanie wizy pobiera się 10 odcisków palców i fotografię cyfrową. Te dane biometryczne, wraz z danymi podanymi w formularzu wniosku wizowego, są zapisywane w bezpiecznej centralnej bazie danych. Ubieganie się o nową wizę, w przypadku osób często podróżujących do strefy Schengen, nie wymaga za każdym razem pobierania odbitek linii papilarnych palców. Raz zapisane w systemie VIS odbitki linii papilarnych palców są dostępne przez okres 5 lat i w tym czasie istnieje możliwość ich wykorzystania przy kolejnych składanych wnioskach wizowych³¹.

²⁵ https://brzesc.msz.gov.pl/pl/informacje_konsularne/sprawy_wizowe/sis/.

²⁶ Dz. Urz. UE L 218 z 13.08.2008 r.

²⁷ Dz. U. nr 165, poz. 1170, z póź. zm.

²⁸ `file:///C:/Users/CLKP%20Z3/Downloads/Sprawozdanie_z_dnia_24_10_2013.pdf`.

²⁹ Decyzja Komisji z dnia 9 października 2009 r. *ustanawiająca specyfikacje dotyczące rozdzielczości oraz korzystania z odcisków palców do identyfikacji i weryfikacji biometrycznej w wizowym systemie informacyjnym*, (Dz. Urz. UE L 270 z 15.10.2009 r.).

³⁰ Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. *w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych*, (Dz. Urz. UE L 218 z 13.08.2008 r.).

³¹ <https://poland.tw/web/tajwan/wizy--informacje-ogolne>.

Na zewnętrznych granicach strefy Schengen obrazy linii papilarnych palców osoby posiadającej wizę są porównywane z danymi znajdującymi się w bazie VIS. Niezgodność danych daktyloskopijnych powoduje rozpoczęcie procedury dalszego sprawdzania tożsamości podróżnego. Organy odpowiedzialne za przeprowadzanie odpraw na granicach zewnętrznych i na terytorium kraju mają dostęp do wyszukiwania informacji w VIS za pomocą numeru naklejki wizowej, łącznie z weryfikacją odbitek linii papilarnych palców posiadacza wizy. Organy te są uprawnione do przeszukiwania VIS w celu weryfikacji tożsamości osoby lub autentyczności wizy, a także potwierdzenia, czy dana osoba spełnia wymagania konieczne do wjazdu, pozostania lub zamieszkiwania na terytorium kraju. Jeżeli wyszukiwanie informacji wskazuje na to, że dane dotyczące posiadacza wizy są zarejestrowane w VIS, właściwy organ kontroli granicznej może przeglądać określone dane zawarte w pliku dotyczącym wniosku wizowego.

W celu zidentyfikowania osoby, która nie spełnia lub przestała spełniać wymagane warunki, właściwe organy mają dostęp do wyszukiwania informacji za pomocą odbitek linii papilarnych palców danej osoby. W przypadku gdy wykorzystanie odbitek palców danej osoby nie jest możliwe lub wyszukiwanie zakończy się wynikiem negatywnym, uprawnione organy mogą przeszukiwać VIS z wykorzystaniem danych alfanumerycznych, takich jak: nazwisko, płeć, data i miejsce urodzenia i inne informacje zawarte w dokumencie podróży. Powyższe kryteria wyszukiwania mogą być wykorzystywane w połączeniu z kryterium narodowości danej osoby.

Organy odpowiedzialne za udzielenie ochrony międzynarodowej mają dostęp do przeszukiwania VIS za pomocą danych daktyloskopijnych, ale tylko w celu określenia kraju UE odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej.

Informacji zawartych w VIS nie przekazuje się krajom trzecim lub organizacjom międzynarodowym, za wyjątkiem sytuacji, gdy przekazanie tych danych jest niezbędne do potwierdzenia tożsamości obywatela państwa trzeciego. Przekazanie informacji może być stosowane tylko w indywidualnych, uzasadnionych przypadkach, bez naruszenia praw uchodźców i osób ubiegających się o ochronę międzynarodową³².

Zakończenie

Analizując zagadnienie wzmocnienia międzynarodowej współpracy opartej na wymianie danych daktyloskopijnych, stwierdzono, iż: istniejące europejskie systemy wielkoskalowe są rozbudowywane o nowe funkcjonalności i szerszy zakres przetwarzanych danych. Dotyczy to systemów SIS, VIS, które jako systemy drugiej generacji są wzbogacone o obrazy

linii papilarnych dłoni i niezidentyfikowanych śladów linii papilarnych zabezpieczonych na miejscu przestępstwa. Powyższe zmiany pociągają za sobą konieczność dostosowania prawodawstwa krajowego, jak również wprowadzenia zmian organizacyjnych w obszarze zadań realizowanych przez zaangażowane we współpracę organy i instytucje. Unia Europejska wypracowała wiele aktów legislacyjnych stanowiących fundament do stworzenia efektywnego systemu walki z terroryzmem i przestępczością transgraniczną. Podstawa tego systemu już funkcjonuje, a jego rozwój w zakresie rozszerzenia możliwości wykorzystywania danych daktyloskopijnych oraz innych danych biometrycznych, np. wizerunku twarzy czy DNA, przyczynia się do wzmocnienia międzynarodowej współpracy organów ścigania i wymiaru sprawiedliwości. Rozszerzenie zakresu przetwarzania danych zwiększa możliwość identyfikacji osób czy wykrycia sprawcy przestępstwa oraz nakłada nowe zadania na Policję. W kolejnym numerze „Problemów Kryminalistyki” opisane zostaną inne systemy wielkoskalowe, tj. Eurodac, Entry.Exit, ECRIS-TCN, oraz założenia interoperacyjności tych systemów jako unijnych narzędzi informatycznych, służących zarządzaniu granicami zewnętrznymi oraz zapobieganiu i zwalczaniu nielegalnej migracji.

Bibliografia

1. Banach-Gutierrez, J. (2008). Współpraca policyjna w Unii Europejskiej: od TREVİ do Schengen III. W: L. Boguni, (red.), *Nowa Kodyfikacja Prawa Karnego: Tom XXIII*. Uniwersytet Wrocławski.
2. Gajda, A. (2019). Interoperacyjność unijnych systemów informacyjnych w zakresie bezpieczeństwa, ochrony granic i zarządzania migracjami. *Kwartalnik Kolegium Ekonomiczno-Społecznego „Studia i Prace”, 1(37)*.
3. Jaroszevska-Choraś, D. (2016). *Biometria. Aspekty prawne*. Wydawnictwo Uniwersytetu Gdańskiego.

Akty prawne

1. Decyzja Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej, Dz. Urz. UE L 210 z 06.08.2008 r.
2. Decyzja Rady 2008/616/WSiSW z dnia 23 czerwca 2008 r. w sprawie wdrożenia decyzji 2008/615/WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej, Dz. Urz. UE L 210/12 z 06.08.2008 r.
3. Decyzja Komisji z dnia 9 października 2009 r. ustanawiająca specyfikacje dotyczące rozdzielczości oraz korzystania z odcisków palców do identyfikacji i weryfikacji biometrycznej w wizowym systemie informacyjnym, Dz. Urz. UE L 270 z 15.10.2009 r.

³² https://brzesc.msz.gov.pl/pl/informacje_konsularne/sprawy_wizowe/sis/.

4. Decyzja Rady z dnia 7 marca 2013 r. ustalająca datę rozpoczęcia stosowania rozporządzenia (WE) nr 1987/2006 Parlamentu Europejskiego i Rady w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II) oraz Decyzja Rady z dnia 7 marca 2013 r. ustalająca datę rozpoczęcia stosowania decyzji 2007/533/WSiSW w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz. Urz. UE L 87/10 z 27.03.2013 r. oraz Dz. Urz. UE L 87/8 z 27.03.2013 r.
5. Decyzja Wykonawcza Komisji (UE) 2017/1528 z dnia 31.08.2017 r. zastępująca załącznik do decyzji wykonawczej Komisji 2013/115/UE w sprawie przyjęcia podręcznika SIRENE i innych środków wykonawczych dla systemu informacyjnego Schengen drugiej generacji (SIS II), Dz. Urz. UE L 231 z 07.09.2017 r.
6. Rozporządzenie (WE) nr 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), artykuł 22, Dz. Urz. UE L 381 z 28.12.2006 r.
7. Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych, Dz. Urz. UE, L 218 z 13.08.2008 r.
8. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1077/2011 z dnia 25 października 2011 r. ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości, Dz. Urz. UE L 286 z 01.11.2011 r.
9. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1726 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA), zmiany rozporządzenia (WE) nr 1987/2006 i decyzji Rady 2007/533/WSiSW oraz uchylecia rozporządzenia (UE) nr 1077/2011, Dz. Urz. UE L 295 z 21.11.2018 r.
10. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylecia decyzji Rady 2007/533/WSiSW oraz uchylecia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE, Dz. Urz. UE L 312 z 7.12.2018 r.
11. Ustawa z dnia 24 sierpnia 2007 roku o udziale Rzeczypospolitej Polskiej w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym, Dz. U. z 2007, nr 165, poz. 117.

Strony internetowe

1. <https://www.policja.pl/pol/sirene/sis/12473,Co-to-jest-System-Informacyjny-Schengen-SIS.html>, (dostęp: 20.05.2022).
2. https://brzesc.msz.gov.pl/pl/informacje_konsularne/sprawy_wizowe/sis/, (dostęp: 07.03.2019).
3. <https://poland.tw/web/tajwan/wizy--informacje-ogolne>, (dostęp: 28.03.2021).