Instytucjonalny wymiar bezpieczeństwa w XXI wieku

REDAKCJA NAUKOWA
Izabela Oleksiewicz
Małgorzata Polinceusz

OFICYNA WYDAWNICZA
POLITECHNIKI RZESZOWSKIEJ

Wydano za zgodą Rektora

R e c e n z e n t
dr hab. Marta POMYKAŁA, prof. PRz

R e d a k t o r n a c z e l n y
Wydawnictw Politechniki Rzeszowskiej
dr hab. inż. Lesław GNIEWEK, prof. PRz

R e d a k t o r
Piotr CYREK

S k ł a d i ł a m a n i e t e k s t u
Mariusz TENDERA

P r o j e k t o k ł a d k i
Joanna MIKUŁA

instytucje, bezpieczeństwo, polityka, cyberprzestrzeń, XXI wiek

institutions, security, politics, cyberspace, 21st century

© Copyright by Oficyna Wydawnicza Politechniki Rzeszowskiej
Rzeszów 2024

Wszelkie prawa autorskie i wydawnicze zastrzeżone. Każda forma powielania oraz przenoszenia na inne nośniki bez pisemnej zgody Wydawcy jest traktowana jako naruszenie praw autorskich, z konsekwencjami przewidzianymi w *Ustawie o prawie autorskim i prawach pokrewnych* (Dz.U. z 2018 r., poz. 1191 t.j.). Autor i Wydawca dołożyli wszelkich starań, aby rzetelnie podać źródło zamieszczonych ilustracji oraz dotrzeć do właścicieli i dysponentów praw autorskich. Osoby, których nie udało się ustalić, są proszone o kontakt z Wydawnictwem.

p-ISBN 978-83-7934-749-0 e-ISBN 978-83-7934-751-3

Oficyna Wydawnicza Politechniki Rzeszowskiej
al. Powstańców Warszawy 12, 35-959 Rzeszów
https://oficyna.prz.edu.pl

Ark. wyd. 6,57. Ark. druk. 6,50.
Wydrukowano w grudniu 2024 r.
Drukarnia Oficyny Wydawniczej,
al. Powstańców Warszawy 12, 35-959 Rzeszów
Zam. nr 45/24

SPIS TREŚCI

Wstęp (Izabela Oleksiewicz, Małgorzata Polinceusz) 5

Julia Gawron, Katarzyna Laska, Zuzanna Ścibura: Bezpieczeństwo informacyjne Polski w erze cyfrowej 9

Julia Mazurkiewicz: Rola i zadania Centralnego Biura Zwalczania Cyberprzestępczości w przeciwdziałaniu współczesnym zagrożeniom cybernetycznym 21

Piotr Padula: Zagrożenia cybernetyczne wyborów prezydenckich w USA w 2024 roku 31

Damian Karol: Zabezpieczenia dowodów cyfrowych w toku postępowania karnego wobec wyzwań postępującej globalizacji i cyfryzacji 43

Kacper Mazurek: Instytucjonalny wymiar polityki migracyjnej w Unii Europejskiej 55

Seweryn Walas: Inspekcja Transportu Drogowego jako instytucja w wymiarze bezpieczeństwa państwa 73

Kinga Matusz, Maciej Żebrakowski, Filip Ferenc: Wykorzystanie badań DNA w kryminalistyce przez Policję 83

Zakończenie (Izabela Oleksiewicz, Małgorzata Polinceusz) 97

Streszczenie 99

Summary 99

WSTĘP

Bezpieczeństwo jest centralnym zjawiskiem teorii i praktyki stosunków międzynarodowych. Mimo to, ciągle istnieje niedorozwój badań na temat desygnatów terminu „bezpieczeństwa" i dynamiki jego ewolucji. Wynika to z braku głębokiego i bardziej ogólnego rozumienia tej kategorii. Konieczne jest rozwijanie badań wykraczających poza dotychczasowe tradycyjne, wąskie i militarne pojmowanie bezpieczeństwa.

Po upadku systemu bipolarnego, który stworzył ważny nowy porządek międzynarodowy, społeczność międzynarodowa stanęła przed kolejnym dylematem dotyczącym nowych struktur i ich działania. System struktur dwubiegunowych, pomimo różnych ocen, nawiązujących do paradygmatu stabilności hegemonicznej, ustabilizował świat głównie w relacjach Wschód – Zachód. Obecnie świat wkroczył w okres radykalnych, dynamicznych i często nieskoordynowanych zmian, które J.N. Rosenau określał mianem turbulencji[1], natomiast Z. Brzeziński[2] już dawno dowodził i ostrzegał, że zachodzące zmiany w ładzie międzynarodowym i państwowym zaczynają wymykać się nam spod kontroli.

Przez wieki, a zwłaszcza od czasu powstania nowoczesnego systemu stosunków międzynarodowych, zwanego westfalskim, rozumienie bezpieczeństwa ulegało ewolucji wraz ze zmianą interesów państw, zmianą źródeł i istoty zagrożeń oraz ogólną ewolucją środowiska międzynarodowego. Największe zmiany związane są z pojawieniem się państw narodowych. Ten nowy i zarazem zasadniczy element w strukturze ładu międzynarodowego doprowadził do podziału świata na terytorialnie zdefiniowane jednostki polityczne, tworząc system samowładnych państw. Tym samym ukształtowana została istotna cecha podmiotowej struktury środowiska międzynarodowego, jaką jest jego anarchiczność w sensie braku centralnej instytucji sterującej ładem międzynarodowym. Tak rozumiana anarchiczność tworzy istotne strukturalne uwarunkowania dla zachowań państw, gdyż nie ma tu, tak jak we wnętrzu państwa, władzy zwierzchniej, która zapewniałaby państwom bezpieczeństwo. Muszą to czynić same. Jednak, jeśli nie ma pewności co do intencji innych państw, występuje zjawisko nieufności i braku poczucia bezpieczeństwa. Jeżeli nieufność jest wzajemna, to mamy do czynienia z sytuacją, gdy brak poczucia bezpieczeństwa w jednym państwie rodzi taka samą sytuację

---

[1] Patrz szerzej: J.N. Rosenau, *Turbulence in World Politics. A Theory of Change and Continuity*, Princeton 1990, s. 205.

[2] Z. Brzeziński, *Between Two Ages: America's Role in the Technetronic Era,* Harmondsworth 1976, s. 5.

w innym. Zjawisko to określane jest mianem „dylematu bezpieczeństwa". Tak rozumiany dylemat bezpieczeństwa stanowi istotną barierę współpracy państw, gdyż nie ufając sobie, obawiają się one angażowania w taką współpracę[3].

Celem monografii jest przedstawienie w literaturze przedmiotu nauki bezpieczeństwo wymiaru instytucjonalnego w XXI wieku na wybranych przykładach. Obejmuje on struktury władzy publicznej i ich kompetencje. Składa się on na przedmiotowy wymiar bezpieczeństwa wewnętrznego państwa. Liczba i zakres działalności struktur władzy powiązane są z narastającymi powinnościami państwa, przez co ulegają stałemu rozszerzeniu i specjalizacji. Wymiar normatywny bezpieczeństwa wewnętrznego to akty, normy i przepisy prawne regulujące sferę bezpieczeństwa wewnętrznego w ujęciu przedmiotowym. Wymiar funkcjonalny jest syntezą dwóch poprzednich. Jego istotą bowiem jest sposób wprowadzania w życie regulacji dotyczących bezpieczeństwa wewnętrznego przez odpowiednie instytucje publiczne. Rozwój zarówno prawa, jak i aparatu władzy publicznej, przy narastających powinnościach państwa, powodują stałą komplikację tego procesu.

W tym miejscu należy podkreślić, że bezpieczeństwo jest najczęściej rozpatrywane według trzech zasadniczych wymiarów, tj. podmiotowego, przedmiotowego i procesualnego[4]. Zgodnie z pierwszym – wymiarem podmiotowym, bezpieczeństwo odnosi się do uczestników życia społecznego. To szczególnego rodzaju bezpieczeństwo ludzkie jest współcześnie najbardziej wszechstronną i zaawansowaną konceptualizacją bezpieczeństwa człowieka jako podmiotu. Istotą jest tu jakość życia w społeczeństwie i w państwie. Natomiast w wymiarze przedmiotowym, bezpieczeństwo dotyczy różnych jego sfer oraz chronionych wartości, kierunków i metod polityki bezpieczeństwa, postrzegania bezpieczeństwa państw. Współcześnie w ramach bezpieczeństwa widoczne jest odejście od ujęcia tradycyjnego, tj. zachowania zdolności militarnej poszczególnych jednostek, do realizacji żywotnych interesów na rzecz zawierania sojuszy i umów międzynarodowych. Sojusze zawierane są na zasadach zaufania do gospodarek wolnorynkowych, instytucji demokratycznych przy jednoczesnym poszanowaniu praw i wolności obywateli.

W ostatnim wymiarze, procesualnym, bezpieczeństwo należy traktować jako proces dynamiczny, zmieniający się w czasie, wynikający z postępu cywilizacyjnego oraz ewolucji myśli społeczno-politycznej. W obecnym bezpieczeństwie zacierają się granice pomiędzy polityką wewnętrzną a międzynarodową. Wymiar ten powinien być traktowany jako droga do osiągnięcia pewnego stanu, definiowanego jako bezpieczeństwo.

Oddajemy w Państwa ręce publikację będącą efektem wstępnych badań studentów Koła Polityki Bezpieczeństwa Państwa. Niniejsza monografia adresowana

[3] Zob. szerzej: *Europa Środkowo-Wschodnia w procesie transformacji i integracji. Wymiar bezpieczeństwa*, red. M. Pietraś, H. Chałupczak, J. Misiągiewicz, Zamość 2016, s. 21 i n.

[4] Por. M. Fałdowski, *Współczesny wymiar bezpieczeństwa*, „Zeszyty Naukowe SGSP" 2018, nr 66, t. 2, s. 112-113.

jest do zróżnicowanego grona odbiorców. Rozdziały są skierowane zarówno do studentów kierunków studiów nauki o bezpieczeństwie, jak i wszystkich innych osób, które interesują się problematyką w niej zawartą.

Izabela Oleksiewicz[5]
Małgorzata Polinceusz[6]

[5] dr hab. Izabela Oleksiewicz, prof. PRz, Politechnika Rzeszowska, Wydział Zarządzania. ORCID: 0000-0002-1622-7467.

[6] dr Małgorzata Polinceusz, Politechnika Rzeszowska, Wydział Zarządzania. ORCID: 0000-0002--1179-6628.

Julia GAWRON[1], Katarzyna LASKA[2], Zuzanna ŚCIBURA[3]

BEZPIECZEŃSTWO INFORMACYJNE POLSKI W ERZE CYFROWEJ

Historia powstania bezpieczeństwa informacyjnego

Już w starożytności pojawiły się pierwsze formy kryptografii. W Rzymie używano prostych szyfrów, takich jak szyfr Cezara, do ochrony wiadomości[4]. Kryptografia w starożytności stanowiła zatem wczesną formę ochrony danych, co pokazuje, jak ważne było zabezpieczanie informacji przed nieuprawnionym dostępem. Zatem pojęcie „bezpieczeństwo informacyjne" nie jest zagadnieniem nowym, jego ślady pojawiły się w VI w. p.n.e. dzięki chińskiemu filozofowi Sun Tzu, który opracował pierwsze strategie walki informacyjnej[5]. W swojej książce pt. *Sztuka wojny* zwracał uwagę na fakt, jak istotne jest posiadanie wiedzy o przeciwniku. Posiadanie dokładnych informacji o opozycji pozwalało na skuteczniejsze planowanie działań, co można uznać za początkową formę bezpieczeństwa informacyjnego.

W średniowieczu rozwój administracji wymagał wprowadzenia dekretów[6] czy testamentów, które były chronione przez pieczęcie, co świadczyło to o autentyczności dokumentu[7]. Stanowiły one formę zabezpieczenia informacji. Także Kościół katolicki odegrał kluczową rolę w kształtowaniu bezpieczeństwa informacyjnego. W klasztorach gromadzono i kopiowano cenne teksty, co bezpośrednio przyczyniało się do ochrony wiedzy oraz informacji.

W tym okresie informacje były często wykorzystywane jako broń w konfliktach. Dlatego ochrona informacji stała się nie tylko kwestią administracyjną, ale także militarną. Praktyki i strategie, które podejmowano, miały długotrwały wpływ na rozwój pojęcia bezpieczeństwa informacyjnego w późniejszych wiekach.

Bezpieczeństwo informacyjne w XV wieku w Polsce znacząco ewaluowało. Występowały konflikty, które wymagały skutecznej ochrony tajnych dokumentów. Utrata takich dokumentów mogła mieć poważne konsekwencje dla wyniku

[1] Politechnika Rzeszowska, Wydział Zarządzania.
[2] Politechnika Rzeszowska, Wydział Zarządzania.
[3] Politechnika Rzeszowska, Wydział Zarządzania.
[4] M. Karbowski, *Podstawy kryptografii,* wyd. II, Gliwice 2008, s. 12.
[5] K. Grzebiela, *Pojęcie i istota bezpieczeństwa informacyjnego*, Kraków 2018, s. 7.
[6] Dekret – w dawnej Polsce: wyrok sądu lub akt normatywny wydany przez króla.
[7] B. Bobowski, *Testament w średniowiecznym prawie polskim*, Częstochowa 2009, s. 2.

bitew oraz stabilności politycznej w regionie. Praktyki stosowane w średniowieczu stanowiły podstawy, na których później rozwijały się bardziej zaawansowane systemy bezpieczeństwa informacyjnego. Wiarygodna, rzetelna, dokładna i aktualna informacja zawsze bowiem była istotna przy podejmowaniu decyzji państwowych, w szczególności w dziedzinie bezpieczeństwa – tak zewnętrznego, jak i wewnętrznego[8].

W XX wieku pojęcie bezpieczeństwa informacyjnego nabrało zupełnie nowego znaczenia. Natomiast termin „bezpieczeństwo informacyjne państwa" (podmiot) został wprowadzony dopiero w drugiej połowie XX wieku[9]. Rozwój technologii, powstanie nowych systemów komunikacyjnych oraz zmiany geopolityczne spowodowały, że ochrona informacji stała się jednym z priorytetów zarówno w sferze militarnej, jak i cywilnej. W pierwszej połowie wieku, bezpieczeństwo informacyjne było ściśle związane z ochroną tajemnic państwowych oraz technikami szyfrowania. W czasie I wojny światowej komunikacja wojskowa bazowała na technikach kryptograficznych. Jednym z najsłynniejszych przykładów jest złamanie niemieckiego szyfru Enigma przez polskich kryptologów: Mariana Rejewskiego, Jerzego Różyckiego i Henryka Zygalskiego[10]. Rozwój technologii komunikacyjnych przyczynił się do powstania nowych metod szyfrowania. Polska musiała zmierzyć się z zachodnimi technikami wywiadowczymi, co prowadziło do ciągłego rozwoju systemów kryptograficznych i zabezpieczeń informacyjnych.

Pod koniec XX wieku, wraz z rozpowszechnieniem komputerów i Internetu, kwestia bezpieczeństwa informacyjnego nabrała zupełnie nowego wymiaru. Rok 1991, który wyznacza rozpoczęcie w Polsce ery Internetu był momentem przełomowym w sferze ochrony informacji[11]. Powstanie cyberprzestrzeni stworzyło nowe wyzwania dla bezpieczeństwa informacyjnego państwa. Polska, podobnie jak inne kraje, musiała dostosować swoje systemy ochrony informacji do nowej rzeczywistości cyfrowej. W tym czasie zaczęły powstawać nowoczesne systemy bezpieczeństwa, takie jak firewalle, antywirusy oraz systemy monitorowania sieci, które stały się standardem ochrony informacji w coraz bardziej cyfrowym świecie[12].

Wraz z nadejściem XXI wieku, gwałtownym rozwojem technologii cyfrowych i masowym przetwarzaniem danych zwiększyła się liczba zagrożeń związanych z cyberprzestrzenią. Cyberzagrożenia, które mają bezpośredni wpływ na bezpieczeństwo informacyjne stały się jednym z priorytetowych wyzwań dla państwa. Polska, jako część globalnej infrastruktury cyfrowej, musiała wprowadzić nowe regulacje oraz mechanizmy obrony przed cyberatakami. Powstały instytucje

---

[8] T.R. Aleksandrowicz, *Bezpieczeństwo informacyjne państwa*, Warszawa 2018, s. 2.

[9] *Ibidem*.

[10] M. Grajek, *Enigma i tajemnica złamania szyfru*, https://ciekawostkihistoryczne.pl/2022/12/25/enigma-i-tajemnica-zlamania-szyfru/ [dostęp: 25.10.2024 r.].

[11] NASK, *Internet w Polsce ma 30 lat*, https://www.nask.pl/pl/aktualnosci/4271,Internet-w-Polsce-ma-30-lat.html [dostęp: 14.10.2024 r.].

[12] R. Niechciał, *Co to firewall? – Rodzaje i działanie*, https://vestigio.agency/pl/blog/co-to-firewall/ [dostęp: 29.09.2024 r.].

państwowe, takie jak Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT), które zajmują się monitorowaniem przestrzeni informacyjnej i aktywnym reagowaniem w przypadku wystąpienia bezpośrednich zagrożeń dla użytkowników[13]. Niezwykle ważne stało się również bezpieczeństwo danych osobowych, co doprowadziło do wejścia w życie 10 maja 2018 roku ustawy o ochronie danych osobowych (RODO)[14].

Historia bezpieczeństwa informacyjnego ukazuje ewolucję tego pojęcia od prostych technik zabezpieczania danych w starożytności po zaawansowane systemy cyfrowe. Obecnie przyjmuje się niemal za pewnik, że rewolucja cyfrowa i rozwój nowych narzędzi komunikacji znacząco wpłynęły na codzienne funkcjonowanie tak instytucji i organizacji, jak też jednostek, które zaadaptowały nowe rozwiązania techniczne[15].

Uwarunkowania bezpieczeństwa informacyjnego i jego wpływ na poszczególne dziedziny życia

Gospodarka

Współczesne rynki są mocno uzależnione od przechowywania i wymiany danych – zarówno w kontekście transakcji finansowych, jak i relacji między firmami a ich klientami. Zabezpieczanie tych danych buduje zarówno zaufanie konsumentów, jak i partnerów biznesowych. Skutkiem utracenia ich jest zniszczenie reputacji firm. Przez tego typu zagrożeniom nastąpił wzrost na rynku ubezpieczeń. Firmy coraz częściej sięgają po polisy przeciw cyberatakom, aby uniknąć ich wystąpienia[16]. Dzięki komputerom oraz Internetowi ludzie zyskali możliwość pracy w międzynarodowych firmach, nie musząc wyjeżdżać za granicę. Coraz bardziej popularna staje się też praca zdalna, czyli tak zwany *home office*, który umożliwia pracowanie z domu, bez konieczności przebywania w firmie. Ludzie zyskali również możliwość załatwiania różnych spraw przez Internet, od możliwości robienia zakupów, aż po podpisywanie dokumentów online, przy użyciu elektronicznego podpisu.

Bezpieczeństwo informacyjne wpływa w szczególności na kształtowanie sposobów, jak chronić własną tożsamość, przekazywać wiedzę czy dzielić się twórczością. Technologie cyfrowe umożliwiają też łatwe udostępnianie twórczości,

---

[13] P. Dmitruk, J. Karpowicz, *Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)*, https://www.gov.pl/web/cyfryzacja/zespol-reagowania-na-incydenty-bezpieczenstwa-komputerowego-csirt [dostęp: 04.10.2024 r.].

[14] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r., poz. 1000 ze zm.).

[15] M. du Vall, *Społeczne bezpieczeństwo informacyjne w erze nowych mediów*, Kraków 2017, s. 10.

[16] E. Mika, *Cyberochrona – ubezpieczenie na wypadek utraty danych i naruszenia bezpieczeństwa informacyjnego*, https://www.temidium.pl/artykul/cyberochrona_ubezpieczenie_na_wypadek_utraty_danych_i_naruszenia_bezpieczenstwa_informatycznego, 4810.html?fbclid=IwY2xjaw F7qZNleHRuA2FlbQIxMAABHYGerTCVMn0YyLIfx36dULjHHk5N21wkaUTQN2 mgzd5t_yeGOmPhXMdwg_aem_XxsdpDaOvOzGzXiHg263YA [dostęp: 30.09.2024 r.].

z czym wiążą się zagrożenia takie jak kradzież praw autorskich czy piractwo. W społeczeństwach multikulturowych Internet może być przestrzenią występowania cyberprzemocy, hejtu czy dyskryminacji.

Kultura

Nowe technologie otaczające człowieka nie tylko ułatwiają mu dostęp do informacji, lecz także wyręczają go w myśleniu. Ich natłok prowadzi niekiedy do dezinformacji. Portale plotkarskie często korzystają z fałszywych informacji, wprowadzając społeczeństwo w błąd. Ludzie przesyceni wiedzą pochodzącą z Internetu, radia czy telewizji często nie wiedzą co jest prawdą a co nie[17]. Chcąc uniknąć takich sytuacji dąży się do edukowania obywateli, jak funkcjonować w sieci. Jednak cenzura, dezinformacja czy propagowanie określonych narracji mogą być wykorzystywane do wpływania na opinię publiczną i destabilizację przeciwników. Występowanie tych działań często współgra z cyberatakami, co z kolei prowadzi do wojny informacyjnej. Pandemia COVID-19 częściowo nauczyła ludzi jak poruszać się w sieci. Przez zamknięcie teatrów, kin, oper, filharmonii, muzeów i bibliotek na skutek wirusa społeczeństwo zyskało możliwość oglądania online występów teatralnych, czy koncertów z opery i filharmonii. Dostęp do kultury bez wychodzenia z domu sprawił, że po zakończeniu pandemii zmniejszyła się liczba osób, chcących korzystać z dóbr kulturowych, tak jak przed pandemią. Kultura uległa spłyceniu. Coraz młodsze pokolenia wolą obejrzeć film w Internecie niż iść do kina. Kulturą stało się oglądanie meczów na kanapie i kibicowanie przed telewizorem. Większość nastolatków otwiera tylko zadane im lektury, bo nauczyciel kazał to zrobić i gdyby nie to, to nie sięgnęliby po daną książkę. Część z nich czyta streszczenia i nie otwiera nawet całych tekstów literatury, które mają być omawiane na lekcji.

Zamiast korzystać z papierowych pomocy naukowych uczniowie używają chatu gpt. Jednak dzięki Internetowi ludzie mogą również poszerzać swoją wiedzę, co ułatwiają im aplikacje, takie jak Quizlet, Duolingo, Kahoot czy Memorized. Papierowe książki i gazety również zostają zastępowane przez e-booki i elektroniczne artykuły. Ludzie przesyceni natłokiem wiedzy czytają tylko nagłówki, nie zwracając uwagi na dalszą część. Niedoinformowani często komentują kontrowersyjne tematy w niemiły sposób. Myśląc, że w sieci jest się anonimowym, nadając sobie wulgarne nicki, nie boją się obrażać innych, okazując im brak szacunku.

Polityka

Cały czas zacierają się granice między rynkiem krajowym a zagranicznym[18]. Dzięki rozwojowi technologicznemu państw możliwe jest nawiązywanie współpracy międzynarodowych, sojuszy, jak również rozwój strategii obronnych. Przykładowo Unia Europejska współpracuje z Europejską Agencją Obrony (EDA),

[17] H. Batorowska, *Kultura bezpieczeństwa informacyjnego,* Rzeszów 2018, s. 93-97.
[18] J. Mączyński, *Transfer technologii a gospodarka,* Politechnika Warszawska, Warszawa 2014, s. 127.

która wspiera państwa członkowskie w kształceniu wykwalifikowanych wojskowych zajmujących się cyberobroną[19].

Rozwój środków masowego przekazu sprawia, że politycy muszą uważać na to co mówią i co umieszczają w Internecie, by nie stracić zaufania publicznego. W sytuacji, gdy obywatele mają wątpliwości co do integralności i wiarygodności danych, mogą zacząć kwestionować decyzje polityczne, co może prowadzić do destabilizacji rządu.

Aby chronić duże bazy danych istnieje polityka programowa. Służy ona do tworzenia programu bezpieczeństwa informacji w organizacjach, wyznaczając kierunek dla zabezpieczeń oraz przydziela zasoby, które można wdrożyć do życia[20]. Państwowym instytutem badawczym w Polsce jest NASK, który zajmuje się poszukiwaniem i wdrażaniem rozwiązań służących do rozwoju sieci teleinformatycznych. Instytut prowadzi badania i działalności na rzecz polskiej cywilnej cyberprzestrzeni oraz edukuje i promuje koncepcje społeczeństwa informacyjnego, głównie aby chronić dzieci i młodzież przed zagrożeniami w sieci[21].

Rozporządzenie Ogólne o Ochronie Danych zapewnia Polsce oraz innym państwom należącym do Unii Europejskiej ochronę danych osobowych. Ustanawia również zasady przetwarzania tych danych i obowiązki dla podmiotów przetwarzających je[22]. Polskie organy ścigania oraz wymiaru sprawiedliwości są natomiast wspierane przez Eurojust i Europol. Przynależność do tych Agencji m.in. zwiększa wydajność krajowych organów śledczych i dochodzeniowych w sprawach dotyczących poważnej przestępczości ponadgranicznej oraz zorganizowanej[23]. Współpraca ta pomaga również ścigać przestępstwa związane z terroryzmem i przestępstwa, które naruszają dobro UE, a także gromadzić, analizować i przetwarzać informacje dotyczące osób i czynów naruszających prawo[24].

Społeczeństwo

Świat wirtualny przenika do świata realnego, a komputeryzacja i robotyzacja stały się codziennością. Przez rozwój Internetu i komputerów aktywności społecznej rozwiniętą bazę informacyjną i komunikacyjną. Polega ono również na tym, że ludzie mogą uczestniczyć w produkcji, gromadzeniu i obiegu informacji[25]. Przez rozwój nowych technologii społeczeństwo stało się uzależnione od cyfryzacji.

---

[19] Rada Europejska, *Unijna współpraca w dziedzinie bezpieczeństwa i obrony*, https://www.consilium.europa.eu/pl/policies/defence-security/?fbclid=IwY2xjawF7q2FleHRuA2FlbQIxMAABHf-0wSxGA92f2fQsBe5f5dm4XS8gPBzyJ3ZXzGWwelD2Jah2GzrUqR8Q_aem_AQ6qhcWTn_Q9dRlHny0Nfg#cyber [dostęp: 30.09.2024 r.].

[20] Ministerstwo Cyfryzacji, *Bezpieczeństwo informacji – wprowadzenie NSC 800-12,* s. 53, https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber [dostęp: 30.09.2024 r.].

[21] https://www.nask.pl/ [dostęp: 30.09.2024 r.].

[22] Cyberbezpieczeństwo – dyrektywy UE i wymagania prawne https://ikmj.com/cyberbezpieczenstwo-dyrektywy-ue-i-wymagania-prawne/ [dostęp: 14.10.2024 r.].

[23] https://www.eurojust.europa.eu/about-us/what-we-do [dostęp: 14.10.2024 r.].

[24] Informacje o Europolu, https://www.europol.europa.eu/about-europol:pl [dostęp: 14.10.2024 r.].

[25] P. Alkowski, *Bezpieczeństwo informacyjne- zarys wybranych aspektów w kontekście problemu bezpieczeństwa państwa,* Białystok 2015, s. 87-89.

Przeciążenie informacyjne prowadzi jednak do powierzchowności w przyswajaniu wiedzy pochodzącej z Internetu, co prowadzi do trudności w funkcjonowaniu poza środowiskiem cybernetycznym[26]. Zbyt długi czas spędzony w sieci prowadzi do niechęci funkcjonowania w realnym środowisku, aspołeczności oraz różnych chorób psychicznych, co miało miejsce po pandemii COVID-19[27]. Po prawie 2-letniej izolacji od świata rzeczywistego ludzie m.in. odzwyczaili się od rozmawiania twarzą w twarz. Pracując i ucząc się przed ekranami komputerów zmniejszył się również czas skupienia uwagi na jednej rzeczy przez dłuższy czas. Młodzież, która komunikowała się za pomocą komunikatorów internetowych, wracając do szkół zamiast rozmawiać z rówieśnikami spędza czas patrząc w telefon. Zamiast wyjść na zewnątrz ludzie ci wolą grać w gry komputerowe, które niekiedy porównują do realnego świata. Swoją wiedzę czerpią z social mediów i nie widzą świata poza nimi. Ludzie żyjąc w wirtualnym świecie nie zwracają uwagi co dzieje się wokół nich. Skutkami tego są np. wypadki drogowe spowodowane przez pieszych zapatrzonych w telefon i niewidzących czerwonego światła. Jednak, gdy wydarzy się coś złego ludzie są bardziej skłonni wyciągnąć telefon i zrobić zdjęcie temu zdarzeniu, niż zadzwonić po służby ratunkowe lub samodzielnie udzielić pomocy.

Cyberprzestrzeń w latach 2019–2024

Wybuch pandemii COVID-19 w wysokim stopniu ukazał, jak znaczącą rolę odgrywa Internet dla sprawnego funkcjonowania gospodarki i społeczeństwa państwa. Wprowadzenie krajowych obostrzeń, spowodowanych koniecznością zapewnienia bezpieczeństwa publicznego, w dużej mierze przeniosło życie do przestrzeni wirtualnej. Lockdown z jednej strony sprawił, że ludzie zostali zmuszeni do edukacji oraz pracy online, a z drugiej większość aktywności przeniosła się do świata wirtualnego. Pojawiły się nowe zagrożenia, zwłaszcza w sieci.

W początkowym okresie pandemii odnotowano niebywały wzrost ilości danych przesyłanych przez sieć komputerową. W krajach OECD (*Organisation for Economic Cooperation and Development* – Organizacja Współpracy Gospodarczej i Rozwoju) co trzecia osoba miała w połowie 2021 roku dostęp do łączy szerokopasmowych, w Polsce o blisko 9% więcej niż przed wybuchem pandemii[28].

Agencja GfK w raporcie „#RegionyNEXERY2020" ukazała jak pandemia zmieniła sposób korzystania z sieci. Wyraźnie wydłużył się czas korzystania z Internetu, zdecydowanie więcej osób wykonywało swoją pracę zdalnie. Rozwinęła się telemedycyna czy e-administracja, o 30% wzrosła liczba mieszkańców załatwiających urzędowe sprawy przez Internet. Powszechne stały się rozmowy wideo, coraz więcej osób zaczęło korzystać z bankowości elektronicznej.

---

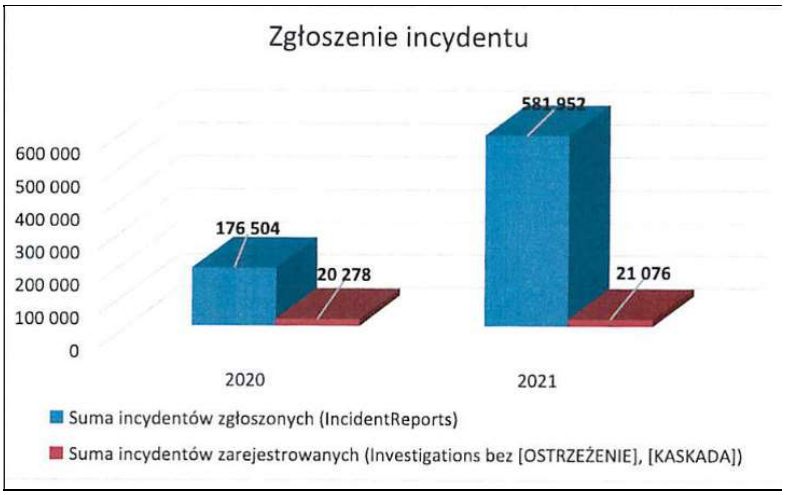
[26] O. Wasiuta, R. Klepka, R. Kopeć, *Vademecum bezpieczeństwa,* Kraków 2018, s. 112-113.

[27] K. Gajda, B. Gierat-Bieroń, *Procesy transformacyjno-reorganizacyjne w sektorze kultury jako odpowiedź na kryzys pandemiczny COVID-19,* Kraków 2021, s. 156-157.

[28] Obserwator Finansowy *Pandemia przyspieszyła rozwój Internetu* https://www.obserwatorfinansowy.pl/bez-kategorii/rotator/pandemia-przyspieszyla-rozwoj-internetu/ [dostęp: 28.09.2024 r.].

Edukacja online nigdy wcześniej nie była stosowana na tak dużą skalę. Połowa uczniów w trakcie izolacji spędzała przed komputerem ponad 6 godzin dziennie. Dla porównania, w czasach przed COVID-19 odsetek dzieci, które spędzały tyle godzin w Internecie wynosił 10,1% w dni robocze oraz 18,8% w dni wolne. Z Internetu w telefonie korzystało natomiast 79% badanych, a w pracy – 46%, o 7 p.p. więcej niż w 2019 roku. Według danych DataReportal już w styczniu 2020 roku w Polsce było 30,63 mln internautów, czyli o 2,3% więcej niż rok wcześniej, a w roku 2021 liczba aktywnych użytkowników Internetu przekroczyła liczbę 4,66 miliarda. Stanowiło to aż 59,5% globalnej populacji.

Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego w okresie od 1 stycznia do 31 października 2021 roku zanotował 581 952 zgłoszonych incydentów, co przełożyło się na 21 076 faktycznych incydentów w systemach teleinformatycznych instytucji administracji rządowej oraz infrastruktury krytycznej.

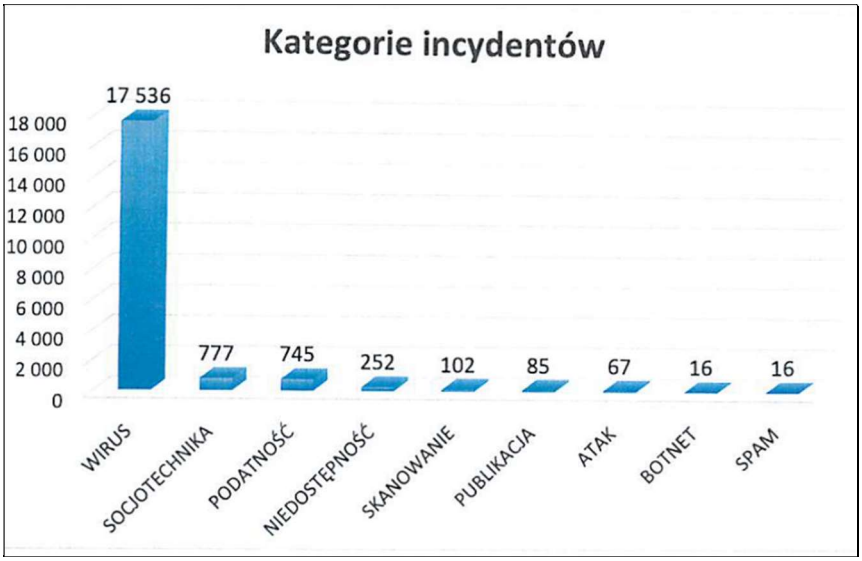


Rys. 1. Liczba zgłoszonych incydentów

Źródło: Rzecznik Prasowy Ministra Koordynatora Służb Specjalnych, *Zagrożenia w cyberprzestrzeni,* https://www.gov.pl/web/sluzby-specjalne/zagrozenia-w-cyberprzestrzeni [dostęp: 30.09.2024 r.].

W stosunku do roku 2020 jest to znaczący, ponad trzykrotny, wzrost liczby incydentów zgłoszonych (w 2020 roku – 176 504), przy jednoczesnym utrzymaniu się liczby faktycznych incydentów na porównywalnym poziomie. Różnica w liczbie zarejestrowanych incydentów wynika przede wszystkim z rosnących możliwości wykrycia systemu wczesnego ostrzegania o zagrożeniach w sieci Internet ARAKIS GOV, co przekłada się na rejestrowanie większej liczby zdarzeń.

Najliczniejszą grupę zgłaszanych incydentów stanowiły wirusy – ponad 17,5 tys. zgłoszeń. Zgłoszenia te mogą świadczyć o uszkodzeniu systemu antywirusowego w instytucji administracji państwowej lub u operatora infrastruktury krytycznej. Do drugiej kategorii najczęściej identyfikowanych incydentów zaliczamy zagrożenia związane z zastosowaniem socjotechniki. Są to między innymi ataki i kampanie phisingowe. W sumie zanotowano 777 takich incydentów. Trzecią grupą pod względem liczności incydentów jest „podatność" (745 zgłoszonych incydentów), rozumiana jako słabość systemu teleinformatycznego, błędy konfiguracyjne oraz brak odpowiedniej polityki bezpieczeństwa związanej z aktualizacją oraz weryfikacją poprawnie wdrożonych rozwiązań teleinformatycznych.

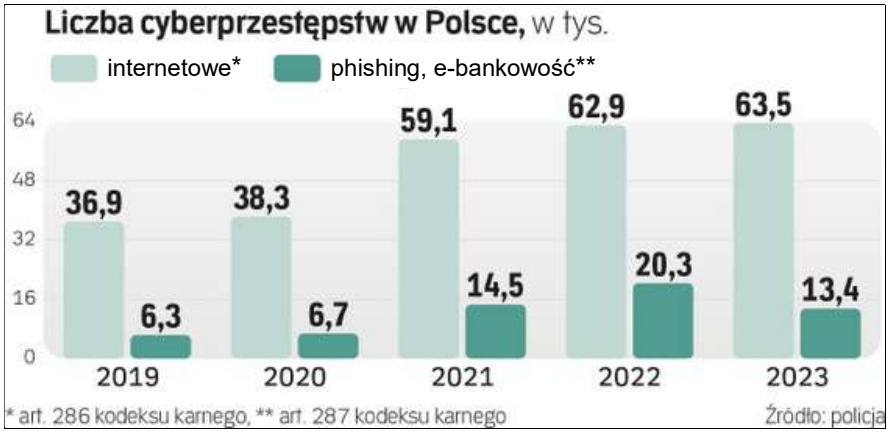


Rys. 2. Kategorie incydentów

Źródło: Rzecznik Prasowy Ministra Koordynatora Służb Specjalnych *Zagrożenia…, op. cit.*

Specjaliści zwracają uwagę, że z roku na rok notujemy coraz większą liczbę cyberprzestępstw w Polsce. Według policyjnych danych dotyczących zdarzeń popełnianych z art. 267 (bezprawne uzyskanie informacji), 286 (oszustwo) i 287 (oszustwo komputerowe) kodeksu karnego, w 2023 roku w Polsce stwierdzono prawie 83 tys. cyberprzestępstw. W ciągu ostatnich pięciu lat liczba cyberprzestępstw wzrosła o 72 %, w 2019 roku było ich „zaledwie" 48,1 tys., dwa lata później już niemal 79 tys., a najwięcej (88,5 tys.) w 2022 roku. W 2023 roku liczba cyberprzestępstw spadła o ponad 6% wobec 2022 roku. Za ten spadek odpowiada wyraźnie mniejsza liczba zdarzeń z art. 287 (phishing, e-bankowość). W 2022 roku było ich ponad 20 tys., a w 2023 roku 13,4 tys.

Dane na rysunku 3. dotyczą liczby cyberprzestępstw w zakresie art. 286 i art. 287 k.k.



Rys. 3. Liczba cyberprzestępstw w Polsce

Źródło: K. Kucharczyk *Zaskakujące dane o atakach hakerskich w Polsce* https://www.rp.pl/biznes/art39842121-zaskakujace-dane-o-atakach-hakerskich-w-polsce [dostęp: 15.02.2024 r.].

Jednym z najpoważniejszych zagrożeń we współczesnym cyfrowym świecie jest wyciek danych. Utrata poufnych informacji może mieć katastrofalne skutki zarówno dla osób prywatnych, jak i całych organizacji. Wyciek danych oznacza, że dane użytkowników z różnych serwisów internetowych zostały upublicznione.

Ile procent Polaków spotkało się w ostatnim roku z próbą wyłudzenia ich danych? Wycieku danych obawia się 40% dorosłych Polaków. W badaniu z „Wiedza na temat bezpieczeństwa ochrony danych osobowych w Polsce"[29] niemal 33% respondentów zadeklarowało, że w ciągu ostatnich 12 miesięcy spotkało się z próbą wyłudzenia ich danych przez fałszywy telefon, SMS lub e-mail, a 25% oznajmiło, że takiej sytuacji doświadczył ich znajomy bądź członek rodziny. Jednocześnie 12,4% badanych przyznało, że oszustom udało się wyłudzić takim sposobem ich dane. 13,1% Polaków mierzyło się z wyciekiem danych z prywatnych firm (7,5%) i instytucji publicznych (5,6%). Podobnie wskazywali w odniesieniu do swoich rodzin i znajomych. 22% ankietowanych osób tak naprawdę nie ma pewności co do tego, czy ich dane nie trafiły tą drogą w ręce przestępców.

Jak wynika ze statystyk Urzędu Ochrony Danych Osobowych, cytowanych w badaniu, liczba zgłaszanych naruszeń ochrony danych osobowych w ostatnich latach rośnie. W 2022 roku do UODO zgłoszono niemal 13 tys. takich przypadków, a dwa lata wcześniej – 7,5 tys. Rzeczywista skala zagrożenia bezpieczeństwa danych osobowych jest jednak znacznie wyższa – uważają eksperci serwisu ChronPESEL.pl.

Użytkownicy Internetu nie przestrzegają podstawowych zasad pracy w sieci, np. nie sprawdzają autentyczności e-maili i linków, w które klikają. Choć jak oceniają eksperci ogromna większość – 86% – deklaruje, że potrafi rozpoznać

[29] Dane z serwisu ChronPESEL.pl i Krajowego Rejestru Długów (KRD).

fałszywą wiadomość bądź telefon, w którym ktoś powołuje się na znaną instytucję lub firmę, to jednak absolutnie pewnych tego faktu jest zaledwie 18,5% ankietowanych[30].

Raport IBM pokazuje, że organizacje wdrażające nową technologię charakteryzują się krótszym czasem reakcji i niższymi kosztami naruszenia bezpieczeństwa danych. Obrona cyberbezpieczeństwa oparta na sztucznej inteligencji, skraca czas wykrycia i ograniczenia naruszeń do 249 dni[31]. W organizacjach wykorzystujących AI oraz automatyzację czas trwania naruszenia danych był o 108 dni krótszy w porównaniu do badanych organizacji, które nie wdrożyły wspomnianych technologii[32].

Współczesne problemy wymagają nowoczesnych rozwiązań – można wykorzystać sztuczną inteligencję bezpieczeństwa do wykrywania i powstrzymywania ataków phishingowych, gdy tylko zainfekowane e-maile dotrą do skrzynek odbiorczych pracowników. Zaawansowane funkcje sztucznej inteligencji, takie jak analiza wiadomości, mogą identyfikować szkodliwe treści na podstawie wielu punktów porównania w celu zwiększenia skuteczności. Włączenie pracowników w środki cyberbezpieczeństwa daje większą szansę na odparcie cyberzagrożeń oraz daje możliwości obronne i może zapobiec kosztownym naruszeniom bezpieczeństwa danych.

Wnioski końcowe

Wpływ technologii na bezpieczeństwo informacyjne w Polsce jest wielowymiarowy i dynamiczny. Internet oferuje nieograniczone możliwości rozwoju. Z drugiej strony rozwijające się środowisko cyberprzestrzeni jest idealnym miejscem dla przestępców internetowych, którzy wraz z postępem technologicznym są coraz bardziej efektywni i posiadają dostęp do coraz pilniej strzeżonych danych. Odpowiednio wczesna reakcja na liczbę wyzwań w cyberprzestrzeni może umocnić nie tylko bezpieczeństwo informacyjne, a co za tym idzie – bezpieczeństwo narodowe. Współczesne problemy wymagają nowoczesnych rozwiązań – można wykorzystać AI bezpieczeństwa do wykrywania i powstrzymywania ataków phishingowych, gdy tylko zainfekowane e-maile dotrą do skrzynek odbiorczych pracowników. Zaawansowane funkcje sztucznej inteligencji, takie jak analiza wiadomości, mogą identyfikować szkodliwe treści na podstawie wielu punktów porównania w celu zwiększenia skuteczności.

---

[30] Polska Agencja Prasowa *Eksperci: 40 proc. dorosłych Polaków obawia się wycieku danych osobowych,* https://www.pap.pl/aktualnosci/eksperci-40-proc-doroslych-polakow-obawia-sie-wycieku-danych-osobowych [dostęp: 14.10.2024 r.].

[31] Z. Amos *Jak sztuczna inteligencja zmniejsza koszty naruszenia danych,* https://www.unite.ai/pl/how-ai-reduces-the-cost-of-a-data-breach/ [dostęp: 23.09.2024 r.].

[32] M. Marszycki *Raport IBM: Średni, globalny koszt naruszenia danych sięgnął 4,45 miliona dolarów,* https://itwiz.pl/raport-ibm-sredni-globalny-koszt-naruszenia-danych-siegnal-445-miliona-dolarow/ [dostęp: 6.09.2024 r.].

Wdrażanie nowoczesnych narzędzi oraz stałe doskonalenie procedur ochronnych stanowi fundament skutecznej obrony przed cyberzagrożeniami. Pozwala to szybciej wykrywać niebezpieczeństwa, minimalizując ryzyko poważnych incydentów. Bezpieczeństwo informacji to nie tylko kwestia technologii, ale również edukacji i ciągłego doskonalenia wszystkich użytkowników i instytucji. Włączenie pracowników w środki cyberbezpieczeństwa daje większą szansę na odparcie cyberzagrożeń oraz daje możliwości obronne i może zapobiec kosztownym naruszeniom bezpieczeństwa danych.

Bibliografia

Aleksandrowicz T.R., *Bezpieczeństwo informacyjne państwa*, Warszawa 2018.

Alkowski P., *Bezpieczeństwo informacyjne – zarys wybranych aspektów w kontekście problemu bezpieczeństwa państwa*, Białystok 2015.

Batorowska H., *Kultura bezpieczeństwa informacyjnego*, Rzeszów 2018.

Bobowski B., *Testament w średniowiecznym prawie polskim*, Częstochowa 2009.

du Vall M., *Społeczne bezpieczeństwo informacyjne w erze nowych mediów*, Kraków 2017.

Gajda K., Gierat-Bieroń B., *Procesy transformacyjno-reorganizacyjne w sektorze kultury jako odpowiedź na kryzys pandemiczny COVID-19*, Kraków 2021.

Grzebiela K., *Pojęcie i istota bezpieczeństwa informacyjnego*, Kraków 2018.

Karbowski M., *Podstawy kryptografii*, wyd. II, Gliwice 2008.

Mączyński J., *Transfer technologii a gospodarka*, Politechnika Warszawska, Warszawa 2014.

Wasiuta O., Klepka R., Kopeć R., *Vademecum bezpieczeństwa*, Kraków 2018.

Akty normatywne

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018, poz. 1000 ze zm.).

Netografia

Amos Z., *Jak sztuczna inteligencja zmniejsza koszty naruszenia danych*, https://www.unite.ai/pl/how-ai-reduces-the-cost-of-a-data-breach/.

Cyberbezpieczeństwo – dyrektywy UE i wymagania prawne, https://ikmj.com/cyberbezpieczenstwo-dyrektywy-ue-i-wymagania-prawne/.

Dane z serwisu ChronPESEL.pl i Krajowego Rejestru Długów (KRD).

Dmitruk P., Karpowicz J., *Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)*, https://www.gov.pl/web/cyfryzacja/zespol-reagowania-na-incydenty-bezpieczenstwa-komputerowego-csirt.

Grajek M., *Enigma i tajemnica złamania szyfru,* https://ciekawostkihistoryczne.pl/2022/12/25/enigma-i-tajemnica-zlamania-szyfru/.

Informacje o Europolu, https://www.europol.europa.eu/about-europol:pl.

Marszycki M., *Raport IBM: Średni, globalny koszt naruszenia danych sięgnął 4,45 miliona dolarów*, https://itwiz.pl/raport-ibm-sredni-globalny-koszt-naruszenia-danych-siegnal-445-miliona-dolarow/.

Mika E., *Cyberochrona- ubezpieczenie na wypadek utraty danych i naruszenia bezpieczeństwa informacyjnego*, https://www.temidium.pl/artykul/cyberochrona_ubezpieczenie_na_wypadek_utraty_danych_i_naruszenia_bezpieczenstwa_informatycznego-4810.html?fbclid=

IwY2xjawF7qZNleHRuA2FlbQIxMAABHYGerTCVMn0YyLIfx36dULjHHk5-N21wka UTQN2mgzd5t_yeGOmPhXMdwg_aem_XxsdpDaOvOzGzXiHg263YA.

Ministerstwo Cyfryzacji, *Bezpieczeństwo informacji – wprowadzenie NSC 800-12,* https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber.

NASK, *Internet w Polsce ma 30 lat*, https://www.nask.pl/pl/aktualnosci/4271,Internet-w-Polsce-ma-30-lat.html.

Niechciał R., *Co to firewall? – Rodzaje i działanie*, https://vestigio.agency/pl/blog/co-to-firewall/.

Polska Agencja Prasowa, *Eksperci: 40 proc. dorosłych Polaków obawia się wycieku danych osobowych* https://www.pap.pl/aktualnosci/eksperci-40-proc-doroslych-polakow-obawia-sie-wycieku-danych-osobowych.

Rada Europejska, *Unijna współpraca w dziedzinie bezpieczeństwa i obrony*, https://www.consilium.europa.eu/pl/policies/defence-security/?fbclid=IwY2xjawF7q2FleH-RuA2FlbQIxMAABHf-0wSxGA92f2fQsBe5f5-dm4XS8gPBzyJ3ZXzGWwelD2Jah2 Gzr-UqR8Q_aem_AQ6qhcWTn_Q9dRlHny0Nfg#cyber.

https://www.nask.pl/.

Obserwator Finansowy *Pandemia przyspieszyła rozwój Internetu* https://www.obserwator-finansowy.pl/bez-kategorii/rotator/pandemia-przyspieszyla-rozwoj-internetu/.

Julia MAZURKIEWICZ[1]

ROLA I ZADANIA CENTRALNEGO BIURA ZWALCZANIA CYBERPRZESTĘPCZOŚCI W PRZECIWDZIAŁANIU WSPÓŁCZESNYM ZAGROŻENIOM CYBERNETYCZNYM

Wstęp

Cyberprzestępczość, zwana również przestępczością cybernetyczną, odnosi się do wszelkich zabronionych działań popełnionych w przestrzeni przetwarzania i wymiany informacji, tworzonej przez systemy teleinformatyczne[2], czyli w cyberprzestrzeni. Zgodnie z definicją wprowadzoną przez rząd Wielkiej Brytanii, cyberprzestrzeń to „wirtualna przestrzeń wszystkich systemów technologii informacyjnej powiązanych na poziomie danych w skali globalnej”[3]. Według Białej Księgi Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej opublikowanej 24 maja 2013 roku w przyszłości zagrożenie cyberprzestępczością będzie się nieustannie zwiększać. Ataki cybernetyczne mogą zostać przeprowadzone zarówno przez władze i służby państw wrogich, gotowych wypowiedzieć wojnę informacyjną, jak też przez wielkie koncerny, organizacje o charakterze pozarządowym i ponadnarodowym, w tym przestępcze, grupy aktywistów, nieformalne grupy użytkowników Internetu, a nawet indywidualnych użytkowników[4].

Po ponad 10 latach od opublikowania Białej Księgi zjawisko to jest jednym z najniebezpieczniejszych i najbardziej skutecznych działalności przestępczych. Z uwagi na stale rozwijającą się cyfryzację i digitalizację, skala zagrożenia związana z cyberprzestępczością każdego roku nieustannie wzrasta, co szczegółowo pokazują statystyki CERT Państwowego Instytutu Badawczego NASK[5]. Do najczęstszych form tej aktywności internetowej zaliczyć można ataki hackerskie,

---

[1] Uniwersytet im. Andrzeja Frycza Modrzewskiego w Krakowie, Wydział Prawa, Administracji i Stosunków Międzynarodowych. ORCID: 0009-0007-3372-1874.

[2] Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego – *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa 2013, s. 5.

[3] M. Pomykała, I. Oleksiewicz, *Zagrożenia i wyzwania bezpieczeństwa w cyberprzestrzeni*, Rzeszów 2024, s. 5.

[4] M. Wróbel, *Cyberprzestępczość w polskim systemie prawnym*, „Wiedza Obronna” 2014, nr 4, s. 73.

[5] https://www.gov.pl/web/baza-wiedzy/krajobraz-bezpieczenstwa-polskiego-internetu-w-2022-roku--raport-roczny-cert-polska [dostęp: 09.10.2024 r.].

kradzież tożsamości i danych osobowych oraz szeroko rozumiane oszustwa internetowe. W dzisiejszych czasach, gdy coraz więcej aspektów naszego życia przenosi się do przestrzeni cyfrowej [...], cyberbezpieczeństwo nie jest już tylko kwestią techniczną, ale także społeczną i gospodarczą. Digitalizacja wszystkich dziedzin współczesnego życia, powszechny dostęp do Internetu i nieograniczona liczba sieci komunikacyjnych ułatwiają różnorodne działania przestępcze, zwłaszcza przestępstwa majątkowe, gospodarcze, narkotykowe i pedofilskie. Nowe technologie dostarczają nowych narzędzi do popełniania przestępstw, choć same mogą być ich celem. Bez odpowiedniej ochrony w tym obszarze zarówno osoby fizyczne, jak i organizacje mogą ponieść poważne straty finansowe i reputacyjne. Zrozumienie cyberbezpieczeństwa stale się rozwija. Jest to niewątpliwie kluczowy element bezpieczeństwa państwa i wymaga stałego zaangażowania i szczególnej uwagi ze stron wielu podmiotów[6]. W obliczu narastającego zagrożenia państwo regularnie podejmuje kroki mające na celu zwiększenie ochrony w tym obszarze. Jednym z kluczowych działań, jakie podjęto w walce z cyberprzestępczością, było utworzenie w 2021 roku Centralnego Biura Zwalczania Cyberprzestępczości. Takie inicjatywy pozwalają państwu umacniać i rozwijać zdolności w zakresie cyberbezpieczeństwa i dostosowywać się do wyzwań, jakie niesie za sobą obecna era Internetu.

Struktura CBZC i podstawy działania

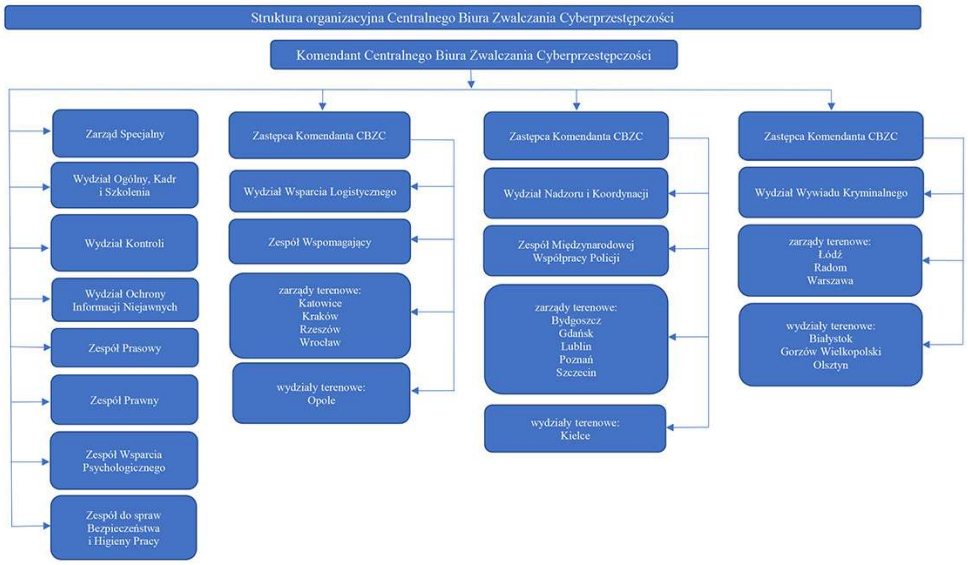
Centralne Biuro Zwalczania Cyberprzestępczości (CBZC) jest jednostką organizacyjną Policji służby zwalczania cyberprzestępczości, odpowiedzialną za realizację na obszarze całego kraju zadań w zakresie:

1) rozpoznawania i zwalczania przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej oraz zapobiegania tym przestępstwom, a także wykrywania i ścigania sprawców tych przestępstw,
2) wspierania w niezbędnym zakresie jednostek organizacyjnych Policji w rozpoznawaniu, zapobieganiu i zwalczaniu przestępstw, o których mowa w pkt 1, a także wykrywaniu i ściganiu sprawców tych przestępstw[7].

Kierownictwo CBZC stanowią Komendant CBZC, Zastępcy Komendanta CBZC oraz kierownicy komórek organizacyjnych oraz zarządów i wydziałów terenowych. Poniżej znajduje się schemat struktury jednostki CBZC.

[6] M. Pomykała, *The Central Cybercrime Bureau as a new police service established to combat cybercrime,* "Humanities and Social Sciences" 2024, Vol. 31, No. 2, s. 132.

[7] Art. 5d ustawy z dnia 6 kwietnia 1990 r. o Policji (Dz.U. z 1990 r., nr 30, poz. 179).



Rys. 1. Struktura CBZC

Źródło: https://cbzc.policja.gov.pl/bzc/o-cbzc/struktura/58,Schemat-organizacyjny-CBZC.html.

Należy jednak podkreślić, że nie jest to pierwsza jednostka Policji powołana do walki z cyberprzestępczością. Już w 2016 roku w strukturze Komendy Głównej Policji utworzono Biuro, któremu powierzono prowadzenie działań związanych z wykrywaniem sprawców przestępstw popełnionych z wykorzystaniem nowoczesnych technologii teleinformatycznych. [...]. Takie struktury Policji funkcjonowały do końca 2021 roku, a zakres ich zadań regularnie się zwiększał. Szczególnym okresem był z pewnością czas pandemii COVID-19, której pierwszy etap przypadł na lata 2020–2021, kiedy to w związku z wprowadzeniem powszechnej izolacji, większa niż dotychczas aktywność społeczna skoncentrowała się w sieci, znacząco zwiększając poziom zagrożenia cyberprzestępczością[8].

Dnia 27 lipca 2021 roku do sejmu wpłynął projekt ustawy powołującej powstanie Centralnego Biura Zwalczania Cyberprzestępczości. Przez kolejne miesiące przygotowywane były rozwiązania organizacje i prawne związane z planowanym utworzeniem tej organizacji. Właściwym początkiem powstania CBZC były daty: 12 stycznia 2022 roku, kiedy to weszła w życie ustawa z dnia 17 grudnia 2021 roku o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości oraz 12 lipca 2022 roku, czyli dzień powołania do instytucji policjantów pełniących służbę w komórkach ds. zwalczania cyberprzestępczości w KGP i w komendach wojewódzkich.

[8] M. Pomykała, *The Central..., op.cit.,* s. 133.

Rodzaje zagrożeń w cyberprzestrzeni

W cyberprzestrzeni występują różnorodne zagrożenia, które Konwencja Rady Europy o cyberprzestępczości ujmuje w cztery kategorie:

- pierwsza obejmuje przestępstwa przeciwko poufności, integralności i dostępności danych informatycznych i systemów, takie jak ataki DDoS lub instalowanie złośliwego oprogramowania,
- druga kategoria to przestępstwa komputerowe, w tym oszustwa i fałszowanie danych w celu osiągnięcia korzyści majątkowych,
- trzecia dotyczy przestępstw wynikających z charakteru zawartych informacji, np. nielegalnej dystrybucji materiałów zakazanych,
- czwarta kategoria obejmuje przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych, takie jak nielegalne udostępnianie chronionych utworów w Internecie[9].

W kontekście rozwijającej się cyfryzacji życia społecznego i gospodarczego, zagrożenia w cyberprzestrzeni stają się coraz bardziej skomplikowane i trudne do zwalczania. Celem ww. konwencji jest pomoc w walce z przestępstwami, które mogą być popełnione wyłącznie przy użyciu technologii, w przypadku których urządzenia są zarówno narzędziem popełnienia przestępstwa, jak i ich celem oraz przestępstwami, w których technologia została wykorzystana do realizacji innego przestępstwa, takiego jak oszustwo. Zawiera wytyczne dla każdego państwa opracowującego krajowe przepisy dotyczące cyberprzestępczości i służy jako podstawa międzynarodowej współpracy między stronami konwencji. Jej celem jest zapewnienie wspólnych zasad na poziomie międzynarodowym w celu zacieśnienia współpracy w zakresie cyberprzestępczości i gromadzenia dowodów w formie elektronicznej na potrzeby dochodzeń lub postępowań karnych[10].

Przykładem przestępstwa komputerowego jest oszustwo nigeryjskie (ang. *nigerian scam*). Jest to oszustwo internetowe polegające na wyłudzeniu pieniędzy pod pretekstem fałszywej obietnicy o zyskach, jakie mogą otrzymać osoby wpłacające niekiedy ogromne sumy pieniędzy na konta osób podających się za majętne lub wysoko postawione w klasie społecznej.

Nazwa odnosi się do wielości oszustw realizowanych w Nigerii. Najczęstszy schemat oszustwa nigeryjskiego polega na kontakcie z potencjalną ofiarą przez wiadomość tekstową na portalach społecznościowych, gdzie przedstawiana jest jej historia osoby, która ma problem z uzyskaniem dostępu do swojego majątku, tym samym przekonując ofiarę do pomocy w transferze niebotycznych sum pieniędzy, które rzekomo należeć mają do osoby kontaktującej się. Ofiara pomagając, poprzez wpłacanie określonych sum pieniędzy na konto oszusta, przekonana jest o słuszności swoich czynów, co prowadzić może do powstania procederu

[9] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2015 r., poz. 728).

[10] https://eur-lex.europa.eu/PL/legal-content/summary/convention-on-cybercrime.html [dostęp: 12.11.2024 r.].

w postaci regularnie wypłacanych kwot przy okazji nowo powstałych problemów u osoby kontaktującej się[11].

Natomiast przykładem przestępstw wynikających z charakteru zawartych informacji są przestępstwa internetowe o podłożu seksualnym. Dnia 7 listopada 2024 roku na stronie CBZC pojawiła się informacja związana z operacją „ENOLA GAY", w wyniku której zatrzymano 75 osób w wieku od 16 do 78 lat, które podejrzane są o posiadanie, rozpowszechnianie i produkowanie materiałów przedstawiających seksualne wykorzystywanie małoletnich osób. Policjanci zarekwirowali różnego rodzaju sprzęt cyfrowy zawierający ponad milion plików przedstawiających seksualne wykorzystanie małoletnich. Ujawniono również, w jakiej liczbie zdjęcia zostały zabezpieczone. U jednego z podejrzanych znaleziono 430 tys. zdjęć z treściami pedofilskimi, a u innego około 150 tys. nagrań. Walka z przestępcami dotyczącymi wykorzystywania dzieci w Internecie jest jednym z priorytetowych zadań policjantów CBZC[12].

Korelacje i współpraca CBZC z innymi instytucjami

Instytucja Centralnego Biura Zwalczania Cyberprzestępczości podejmuje współpracę zarówno z krajowymi, jak i międzynarodowymi organizacjami. Współpraca ta jest kluczowa w kwestii zwalczania cyberprzestępczości, gdyż ma ona charakter globalny i międzyinstytucjonalny. CBZC jest częścią polskiej Policji, więc współpracuje ściśle z innymi jej jednostkami, w szczególności z wydziałami zajmującymi się przestępczością gospodarczą i kryminalną. Na poziomie krajowym instytucja ta współpracuje również z prokuraturą, w związku z prowadzeniem śledztw w przestrzeni internetowej. CBZC kooperuje z Państwowym Instytutem Badawczym NASK, który realizowany jest poprzez; wymianę informacji o technikach i sposobach działań przestępców, a także skali ich występowania w zakresie spraw obsługiwanych przez CSIRT (*Computer Security Incident Response Team*) NASK, o ile nie są one objęte żadną ze znanych NASK tajemnic prawnie chronionych; wymianę doświadczeń i pomysłów w tworzeniu oraz użytkowaniu technologii informatycznych – sprzętowych i programowych; nieodpłatne użyczenie technologii informatycznych – sprzętowych i programowych, wspomagających pracę funkcjonariuszy i pracowników CBZC; realizację wspólnych projektów i przedsięwzięć związanych ze zwalczaniem cyberprzestępczości, działań prewencyjnych oraz szkoleń; podejmowanie wspólnych przedsięwzięć edukacyjnych, profilaktycznych oraz informacyjnych, wynikających z bieżących potrzeb[13].

[11] https://cbzc.policja.gov.pl/bzc/zagrozenia-w-sieci [dostęp: 30.10.2024 r.].

[12] https://cbzc.policja.gov.pl/bzc/aktualnosci/433,Krzywdzili-dzieci-zostali-zatrzymani-przez-policjantow-CBZC.html [dostęp: 11.11.2024 r.].

[13] https://www.nask.pl/pl/aktualnosci/5258,Wspolpraca-miedzy-NASK-a-CBZC-podpisano-specjalne-porozumienie.html [dostęp: 11.11.2024 r.].

Zgodnie z raportem z działalności CBZC z 2023 roku instytucja ta pomagała przy realizacji 440 czynności wykonanych dla Centralnego Biura Śledczego, Komendy Wojewódzkiej Policji, Komendy Miejskiej Policji oraz Komendy Powiatowej Policji. Przy czynnościach związanych z zagrożeniem życia i zdrowia ludzkiego CBZC współpracuje z Biurem Rzecznika Praw Dziecka, Dyżurnet.pl NASK, Fundacją Dajemy Dzieciom Siłę, Niebieską Linią, Towarzystwem Przyjaciół Dzieci oraz innymi organizacjami, których zadania powiązane są z udzieleniem pomocy osobom w kryzysie[14].

Podczas spotkania, które miało miejsce w dniu 6 grudnia 2021 roku w Komendzie Głównej Policji uczestnicy spotkania zwrócili uwagę na fakt, że cyberprzestępczość jest jednym z najdynamiczniej rozwijających się obszarów przestępczości, który wymaga szczególnej uważności i zaadresowania ze strony organów ścigania. W związku z ówcześnie nowo powstałą instytucją CBZC i stanowiskiem Zgromadzenia Ogólnego Interpolu w sprawie ograniczenia globalnego wpływu cyberprzestępczości oraz ochrony społeczności dla zapewnienia bezpieczniejszego świata, polska Policja i Interpol zacieśnili współpracę w walce z cyberprzestępczością. Obie strony zapewniły o swojej gotowości do współpracy, wymiany doświadczeń oraz woli podejmowania wspólnych inicjatyw na rzecz budowy i wzmacniania bezpieczeństwa cyfrowego[15]. Kolejnym przykładem współpracy międzynarodowej jest Międzynarodowa Współpraca CBZC z organami ścigania Ukrainy. Biuro Bezpieczeństwa Gospodarczego Ukrainy (*Economic Security Bureau of Ukraine*) w ramach zleconej międzynarodowej pomocy prawnej zainicjowanej poprzez wspólne działania Prokuratury Regionalnej w Rzeszowie oraz Zarządu w Rzeszowie Centralnego Biura Zwalczania Cyberprzestępczości, zrealizowało przeszukania na terenie Ukrainy, w ramach których dokonano likwidacji biura Call Center, związanego ze środowiskiem platform inwestycyjnych, dokonujących oszustw na szkodę obywateli Rzeczypospolitej Polskiej. Pracownicy nielegalnych platform inwestycyjnych działali pod pozorem możliwości realizacji szybkich i korzystnych inwestycji na rynkach finansowych m.in. w kryptowaluty oraz pozostałe waluty rynkowe[16].

Funkcje CBZC w zakresie przeciwdziałania cyberprzestępczości

Instytucja Centralnego Biura Zwalczania Cyberprzestępczości poza działaniami represyjnymi podejmuje działania prewencyjne, tj. monitorowanie zagrożeń w cyberprzestrzeni, podnoszenie świadomości i edukacja społeczeństwa poprzez

[14] wyniki_statystyczne_centralnego_biura_zwalczania_cyberprzeste__pczos__ci_za_2023_rok.pdf [dostęp: 11.11.2024 r.].

[15] https://www.policja.pl/pol/aktualnosci/211523,Polska-Policja-i-INTERPOL-zaciesniaja-wspolprace-w-walce-z-cyberprzestepczoscia.html [dostęp: 13.11.2024 r.].

[16] https://cbzc.policja.gov.pl/bzc/aktualnosci/388,Miedzynarodowa-wspolpraca-CBZC-z-organami-scigania-Ukrainy-pozwolila-na-likwidac.html [dostęp: 13.11.2024 r.].

kampanie społeczne, szkolenia dla poszczególnych instytucji oraz doradztwo w zakresie cyberprzestrzeni. W ramach realizacji „Programu wzmacniania uczciwości i zapobiegania korupcji w Policji na lata 2021–2023" w CBZC powołany został doradca do spraw etyki. Do jego najistotniejszych zadań należy w szczególności prowadzenie działań; doradczych w sytuacjach wątpliwych etycznie, związanych z wykonywaniem zadań służbowych przez policjantów i pracowników CBZC; informacyjno-edukacyjnych mających na celu podnoszenia świadomości etycznej oraz promowanie uczciwości wśród policjantów CBZC; informacyjno-edukacyjnych mających na celu podnoszenia świadomości w zakresie przestrzegania zasad służby cywilnej oraz w sprawie zasad etyki korpusu służby cywilnej[17].

Natomiast w zakresie tegorocznej kampanii Europejskiego Miesiąca Cyberbezpieczeństwa (*European Cyber Security Month* – ECSM) NASK-PIB we współpracy z Centralnym Biurem Zwalczania Cyberprzestępczości przygotował kampanię informacyjną poświęconą problemowi „mułów finansowych" – osób wykorzystywanych przez cyberprzestępców do prania pieniędzy pochodzących z nielegalnych działań. Celem zaplanowanych działań jest zwiększenie świadomości społeczeństwa na temat zagrożeń związanych z tego typu oszustwami w sieci oraz zwrócenie uwagi na socjotechniki, które przestępcy stosują do manipulowania[18]. Przeprowadzono również debatę pt. „Cyberbezpieczeństwo – Bądź Bezpieczny w Sieci", skierowaną do młodzieży. Poruszona została na niej problematyka odpowiedzialności prawnej osób nieletnich zwłaszcza w kontekście cyberprzemocy oraz zagrożeń wynikających z codziennego użytkowania sieci[19]. Dodatkowo CBZC wraz z NASK – Państwowym Instytutem Badawczym oraz Warszawskim Instytutem Bankowości przygotowały kompleksowy poradnik „#Halo! Tu cyberbezpieczny Senior!", który zawiera praktyczne wskazówki, przykłady działań oszustów i liczby obrazujące skalę zagrożeń[20].

Na stronie internetowej CBZC regularnie publikowane są rezultaty akcji policyjnych, których głównym celem jest przestrzeżenie społeczeństwa przed coraz to nowszymi formami cyberataków. Prokurator z podkarpackiego pionu PZ PK w dniu 30 października 2024 roku skierował do Sądu Okręgowego w Rzeszowie akt oskarżenia w sprawie udziału w zorganizowanej grupie przestępczej mającej na celu popełnianie oszustw internetowych związanych z oferowaniem zakupu w walucie kryptograficznej Bitcoin za pośrednictwem platform internetowych oraz prania brudnych pieniędzy przeciwko obywatelowi Gruzji i obywatelce Ukrainy. Akt oskarżenia jest efektem śledztwa prowadzonego przez zespół powołany Zarządzeniem Zastępcy Prokuratora Generalnego do Spraw Przestępczości

[17] https://cbzc.policja.gov.pl/bzc/o-cbzc/doradca-do-spraw-etyki/53,Doradca-do-spraw-etyki-w-CBZC.html [dostęp: 13.11.2024 r.].

[18] https://cbzc.policja.gov.pl/bzc/aktualnosci/424,Kampania-o-mulach-finansowych.html [dostęp: 13.11.2024 r.].

[19] https://cbzc.policja.gov.pl/bzc/aktualnosci/432,Cyberprofilaktyczne-spotkania.html [dostęp: 13.11.2024 r].

[20] https://bezpiecznymiesiac.pl/bm/aktualnosci/1425,Poradnik-Halo-Tu-cyberbezpieczny-Senior-Podaruj-bliskim-wiedze-i-spokoj-z-okazji.html [dostęp: 14.11.2024 r.].

Zorganizowanej i Korupcji z dnia 6 września 2023 roku, nr 20/23 złożony z prokuratorów podkarpackiego pionu PZ PK oraz funkcjonariuszy Zarządu w Rzeszowie Centralnego Biura Zwalczania Cyberprzestępczości[21]. Jest to jedna ze spraw, której rezultaty regularnie publikowane są na stronie CBZC w celu przestrzeżenia społeczeństwa przed coraz to nowszymi formami cyberataków i ukazaniem jakości i szybkości działań instytucji państwowych.

Analiza działań CBZC na przestrzeni lat

Centralne Biuro Zwalczania Cyberprzestępczości konsekwentnie aktywizuje swoje działania w walce z cyberprzestępczością. Z raportu z działalności jednostki z 2023 roku wynika, że CBZC prowadziło ponad 600 postępowań przygotowawczych, z czego blisko połowa wynikała z pracy operacyjnej. Nieodłącznym elementem strategii Biura pozostaje edukacja społeczeństwa w zakresie cyberbezpieczeństwa, w szczególności młodzieży i seniorów, która jest najbardziej narażone na cyberzagrożenia. Zauważalna jest znaczna intensyfikacja działań prewencyjnych, gdyż jednostka regularnie organizuje kampanie informacyjne, których celem jest zwiększenie świadomości wśród obywateli o metodach stosowanych przez cyberprzestępców oraz o sposobach zabezpieczania swoich danych osobowych i finansowych w sieci.

Najczęściej zgłaszane przypadki dotyczyły oszustw internetowych oraz przestępstw związanych z materiałami nielegalnymi (CSAM). Wzrost liczby zgłoszeń dotyczących oszustw online wskazuje, że świadomość społeczna w tym zakresie wzrasta, a obywatele coraz częściej zgłaszają podejrzane aktywności. Raport z 2023 roku wskazuje, że aż 35% prowadzonych spraw dotyczyło przestępstw finansowych w środowisku cyfrowym, złośliwych oprogramowań, podrabiania dokumentów oraz przestępstw skarbowych. W wyniku działań jednostki zabezpieczono znaczące ilości zasobów cyfrowych, w tym skradzionych danych osobowych i cyfrowych środków płatniczych[22].

Efektywność CBZC widoczna jest poprzez rosnącą liczbę zatrzymań osób odpowiedzialnych za cyberprzestępstwa, gdyż jednostka monitoruje zarówno krajowe, jak i zagraniczne portale społecznościowe, na których dochodzi do nielegalnej wymiany danych. Niepokojącą tendencję obrazuje statystyka czynności związanych z zagrożeniem życia i zdrowia ludzkiego, gdyż z 2380 zdarzeń zrealizowanych przez funkcjonariuszy, 1645 dotyczy osób małoletnich[23]. Niemniej jednak, przeprowadzane są regularnie szkolenia policjantów CBZC, takie jak np. przeprowadzone 29 października 2024 roku szkolenie z cyberzagrożeń w sieci. Szkolenie to zostało przeprowadzone w ramach doskonalenia zawodowego oraz miało

[21] https://www.gov.pl/web/prokuratura-krajowa/akt-oskarzenia-w-sprawie-oszustwa-na-szkode-ponad-600-osob-w-zwiazku-z-zakupem-kryptowaluty-bitcoin [dostęp: 14.11.2024 r.].

[22] wyniki_statystyczne_centralnego_biura_zwalczania_cyberprzeste__pczos__ci_za_2023_rok.pdf [dostęp: 14.11.2024 r.].

[23] *Ibidem*.

podnieść kompetencje funkcjonariuszy[24]. Dodatkowo współpraca z międzynarodowymi agencjami niewątpliwie umożliwiła szybsze i bardziej skuteczne usuwanie tego typu treści z globalnej sieci oraz zatrzymanie osób odpowiedzialnych za ich dystrybucję.

Podsumowanie

Centralne Biuro Zwalczania Cyberprzestępczości wyrasta na kluczowy filar polskiego systemu obrony przed dynamicznie rozwijającymi się zagrożeniami w cyberprzestrzeni. Kradzież danych osobowych stanowi w tych czasach poważny problem, gdyż przestępcy są w stanie pozyskać dane finansowe, hasła i tożsamość użytkowników, co pozwala im na przejęcie kontroli nad kontami bankowymi i internetowymi usługami. Kolejnym zagrożeniem są ataki phishingowe, w których przestępcy manipulują użytkownikami, aby wyłudzić dane logowania czy informacje płatnicze poprzez fałszywe strony internetowe lub wiadomości e-mail. W obliczu błyskawicznego rozwoju technologii cyberprzestrzeń staje się areną coraz bardziej złożonych i zaawansowanych zagrożeń, które nie tylko zmieniają swoje formy, ale i narzędzia, jakie wykorzystują cyberprzestępcy. Wymaga to wielopoziomowego podejścia i innowacyjnych rozwiązań w zwalczaniu skutków cyberprzestępczości. CBZC swoją skuteczność zawdzięcza nie tylko technologiom i metodom operacyjnym, ale przede wszystkim aktywnej współpracy na poziomie krajowym i międzynarodowym. W przyszłości ich znaczenie będzie wzrastać, a zakres jego zadań prawdopodobnie obejmie nowe kategorie zagrożeń, wynikające z rozwoju sztucznej inteligencji oraz innych zaawansowanych technologii, które mogą być wykorzystywane do celów przestępczych. Kluczowym wyzwaniem pozostaje zatem nie tylko reagowanie na istniejące przestępstwa, ale także przewidywanie mechanizmów przestępczych w cyberprzestrzeni i przygotowanie społeczeństwa oraz instytucji na nowe formy zagrożeń.

Bibliografia

Ministerstwo Administracji i Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego – *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa 2013.

Pomykała M., Oleksiewicz I., *Zagrożenia i wyzwania bezpieczeństwa w cyberprzestrzeni*, Rzeszów 2024.

Pomykała M., *The Central Cybercrime Bureau as a new police service established to combat cybercrime,* "Humanities and Social Sciences" 2024, Vol. 31, No. 2.

Wróbel M., *Cyberprzestępczość w polskim systemie prawnym*, Warszawa 2014.

Akty normatywne

Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r., (Dz.U. z 2015 r., poz. 728).

[24] https://szczecinek.policja.gov.pl/zsz/dzialania-policji/aktualnosci/67367,Szkolenie-szczecineckich-funkcjonariuszy-z-cyberzagrozen-w-sieci.html [dostęp: 12.10.2024 r.].

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz.U. z 2024 r., poz. 145).

Netografia

https://bezpiecznymiesiac.pl/bm/aktualnosci/1425,Poradnik-Halo-Tu-cyberbezpieczny-Senior-Podaruj-bliskim-wiedze-i-spokoj-z-okazji.html.

https://cbzc.policja.gov.pl/bzc/aktualnosci/388,Miedzynarodowa-wspolpraca-CBZC-z-organami-scigania-Ukrainy-pozwolila-na-likwidac.html.

https://cbzc.policja.gov.pl/bzc/aktualnosci/424,Kampania-o-mulach-finansowych.html.

https://cbzc.policja.gov.pl/bzc/aktualnosci/432,Cyberprofilaktyczne-spotkania.html.

https://cbzc.policja.gov.pl/bzc/aktualnosci/433,Krzywdzili-dzieci-zostali-zatrzymani-przez-policjantow-CBZC.html.

https://cbzc.policja.gov.pl/bzc/o-cbzc/doradca-do-spraw-etyki/53,Doradca-do-spraw-etyki-w-CBZC.html

https://cbzc.policja.gov.pl/bzc/o-cbzc/struktura/58,Schemat-organizacyjny-CBZC.html.

https://cbzc.policja.gov.pl/bzc/zagrozenia-w-sieci.

https://eur-lex.europa.eu/PL/legal-content/summary/convention-on-cybercrime.html.

https://szczecinek.policja.gov.pl/zsz/dzialania-policji/aktualnosci/67367,Szkolenie-szczecineckich-funkcjonariuszy-z-cyberzagrozen-w-sieci.html.

https://www.gov.pl/web/prokuratura-krajowa/akt-oskarzenia-w-sprawie-oszustwa-na-szkode-ponad-600-osob-w-zwiazku-z-zakupem-kryptowaluty-bitcoin.

https://www.nask.pl/pl/aktualnosci/5258,Wspolpraca-miedzy-NASK-a-CBZC-podpisano-specjalne-porozumienie.html.

https://www.policja.pl/pol/aktualnosci/211523,Polska-Policja-i-INTERPOL-zaciesniaja-wspolprace-w-walce-z-cyberprzestepczoscia.html.

Raport roczny CERT za 2022 rok (https://www.gov.pl/web/baza-wiedzy/krajobraz-bezpieczenstwa-polskiego-internetu-w-2022-roku--raport-roczny-cert-polska).

wyniki_statystyczne_centralnego_biura_zwalczania_cyberprzeste__pczos__ci_za_2023_rok.pdf.

Piotr PADULA[1]

ZAGROŻENIA CYBERNETYCZNE WYBORÓW PREZYDENCKICH W USA W 2024 ROKU

Wstęp

Instytucja prezydenta zawiera w swoim zakresie rozmaite kompetencje. Ze względu na system polityczny, jaki dane państwo posiada, tak też i rola prezydenta różni się. Charakter tej tezy podkreśla Stanisław Bożyk, który stwierdził, że: „Pozycja prezydenta w określonym systemie ustrojowym uzależniona jest w głównej mierze od jego usytuowania wśród konstytucyjnych organów państwa, zakresu przyznanych mu kompetencji oraz przyjętych zasad jego odpowiedzialności”[2]. Kluczowe wydaje się spojrzenie na ten organ od strony nie samych efektów pracy politycznej, ale z perspektywy okresu ubiegania się o to stanowisko. Wybory „głowy” państwa wiążą się z kampanią wyborczą, która poprzedza sam czas oddawania głosów, jest przestrzenią do zaprezentowania swoich racji, pomysłów, planów. Okres ten odgrywa kluczową rolę, z tej racji powstaje wiele zmiennych, które wpływają na ostateczną decyzję, jaką podejmie oddający głos obywatel.

Stany Zjednoczone są państwem, które należy postrzegać w kategorii mocarstwa, które wpływa na konkretne dziedziny życia całego świata. Pozycja, jaką wypracowało sobie USA wiąże się z pewną odpowiedzialnością, jaką musi „nieść” władza. Uzasadnione wydaje się stwierdzenie, iż wybory prezydenta Stanów Zjednoczonych to jedne z najważniejszych tego typu wydarzeń na świecie. Nierozerwalną częścią tego procesu jest napięcie, które towarzyszy nie tylko samym kandydatom wraz z ich sztabami, lecz również rządom innych państw czy też organizacji powiązanych bądź oportunistycznych do USA. „Prezydent jest jedynym reprezentantem kraju w stosunkach zewnętrznych i jedynym reprezentantem wobec innych państw”[3], można zatem ocenić, że prezydent USA jest tym, którego decyzje kształtują porządek świata.

---

[1] Politechnika Rzeszowska, Wydział Zarządzania. ORCID: 0009-0004-8353-6675.

[2] S. Bożyk, *Wybory prezydenckie*, Temida 2, Białystok 1995, s. 5.

[3] „The President is the sole organ of the nation in its external relations, and its sole representative with foreign nations” – cyt. za: L. Kański, *Kompetencje Kongresu w zakresie kształtowania polityki zagranicznej Stanów Zjednoczonych Ameryki*, Wydawnictwo Naukowo Uniwersytetu im. Adama Mickiewicza, Poznań 1982, s. 33, przypis 66.

Rola prezydenta w systemie politycznym USA

Rozważając problematykę związaną z wyborami w USA uzasadnione wydaje się zwrócenie szczególnej uwagi na dwie kluczowe kwestie. Z jednej strony przede wszystkim na sam system wyboru prezydenta. Z drugiej zaś na to, jakie są główne kompetencje osoby piastującej to stanowisko, a przy tym jak znaczący mają one wpływ na prowadzenie polityki USA.

Na świecie dominują dwa systemy polityczne: parlamentarny oraz prezydencki. Stany Zjednoczone są państwem, gdzie występuje system oparty na prezydencie. Trafnie oba systemy porównuje Jarosław Szymanek oceniając, iż: „Stany Zjednoczone Ameryki są wzorcem systemu, który zwykło się nazywać prezydenckim, a który, obok sytemu parlamentarnego, tworzy drugi wielki system rządów. Te dwa krańcowo odmienne systemy są ciągle podstawowymi modelami ułożenia relacji między legislatywą a egzekutywą w demokratycznej hemisferze ustrojowej. O ile jednak system parlamentarny występuje często i gęsto, w praktyce tworząc całą mozaikę systemów genetycznie tkwiących (mniej lub więcej) w regule rządów parlamentarnych, o tyle system prezydencki pozostaje systemem endemicznym, właściwym jedynie dla USA”[4]

Filozofia wyboru tak ważnego organu obwarowana jest pewnymi procedurami oraz zasadami, które kształtują jego przebieg. Stany Zjednoczone posiadają sposób rozstrzygnięcia kampanii, który jest pośrednim wyborem, opartym na dwóch stopniach. Obywatele oddają bowiem głosy w wyborach powszechnych na elektorów, następnie wybrane grono poprzez głosowanie wybiera nowego prezydenta USA. W głosowaniu przedstawiciele społeczności amerykańskiej[5] wybierają prezydenta i wiceprezydenta[6] Stanów Zjednoczonych, jednak rozstrzygnięcie obu stanowisk odbywa się w osobnych głosowaniach. Elektorzy wybierając zarówno osoby, na jedno, jak i drugie stanowisko muszą kierować się konstytucyjną zasadą stanowiącą, że: „Elektorzy będą się zbierać w swoich stanach i w głosowaniu tajnym wybierać Prezydenta i na Wiceprezydenta, z których przynajmniej jeden nie będzie mieszkańcem tego samego stanu co oni”[7].

Kluczowe w analizie systemy wyboru szefa egzekutywy jest zwrócenie uwagi na kolegium elektorskie jako ograniczoną liczbę działaczy politycznych reprezentujących daną partię, wybieranych co 4 lata. Takich przedstawicieli jest 538, każdy

[4] J. Szymanek, *Determinanty amerykańskiego systemu prezydenckiego,* Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2014, s. 205.

[5] Przedstawiciele amerykańskiej społeczności – elektorzy.

[6] Wiceprezydent – stanowisko, które po wprowadzeniu pierwotnie piastowane było przez kandydata, który uzyskał drugą zaraz po zwycięzcy wyborów liczbę głosów elektorskich. Wraz z poprawką XII do Konstytucji USA Kolegium Elektorów w osobnym głosowaniu wybiera również wiceprezydenta. Zastępca szefa egzekutywy staje się prezydentem, jeśli osoba piastująca dotychczas to stanowisko została z niego usunięta, stwierdzono u niej niezdolność do wykonywania urzędu, zmarła bądź z niego zrezygnowała. Wiceprezydent obejmuje stanowisko na czas wyboru nowego prezydenta lub ustąpienia okoliczności wyłączającej możliwości wykonywania urzędu.

[7] A. Pułło (tł.), *Konstytucja Stanów Zjednoczonych Ameryki*, Wydawnictwo Sejmowe, Warszawa 2002, poprawka XII, s. 57.

stan wyznacza elektorów w sposób określony przez własne prawodawstwo, spośród którego dominują dwa systemy: powoływania bądź głosowania. Każdy stan posiada odrębną liczbę głosów w KE[8], związane jest to z liczbą miejsc, jakie przypadają danej jednostce w Kongresie, przy czym każdy reprezentowany jest przez 2 senatorów. Pozostała liczba głosów elektorskich zależna jest od liczby deputowanych w Izbie Reprezentantów, a więc od liczebności ludności zamieszkującej dany stan. Dodatkowe trzy miejsca w Kolegium zagwarantowano Dystryktowi Kolumbii[9].

Uzupełniając proces wyboru najważniejszego organu monokratycznego USA należy zwrócić szczególną uwagę na fakt, iż stanowiący Konstytucję przewidzieli sytuację, w której żaden spośród kandydatów nie uzyskał większości głosów elektorskich. Zapobiegliwość takiego stanu rozwiązano poprzez kolejne głosowanie, w którym udział biorą członkowie izby niższej Kongresu. Zmianie podlega w tym przypadku sposób oddawania głosu. Zrezygnowano z liczenia głosów deputowanych Izby Reprezentantów, a zamiast tego członkowie IR[10] oddają go jako delegacja stanowa, przy czym każdy stan posiada jeden głos.

By ubiegać się o stanowisko we władzy wykonawczej w Stanach Zjednoczonych Ameryki, należy, jak wyznacza Konstytucja, kraju spełnić trzy warunki, tj.:

- posiadać od urodzenia obywatelstwo USA,
- ukończyć 35 lat życia,
- mieszkać na terenie USA przynajmniej od 14 lat[11].

Bierne prawo wyborcze przysługuje kandydatowi, którego kwalifikują jednocześnie wypełnione warunki prawne.

Rzeczą intersującą jest nie tylko sam proces wyboru prezydenta, lecz również pozycja, jaką mu gwarantuje Konstytucja poprzez kompetencje, z którymi związane jest to stanowisko.

Wśród uprawnień tego organu znajduje się bowiem:

- „Prezydent będzie miał prawo zawieszania wykonania lub darowania kary orzeczonej za przestępstwo przeciwko Stanom Zjednoczonym, z wyjątkiem spraw rozpatrywanych w trybie impeachmentu[12]”[13]. Prawo łaski nie dotyczy wszystkich szczebli administracyjnych. Wyłączność w gestii tej kompetencji związane jest z poziomem federalnym. Kompetencje w zakresie stanowym posiada bowiem gubernator, prezydent może natomiast zmniejszyć wymiar kary.

---

[8] KE – skrót od Kolegium Elektorów.

[9] A. Pułło (tł.), *Konstytucja Stanów Zjednoczonych Ameryki*, Wydawnictwo Sejmowe, Warszawa 2002, poprawka XXIII, s. 64.

[10] IR – skrót od Izba Reprezentantów.

[11] A. Pułło (tł.), *Konstytucja Stanów Zjednoczonych Ameryki*, Wydawnictwo Sejmowe, Warszawa 2002, art. II, sekcja I, klauzula IV, s. 48.

[12] Tryb impeachmentu – tryb związany z postawienie w stan oskarżenia z powodu nadużycia popełnionego w czasie sprawowania urzędu państwowego.

[13] A. Pułło (tł.), *Konstytucja Stanów Zjednoczonych Ameryki*, Wydawnictwo Sejmowe, Warszawa 2002, art. II, sekcja II, klauzula I, s. 48.

- Szef egzekutywy posiada tzw. administrację prezydencką. Departamenty odpowiedzialne za realizację podstawowych kompetencji prezydenta stanowią organ wspomagająco-doradczy funkcjonowania osoby pełniącej to stanowisko.
- Prezydent jest naczelnym dowódcą Sił Zbrojnych USA. Kompetencja ta poprzez monokratyczny dobór zwierzchnika umożliwia sprawne podejmowanie decyzji w przypadku wystąpienia bezpośredniego zagrożenia dla państwa, jego interesów lub gdy użycie SZA[14] spowodowane jest wypełnieniem porozumień międzynarodowych bądź sojuszniczych.
- Prezydent jest reprezentantem w sprawach zagranicznych. Za zgodą Senatu (2/3 obecnych na posiedzeniu senatorów) zawiera traktaty[15]. Historia XX wieku w USA wskazuje na umocnienie władzy wykonawczej w zakresie prowadzenia polityki międzynarodowej poprzez tzw. porozumienia władzy wykonawczej w dwojaki sposób jako:
  - porozumienia prezydenckie – zawierane przez prezydenta (brak konieczności właściwego upoważnienia ze strony Kongresu),
  - porozumienia kongresowe – zawierane za zgodą Kongresu (konieczność właściwego upoważnienia).
- Prezydent jest osobą odpowiedzialną za mianowanie urzędników państwowych odpowiedzialnych za kluczowe rejony działalności państwa, m.in. ambasadorów, ministrów pełnomocnictw, konsulów czy sędziów Sądu Najwyższego[16].
- Szef egzekutywy, jak analizuje Paweł Laidler: „W przypadku pilnej konieczności wypełnienia wakansu (sędziowskiego lub departamentowego) podczas przerw w obradach Senatu, prezydent ma prawo mianować daną osobę na stanowisko, ale tylko do momentu zakończenia trwającej sesji Senatu. Wówczas nowo wybrani senatorowie mogą przegłosować pozostanie lub usunięcie urzędnika z zajmowanego stanowiska, co będzie równoznaczne z realizacją uprawnienia »rady i zgody« (*advice and consent*)”[17].
- Prezydent czuwa nad wiernym wykonywaniem prawa.

Kandydaci wyborów prezydenckich w 2024 roku

Wybory prezydenckie w Stanach Zjednoczonych przypadające na rok 2024 są efektem zapisu Konstytucji USA, która w artykule II sekcji I klauzuli I stanowi,

[14] SZA – skrót od Siły Zbrojne Ameryki.

[15] W kompetencji prezydenta należy podpisanie umowy międzynarodowej, a w gestii Senatu pozostaje jej ratyfikacja większością dwóch trzecich głosów członków.

[16] R. Wszołek, *Władza ustawodawcza, wykonawcza i sądownicza w ustroju Stanów Zjednoczonych Ameryki* [w:] *Konstytucja USA. Ze studiów nad amerykańskim systemem politycznym,* red. M. Urbańczyk, Ł. Bartosik, M. Tomczak, Wydawnictwo ArchaeGraph, Poznań–Łódź 2018, s. 110-111.

[17] P. Laidler, *Konstytucja Stanów Zjednoczonych Ameryki. Przewodnik,* Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2007, s. 85.

że: „Władza wykonawcza zostanie powierzona Prezydentowi Stanów Zjednoczonych Ameryki. Będzie on sprawował swój urząd przez czteroletnią kadencję razem z Wiceprezydentem, powoływanym na taką samą kadencję”[18]. Wybory prezydenckie w 2020 roku wygrał Joe Biden. Kampania wyborcza w 2024 roku to starcie przede wszystkim kandydatów dwu partii: Republikanów i Demokratów[19]. Od samego początku pretendentem od strony pierwszego ugrupowania był Donald Trump. Natomiast stronnictwo Demokratów zmierzyć musiało się ze zmianami, bowiem ich pierwotny reprezentant, zwycięzca poprzednich wyborów, prezydent Joe Biden miał tak jak w roku 2020 konkurować o zwycięstwo w wyborach z 45. prezydentem USA[20]. Forma prowadzenia przez Bidena kampanii wyborczej, a przede wszystkim czerwcowa debata prezydencka, w której wypadł on wizerunkowo nieudanie, doprowadziła do wyjątkowo niekorzystnych notowań w sondażach dla kandydata Demokratów. W obliczu słabnącego poparcia Joe Biden zrezygnował z ubiegania się o reelekcję, „21 lipca prezydent Stanów Zjednoczonych Joe Biden ogłosił, że rezygnuje z ubiegania się o reelekcję w wyborach prezydenckich z ramienia Partii Demokratycznej (PD). Poparł wiceprezydent Kamalę Harris, wskazując ją jako kandydatkę do reprezentowania Demokratów. Kluczem do powodzenia Harris będzie konsolidacja PD wokół jej kandydatury i przeprowadzenie skutecznej kampanii w obliczu rosnącego poparcia dla kandydata Partii Republikańskiej – Donalda Trumpa”[21] – komentują Andrzej Dąbrowski oraz Mateusz Piotrowski, analitycy ds. Stanów Zjednoczonych Polskiego Instytutu Spraw Międzynarodowych (PISM). Wybory 47. prezydenta USA, to kolejne historyczne tego typu wydarzenie[22], w którym o stanowisko „głowy” państwa mierzyć będzie się ze strony Demokratów kobieta, a ze strony Republikanów mężczyzna. Podobnie jak w 2016 roku, tak i w 2024 roku naprzeciw kandydatki partii Demokratów stanął Donald Trump.

Poddając analizie zagrożenia cybernetyczne, z jakimi mierzyły się obozy kandydatów, warto zilustrować historie, poglądy, czy doświadczenie obu postaci w celu ocenienia powodów, jakie były uwarunkowaniem konkretnych ataków.

---

[18] A. Pułło (tł.), *Konstytucja Stanów Zjednoczonych Ameryki*, Wydawnictwo Sejmowe, Warszawa 2002, art. II, sekcja I, klauzula I, s. 47.

[19] Pod względem formalnym w wyborach prezydenckich nie można stwierdzić, iż kandydują wyłącznie przedstawiciele partii Republikanów oraz Demokratów. Kandydują również inni obywatele, lecz ich znaczenie w odniesieniu do całych wyborów jest marginalne, co powoduje złudzenie wyborów pomiędzy dwoma kandydatami. Jedyny wpływ, jaki wywierają pozostali kandydaci, to fakt „oddania na nich głosów” przez Amerykanów, który powoduje utratę poparcia przez przedstawicieli głównych partii, co może spowodować porażkę w danym stanie (kandydat z małej partii pozyska głosy, które mógłby teoretycznie zdobyć Demokrata czy Republikanin).

[20] Donald Trump – prezydent Stanów Zjednoczonych w latach 2017–2021.

[21] A. Dąbrowski, M. Piotrowski, *Joe Biden rezygnuje z walki o reelekcję,* Polski Instytut Spraw Międzynarodowych, nr 52/2024, 22 lipca 2024 roku.

[22] Pierwszymi wyborami prezydenckimi USA, gdzie kandydatem była kobieta, były wybory w 2016 roku. Wówczas kandydatem Demokratów była żona byłego prezydenta i była sekretarz stanu Hillary Clinton, natomiast od strony partii Republikanów kandydował Donald Trump.

Trump to człowiek przede wszystkim z ogromnym doświadczeniem nie tylko w sferze biznesowej, jak również piastowania urzędu prezydenckiego, wygrał bowiem wybory w 2016 roku stając się 45. prezydentem Stanów Zjednoczonych. Przez kolejne trzy kampanie wyborcze (w 2016, 2020 oraz 2024 roku) brał udział w nich jak kandydat partii Republikanów na ten urząd. Jak podają badania portalu Forbes, pod względem majątkowym Trump to miliarder, którego majątek szacuje się na 6,2 mld dolarów, co czyni go 525 najbogatszym człowiekiem na świecie (na dzień 24.10.2024 r.)[23]. Działalność biznesowa 45. prezydenta USA skupiona jest przede wszystkim wokół nieruchomości. Pod względem politycznym debiutem kandydata na prezydenta USA były zwycięskie wybory w 2016 roku. Pomimo iż wielu ekspertów sceptycznie podchodziło do tez głoszonych w czasie trwania kampanii przez Trumpa, jak choćby w zakresie polityki zagranicznej, pokonał on Hillary Clinton. „Z dotychczasowych wypowiedzi Trumpa wynika, że chciałby on ograniczyć rolę USA w Europie i ich zaangażowanie w utrzymywanie pokoju na świecie. Można się też spodziewać prób szukania porozumienia z autorytarną Rosją Putina, napięć w stosunkach z Chinami, a także odwrotu od promocji idei wolnego handlu w świecie”[24] – tak kampanię komentował Marek Wąsiński z Polskiego Instytutu Spraw Międzynarodowych (PISM). Prowadzona przez Donalda Trumpa polityka uznawana jest za twardą, stanowczą, zmierzającą do jednoosobowego podejmowania decyzji (za pomocą dekretów, tzw. aktów wykonawczych).

Kamala Harris to typ człowieka reprezentujący odmienne podejście w dużej mierze nie tylko polityczne, ale i samych stanowisk politycznych niż Trump. Ukończyła Howard University i University of California Hastings College of Law. Harris piastowała urząd wiceprezydenta w administracji ustępującego Joe Bidena. Pełniła również takie stanowiska jak: prokurator okręgowy w San Francisco, prokurator generalny w Kalifornii, a w 2017 roku została zaprzysiężona do Senatu USA. Stanowisko Kamali Harris jako wiceprezydenta Stanów Zjednoczonych ukierunkowywało na nowo wizję kobiety w polityce i administracji państwa. Wydarzenie z 20 stycznia 2021 roku[25] sprawiło, że stała się ona pierwszą osobą płci żeńskiej, jak także, pierwszą czarnoskórą Amerykanką i pierwszą Amerykanką pochodzenia południowoazjatyckiego znajdującą się na tym stanowisku. Fenomen kariery w administracji USA Amerykanki komentuje Andrew Franks oceniając: „Żadna kobieta nigdy nie piastowała stanowiska prezydenta ani wiceprezydenta, a kobiety (ponad 50% wyborców) nigdy nie piastowały więcej niż 24% miejsc w Kongresie USA ani więcej niż 18% stanowisk gubernatorskich. Bez wsparcia i zachęty ze strony innych, kobiety są mniej skłonne niż mężczyźni o porówny-

[23] https://www.forbes.com/profile/donald-trump/ [dostęp: 24.10.2024 r.].

[24] M. Wąsiński, *Polityka zagraniczna w kampanii wyborczej Donalda Trumpa,* Biuletyn, Polski Instytut Spraw Międzynarodowych, nr 38 (1388), 16 czerwca 2016 roku.

[25] 20 stycznia 2021 roku – data zaprzysiężenia Kamali Harris na stanowisko wiceprezydenta Stanów Zjednoczonych w administracji prezydenta Joe Bidena.

walnym pochodzeniu do ubiegania się o urząd publiczny”[26]. Wśród dotychczasowych działań politycznych Harris dominują te, których głównym celem były kwestie społeczne, w głównej mierze dotyczące nierówności i dyskryminacji.

Ataki cybernetyczne wymierzone w kampanię prezydencką

Kampania prezydencka w USA kluczowa jest nie tylko z punktu widzenia przeciętnego Amerykanina. Poprzez niezwykle silną pozycję na arenie międzynarodowej fakt tego kto będzie przewodniczył prowadzonej polityce szczególnie zagranicznej w Stanach Zjednoczonych obserwowany jest także przez przywódców i liderów ugrupowań z całego świata. Nierozerwalna wydaje się opinia, iż poglądy prezydenta USA wpływają na prowadzoną politykę w wielu zakątkach świata. Z tego to powodu powstała grupa interesantów, która nie pozostała jedynie biernym obserwatorem wyboru szefa egzekutywy USA, lecz poprzez rozmaite środki wpływała na opinię publiczną, na fakt postrzegania przez obywateli danego kandydata. Należy przypuszczać, że poprzez różnego rodzaju nośniki, szczególnie związane z mediami społecznościowymi, manipulacją treścią docierającą z precyzją do zamierzonego odbiorcy, ataki cybernetyczne dany napastnik usiłuje wpłynąć na głos wyborcy tak, aby ten wybrał kandydata, którego poglądy są najbardziej zbliżone do działań prowadzonych przez napastnika (lub organu zlecającego dokonanie danej operacji). Należy więc rozważyć przypadki ataków wymierzonych, co warto podkreślić, w obozy obu głównych kandydatów, analizując powiązania grup napastniczych i prawdopodobny cel, jaki zamierzały osiągnąć.

Donald Trump to polityk, który w otwarty sposób deklaruje swoje poglądy. Następstwem tak stawianej sprawy jest fakt prowadzenia działań mających na celu wzmocnienie bądź osłabienie pozycji w wyborach.

Główni „aktorzy”, którzy podjęli działania zamierzone w kierunku rozstrzygnięcia wyborów prezydenckich to przede wszystkim, przodująca w wykorzystaniu technik dezinformacyjnych i cybernetycznych Federacja Rosyjska, a także Iran czy Chińska Republika Ludowa.

Najmniej zaangażowana wydaje się być ChRL[27]. Podczas trwania wyborów ujawniono, iż przy pomocy narzędzia dezinformacji Chińczycy poprzez współpracę z rodzimą spółką poprawiali skuteczność treści tworzonych w operacjach mających na celu poszerzanie wpływu. W obliczu sytuacji geopolitycznej, gdzie konkurencja pomiędzy Chinami a USA wzrasta, z pewnością nie można uznać, że działania ze strony mocarstwa z Azji miały w swym zamiarze znikome oddziaływanie. Należy przewidywać dwie drogi działania, które objęła ChRL. Z jednej strony ataki o niewielkim, bezpośrednim wpływie na głosy wyborców, które w swym celu zakładały poszerzenie tolerancji na kwestie, za pomocą których

[26] A.S. Franks, *Warunkowe skutki płci i seksizmu kandydatów na postrzeganą wybieralność i intencje wyborcze: dowody z prawyborów Demokratów w 2020 r.*, „Anal Soc Issues Public Policy” 2021, t. 21, nr 1, s. 12.

[27] ChRL – skrót od Chińska Republika Ludowa.

zapewne prowadzona przez Chiny polityka, będzie chciała oddziaływać na stronę amerykańską już po wyborze prezydenta. Prawdopodobne wydaje się, że rząd azjatyckiego giganta w swoim wysiłku skupił się na tworzeniu następstw, z którymi zmierzyć będzie się musiał 47. prezydent Stanów Zjednoczonych, co będzie okazją do zyskania przewagi na rynku międzynarodowym Chin. Z drugiej zaś strony należy rozważyć, że ujawnione próby ingerencji, wszelkich ataków cybernetycznych były zmasowane, ale wyjątkowo nieskuteczne, co przełożyło się na nikły wpływ. Bez względu na przyjęty plan, pewne jest jedno. Chińska Republika Ludowa usiłuje zyskać przewagę nad USA, doprowadzić do destabilizacji, która utworzy przestrzeń do przejęcia roli Stanów Zjednoczonych w osłabłej dziedzinie.

Zupełnie inną rolę odgrywa Iran. Z racji kierunku, w jakim zmierza polityka Iranu, preferowanym kandydatem wydaje się przedstawicielka Demokratów. Kamala Harris jako polityk bardziej o poglądach lewicowych będzie zmierzać w kierunku zrównoważonego podejścia w sprawach kluczowych dla polityki Iranu, a więc kwestii Izraela i wojny z Hamasem. Ponowny wybór na szefa egzekutywy Trumpa wydaje się pozostawać w sprzeczności z interesem Iranu, co również miało miejsce w trakcie trwania kadencji 2016–2020. W trakcie swojej pierwszej prezydentury kandydat Republikanów kierunkował politykę zagraniczną USA, w sposób pozostający w kolizji z postępowaniem Iranu. Stosowne wydaje się stwierdzenie, iż uznanie Jerozolimy za stolicę Izraela, wycofanie się z porozumienia JCPOA[28], zabicie gen. Solejmaniego[29], a także prawdopodobne w obliczu uzyskania prezydenckiej reelekcji wspieranie polityki Izraela jest przyczyną, że ataki i manipulacje cybernetyczne Iranu dążyły nie tylko do podziału społeczeństwa, ale także utraty zaufania względem Trumpa wśród Amerykanów.

Główne cyberzagrożenia wyborów prezydenckich można podzielić na dwie grupy, takie, które:

- atakują osoby mające dostęp do wrażliwych informacji na temat przebiegu kampanii,
- atakują wyborców poprzez fałszywe informacje podawane w Internecie.

Za obie formy ingerencji odpowiedzialne były grupy hakerów, m.in.: Sefid Flood, APT42/Mint Sandstorm, APT-33/Peach Sandstorm działające we współpracy z Iranem. W trakcie trwania kampanii wyborczej 2024 roku wielokrotnie dochodziło do próby poprzez e-maile z linkiem phishingowym włamania się do danych urzędników związanych z obozem Trumpa, część z nich przyniosła pożądany efekt. W sierpniu 2024 roku portal Politico otrzymał bowiem dokumenty dotyczące kampanii kandydata Republikanów – autorstwo tego przypisuje się

[28] JCPOA – (ang. *Joint Comprehensive Plan of Action*), porozumienie nuklearne pomiędzy członkami stałymi Rady Bezpieczeństwa ONZ (Chiny, Francja, Rosja, Wielka Brytania, USA oraz dodatkowo Niemcy) a Iranem. Program zakładał ograniczenie irańskiego programu nuklearnego w zamian za złagodzenie sankcji.

[29] Gen. Kasam Solejmani – dowódca Korpusu Strażników Rewolucji Islamskiej (wojsko Iranu), zabity podczas amerykańskiego ataku powietrznego na miasto Bagdad.

właśnie działaczom z Iranu, mimo że oficjalnie rząd zdementował doniesienia[30]. W kontekście bezpośredniego wpływu należy szczególną uwagę poświęcić oddziaływaniu mającemu za pomocą fałszywych: profili, filmów, artykułów, narzędzi internetowych, przekonać do głosowania przeciw Trumpowi nie tylko osoby niezdecydowane, lecz także jego zwolenników. Rzeczą wartą zauważenia jest tutaj wykorzystanie sztucznej inteligencji, która wspomagała proces tworzenia treści, niejednokrotnie zbudowanych w taki sposób, aby odbiorca z trudnością rozpoznał fakt fałszywego wykreowania danego obrazu czy nagrania. Poprzez tak wszechstronną porcję dostarczanych *fake newsów*, rozmazane wydaje się to, co prawdą jest, a co nią nie jest; prowadzi to do polaryzacji społeczeństwa, zwiększenia dystansów pomiędzy zwolennikami danej partii. Amerykańscy wyborcy Trumpa wielokrotnie mierzyli się z treściami, które zaburzały ich sympatie polityczne, które kłóciły się z ich dotychczasowymi poglądami o danym kandydacie. Nierzadko, na co należy zwrócić uwagę, fałszywe doniesienia obejmowały w danym regionie kwestie polaryzujące, sprawiające, że w obliczu dobrze zmanipulowanego przekazu odbiorca doznawał rozterki na temat tego na kogo zagłosuje.

Federacja Rosyjska podchodziła w sposób niezwykle podobny do wywierania wpływu jak Iran, zasadniczą różnicę stanowi jednak kierunek działań. Polityka Kremla zmierza bowiem w stronę zwycięstwa w wyborach prezydenckich kandydata Republikanów. Nie ulega wątpliwości, że podejście Donalda Trumpa do wojny na Ukrainie sprawia, iż Moskwa liczy na rozstrzygnięcie na warunkach jakie sama postawi. Podobne stanowisko w tej sprawie wyraża Filip Baryjka twierdząc, że: „Rosja wspiera kandydaturę Donalda Trumpa, licząc, że jego nieprzewidywalność i transakcyjne podejście w polityce międzynarodowej pozwolą narzucić Ukrainie pokój na preferowanych przez Rosję warunkach. Do takich kalkulacji mogą skłaniać kontrowersyjne wypowiedzi Trumpa na temat kosztów wspierania Ukrainy, planu zaprowadzenia pokoju w 48 godzin po objęciu prezydentury czy podważanie sensu istnienia NATO”[31].

Rosja działa nie w sposób bezpośredni, wykorzystywała bowiem grupy hackerskie do działań wśród wyborców amerykańskich. W kontekście wyborów prezydenckich w USA Moskwa współpracowała m.in.: z Ruza Flood/Doppelganger, Storm1516, Storm-1841/Rybar. Podobnie jak w przypadku Iranu, wykonywały one zlecone zadania nie tylko za pomocą dotychczas znanych narzędzi, które można określić w odniesieniu do tej dziedziny za tradycyjne, lecz uzupełniały znane im techniki o AI[32]. Działania w obszarze upowszechniania dezinformacji są pewnego rodzaju znakiem rozpoznawalnym grup hackerskich powiązanych z FR[33]. Nie dziwi więc fakt doprecyzowania i kunszt stosowanych środków.

[30] D. Sieńkowski (opr.), *Trump ofiarą ataku hakerskiego? "Ingerencja w wybory", „*Do Rzeczy” z dnia 11.09.2024 roku [dostęp: 11.11.2024 r.].

[31] F. Baryjka, *Ingerencje Rosji i Iranu w wybory prezydenckie w USA,* Biuletyn PISM, nr 128(2938), 02.10.2024 r.

[32] AI – sztuczna inteligencja.

[33] FR – skrót od Federacja Rosyjska.

Koncentrując się na zagrożeniach warto zauważyć, że rosyjscy cyberhackerzy powodowali dezinformację poprzez generowanie stron internetowych imitujących znane lokalne gazety takie jak „Houston Post", „Chicago Crier" czy „Boston Times". „Pranie" informacji ma jednak daleko idące skutki, bowiem agenci rosyjscy uwiarygadniali treści poprzez inne formy źródeł potwierdzających tę samą fałszywą tezę bądź prawdziwe zdarzenia, manipulowane w taki sposób, aby odpowiadały elektoratowi Trumpa, a więc środowisku konserwatywnemu. Zdjęcia, filmy, wypowiedzi ekspertów, sygnalistów, dokumenty stworzone przez AI w połączeniu z doświadczeniem prowadzących dezinformację z pewnością w skuteczny sposób oddziaływały na odbiorcę amerykańskiego, dla którego mogło to być nowe zjawisko.

Podsumowanie i wnioski

Współczesny wymiar kampanii prezydenckiej w USA obwarowany był nie tylko problematyką związaną z samym faktem przekonania wyborców do swoich racji, lecz także miał inny wymiar – wpływu cybernetycznego. Ataki godzące w dobro kampanii prowadzonej zarówno przez obóz Donalda Trumpa, jak i Kamali Harris z pewnością można uznać za nowy wymiar „pojedynku o głosy". Współczesna sztuka prowadzenia kampanii politycznej nierozerwalnie związana jest z odszukiwaniem nowych przestrzeni do przedstawiania swojej wizji. Jednak ten wymiar budzi nie tylko szanse, lecz także zagrożenia. Szkodliwość cybernetyczna w postaci akcji prowadzonych przeciwko przedstawicielom partii Republikanów i Demokratów uwydatnia wagę wyborów nie tylko dla losów USA, lecz również dla polityki innych krajów. Manipulacje informacją wspartą nowoczesnymi technologiami sztucznej inteligencji, tworzą przestrzeń nowych wyzwań. Wyborcy szczególnie, jak nigdy dotąd, muszą rozgraniczać rzeczywistość z wytworzonym fałszywymi wydarzeniami. Dzięki wykorzystaniu zaawansowanych technik dezinformacyjnych, takich jak deepfake, boty społeczne czy personalizowane reklamy cyfrowe, obce państwa oraz organizacje mogą kształtować narrację wokół kampanii i kandydatów, co może wprowadzić wyborców w błąd lub zapobiec ich udział w głosowaniu.

Kampania przeprowadzona w warunkach narażenia na cyberataki i manipulacje informacyjne jest niezwykle ciekawym, a zarazem nowym zjawiskiem, które z pewnością będzie się rozwijać. Kluczowe będzie więc odnalezienie adekwatnych sposobów radzenia sobie przez obozy wyborcze w stosunkowo niedoszacowanym wymiarze wyborów. Sztaby polityczne na całym świecie muszą dostosować się do nowej rzeczywistości, w której cyfrowe zagrożenia są niemalże normą. Kampanie przyszłości będą wymagały nie tylko sprawnego zarządzania wizerunkiem, ale również monitorowania oraz natychmiastowego reagowania na próby dezinformacji i cyberataków.

Zwycięstwo Donalda Trumpa[34] w wyborach, w obliczu wspomnianych wyzwań cybernetycznych, ukazuje, jak istotny jest wpływ technologii informacyjnych i kampanii dezinformacyjnych na współczesny proces demokratyczny. Wnioski płynące z tej sytuacji odnoszą się zarówno do bezpieczeństwa wyborów, jak i do zmieniających się strategii politycznych oraz zachowań wyborców. Wygrana Trumpa, mimo intensywnych działań dezinformacyjnych i prób zakłócenia jego kampanii, uwypukla konieczność inwestowania w nowoczesne systemy cyberbezpieczeństwa, które mogą skutecznie przeciwdziałać manipulacjom. Utrzymanie integralności procesu wyborczego staje się kluczowe, a USA, jako jedno z wiodących państw na arenie międzynarodowej, muszą podjąć działania wzmacniające infrastrukturę ochronną na poziomie cyfrowym.

Pomimo obecności manipulacji i dezinformacji, wygrana Trumpa może świadczyć o rosnącej świadomości wyborców co do zagrożeń cyfrowych i ich umiejętności oddzielania prawdziwych informacji od fałszywych. Zjawisko to pokazuje, że odpowiednio wyedukowani wyborcy mogą stawić opór próbom wpływu i manipulacji. W przyszłości konieczne będzie dalsze kształcenie społeczeństwa w zakresie krytycznego myślenia i rozpoznawania źródeł wiarygodnych informacji.

Mimo licznych zagranicznych prób wpłynięcia na wybory, zwycięstwo Donalda Trumpa dowodzi, że amerykańska scena polityczna pozostaje kluczowym polem rywalizacji dla różnych państw o sprzecznych interesach. Wygrana kandydata o określonej wizji polityki międzynarodowej niesie ze sobą zmiany w relacjach USA z krajami na całym świecie, co może wywołać dalsze działania przeciwdziałające destabilizacji w kolejnych kampaniach.

Informacja o zwycięstwie kandydata Republikanów, już w chwili ogłoszenia wpłynęła na politykę świata. W Republice Federalnej Niemiec doszło bowiem do rozpadu koalicji rządzącej, wobec czego kanclerz Schloz zarządził głosowanie nad wotum zaufania dla obecnego rządu. Warto zauważyć, iż prawdopodobnym efektem będzie brak uzyskania poparcia, czego skutkiem będą nowe wybory do Bundestagu[35]. W tym wydarzeniu należy doszukiwać się nie tylko przyczyn wewnętrznych, lecz także wpływu zewnętrznego, tzn. zwycięstwa w wyborach prezydenckich w USA Trumpa. Należy przypuszczać, iż taki stan rzeczy spowodowany jest prawdopodobnym kierunkiem współpracy Niemiec. Utworzenie silnego sojuszu na linii Berlin – Waszyngton ma zagwarantować utrzymanie silnej pozycji na arenie europejskiej w pierwszej kolejności, a także międzynarodowej. Spodziewać należy się próby budowania stosunków politycznych w oparciu o nowy rząd, którego kierunki działania będą silnie związane z poglądami Trumpa.

Rzeczą prawdopodobną jest, że zwycięstwo kandydata Republikanów doprowadzi również do daleko idących skutków dot. wojny na Ukrainie. Poglądy

[34] Podczas wyborów powszechnych 05.11.2024 roku w Ameryce Republikanie zyskali 312 głosów elektorskich, a Demokraci tylko 226.

[35] I. Weidmann, *Przedterminowe wybory w Niemczech wyzwaniem politycznym i organizacyjnym,* PAP, z dnia 12.11.2024 roku [dostęp: 12.11.2024 r.].

prezydenta elekta wskazują na dążenie do rozwiązania konfliktu. Rezultatem prowadzonej polityki zagranicznej USA będzie doprowadzenie do podpisania przez obie strony pokoju. Intersującym polem staną się zapewne warunki pokoju, których beneficjentem z pewnością będzie Waszyngton. Przewidywać można zbudowanie wpływu USA na wydobycie złóż surowców znajdujących się na ziemiach Ukrainy.

Bibliografia

Baryjka F., *Ingerencje Rosji i Iranu w wybory prezydenckie w USA,* Biuletyn PISM, nr 128(2938), 2 września 2024 roku.

Bożyk S., *Wybory prezydenckie*, „Temida 2", Białystok 1995.

Dąbrowski A., Piotrowski M., *Joe Biden rezygnuje z walki o reelekcję,* Polski Instytut Spraw Międzynarodowych, nr 52/2024, 22 lipca 2024 roku.

Franks A.S., *Warunkowe skutki płci i seksizmu kandydatów na postrzeganą wybieralność i intencje wyborcze: dowody z prawyborów Demokratów w 2020 r*., „Anal Soc Issues Public Policy" 2021, t. 21, nr 1.

Kański L., *Kompetencje Kongresu w zakresie kształtowania polityki zagranicznej Stanów Zjednoczonych Ameryki,* Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza, Poznań 1982.

Laidler P., *Konstytucja Stanów Zjednoczonych Ameryki. Przewodnik,* Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2007.

Pułło A. (tł.), *Konstytucja Stanów Zjednoczonych Ameryki*, Wydawnictwo Sejmowe, Warszawa 2002.

Sieńkowski D. (opr.), *Trump ofiarą ataku hakerskiego? "Ingerencja w wybory",* „Do Rzeczy" z dnia 11.09.2024 roku.

Szymanek J., *Determinanty amerykańskiego systemu prezydenckiego,* Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2014.

Wąsiński M., *Polityka zagraniczna w kampanii wyborczej Donalda Trumpa,* Biuletyn, Polski Instytut Spraw Międzynarodowych, nr 38(1388), 16 czerwca 2016 roku.

Weidmann I., *Przedterminowe wybory w Niemczech wyzwaniem politycznym i organizacyjnym*, PAP z dnia 12.11.2024 roku.

Wszołek R., *Władza ustawodawcza, wykonawcza i sądownicza w ustroju Stanów Zjednoczonych Ameryki* [w:] *Konstytucja USA. Ze studiów nad amerykańskim systemem politycznym,* red. M. Urbańczyk, Ł. Bartosik, M. Tomczak, Wydawnictwo ArchaeGraph, Poznań–Łódź 2018.

Netografia

CyberDefence24, https://cyberdefence24.pl/polityka-i-prawo/wybory-usa-dezinformacja-cyberataki.

CyberDefence24, https://cyberdefence24.pl/cyberbezpieczenstwo/wybory-w-usa-iran-probuje-namieszac.

Forbes, https://www.forbes.com/profile/donald-trump/.

WH. GOV, https://www.whitehouse.gov/administration/vice-president-harris/.

Damian KAROL[1]

ZABEZPIECZENIA DOWODÓW CYFROWYCH W TOKU POSTĘPOWANIA KARNEGO WOBEC WYZWAŃ POSTĘPUJĄCEJ GLOBALIZACJI I CYFRYZACJI

Skutki rozwoju technologii i Internetu

Pierwsze dwie dekady XXI wieku przyniosły ze sobą niespotykany dotąd skokowy rozwój nowoczesnych technologii, rozpowszechnienie na skalę światową zaawansowanej elektroniki, a w konsekwencji urzeczywistnienie pojęcia „globalnej wioski" Herberta McLuhana[2]. Przywołać należy szacunki wskazujące, że w 2000 roku dostęp do Internetu posiadało około 361 milionów osób. W 2010 roku liczba ta wzrosła do około 1 967 miliarda. Obecnie szacuje się, że w 2023 roku dostęp do Internetu posiada około 5 350 miliarda osób[3].

Niewątpliwie tak dynamiczny rozwój dostępu do Internetu oraz technologii (pierwszym smartfonem we współczesnym rozumieniu tego terminu był iPhone, którego premiera miała miejsce w czerwcu 2007 roku[4]) przyczynił się do istotnych zmian w życiu dzięki połączeniu szeregu funkcji w jednym urządzeniu. Obecnie nie jest niczym niespotykanym, aby przy użyciu tylko jednego urządzenia, a w szczególności smartfona, zorganizować całe swoje codzienne życie. Urządzenia te umożliwiają już nie tylko rozmowę i wysyłanie wiadomości SMS, lecz również śledzenie mediów społecznościowych, robienie zakupów online, wykonywanie transakcji bankowych, opłacanie rachunków oraz instalowanie wszelkich aplikacji o różnym przeznaczeniu.

Wszystkie wskazane powyżej udogodnienia, które przyniósł ze sobą początek XXI w., nie pozostały jednak bez negatywnego wpływu na życie codzienne oraz związane z nim ryzyka. Jedną z negatywnych konsekwencji rozwoju technologii, elektroniki oraz powszechnego dostępu do Internetu jest wzrost przestępczości.

---

[1] Asesor Prokuratury Rejonowej dla miasta Rzeszów. ORCID: 0009-0004-8831-4633.

[2] Pojęcie wprowadzone przez M. McLuhana w książce *The Gutenberg galaxy. The making of typographic man*, Toronto Press, Canada 1962 r., ukazujące kierunek zmian zachodzących w mediach elektronicznych, które stopniowo obalają bariery przestrzenne i umożliwiają komunikację na masową skalę.

[3] https://www.forbes.com/home-improvement/internet/internet-statistics/

[4] https://www.apple.com/newsroom/2007/01/09Apple-Reinvents-the-Phone-with-iPhone/

Do najczęściej popełnianych przestępstw, do których dochodzi przy wykorzystaniu telefonów, komputerów oraz Internetu jest czyn stypizowany w art. 286 § 1 kodeksu karnego, to jest przestępstwo oszustwa. Co kluczowe, przepis ten pozostał w zasadzie w niezmienionej formie od czasów kodeksu karnego z 1932 roku[5].

Już wówczas do znamion wskazanego przestępstwa należały znamiona czynu zabronionego, które funkcjonują także obecnie, a przede wszystkim działanie w celu osiągnięcia korzyści majątkowej, wprowadzenie drugiej osoby w błąd co do zamiaru wywiązania się z zawieranej umowy, a finalnie doprowadzenie jej do niekorzystnego rozporządzenia mieniem.

Nie ulega zatem wątpliwości, że twórcy kodeksu karnego z 1932 roku, formułując znamiona przedmiotowe oraz podmiotowe przestępstwa oszustwa nie mogli przewidzieć rozwoju technologii, Internetu, komputerów czy telefonów, a w konsekwencji wykorzystania ich do popełniania przestępstw. Niemniej jednak, stosując się do zasad prawidłowych technik legislacji polegających na tworzeniu przepisów o charakterze możliwie generalnym i abstrakcyjnym, znalazł on skuteczne zastosowanie we współczesnych realiach. Brak jest bowiem ograniczeń, w jaki sposób sprawca czynu zabronionego wprowadza pokrzywdzonego w błąd. Nie ma zatem żadnych przeszkód, aby do wprowadzenia w błąd doszło także za pomocą środków porozumiewania się na odległość, w tym przy wykorzystaniu wszelkich komunikatorów Internetowych i platform społecznościowych.

Zgodnie ze statystykami prowadzonymi przez Policję, w 2000 roku popełniono 80 368 przestępstw oszustwa[6]. W 2010 roku liczba stwierdzonych oszustw utrzymywała się na względnie jednakowym poziomie osiągając liczbę 86 366 czynów zabronionych[7]. Obecnie jednak przestępstwo z art. 286 § 1 k.k. jest jednym z najczęściej popełnianych dochodząc w 2023 roku do poziomu 146 553 popełnionych czynów zabronionych[8]. Dla porównania, odmienna tendencja ma miejsce w przypadku przestępstwa kradzieży stypizowanego w art. 278 § 1 k.k. – w roku 2000 roku stwierdzono popełnienie 226 642 przestępstw kradzieży[9]. W 2010 roku liczba ta nieznacznie spadła do 212 480, jednakże w 2023 roku wyniosła już tylko 110 443[10].

Można zatem wysnuć wniosek, że paradoksalnie rozwój technologii przyczynił się do zmniejszenia ilości przestępstw kradzieży, co można wiązać z upowszechnieniem się możliwości rejestracji obrazu i dźwięku za pomocą kamer monitoringu, zarówno miejskiego jak i prywatnego, telefonów komórkowych, ale także nadajników GPS, które pozwalają zlokalizować skradzione mienie. Z jednej strony zatem skok technologiczny spowodował zwiększenie obawy wykrycia dla

[5] Rozporządzenie Prezydenta Rzeczypospolitej z dnia 11 lipca 1932 r. (Dz.U. z 1932 r., nr 571).
[6] https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-16/63976,Oszustwo-art-286.html.
[7] *Ibidem.*
[8] *Ibidem*.
[9] https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-16/63961,Kradziez-art-278.html.
[10] *Ibidem*.

sprawców typowych przestępstw popełnianych w sposób fizyczny, bezpośredni, z drugiej zaś strony otworzył zupełnie nowe możliwości w zakresie wykwalifikowanej cyberprzestępczości, która pozostaje znacznie trudniejsza do zwalczania dla organów ścigania.

Ślad kryminalistyczny a ślad cyfrowy

Jednym z celów postępowania karnego wskazanych w art. 297 k.p.k. jest wykrycie i ujęcie sprawcy. W przypadku przestępstw popełnianych klasycznie, gdy sprawca rzeczywiście jest na miejscu przestępstwa, co do zasady zawsze dochodzi do pozostawienia fizycznych śladów jego obecności. Przez samo pojęcie śladu w rozumieniu kryminalistycznym należy rozumieć stan rzeczywistości w postaci zjawisk i obiektów materialnych mających związek z badanym zdarzeniem, który jest możliwy i przydatny do badań dla celów kryminalistycznych[11]. Zgodnie z teorią Edmonda Lockarda, francuskiego kryminologa i jednego z ojców współczesnej medycy sądowej, sprawca będący na miejscu przestępstwa zawsze pozostawia za sobą ślad, jak też coś ze sobą zabiera, zgodnie z zasadą, że każdy kontakt zostawia ślad[12].

Powyższe można z łatwością zobrazować na przykładzie przestępstwa kradzieży polegającego na włamaniu do domu. W toku całego procesu sprawca niejako ma szansę na popełnienie licznych błędów, które mogą przyczynić się do jego wykrycia i ujęcia. Zwyczajowo przestępca, który nie posiada wiedzy z zakresu kryminalistyki może chociażby przyłożyć ucho na okna, drzwi celem nasłuchiwania, całkowicie nieświadomy istnienia takiej dziedziny nauki jak otoskopia kryminalistyczna – nauka zajmująca się identyfikacją człowieka na podstawie śladów pozostawionych przez małżowinę uszną[13]. Przykładając ucho do płaskiej powierzchni sprawca może pozostawić nie tylko odbitkę małżowiny, ale również swoje DNA pochodzące z naskórka czy potu. Przedostając się do wnętrza, przełamując zabezpieczenia w postaci zamków, kłódek, sprawca może również nanieść unikatowe ślady w mechaniczne powstałe w wyniku użycia określonego narzędzia i mogące być przedmiotem ekspertyzy mechanoskopijnej[14]. Przemieszczając się po danym pomieszczeniu istnieje realna możliwość pozostawienia śladów obuwia, włosów, odbitek daktyloskopijnych oraz szeregu innych śladów. Jednocześnie, pomijając oczywiście przedmiot kradzieży, sprawca może z miejsca popełnienia

[11] E. Gruza i in., *Kryminalistyka, czyli o współczesnych metodach dowodzenia przestępstw*, Wolters Kluwer, Warszawa, 2020 r., s. 37. Zob. także T. Hanausek, *Kryminalistyka. Zarys wykładu,* Kraków 2005, s. 90; B. Hołyst, *Kryminalistyka,* Warszawa 2018, s. 211.

[12] E. Mistek i in., *Toward Locard's Exchange Principle: Recent Developments in Forensic Trace Evidence Analysis*, "Analytical Chemistry" 2019, Vol. 91, s. 637

[13] B. Hołyst, *Kryminalistyka*, Warszawa 2018, s. 480.

[14] Mechanoskopia – dział kryminalistyki obejmujący ogół metod i środków służących do wykrywania, zabezpieczania i badania w celach identyfikacyjnych śladów, które powstały w wyniku wzajemnego oddziaływania na sienie dwóch lub więcej rzeczy, względnie jednej z nich nas drugą – E. Gruza, i in., *Kryminalistyka..., op.cit.*, s. 569.

czynu, całkowicie nieświadomie zabrać ze sobą ślady w postaci pyłów czy włókien materiałów, z którymi miał styczność.

W przypadku przestępstw popełnianych za pomocą sieci Internet brak jest śladów w powyższym ich rozumieniu, co nie znaczy jednak, że takich śladów nie ma. W przypadku przestępstw popełnianych za pośrednictwem Internetu sprawca może pozostawić za sobą bowiem ślad cyfrowy[15]. Najważniejszym śladem o charakterze cyfrowym pozostawianym przez sprawcę przestępstwa popełnionego za pośrednictwem Internetu jest niewątpliwie adres IP[16]. Oczywiście celem ustalenia sprawcy można również dokonać zabezpieczenia urządzeń cyfrowych takich jak dyski twarde, routery, modemy czy telefony, które przechowują co do zasady dowody cyfrowe w postaci danych świadczących o popełnieniu przestępstwa. Zazwyczaj jednak czynności te są wykonywane jako finalizacja pewnego procesu dowodowego, który doprowadził organy ścigania do miejsca faktycznego pobytu sprawcy czynu zabronionego.

W dobie wspomnianej globalizacji zabezpieczanie śladów o charakterze cyfrowym nastręcza liczne problemy proceduralne organom ścigania. W typowym schemacie przestępstwa oszustwa popełnionego za pośrednictwem Internetu, organy ścigania powinny dokonać ustalenia adresu IP, który został przydzielony przez operatora telekomunikacyjnego sprawcy w czasie popełnienia przestępstwa. Działanie sprawcy, które pozostawia ów cyfrowy ślad będzie zazwyczaj związane z logowaniem się na konto na określonej platformie, z którego następnie dopuścił się przestępstwa, na przykład oszustwa wprowadzając pokrzywdzonego w błąd co do faktycznego zamiaru sprzedaży danego przedmiotu lub na urządzeniu samego pokrzywdzonego przy użyciu ogólnodostępnych aplikacji takich jak AnyDesk[17]. Po ustaleniu adresu IP oraz jego dostawcy, organy ścigania powinny zwrócić się do podmiotu, w którego zasobach dany adres się znajduje celem ustalenia danych osobowych osoby której ustalony adres IP został przydzielony o konkretnej godzinie z dokładnością do sekundy. Po uzyskaniu wskazanych danych oraz po ustaleniu tożsamości należałoby rozważyć dokonanie przeszukania, zatrzymania rzeczy w postaci wszelkiej elektroniki mogącej zawierać dalsze dowody w sprawie, a następnie zlecić biegłym z zakresu informatyki sporządzenie ekspertyzy, by finalnie ogłosić zarzut. Taki scenariusz jest jednak niezwykle rzadki.

Sprawcy przestępstw informatycznych na przestrzeni lat dokonali swoistej ewolucji oraz nie stosują już tak archaicznych schematów umożliwiających ich

---

[15] Obszernie na temat cyfrowych śladów – H. Arsham i in., *Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence*, „Journal of Information Processing System" 2018, Vol. 14, No. 2.

[16] Adres IP pełni funkcję podstawowego identyfikatora w komunikacji cyfrowej umożliwiając ustalenie miejsca źródłowego oraz docelowego określonej transmisji danych – N. Soni i in., *A forensic analysis of AnyDesk Remote Access application by using various forensic tools and techniques*, Forensic Science International: Digital Investigation, 2024.

[17] AnyDesk jest międzyplatformowym oprogramowaniem, które umożliwia jego użytkownikowi zdalny dostęp do innego urządzenia przy użyciu indywidualnego profilu AnyDesk – N. Soni i in., *A forensic analysis of AnyDesk…*, *op.cit.*

wykrycie, co w konsekwencji powoduje szereg trudności w ich ujęciu. Wskazać należy, że dla sprawców przestępstw z wykorzystaniem Internetu nie ma obecnie granic co do miejsca ich działania. Nie ma przeszkód, by dokonać oszustwa na terenie Polski, działając jednak z terytorium jakiegokolwiek innego państwa na świecie. Skupiając się na terytorium Unii Europejskiej istotne znaczenie miało wejście Polski do strefy Schengen w dniu 21 grudnia 2007 roku[18]. Wraz z przystąpieniem Polski do Unii Europejskiej, a następnie do strefy Schengen doszło do otwarcia granic oraz przepływu ludzi i towarów na niespotykaną dotąd skalę. Z danych Głównego Urzędu Statystycznego wynika, że w 2004 roku do Wielkiej Brytanii wyemigrowało około 150 000 Polaków. W 2005 roku liczba ta wzrosła do 340 000, by następnie w 2010 roku osiągnąć poziom 580 000[19].

Wraz z masową emigracją, głównie w celach zarobkowych, nierozerwalnie powiązana jest również emigracja w celach przestępczych. Osoby mające bowiem głównie na celu popełnianie przestępstw doskonale wiedzą, że przebywanie poza terytorium jurysdykcji danego państwa, na terenie którego chcą popełnić przestępstwo znacznie utrudnia pociągnięcie ich do odpowiedzialności karnej. Z tym właśnie problemem mierzyły się i nadal mierzą władze poszczególnych państw, jak też Unii Europejskiej.

Ograniczenia w zakresie zabezpieczania dowodów cyfrowych

Dotychczasową metodą działania organów ścigania realizowaną na podstawie umów bilateralnych z poszczególnymi państwami lub umów wielostronnych było kierowanie wniosków o udzielenie międzynarodowej pomocy prawnej w oparciu o przepisy Europejskiej Konwencji o pomocy prawnej w sprawach karnych z dnia 20 kwietnia 1959 roku. Do polskiego porządku prawnego Konwencja ta weszła w życie z dniem 17 czerwca 1996 roku[20]. Znalazła ona swój wydźwięk w przepisach polskiej procedury karnej. Wskazane przepisy były następnie uzupełniane Decyzjami Ramowymi Rady 2003/577/WSiSW z dnia 22 lipca 2003 roku w sprawie wykonania w Unii Europejskiej postanowień o zabezpieczeniu mienia i środków dowodowych[21] oraz 2008/978/WSiSW w sprawie europejskiego nakazu dowodowego dotyczącego przedmiotów, dokumentów i danych, które mając zostać wykorzystane w postępowaniach w sprawach karnych[22]. Jednakże wskazane

[18] Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 20 grudnia 2007 r. w sprawie wejścia Polski do strefy Schengen (M.P. 2007.100.1085).

[19] https://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5471/2/14/1/informacja_o_rozmiarach_i_kierunkach_czasowej_emigracji_z_polski_w_latach_2004-2020.pdf.

[20] Europejska Konwencja o pomocy w sprawach karnych, sporządzona w Strasburgu dnia 20 kwietnia 1959 r. (Dz.U. 1999.76.854).

[21] Decyzja Ramowa Rady 2003/577/WSiSW z dnia 22 lipca 2003 r. w sprawie wykonania w Unii Europejskiej postanowień o zabezpieczeniu mienia i środków dowodowych (Dz.U. UE. L. 2003.196.45).

[22] Decyzja Ramowa Rady 2008/978/WSiSW w sprawie europejskiego nakazu dowodowego dotyczącego przedmiotów, dokumentów i danych, które mając zostać wykorzystane w postępowaniach w sprawach karnych (Dz.U. UE. L. 2014.130.1.).

wyżej przepisy nie były wystarczające i wraz z rosnącą przestępczością pozostawały w tyle za oczekiwaniami organów ścigania.

Wobec powyższego, w dniu 3 kwietnia 2014 roku wydana została Dyrektywa Parlamentu Europejskiego i Rady nr 2014/41/UE w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych[23]. Dyrektywa ta została implementowana do polskiej procedury karnej ustawą z dnia 10 stycznia 2018 roku o zmianie ustawy Kodeks postępowania karnego oraz niektórych innych ustaw[24]. Celem wprowadzenia Europejskiego Nakazu Dochodzeniowego było między innymi ustalenie jednego wspólnego instrumentu prawnego dla wszystkich sygnatariuszy, aby doprowadzić do ujednolicenia i przyspieszenia uzyskiwania dowodów w toku postępowania karnego. Należy zatem zadać pytanie, czy obowiązujące rozwiązania sprostały oczekiwaniom i pozwalają na skuteczne ściganie sprawców przestępstw popełnianych za pośrednictwem sieci Internet.

Działalność przestępcza w Internecie ma na celu przede wszystkim nie tyle nie zostawianie za sobą śladów, co ich skuteczne zamaskowanie. W tym celu sprawcy używają wielu środków technicznych uniemożliwiających ustalenie miejsca ich działania, a w konsekwencji również tożsamości. Najbardziej powszechnymi sposobami ukrywania swojej aktywności w sieci są chociażby VPN (*Virtual Private Network*[25]), sieć TOR (*The Onion Routing*[26]) czy tworzenie tzw. sieci botnet[27]. Celem każdego ze wskazanych rozwiązań technologicznych, nie zagłębiając się ściśle w sposób ich działania, jest ukrycie własnego adresu IP poprzez zainicjowanie połączenia bądź szeregu połączeń przy wykorzystaniu urządzeń pośredniczących, a w rezultacie zapewnienie użytkownikowi anonimowości w sieci. Co kluczowe, rozwiązania te są powszechne, darmowe, dostępne dla ogółu i nie wymagają znaczącej wiedzy informatycznej.

W praktyce, dla organów ścigania, wykorzystywanie tych ogólnodostępnych środków w działalności przestępczej stwarza wiele problemów proceduralnych z zakresu gromadzenia dowodów. Używając za przykład przestępstwa oszustwa popełnionego za pośrednictwem Internetu, polegającego na wyłudzeniu od pokrzywdzonego pieniędzy w ramach wprowadzenia go w błąd co do zamiaru sprzedaży określonego przedmiotu, po wpłynięciu zawiadomienia o podejrzeniu

[23] Dyrektywa Parlamentu Europejskiego i Rady nr 2014/41/UE w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych z dnia 3 kwietnia 2014 r. (Dz.U. L. 130.1.5.2014).

[24] Ustawa z dnia 10 stycznia 2018 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (Dz.U. z 2018 r., poz. 201).

[25] VPN jest urządzeniem maskującym, serwerem proxy, który pełni funkcję ogniwa pośredniczącego w wymianie informacji między komputerem użytkownika a serwerem docelowym; umożliwia zatajenie adresu IP komputera użytkownika – P. Opitek, *Cyberprzestępczość w pracy prokuratora*, „Prokuratura Krajowa" 2018, s. 63.

[26] Tor jest bezpłatnym oprogramowaniem open source i otwartą siecią umożliwiającą anonimowe przeglądanie Internetu – D. Hayes, *Informatyka w kryminalistyce. Praktyczny przewodnik*, wyd. II, Helion S.A., Gliwice 2021, s. 214.

[27] Botnet to grupa komputerów zainfekowanych złośliwym oprogramowaniem pozostającym w ukryciu przed użytkownikiem i pozwalającym jego twórcy na sprawowanie zdalnej kontroli nad wszystkimi komputerami grupy – B. Hołyst, *Kryminalistyka..., op.cit.,* s. 942.

popełnienia przestępstwa, jak wspomniano powyżej, pierwszą czynnością jest ustalenie adresu IP, przy wykorzystaniu którego sprawca działał – zazwyczaj będzie to dotyczyło adresu IP używanego podczas logowania się na określonej platformie. W tym zakresie należy co do zasady zwrócić się do określonej platformy z postanowieniem o żądaniu wydania rzeczy i zwolnieniu z tajemnicy. Uzyskanie takich danych trwa zazwyczaj do 14 dni. Po wpłynięciu odpowiedzi, za pomocą ogólnodostępnych stron internetowych, można ustalić podmiot świadczący usługi telekomunikacyjne, który posiada w swoich zasobach określony adres IP – co do zasady, w przypadku zaawansowanej przestępczości, będzie to jednak podmiot zagraniczny.

W tym momencie organy ścigania powinny zatem wystąpić z Europejskim Nakazem Dochodzeniowym do państwa członkowskiego-sygnatariusza, na terytorium którego dany podmiot telekomunikacyjny prowadzi działalność. Czynność ta wymaga dopełnienia szeregu wymogów formalnych, takich jak dokonanie tłumaczenia na język urzędowy państwa wykonania nakazu, jak również przekazanie nakazu poprzez określony sąd okręgowy, Ministra Sprawiedliwości, prokuratora okręgowego lub Prokuratora Krajowego – co wynika wprost z przepisu art. 589zb § 1 k.p.k. Oznacza to zatem, że prokuratury rejonowe, w których prowadzone jest zasadnicza większość wszystkich postępowań przygotowawczych nie mają możliwości kierowania nakazów bezpośrednio do krajów członkowskich, bez nadzoru wskazanych powyżej organów. Przepisy w zakresie wystąpienia do państwa członkowskiego nie regulują również czasu, w jakim dane państwa powinno wykonać nakaz. Zgodnie jednak z art. 12 ust. 4 Dyrektywy Parlamentu Europejskiego i Rady nr 2014/41/UE w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych, termin ten winien wynosić 90 dni. Wskazany termin nie jednak wiążący i może być jednak wydłużony, przy wymogu powiadomienia organu państwa występującego o przyczynach opóźnienia.

Po otrzymaniu nakazu przez państwo jego wykonania, odpowiedni organ powinien wystąpić do wskazanego operatora oraz uzyskać dane osoby, któremu dany adres IP został przydzielony w czasie popełnienia czynu zabronionego, a następnie uzyskane dane przekazać do organu państwa występującego z nakazem. Co do zasady jednak uzyskane dane osobowe nie są danymi sprawcy przestępstwa. W rzeczywistości bowiem, w sposób całkowicie nieświadomy urządzenie osoby, której został przydzielony ustalony adres IP mogło zostać wykorzystane przez sprawcę w ramach sieci botnet, VPN albo TOR. Dla ustalenia zatem faktycznego sprawcy niezbędne w zasadzie byłoby zabezpieczenie urządzenia (komputer, tablet, telefon), a następnie zasięgnięcie opinii biegłego z zakresu informatyki celem uzyskania danych dotyczących ewentualnych adresów IP, z których inne urządzenia łączyły się z urządzeniami zabezpieczonymi. Po uzyskaniu tych danych, to jest adresu IP, z którego inne urządzenie nawiązało połączenie z urządzeniami zabezpieczonymi, cała procedura związana z ustaleniem danych osobowych i wystąpieniem z nakazem się powtarza.

Wskazana procedura rodzi wiele problemów przede wszystkim w zakresie retencji danych[28], kosztów postępowania oraz czasu jego trwania. Liczba opisanych powyżej węzłów połączeń może bowiem wynosić od kilku do nawet kilkudziesięciu czy kilkuset. Nie ma zatem faktycznej możliwości w dobie powszechnej globalizacji dla organów ścigania, by skutecznie zabezpieczać dane cyfrowe związane z działalnością przestępczą w Internecie na terenie całego globu. Podkreślić należy, że już samo działanie z terytorium innego państwa, nawet i bez wykorzystywania rozwiązań mających na celu zachowanie anonimowości w sieci, jest istotnie utrudnione, wiąże się z długim czasem oczekiwania na uzyskanie żądanych danych, które następnie należy poddać analizie, w wyniku której możliwe będzie podjęcie dalszych czynności procesowych, w tym wystąpienie z dalej idącym nakazem. To wszystko, dodatkowo przy założeniu, że sprawca przestępstwa działa z terytorium Unii Europejskiej, nie zaś państw położonych poza Wspólnotą – dla przykładu wskazać należy, że na realizację międzynarodowej pomocy prawnej skierowanej do Republiki Chińskiej, przy założeniu, że zostanie ona w ogóle wykonana, oczekuje się nawet i kilka lat – powoduje, że ustalenie tożsamości faktycznego sprawcy przestępstwa staje się w zasadzie niemożliwie, zaś organy ścigania pozostają bezradne. Jedyną bowiem możliwością ustalenia tożsamości sprawcy czynu zabronionego jest popełnienie przez niego błędu w toku czynności anonimizujących aktywność w sieci i dokonanie przestępstwa przy użyciu własnego, autentycznego adresu IP. Podkreślić jednak należy, że nawet w przypadku popełnienia takiego błędu przez sprawcę czynu zabronionego, wymaga to zabezpieczenia możliwie najszerszych danych dotyczących logowań, nierzadko wykraczających poza początkowe ramy postępowania, oraz przeprowadzenia wnikliwej analizy każdego pojedynczego logowania. Czynności te jednak i tak nie gwarantują sukcesu, gdyż o ile wykorzystywane przez sprawcę połączenie nie jest łączem stacjonarnym, a mobilnym, może on do połączenia wykorzystywać karty SIM zarejestrowane na tzw. słupy[29] w krajach spoza Unii Europejskiej bądź karty prepaid pochodzące z państw, w których nie ma obowiązku rejestracji numerów, a które to karty są również powszechnie dostępne do zakupu.

W tym miejscu zarysowuje się również inny problem w postaci odzyskania mienia pokrzywdzonego. Jak bowiem wspomniano powyżej, od momentu złożenia zawiadomienia o podejrzeniu popełnienia przestępstwa przez pokrzywdzonego do czasu uzyskania pierwszych danych pozwalających na podjęcie dalszych czynności dowodowych w sprawie takich jak adresy IP, adresy poczty elektronicznej

[28] Zgodnie z Dyrektywą 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz.U. L. 105.13.04.2006 r.), państwa członkowskie gwarantują retencję danych telekomunikacyjnych na czas nie krótszy niż 6 miesięcy oraz nie dłuższy niż 2 lata.

[29] Mianem „słupa" określa się osobę fizyczną, która z uwagi najczęściej na przymusowe położenie lub niski stopień intelektu jest wykorzystywana, co do zasady nieświadomie, przez sprawców przestępstw, którzy wykorzystują jej dane osobowe.

czy numery telefonów upływa zazwyczaj okres do 14 dni. W tym jednak czasie sprawca czynu zabronionego, po uzyskaniu środków pieniężnych od pokrzywdzonego, ma w zasadzie nieograniczone możliwości korzystania z nich oraz dalszego przekazywania na zagraniczne konta, poprzez zagranicznych pośredników płatności, kończąc na wprowadzeniu ich na giełdy kryptowalutowe. Powyższe prowadzi do sytuacji, w której odzyskanie środków należących do pokrzywdzonego jest mało prawdopodobne. Wyjątkiem są sytuacje, w których algorytmy banków po wytypowaniu podejrzanych transakcji dokonają blokady środków na danym rachunku.

Postulaty w zakresie zmian legislacyjnych

Przedstawiona problematyka wymaga zatem, przynajmniej w zakresie rozwiązań obowiązujących na terytorium Unii Europejskiej, poczynienia działań mających na celu pogłębienie współpracy międzynarodowej w ramach prowadzonych postępowań karnych.

W tym aspekcie podejmowane są określone działania jak chociażby utworzenie Prokuratury Europejskiej na podstawie Rozporządzenia Rady (UE) 2017/1939 z dnia 12 października 2017 roku[30], która rozpoczęła swoją działalność z dniem 1 czerwca 2021 roku. Działalność Prokuratury Europejskiej ogranicza się jednak do zwalczania przestępczości finansowej godzącej interesy finansowe Unii Europejskiej oraz państw członkowskich, specjalizując się w szczególności w zwalczaniu transgranicznej przestępczości VAT-owskiej.

Kolejnym ważnym krokiem, o którym należy wspomnieć, jest wprowadzenie w oparciu o Rozporządzenie Parlamentu Europejskiego z dnia 12 lipca 2023 roku w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności[31] systemu E-evidence. System ten umożliwi bowiem bezpośrednią, elektroniczną komunikację pomiędzy organami ścigania poszczególnych państw (przy zachowaniu wymogów z art. 589zb § 1 k.p.k.) zapewniając możliwość elektronicznego kierowania Europejskich Nakazów Dochodzeniowych. Ponadto możliwe będzie załączanie przez organ państwa wykonującego nakaz w systemie informatycznym wszelkich uzyskanych dowodów, które będą niezwłocznie możliwe do pobrania przez organ państwa wydającego. Podkreślić należy, że nadal niezbędne będzie sporządzenie Europejskiego Nakazu Dochodzeniowego i skierowanie go do właściwego organu zagranicznego, jednakże przeniesienie większości czynności formalnych do

[30] Rozporządzenie Rady (UE) 2017/1939 z dnia 12 października 2017 r. wdrażające wzmocnioną współpracę w zakresie ustanawiania Prokuratury Europejskiej (Dz.U. L. 283. 31.10.2017 r.).

[31] Rozporządzenie Parlamentu Europejskiego z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności (Dz.U. L. 191. 28.07.2023 r.).

systemu elektronicznego bezsprzecznie wpłynie na skrócenie czasu niezbędnego do uzyskania wnioskowanych danych. System ten obecnie znajduje się jednak w fazie testowej.

Wskazane powyżej rozwiązania nie są jednak wystarczające. Powyższe można osiągnąć chociażby poprzez umożliwienie organom występującym z nakazem oraz wykonującym nakaz, bezpośrednią komunikację (jak w przypadku systemu E-evidence), z pominięciem struktur organizacyjnych organów wymiaru sprawiedliwości poszczególnych państw. W tym zakresie należałoby również w ocenie autora odejść od systemu Europejskich Nakazów Dochodzeniowych bądź przemodelować go w sposób, który pozwoli na jego znaczne odformalizowanie. Zauważyć bowiem należy, że występując z nakazem, w sytuacji nawet zwrócenia się z wnioskiem o wykonanie przez organ państwa wykonującego nakaz jednej czynności procesowej, każdorazowo należy kierować formularz składający się łącznie z co najmniej 16 stron. Uwzględniając ponadto konieczność jego drukowania, załączania do akt, przekazywania do organu nadzorującego oraz wykonywania tłumaczeń, celem uzyskania danych, które co do zasady na terytorium państwa wydającego nakaz wymagają wydania jednostronicowego postanowienia, w przypadku nakazu może być koniecznie wydrukowanie ponad 100 stron.

Kluczową jednak zmianą byłoby wprowadzenie na poziomie unijnym przepisów, które zobowiązywałyby operatorów telekomunikacyjnych, pośredników płatności internetowych oraz administratorów danych szeroko pojętych social mediów, oferujących swoje usługi na terytorium Unii Europejskiej, udostępnianie danych na żądanie skierowane przez jakikolwiek uprawniony organ wymiaru sprawiedliwości państwa członkowskiego, całkowicie pomijając konieczność występowania z Europejskim Nakazem Dochodzeniowym. W tym aspekcie, w przeciwieństwie do nadzoru stosowanego w Europejskich Nakazach Dochodzeniowych, można wprowadzić katalog uprawnionych podmiotów na poziomie Prokuratur Okręgowych lub Regionalnych oraz Sądów Okręgowych lub Apelacyjnych z poszczególnych państw, które takie postanowienia mogłyby przekazywać bezpośrednio do danego podmiotu zagranicznego. Jednocześnie podmiot ten dysponując wykazem uprawnionych organów nie miałby wątpliwości co do zasadności i legalności otrzymanego żądania – nie można bowiem wymagać od podmiotów prywatnych, aby znały struktury organizacyjne organów wymiaru sprawiedliwości każdego państwa członkowskiego Unii Europejskich. Rozwiązanie takie nie tylko przyczyniłoby się do szybkości zabezpieczania danych cyfrowych, ale ponadto znacznie uprościłoby procedury związane z ich uzyskiwaniem, jak też istotnie zmniejszyłoby koszty prowadzenia postępowań oraz ograniczałoby się w zasadzie do sporządzenia jednego postanowienia wraz z tłumaczeniem, bez konieczności dokonywania wydruku kilkudziesięciu czy nawet kilkuset stron.

Powyższa propozycja może jednak rodzić znaczne problemy natury prawnej, a w szczególności politycznej. Zauważyć bowiem należy rosnące w ostatnich latach w Europie poparcie dla prawicowych partii politycznych, które co do zasady sprzeciwiają się dalszemu zacieśnianiu więzi i współpracy w rozumieniu

centralizacji organów unijnych pomiędzy państwami członkowskimi proponując tzw. Europę narodów. W tym ujęciu próba wprowadzenia przepisów zobowiązujących zagraniczne podmioty prywatne do udzielania odpowiedzi na żądanie właściwych organów wymiaru sprawiedliwości państw członkowskich może być potraktowana jako naruszenie suwerenności, wejście w uprawnienia ściśle związane z jurysdykcją na terytorium danego państwa oraz oddanie części kompetencji w tak newralgicznej sferze jak postępowanie karne.

Podkreślić jednak należy, że wszelki opór i zgłaszane wątpliwości we wprowadzaniu dalszej integracji pozostają korzystne dla sprawców przestępstw. Dla osób specjalizujących się w przestępstwach międzynarodowych nie istnieją bowiem granice administracyjne państw, bariery suwerenności czy podległości jurysdykcyjnej na obszarze danego państwa. W tym aspekcie przestępczość międzynarodowa, a w szczególności ukierunkowana na popełnianie czynów zabronionych w Internecie pozostaje w dalszym ciągu przed organami ścigania, które nie są wyposażone w dostateczne metody jej zwalczania oraz zapobiegania. Niewątpliwie w aspekcie globalnym nie jest możliwa ścisła, szybka oraz skuteczna współpraca, wzajemna pomoc pomiędzy organami wymiaru sprawiedliwości poszczególnych państw. Tym niemniej na obszarze Unii Europejskiej daje się odczuć zrozumienie tej problematyki i wprowadzanie dalszych rozwiązań mających na celu usprawnienie działalności organów ścigania (E-evidence). Rozwiązania te, pomimo że przecież przełomowe, nie są jednak w dalszym ciągu wystarczające. Należy zatem mieć nadzieję, że kolejnym etapem integracji będzie zwiększenie zakresu uprawnień Prokuratury Europejskiej oraz stopniowe ujednolicanie jej struktur wraz ze strukturami organów ścigania poszczególnych państw.

Kluczowe jednak byłoby zaproponowanie rozwiązań umożliwiających uzyskiwanie danych cyfrowych bezpośrednio przez organy wymiaru sprawiedliwości poszczególnych państw, z pominięciem jurysdykcji terytorialnej, co w sposób istotny skróciłoby czas niezbędny dla ich uzyskania, a w konsekwencji ustalenia tożsamości sprawcy przestępstwa, zwiększania szans na zabezpieczenie środków pochodzących z czynów zabronionych oraz realizację szeroko pojętych celów postępowania karnego.

Bibliografia

Arsham H. et al., *Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence*, „Journal of Information Processing System" 2018, Vol. 14, No. 2.

Gruza E. et al., *Kryminalistyka, czyli o współczesnych metodach dowodzenia przestępstw*, Wolters Kluwer, Warszawa, 2020.

Hanausek T., *Kryminalistyka. Zarys wykładu,* Kraków 2005.

Hayes D., *Informatyka w kryminalistyce. Praktyczny przewodnik*, wyd II, Helion S.A., Gliwice 2021.

Hołyst B., *Kryminalistyka,* Warszawa 2018.

McLuhan M., *The Gutenberg galaxy. The making of typographic man*, Toronto Press, Canada 1962.

Mistek E. et al., *Toward Locard's Exchange Principle: Recent Developments in Forensic Trace Evidence Analysis*, "Analytical Chemistry" 2019, Vol. 91.

Opitek P., *Cyberprzestępczość w pracy prokuratora*, „Prokuratura Krajowa" 2018.

Soni N. et al., *A forensic analysis of AnyDesk Remote Access application by using various forensic tools and techniques*, Forensic Science International: Digital Investigation, 2024.

Akty normatywne

Decyzja Ramowa Rady 2003/577/WSiSW z dnia 22 lipca 2003 r. w sprawie wykonania w Unii Europejskiej postanowień o zabezpieczeniu mienia i środków dowodowych (Dz.U. UE. L. 2003.196.45).

Decyzja Ramowa Rady 2008/978/WSiSW w sprawie Europejskiego Nakazu Dowodowego dotyczącego przedmiotów, dokumentów i danych, które mając zostać wykorzystane w postępowaniach w sprawach karnych (Dz.U. UE. L. 2014.130.1.).

Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE (Dz.U. L. 105.13.04.2006 r.)

Dyrektywa Parlamentu Europejskiego i Rady nr 2014/41/UE w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych z dnia 3 kwietnia 2014 r. (Dz.U. L. 130.1.5.2014).

Europejska Konwencja o pomocy w sprawach karnych, sporządzona w Strasburgu dnia 20 kwietnia 1959 r. (Dz.U. 1999.76.854).

Rozporządzenie Parlamentu Europejskiego z dnia 12 lipca 2023 r. w sprawie europejskich nakazów wydania i europejskich nakazów zabezpieczenia dowodów elektronicznych w postępowaniu karnym oraz w postępowaniu karnym wykonawczym w związku z wykonaniem kar pozbawienia wolności (Dz.U. L. 191. 28.07.2023 r.).

Rozporządzenie Prezydenta Rzeczypospolitej z dnia 11 lipca 1932 r. (Dz.U. z 1932 r., nr 571).

Rozporządzenie Rady (UE) 2017/1939 z dnia 12 października 2017 r. wdrażające wzmocnioną współpracę w zakresie ustanawiania Prokuratury Europejskiej (Dz.U. L. 283. 31.10.2017 r.).

Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 20 grudnia 2007 r. w sprawie wejścia Polski do strefy Schengen (M.P. 2007.100.1085).

Ustawa z dnia 10 stycznia 2018 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (Dz.U. z 2018 r., poz. 201).

Netografia

https://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5471/2/14/1/informacja_o_rozmiarach_i_kierunkach_czasowej_emigracji_z_polski_w_latach_2004-2020.pdf.

https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-16/63976,Oszustwo-art-286.html.

https://statystyka.policja.pl/st/kodeks-karny/przestepstwa-przeciwko-16/63961,Kradziez-art-278.html.

https://www.apple.com/newsroom/2007/01/09Apple-Reinvents-the-Phone-with-iPhone/.

https://www.forbes.com/home-improvement/internet/internet-statistics/.

Kacper MAZUREK[1]

INSTYTUCJONALNY WYMIAR POLITYKI MIGRACYJNEJ W UNII EUROPEJSKIEJ

Wstęp

Polityka migracyjna Unii Europejskiej stanowi jeden z fundamentalnych obszarów współpracy państw członkowskich. Jego znaczenie w ostatnich dekadach, w kontekście kryzysów migracyjnych i rosnącej liczby osób ubiegających się o azyl, stało się szczególnie widoczne. Zjawisko migracji międzynarodowych ma wymiar globalny i jest ściśle związane z szerokim wachlarzem kwestii politycznych, społecznych, ekonomicznych i humanitarnych. Działania podejmowane przez Unię Europejską w tej dziedzinie nie są przypadkowe ani nie stanowią też wynik doraźnych potrzeb. Stanowią one efekt wieloletnich procesów instytucjonalnych, które kształtowały wspólną politykę migracyjną bazując na wartościach solidarności, sprawiedliwości i poszanowania praw człowieka. Instytucjonalny wymiar polityki migracyjnej w UE jest wynikiem skomplikowanej interakcji pomiędzy instytucjami unijnymi, państwami członkowskimi oraz różnorodnymi agencjami i organizacjami międzynarodowymi.

W ciągu ostatnich lat, kwestie migracyjne w UE stały się również przedmiotem intensywnej debaty politycznej, w której szczególnie ważne są różnice zdań pomiędzy krajami „starej" i „nowej" Europy. Państwa członkowskie różnią się nie tylko w kwestii liczby migrantów, których są w stanie przyjąć, ale także w ocenie efektywności polityki azylowej oraz jej wpływu na systemy społeczno-ekonomiczne. Istnieje także problem zdefiniowania wspólnego stanowiska w zakresie reformy polityki azylowej i migracyjnej, która w kontekście narastających napięć politycznych w UE oraz zmieniających się wyzwań globalnych, wymaga nowego podejścia[2].

Warto więc zwrócić uwagę na to, czym są migracje. *Encyklopedia PWN* definiuje je jako: „migracje [łac. *migratio* 'przesiedlenie'], demogr. wędrówki albo ruch mechaniczny (fizyczny) ludności; element i podstawowa (obok cyrkulacji) forma mobilności przestrzennej; oznaczają przemieszczenia terytorialne związane ze względnie trwałą zmianą miejsca zamieszkania. Oznaczają przemieszczenia

[1] Politechnika Rzeszowska, Wydział Zarządzania. ORCID: 0009-0002-0818-7407.

[2] A. Nickel, A. Nowak, *Trendy migracyjne w XXI wieku*, „Roczniki Studenckie Akademii Wojsk Lądowych" 2017, nr 1, s. 109.

terytorialne związane ze względnie trwałą zmianą miejsca zamieszkania. Według kryterium czasu migracje dzieli się na stałe (trwała zmiana miejsca zamieszkania), czasowe (sezonowa lub okresowa zmiana miejsca zamieszkania), wahadłowe (codzienne dojazdy z miejsca zamieszkania do miejsca pracy lub nauki). Ze względu na odległość rozróżnia się migracje: wewnętrzne (w obrębie danego państwa – wewnątrzregionalne lub międzyregionalne), zewnętrzne (poza granice państwa – kontynentalne, międzykontynentalne). Biorąc pod uwagę organizację można wyróżnić migracje: żywiołowe, planowe (np. repatriację), legalne, nielegalne, dobrowolne, przymusowe (przesiedlenia, wysiedlenia, deportacje). W zależności od przyczyn migracje dzieli się na: zarobkowe, rodzinne, narodowościowe, religijne, polityczne, rekreacyjne, turystyczne. Specyficzne są migracje pozorne spowodowane zmianami administracyjnymi jednostek osiedleńczych, np. włączeniem wsi do obszaru miasta. Napływ ludności na dane terytorium to imigracja, odpływ to emigracja. Powrót do dawnego miejsca zamieszkania (migracja powrotna), to reemigracja. Miary zjawisk migracji stosowane w demografii to: migracja brutto – suma imigracji i emigracji; saldo migracji (migracja netto) – różnica między napływem i odpływem ludności”[3]. Tak więc migracje są niezwykle rozbudowanym zjawiskiem, mającym zależnie od ich rodzaju zupełnie inne podłoże. Z tego względu stanowią one wyzwanie dla całej Unii Europejskiej.

Historia polityki migracyjnej w Unii Europejskiej

Po zakończeniu II wojny światowej jednym z głównych celów powstających Wspólnot Europejskich, w skład których wchodziły Europejska Wspólnota Węgla i Stali, Europejska Wspólnota Gospodarcza (od 1993 roku pod nazwą Wspólnota Europejska) i Europejska Wspólnota Energii Atomowej, była odbudowa gospodarki. Wiązało się to z potrzebą zapewnienia taniej siły roboczej[4]. W latach 50. i 60. XX wieku państwa członkowskie Wspólnot Europejskich podpisały umowy z krajami takimi jak Turcja, Maroko czy Włochy, umożliwiając ich obywatelom migrację do Europy w celu podjęcia pracy. Była to głównie migracja zarobkowa, na którą odpowiadały polityki imigracyjne ukierunkowane na zapewnienie siły roboczej. W tym okresie Wspólnoty Europejskie koncentrowały się przede wszystkim na integracji gospodarczej, a polityki migracyjne były w dużej mierze uzależnione od potrzeb rynku pracy, a nie na poziomie wspólnotowym. Po zakończeniu boomu gospodarczego w latach 70. i kryzysie naftowym[5], migracja zarobkowa

[3] *Encyklopedia powszechna PWN,* Warszawa 2010, t. 21, s. 384.

[4] A. Gruszczak, *Historia współpracy w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych: od TREVI do Tampere* [w:] *Obszar wolności, bezpieczeństwa i sprawiedliwości Unii Europejskiej. Geneza, stan i perspektywy rozwoju*, red. F. Jasiński, K. Smoter, Warszawa 2005, s. 7.

[5] Mowa o kryzysie naftowym z 1973 roku. Powodem kryzysu było embargo naftowe ogłoszone przez państwa członkowskie Organizacji Krajów Eksportujących Ropę Naftową (OPEC). Celem embargo było odwetowanie na Zachodzie za wsparcie udzielane Izraelowi w trakcie wojny Jom Kipur (wojna Izraela z koalicją Egiptu i Syrii). Wówczas kraje należącym do OPEC (Arabia Saudyjska, Iran i Irak) skoordynowały swoje działania i wprowadziły ograniczenia w eksporcie

zaczęła maleć, a niektóre państwa zaczęły podejmować pierwsze próby regulacji napływu imigrantów. W latach 80. i 90. XX wieku wraz z rozwojem Jednolitego Rynku Europejskiego migracja stała się coraz bardziej złożonym zagadnieniem. Z jednej strony, w ramach przynależności do Wspólnoty Europejskiej, obywatele państw członkowskich mogli swobodnie przemieszczać się i osiedlać w innych krajach członkowskich. Z drugiej strony narastały problemy związane z migracją spoza Wspólnoty Europejskiej, zarówno w kontekście osób szukających pracy, jak i uchodźców[6].

Po zakończeniu zimnej wojny doszło do otwarcia nowych granic, co doprowadziło do nowych wyzwań migracyjnych, w tym do napływu uchodźców z krajów ogarniętych konfliktami takich jak Bałkany czy Bliski Wschód[7]. W 1990 roku przyjęto Konwencję Dublińską, której celem było ustalenie zasad odpowiedzialności państw członkowskich za rozpatrywanie wniosków o azyl. Konwencja miała na celu zapobieganie tzw. forum shopping, czyli składaniu wielu wniosków o azyl w różnych krajach UE, co mogło prowadzić do nadmiernych obciążeń niektórych państw. Po utworzeniu Unii Europejskiej z państw członkowskich Wspólnot Europejskich w 1993 roku kwestie migracji zaczęły stawać się integralną częścią polityki zewnętrznej UE. W 2001 roku, w wyniku zamachów z 11 września w Stanach Zjednoczonych[8], zaczęto zauważać potrzebę zacieśnienia współpracy w zakresie polityki azylowej i ochrony granic[9].

W 2004 roku powołano Europejską Agencję Straży Granicznej i Przybrzeżnej – Frontex[10]. Miała ona na celu wspomaganie państw członkowskich w zarządzaniu granicami zewnętrznymi UE oraz monitorowanie sytuacji migracyjnej. W 2004 roku, po rozszerzeniu UE o państwa Europy Środkowej i Wschodniej, migracja stała się jednym z kluczowych tematów w dyskusji na temat przyszłości Unii. Nowe państwa członkowskie, takie jak Polska, Czechy czy Węgry stanowiły głównych beneficjentów swobody przepływu osób w ramach rynku pracy UE. Jednocześnie państwa te wprowadziły nowe wyzwania związane z różnicami w politykach migracyjnych między starymi a nowymi członkami Unii.

---

ropy naftowej do krajów zachodnich, w tym do Stanów Zjednoczonych i Europy. Spowodowało to nagły spadek dostępności ropy na światowym rynku i gwałtowny wzrost cen surowca. Ponadto do kryzysu naftowego przyczyniło się również narastające zapotrzebowanie na ropę naftową ze strony rozwijających się gospodarek, takich jak Japonia i kraje europejskie, https://hist.pl/rewolucyjny-kryzys-naftowy-1973-jak-ropa-naftowa-pokonala-swiat/ [dostęp: 09.11.2024 r.].

[6] J. Jagielski, *Status cudzoziemca w Polsce*, Warszawa 1997, s. 87.

[7] J. Chlebny, *Postępowanie w sprawie o nadanie statusu uchodźcy*, Warszawa 2011, s. 15.

[8] Mowa o zamachu dokonanego przez grupę dziewiętnastu osób powiązanych z Al-kaidą. Rano 11 września 2001 roku zakupili oni bilety na cztery samolotowe loty krajowe. Następnie po ich przejęciu skierowali je w strategiczne cele na terenie Stanów Zjednoczonych, https://historia.dorzeczy.pl/historia-wspolczesna/199495/zamach-na-world-trade-center-11-wrzesnia-2001-trauma-usa-trwa-do-dzis.html [dostęp: 09.11.2024 r.].

[9] M. Pacek, *Polska polityka migracyjna na tle rozwiązań i doświadczeń Unii Europejskiej*, „Studia Europejskie" 2005, nr 4, 2005, s. 48-50.

[10] Frontex – szerzej zostanie ona omówiona w dalszej części rozdziału.

Kryzys migracyjny z lat 2015–2016[11] stanowił punkt zwrotny w historii polityki migracyjnej UE. Napływ uchodźców z Syrii, Afganistanu, Iraku i innych krajów objętych wojną i niestabilnością wywołał debatę na temat solidarności państw członkowskich[12]. W wyniku tego kryzysu UE wprowadziła szereg rozwiązań mających na celu zarządzanie migracją takich jak obowiązkowe systemy relokacji uchodźców i zwiększenie finansowania dla państw sąsiednich, które przyjmowały ich największą liczbę.

Po kryzysie migracyjnym z lat 2015–2016 polityka migracyjna UE stała się bardziej zróżnicowana. Z jednej strony Unia Europejska starała się kontynuować proces integracji migrantów i uchodźców, zwłaszcza poprzez zwiększenie współpracy z państwami trzecimi[13] i wzmocnienie mechanizmów azylowych. Z drugiej strony, pod wpływem rosnącej fali populistycznych nastrojów w niektórych państwach członkowskich, polityka UE zaczęła bardziej koncentrować się na bezpieczeństwie granic i kontrolach migracyjnych.

Wprowadzono nowe regulacje w zakresie polityki azylowej, takie jak tzw. Nowy Pakt w sprawie Migracji i Azylu z 2020 roku, który miał na celu poprawę współpracy państw członkowskich w kwestiach przyjmowania i rozpatrywania wniosków o azyl, a także wzmocnienie współpracy z krajami pochodzenia migrantów. Pakt ten jednak nie rozwiązał wszystkich napięć w Unii, szczególnie w kwestii podziału odpowiedzialności między państwa członkowskie w zakresie przyjmowania uchodźców.

Wyzwania związane z migracją zmieniają się w zależności od sytuacji globalnej i regionalnej. Rośnie liczba osób migrujących z powodu zmian klimatycznych, niestabilności politycznej, a także rosnących nierówności gospodarczych. Problemy związane z nielegalną migracją, handlem ludźmi i kryzysami humanitarnymi pozostają kwestiami, które wymagają coraz bardziej skoordynowanych działań zarówno w obrębie UE, jak i spoza niej. Wspólna polityka migracyjna UE zmienia się w odpowiedzi na te wyzwania, balansując pomiędzy ochroną granic, zapewnieniem prawa do azylu, integracją migrantów a utrzymaniem solidarności między państwami członkowskimi[14]. Decyzje podejmowane na poziomie unijnym wpływają nie tylko na przyszłość polityki migracyjnej, ale również na spójność społeczną i polityczną Unii Europejskiej.

---

[11] Kryzys migracyjny z lat 2015–2016 był spowodowany postępującą destabilizacją na Bliskim Wschodzie i w Afryce, który osiągnął swoje apogeum w latach 2015–2016. P. Kolbusz, *Kryzys migracyjny 2015 roku w Europie i sytuacja uchodźców w czasie pandemii – czy kryzys skończył się na dobre i jaki wpływ na migrantów ma epidemia wirusa COVID-19?*, „Acta Erasmiana", red. M. Sadowski, K. Gaweł, M. Popielarski, K. Strużyński, t. 20, Wrocław 2021, s. 26.

[12] D. Heinrich-Hamera, *Międzynarodowa ochrona uchodźców wewnętrznych. Aspekty prawne i praktyka*, Warszawa 2005, s. 17-31.

[13] Państwa trzecie – są to państwa niebędące członkami Unii Europejskiej.

[14] A. Potyrała, *Kryzys uchodźczy a przyszłość unijnego systemu azylowego* [w:] *Uchodźcy w Europie – uwarunkowania, istota, następstwa*, red. K.A. Wojtaszczyk, J. Szymańska, Wydawnictwo ASPRA-JR, Warszawa 2016, s. 159-164.

Instytucje kontrolujące przepływ migracji w Unii Europejskiej

W odpowiedzi na wzrost liczby osób ubiegających się o azyl Unia Europejska opracowała szereg mechanizmów kontrolujących ten proces. Przepływ migrantów regulują zarówno instytucje unijne, jak i państwa członkowskie, które współpracują ze sobą w celu zapewnienia bezpieczeństwa, sprawiedliwości i efektywności w zarządzaniu migracją.

Jedną z kluczowych instytucji odpowiedzialnych za kontrolowanie przepływu migrantów w Unii Europejskiej jest Frontex[15], czyli Europejska Agencja Straży Granicznej i Przybrzeżnej. Została ona utworzona w 2004 roku na podstawie Rozporządzenia Rady (WE) nr 2007/2004 z dnia 26 października 2004 r. ustanawiającej Europejską Agencję Zarządzania Współpracą Operacyjną na Zewnętrznych Granicach Państw Członkowskich Unii Europejskiej i ma za zadanie wspierać państwa członkowskie UE w zarządzaniu granicami zewnętrznymi, zarówno w zakresie ochrony granic, jak i w zapewnianiu bezpieczeństwa. Frontex koordynuje operacje patrolowe na granicach, organizuje akcje ratunkowe na morzu, a także pomaga w zarządzaniu procedurami związanymi z migracją i weryfikacją dokumentów. Agencja ma również uprawnienia do przeprowadzania działań prewencyjnych w zakresie zapobiegania nielegalnej migracji, przemytowi ludzi, czy też handlowi ludźmi. W ostatnich latach rola Frontexu została znacząco wzmocniona, szczególnie w kontekście kryzysów migracyjnych, takich jak kryzys uchodźczy z 2015 roku. Frontex współpracuje z innymi agencjami unijnymi zajmującymi się ochroną granic państw członkowskich, aby skutecznie zarządzać migracją.

EASO[16] (*European Asylum Support Office*) to agencja Unii Europejskiej, która pełni ważną rolę w zakresie wspierania procedur azylowych w państwach członkowskich. Została utworzona w 2010 roku na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 439/2010 z dnia 19 maja 2010 roku w sprawie utworzenia Europejskiego Urzędu Wsparcia w dziedzinie Azylu, a jej głównym celem jest zapewnienie jednolitych standardów i procedur w sprawach azylowych na terenie całej UE. EASO pomaga w przetwarzaniu wniosków azylowych, organizuje szkolenia dla pracowników administracji krajowej, a także dostarcza analizy na temat sytuacji uchodźczej w różnych regionach świata. Agencja wspiera również państwa członkowskie w zakresie oceny i przyjmowania wniosków azylowych oraz integracji uchodźców. Ponadto EASO współpracuje z Frontexem, organizując wspólne operacje, które pomagają w ochronie granic oraz w procesie selekcji wniosków azylowych, szczególnie w państwach, które borykają się z największymi obciążeniami w tej dziedzinie.

---

[15] Rozporządzenie Rady (WE) nr 2007/2004 z dnia 26 października 2004 r. ustanawiające Europejską Agencję Zarządzania Współpracą Operacyjną na Zewnętrznych Granicach Państw Członkowskich Unii Europejskiej (Dz.U. L 349 z 25.11.2004 r.), p. 1-11.

[16] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 439/2010 z dnia 19 maja 2010 r. w sprawie utworzenia Europejskiego Urzędu Wsparcia w dziedzinie Azylu (Dz.U. L 132 z 29.05.2010 r.), p. 11-28.

Europol[17] – agencja zajmująca się współpracą policyjną na poziomie Unii Europejskiej. Została powołana na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 roku w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol). Jej celem jest wspieranie krajowych służb porządkowych w walce z międzynarodową przestępczością, w tym z nielegalną migracją. Europol dostarcza państwom członkowskim informacje wywiadowcze, które pomagają w zwalczaniu organizacji przestępczych zajmujących się handlem ludźmi czy przemytem migrantów. Europol pomaga także w koordynowaniu działań między krajami UE w zakresie rozwoju polityk i strategii przeciwdziałania nielegalnej migracji. Zajmuje się również wspieraniem ścigania przestępców organizujących nielegalne przejścia graniczne, handel ludźmi, czy inne formy przestępczości związanej z migracją.

Komisja Europejska[18] powstała na podstawie Traktatu o Unii Europejskiej. Pełni kluczową rolę w opracowywaniu polityki migracyjnej UE. To właśnie ona proponuje nowe przepisy dotyczące migracji, azylu i kontroli granic. Jej zadaniem jest także monitorowanie wdrażania tych przepisów przez państwa członkowskie. Komisja Europejska nadzoruje w szczególności system Dublina, który określa, który kraj UE jest odpowiedzialny za rozpatrzenie wniosku o azyl. Jej działania obejmują także opracowywanie i wdrażanie programów mających na celu integrację migrantów, w tym uchodźców, oraz zapewnianie sprawiedliwego dostępu do azylu.

Trybunał Sprawiedliwości Unii Europejskiej[19] powstał na podstawie art. 13 i 257 Traktatu o Unii Europejskiej. TSUE odgrywa istotną rolę w zapewnianiu przestrzegania prawa UE w kontekście migracji. Rozpatruje również sprawy dotyczące interpretacji przepisów unijnych, w tym tych odnoszących się do prawa azylowego i migracyjnego. Jego wyroki mają kluczowe znaczenie w kształtowaniu polityki migracyjnej, szczególnie w przypadku spornych kwestii między państwami członkowskimi a instytucjami unijnymi. TSUE ma również wpływ na orzecznictwo związane z ochroną praw migrantów, zwłaszcza w kontekście zapewniania godziwych warunków przyjmowania uchodźców czy przestrzegania zasad procedur azylowych.

FRA[20] (*Fundamental Rights Agency*) powstała na podstawie Rozporządzenia Rady (WE) nr 168/2007 z dnia 15 lutego 2007 roku ustanawiającego Agencję Praw Podstawowych Unii Europejskiej. Zadaniem agencji jest monitorowanie i wspieranie przestrzegania praw podstawowych na terenie Unii Europejskiej. W kontekście migracji, agencja skupia się na ochronie ich praw, zapewniając im dostęp do

[17] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz.U. L 135 z 24.05.2016 r.), p. 53-114.

[18] Traktat o Unii Europejskiej (Dz.U. C 191 z 29.7.1992 r.), s. 1-112.

[19] *Ibidem*.

[20] Rozporządzenie Rady (WE) nr 168/2007 z dnia 15 lutego 2007 r. ustanawiające Agencję Praw Podstawowych Unii Europejskiej (Dz.U. L 53 z 22.02.2007 r.), p. 1-14.

sprawiedliwości, ochrony przed dyskryminacją oraz innych praw wynikających z przynależności do UE. FRA współpracuje z państwami członkowskimi, organizacjami pozarządowymi i innymi instytucjami unijnymi, aby poprawić sytuację migrantów, szczególnie w kontekście problemów związanych z ich przyjęciem, procedurą azylową i integracją.

Ponadto Wspólna Polityka Migracyjna[21] UE (*Common Migration Policy*) została utworzona na podstawie Traktatu z Amsterdamu i ma kluczowe znaczenie w zarządzaniu migracją na poziomie całej Unii. Ma ona na celu zapewnienie jednolitego podejścia do kwestii migracyjnych, które obejmują nie tylko kontrolowanie granic, ale także wprowadzanie odpowiednich mechanizmów integracyjnych dla migrantów. Polityka ta jest realizowana przez różne mechanizmy, takie jak systemy wymiany informacji, wspólne działania w zakresie bezpieczeństwa czy umowy z państwami spoza UE dotyczące współpracy w kwestii migracji. Unia Europejska stara się stworzyć ramy dla legalnej migracji, które pozwalają migrantom na przybycie i pracę w UE w sposób zgodny z jej zasadami, z uwzględnieniem potrzeb rynku pracy poszczególnych państw członkowskich.

Dodatkowo UE promuje integrację migrantów poprzez różne inicjatywy i projekty, które wspierają ich aktywność na rynku pracy, edukację, uczestnictwo społeczne oraz dostęp do podstawowych usług publicznych. W związku z nią organizowany jest również Wspólny Europejski System Azylowy (*Common European Asylum System* – CEAS). Ten filar polityki migracyjnej ma na celu zapewnienie ochrony osobom uciekającym przed prześladowaniami i zagrożeniami w ich krajach pochodzenia, zgodnie z międzynarodowym prawem i wartościami unijnymi.

System azylowy bazuje na wspólnych standardach i procedurach dotyczących przyjmowania uchodźców i rozpatrywania wniosków azylowych. Ponadto celem Wspólnej polityki migracyjnej jest zwalczanie nielegalnej migracji i ochrona granic zewnętrznych. Wspólna Polityka Migracyjna kładzie duży nacisk na walkę z organizacjami przemytniczymi, które nielegalnie sprowadzają migrantów na teren UE, często naruszając prawa człowieka. UE dąży do współpracy z krajami pochodzenia i tranzytu migrantów, aby wspólnie zarządzać migracją, kontrolować przepływy migracyjne oraz zapobiegać przyczynom migracji, takim jak ubóstwo, konflikty i brak perspektyw gospodarczych. Ta współpraca obejmuje umowy powrotowe, wspólne projekty rozwojowe i inne formy współpracy.

W ramach Wspólnej Polityki Migracyjnej podkreśla się konieczność współpracy i dzielenia się odpowiedzialnością między państwami członkowskimi. Celem jest zapewnienie, że obciążenie związane z migracją jest równomiernie rozłożone w całej Unii, zwłaszcza w sytuacjach kryzysowych.

[21] Traktat z Amsterdamu zmieniający Traktat o Unii Europejskiej, traktaty ustanawiające Wspólnoty Europejskie i niektóre związane z nimi akty (Dz.U. C 340 z 10.11.1997 r.), s. 1-144.

Najważniejsze regulacje migracji w Unii Europejskiej

Na przestrzeni lat funkcjonowania UE wprowadzono, zmieniono, a także uchylono szereg dokumentów dotyczących migracji. Celem takich zmian jest proces aktualizowania i dostosowania prawa do sytuacji panującej zarówno w UE, jak i poza jej granicami.

Dyrektywa Rady 2003/109/WE z dnia 25 listopada 2003 roku dotycząca statusu obywateli państw trzecich będących rezydentami długoterminowymi[22] ma na celu uregulowanie sytuacji osób, które nie są obywatelami państw członkowskich Unii Europejskiej, ale zamieszkują na jej terytorium przez dłuższy czas. Dyrektywa ustanawia ich prawo do pobytu, pracy, dostępu do świadczeń społecznych oraz w odniesieniu do integracji społecznej i gospodarczej w państwach członkowskich. Dodatkowo ustanawia wspólne zasady dotyczące przyznawania statusu rezydenta długoterminowego dla obywateli państw trzecich. Jej celem jest ujednolicenie standardów w państwach członkowskich UE dotyczących wydawania zezwoleń na pobyt długoterminowy. Obywatele państw trzecich, którzy uzyskają status rezydenta długoterminowego mają prawo do porównywalnych warunków życia i pracy z obywatelami państw członkowskich UE. W ten sposób dyrektywa wspiera ich integrację w społeczeństwie oraz rynku pracy UE. Ponadto wzmacnia prawa rezydentów długoterminowych oferując im pewne prawa i przywileje takie jak możliwość zmiany miejsca zamieszkania w obrębie Unii, dostęp do edukacji, opieki zdrowotnej oraz zabezpieczeń społecznych.

Rozporządzenie (WE) nr 1987/2006, znane również jako rozporządzenie ustanawiające System Informacyjny Schengen drugiej generacji (SIS II)[23], odgrywa kluczową rolę w zarządzaniu granicami i kontrolach migracyjnych w ramach strefy Schengen. Celem tego rozporządzenia jest utworzenie, funkcjonowanie i użytkowanie systemu, który umożliwia szybsze i bardziej efektywne wymiany informacji między państwami członkowskimi. SIS II pozwala na wpisanie danych osób, którym odmówiono wjazdu do państw Schengen lub został wydany nakaz deportacji. System umożliwia służbom granicznym oraz policji weryfikowanie czy osoby przekraczające granicę są poszukiwane. Przez gromadzenie i udostępnianie informacji o osobach podejrzanych o nielegalną migrację lub przestępstwa związane z nielegalnym przekraczaniem granic SIS II umożliwia szybkie podjęcie działań na poziomie granicy. Osoby, które zostały zidentyfikowane w systemie mogą zostać zatrzymane i poddane dalszej weryfikacji, w tym sprawdzeniu tożsamości, statusu prawnego i ewentualnych powiązań z działalnością przestępczą. Dzięki SIS II służby graniczne mogą sprawniej identyfikować osoby, które próbują przekroczyć granice w sposób nielegalny oraz prowadzić skuteczniejsze procedury deportacyjne. W przypadku migrantów, którzy mają zakaz

[22] Dyrektywa Rady 2003/109/WE z dnia 25 listopada 2003 r. dotycząca statusu obywateli państw trzecich będących rezydentami długoterminowymi (Dz.U. L 16 z 23.01.2004 r.), p. 44-53.

[23] Rozporządzenie (WE) nr 1987/2006 – utworzenie, funkcjonowanie i użytkowanie Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. L 381 z 28.12.2006 r.), p. 4-23.

wjazdu lub są poszukiwani system pozwala na ich natychmiastowe zatrzymanie i podjęcie odpowiednich działań prawnych. SIS II pozwala na monitorowanie dokumentów podróży, takich jak paszporty i wizy, które mogą być używane do nielegalnego przekraczania granic. Może to obejmować wykorzystywanie fałszywych lub skradzionych dokumentów przez migrantów starających się o azyl lub próbujących wejść do strefy Schengen bez ważnych dokumentów.

Dyrektywa Rady 2009/50/WE z dnia 25 maja 2009 roku w sprawie warunków wjazdu i pobytu obywateli państw trzecich w celu podjęcia pracy w zawodzie wymagającym wysokich kwalifikacji[24], znana jako Dyrektywa o Niebieskiej Karcie UE, ma na celu ułatwienie migracji wykwalifikowanych pracowników z państw trzecich do krajów Unii Europejskiej. Dyrektywa wprowadza jednolite zasady dotyczące warunków wjazdu i pobytu obywateli państw trzecich, którzy przyjeżdżają do UE w celu podjęcia pracy w zawodzie wymagającym wysokich kwalifikacji. Jest to element polityki migracyjnej Unii Europejskiej, który ma na celu przyciągnięcie wysoko wykwalifikowanych specjalistów do Europy. Powodem jest zapotrzebowanie w takich branżach jak technologie informacyjne, inżynieria, nauki przyrodnicze czy medycyna. Dyrektywa ma na celu uproszczenie procedur migracyjnych dla pracowników o wysokich kwalifikacjach. Ponadto wprowadza wspólne ramy prawne dla wszystkich państw członkowskich Unii Europejskiej, które mają obowiązek dostosowania swoich krajowych przepisów do wymogów dyrektywy. Dzięki temu proces ubiegania się o wjazd i pobyt staje się bardziej przejrzysty i jednolity w całej Unii.

Dyrektywa zakłada również, że państwa członkowskie będą stosować uproszczone procedury przyznawania zezwoleń na pobyt i pracę. Wszystko to ma na celu zachęcenie wysoko wykwalifikowanych pracowników do wyboru UE jako miejsca do pracy i życia. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 439/2010 z dnia 19 maja 2010 roku dotyczy utworzenia Europejskiego Urzędu Wsparcia w dziedzinie Azylu[25] (EASO). Rozporządzenie ma kluczowe znaczenie w kontekście migracji oraz systemu azylowego Unii Europejskiej. EASO ma na celu wspieranie państw członkowskich Unii Europejskiej w obszarze zarządzania wnioskami o azyl oraz poprawę współpracy między krajami UE w tej dziedzinie.

Celem EASO jest zwiększenie współpracy między państwami członkowskimi w zakresie wspólnych wyzwań związanych z azylem i migracją. Urząd wspiera krajowe organy zajmujące się azylem, np. w zakresie organizowania wspólnych szkoleń dla urzędników, udzielania ekspertów, analizowania danych oraz harmonizowania praktyk azylowych. EASO pomaga państwom członkowskim UE w poprawie funkcjonowania ich krajowych systemów azylowych.

[24] Dyrektywa Rady 2009/50/WE z dnia 25 maja 2009 r. w sprawie warunków wjazdu i pobytu obywateli państw trzecich w celu podjęcia pracy w zawodzie wymagającym wysokich kwalifikacji (Dz.U. L 155 z 18.06.2009 r.), s. 17-29.

[25] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 439/2010 z dnia 19 maja 2010 r. w sprawie utworzenia Europejskiego Urzędu Wsparcia w dziedzinie Azylu (Dz.U. L 132 z 29.05.2010 r.), p. 11-28.

Poprzez dostarczanie ekspertów i zasobów urząd wspiera państwa członkowskie w zapewnianiu szybszego i sprawiedliwego rozpatrywania wniosków o azyl. EASO ma również za zadanie wspierać wdrażanie wspólnej polityki azylowej Unii Europejskiej zgodnie z zasadami określonymi w tzw. Dublińskim systemie, odpowiedzialnym za regulowanie, który kraj członkowski jest odpowiedzialny za rozpatrzenie wniosku o azyl. Urząd współpracuje także z innymi agencjami UE, takimi jak Frontex, aby zapewnić kompleksowe podejście do zarządzania granicami i migracjami. EASO zostało powołane również z myślą o reagowaniu na sytuacje kryzysowe związane z migracją, takie jak masowe napływy uchodźców w wyniku wojen, prześladowań czy innych katastrof humanitarnych. Urząd pomaga w organizowaniu i koordynowaniu działań wsparcia dla państw, które borykały się z dużą liczbą wniosków o azyl, oferując np. Personel i materiały. Choć głównie skupia się na wsparciu procedur azylowych, rozporządzenie EASO obejmuje także współpracę z państwami członkowskimi w kwestii dobrowolnych powrotów migrantów, którzy nie spełnili warunków do uzyskania statusu uchodźcy.

W ramach tej działalności urzędnicy EASO pomagają w organizacji procedur powrotów, a także w reintegracji migrantów w krajach ich pochodzenia. Ponadto EASO pełni rolę centralnego ośrodka zbierającego i analizującego dane dotyczące migracji, wniosków azylowych oraz sytuacji w krajach trzecich, co pozwala na lepsze prognozowanie i reagowanie na zmieniające się trendy migracyjne. Dzięki Rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 439/2010 z dnia 19 maja 2010 roku w sprawie utworzenia Europejskiego Urzędu Wsparcia w dziedzinie Azylu Unia Europejska może korzystać z EASO, aby lepiej dostosować swoje polityki azylowe i migracyjne. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 604/2013 z dnia 26 czerwca 2013 roku w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca[26], znane jako Rozporządzenie Dublin III, jest kluczowym aktem prawnym w kontekście zarządzania migracją w Unii Europejskiej.

Rozporządzenie to reguluje tzw. system Dubliński mający na celu określenie, które państwo członkowskie UE jest odpowiedzialne za rozpatrzenie wniosku o azyl w przypadku osoby, która przekroczyła granice UE. Zasada ta opiera się na pierwszym kraju wejścia. Jest to więc kraj, przez który migrant po raz pierwszy wszedł na terytorium UE lub które było pierwszym miejscem składania wniosku o azyl. System ten ma na celu zapobieganie tzw. forum shopping, czyli unikaniu sytuacji, w których migranci mogą wielokrotnie składać wnioski o azyl w różnych państwach członkowskich. Ponadto, jeśli dana osoba znajduje się w państwie

[26] Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 604/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca (Dz.U. L 180 z 29.06.2013 r.), p. 31-59.

członkowskim, które nie jest odpowiedzialne za rozpatrzenie jej wniosku, to w ramach systemu Dublińskiego możliwe jest jej odesłanie do państwa odpowiedzialnego. Jednakże rozporządzenie to nie może naruszać zasady *non-refoulement,* która zakazuje deportacji osób do krajów, w których ich życie lub wolność może być zagrożona[27]. W związku z tym przed podjęciem decyzji o odesłaniu osoby należy zapewnić, że w kraju, do którego ma zostać odesłana nie będzie ona narażona na niebezpieczeństwo.

Rozporządzenie przewiduje możliwość odwołania się od decyzji o odesłaniu osoby ubiegającej się o azyl do innego państwa członkowskiego. Takie prawo przysługuje im w przypadku, gdy uważają, że decyzja jest niezgodna z przepisami prawa lub mogą zostać naruszone ich prawa fundamentalne. Rozporządzenie wprowadza również szczególne zasady w przypadku rodzin mające na celu zapewnić, że członkowie rodziny będą mogli ubiegać się o azyl w tym samym państwie członkowskim. Ma to na celu ochronę integralności rodziny i zapobieganie jej rozdzieleniu na etapie ubiegania się o ochronę międzynarodową. Ponadto w stosunku do wcześniejszych wersji rozporządzenia (Dublin II), wersja III (obowiązująca od 2013 roku) wprowadza pewne modyfikacje, takie jak m.in. wzmocnienie mechanizmów odwoławczych oraz rozszerzenie współpracy z Europejskim Urzędem Wsparcia w Dziedzinie Azylu (EASO). Wprowadza także procedury przyspieszonego odsyłania, a w szczególnie dla osób, które znajdują się w sytuacji tzw. przypadków jednoznacznych (np. osoby, które już zostały deportowane z innego państwa). Mimo że system Dubliński miał na celu uporządkowanie procedur azylowych to w praktyce w dużej mierze obciążył kraje znajdujące się na zewnętrznych granicach UE takie jak Włochy, Grecja czy Hiszpania. Są one bowiem pierwszymi punktami wejścia dla wielu migrantów. W sytuacjach kryzysowych (np. kryzys migracyjny z lat 2015–2016) system Dubliński doprowadził do licznych obciążeń administracyjnych i humanitarnych w państwach granicznych UE.

Dyrektywa Parlamentu Europejskiego i Rady 2013/33/UE z dnia 26 czerwca 2013 roku w sprawie ustanowienia norm dotyczących przyjmowania wnioskodawców ubiegających się o ochronę międzynarodową[28] została przyjęta w odpowiedzi na rosnącą liczbę wniosków o azyl w Europie. Jej nadrzędnym celem jest zapewnienie jednolitych standardów traktowania osób ubiegających się o azyl w różnych państwach członkowskich. Dyrektywa ma również za zadanie poprawienie jakości życia migrantów poprzez zapewnienie im odpowiednich warunków przyjmowania podczas procedury azylowej. Ponadto przewiduje zapewnienie, aby osoby ubiegające się o azyl nie były traktowane w sposób nieludzki lub poniżający oraz że nie będą narażone na dodatkowe trudności podczas oczekiwania na decyzję w sprawie

[27] M. Kowalski, *Znaczenie art. 14 Powszechnej Deklaracji Praw Człowieka dla międzynarodowego prawa uchodźczego* [w:] *70 lat Powszechnej Deklaracji Praw Człowieka*, red. M. Florczak-Wątor, M. Kowalski, Kraków 2019, s. 84-89.

[28] Dyrektywa Parlamentu Europejskiego i Rady 2013/33/UE z dnia 26 czerwca 2013 r. w sprawie ustanowienia norm dotyczących przyjmowania wnioskodawców ubiegających się o ochronę międzynarodową (Dz.U. L 180 z 29.06.2013 r.), p. 96-116.

azylu. Dyrektywa ma na celu zharmonizowanie polityk państw członkowskich, które wcześniej miały bardzo zróżnicowane podejście do kwestii przyjmowania osób ubiegających się o azyl. Ponadto dzięki niej wprowadzono bardziej jednolite standardy jednocześnie pozostawiając pewną swobodę dla państw członkowskich w zakresie implementacji tych przepisów.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 656/2014 z dnia 15 maja 2014 roku ustanawiające zasady ochrony zewnętrznych granic morskich w kontekście współpracy operacyjnej koordynowanej przez Europejską Agencję Zarządzania Współpracą Operacyjną na Granicach Zewnętrznych państw członkowskich Unii Europejskiej[29] jest jednym z kluczowych aktów prawnych dotyczących ochrony zewnętrznych granic Unii Europejskiej, szczególnie w kontekście współpracy operacyjnej w zakresie zarządzania migracją i reagowania na kryzysy humanitarne.

Rozporządzenie to ustanawia zasady dotyczące współpracy państw członkowskich UE w zakresie ochrony morskich granic zewnętrznych oraz koordynacji działań przez Europejską Agencję Zarządzania Współpracą Operacyjną na Granicach Zewnętrznych (Frontex). Rozporządzenie ma na celu zapewnienie skutecznej ochrony granic zewnętrznych Unii Europejskiej, zwłaszcza w kontekście migracji i walki z nielegalnym przekraczaniem granic. Zasady dotyczące współpracy operacyjnej na morzu mają zapewnić zgodność z prawem międzynarodowym, w tym konwencjami dotyczącymi ochrony praw człowieka. Europejska Agencja Zarządzania Współpracą Operacyjną na Granicach Zewnętrznych (Frontex) odgrywa kluczową rolę w koordynowaniu działań państw członkowskich UE zapewniając wsparcie w zakresie ochrony granic morskich. Frontex organizuje i nadzoruje wspólne operacje morskie, angażując zasoby i specjalistów z różnych państw członkowskich. Celem jest zwiększenie efektywności działań granicznych, szczególnie w obliczu wzrostu migracji.

Rozporządzenie reguluje zasady przeprowadzania operacji kontrolnych na morzu, w tym wykorzystywania jednostek pływających (np. statków patrolowych, łodzi). Określa ono szczegółowo, jak powinny być przeprowadzane operacje monitorowania, kontroli granic, a także działania mające na celu zapobieganie nielegalnym migracjom oraz zwalczanie przestępczości transgranicznej, w tym przemytu ludzi. Ponadto rozporządzenie nakłada na państwa członkowskie obowiązek przestrzegania praw osób znajdujących się na morzu, w tym osób ubiegających się o azyl i uchodźców. W ramach operacji morskich zapewnia się, że osoby ratowane na morzu otrzymują odpowiednią pomoc i nie są narażone na niebezpieczeństwo[30]. Kluczowe jest, aby działania podejmowane w ramach operacji były zgodne

[29] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 656/2014 z dnia 15 maja 2014 r. ustanawiające zasady ochrony zewnętrznych granic morskich w kontekście współpracy operacyjnej koordynowanej przez Europejską Agencję Zarządzania Współpracą Operacyjną na Granicach Zewnętrznych państw członkowskich Unii Europejskiej (Dz.U. L 189 z 27.06.2014 r.), p. 93-107.

[30] I. Oleksiewicz, K. Stachurska-Szczesiak, *Polityka wobec uchodźców i zintegrowana polityka morska a bezpieczeństwo Unii Europejskiej*, Lublin 2017, s. 44-45.

z międzynarodowym prawem humanitarnym. W sytuacjach kryzysowych, takich jak masowe napływy migrantów przez morze (np. na Morzu Śródziemnym) Frontex może angażować zasoby z państw członkowskich, organizując wspólne operacje, które obejmują m.in. patrole, eskortowanie jednostek morskich, monitorowanie granic, a także udzielanie wsparcia logistycznego i technicznego.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2019/1896[31] z dnia 10 października 2019 roku ustanawiające Europejską Agencję Straży Granicznej i Przybrzeżnej (znane również jako rozporządzenie EBCG) ma na celu wzmocnienie zarządzania granicami zewnętrznymi Unii Europejskiej oraz poprawę zarządzania migracją. Rozporządzenie wzmacnia mandat Frontexu, rozszerzając jego kompetencje w zakresie monitorowania i kontrolowania granic zewnętrznych UE. Zakłada również zwiększenie liczby strażników granicznych oraz dostarczenie odpowiednich zasobów takich jak sprzęt technologiczny i środki logistyczne, które mają ułatwić skuteczną kontrolę migracji.

W ramach rozporządzenia utworzono specjalną jednostkę mobilną będącą w stałej gotowości do szybkiej reakcji na zmieniające się warunki kryzysowe (np. w przypadku napływu dużej liczby migrantów w krótkim czasie). Celem rozporządzenia jest także zapewnienie skuteczniejszej ochrony granic zewnętrznych Unii. Obejmuje to zarówno tradycyjne metody kontroli granicznych, jak i nowoczesne technologie takie jak systemy monitorowania granic czy analizowanie danych wywiadowczych. W szczególności ważnym elementem jest tworzenie i wykorzystywanie wspólnych baz danych (np. SIS – *Schengen Information System*) oraz systemów wymiany informacji, które pozwalają na szybsze wykrywanie osób przebywających na terytorium UE nielegalnie. Rozporządzenie podkreśla również konieczność współpracy z państwami trzecimi w zakresie zapobiegania nielegalnej migracji. UE stara się wspierać państwa pozaeuropejskie w rozwiązywaniu problemów związanych z migracją, na przykład poprzez pomoc w zarządzaniu granicami czy współpracę w zakresie zwalczania przestępczości transgranicznej (np. przemyt ludzi). Celem jest ograniczenie liczby migrantów, którzy nielegalnie przedostają się na terytorium Unii.

W ramach rozporządzenia rozwija się również współpraca w zakresie powrotów osób, które przebywają w UE bez odpowiednich dokumentów. Ważnym aspektem rozporządzenia jest uwzględnienie zasad ochrony praw człowieka, w tym prawa do azylu i ochrony przed nielegalnym zatrzymaniem lub deportacją. Wspólna polityka migracyjna i graniczna ma na celu zapewnienie, że procedury są zgodne z europejskimi standardami praw człowieka oraz konwencjami międzynarodowymi. Rozporządzenie nr 2019/1896 zostało opracowane w odpowiedzi na rosnące wyzwania związane z migracją do Europy. Szczególnie w kontekście kryzysu migracyjnego, który miał miejsce w latach 2015–2016, kiedy to tysiące osób z Bliskiego Wschodu, Afryki Północnej i innych regionów zaczęły przybywać do

[31] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1896 z dnia 13 listopada 2019 r. w sprawie Europejskiej Straży Granicznej i Przybrzeżnej oraz uchylenia rozporządzeń (UE) nr 1052/2013 i (UE) 2016/1624 (Dz.U. L 295 z 14.11.2019 r.), p. 1-131.

Europy, w wielu przypadkach nielegalnie. Wzrost liczby osób ubiegających się o azyl oraz nasilający się kryzys związany z nielegalnym handlem ludźmi i przemytem migrantów skłoniły UE do wzmocnienia kontroli granic zewnętrznych oraz opracowania bardziej spójnej i kompleksowej polityki migracyjnej. Rozporządzenie to stanowi ważny element szerokiej polityki Unii w zakresie migracji i ochrony granic. Ma ono na celu zapewnienie bezpieczeństwa, zarządzanie migracjami i jednoczesne przestrzeganie praw człowieka.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1717 z dnia 13 czerwca 2024 roku wprowadza zmiany do rozporządzenia (UE) 2016/399, które dotyczą unijnego kodeksu zasad regulujących przepływ osób przez granice[32]. W kontekście migracji głównym celem rozporządzenia 2024/1717 jest dostosowanie unijnych regulacji do zmieniających się realiów związanych z rosnącymi wyzwaniami migracyjnymi i zapewnienie lepszej kontroli nad przepływem osób przez granice zewnętrzne Unii Europejskiej. Rozporządzenie wprowadza bardziej rygorystyczne zasady dotyczące kontroli granicznych, zwłaszcza w kontekście osób przybywających do UE z krajów trzecich. Wprowadza nowe procedury mające na celu szybkie identyfikowanie osób, które nie spełniają wymogów wjazdu lub mają nieuregulowany status migracyjny. Wspiera również legalne i zorganizowane przepływy migracyjne. W szczególności stawia nacisk na uproszczenie procedur dla osób, które spełniają wymagania wjazdu do UE takich jak podróże służbowe, edukacyjne, turystyczne czy związane z łączeniem rodzin.

Zmiany dotyczą także procedur związanych z osobami ubiegającymi się o azyl lub ochronę międzynarodową. W przypadku osób, które nie spełniają standardów wjazdu wprowadzono nowe mechanizmy, które pozwalają na szybszą identyfikację osób ubiegających się o ochronę i przeprowadzenie odpowiednich procedur w tym zakresie. Rozporządzenie podkreśla potrzebę intensyfikacji współpracy między państwami członkowskimi w zakresie zarządzania granicami zwłaszcza w kontekście wymiany informacji o osobach przekraczających granice. Ma to na celu usprawnienie monitorowania migracji oraz walki z nielegalnym przekraczaniem granicy, handlem ludźmi i innymi formami przestępczości transgranicznej. Wprowadzenie nowych technologii w zarządzaniu granicami, takich jak systemy biometryczne czy inne technologie identyfikacji jest kluczowym elementem zmian. Dzięki nim możliwe jest skuteczniejsze monitorowanie przepływu osób i szybsze podejmowanie decyzji o ich statusie na granicy.

Rozporządzenie uwzględnia rosnące wyzwania związane z migracją takie jak zmieniające się trendy migracyjne, zmiany klimatyczne, konflikty czy niestabilność polityczna w krajach pochodzenia migrantów. Dzięki temu wprowadza bardziej elastyczne mechanizmy reagowania na nagłe wzrosty liczby osób przybywających na terytorium UE, w tym także na granice zewnętrzne.

[32] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1717 z dnia 13 czerwca 2024 r. dotyczące zmiany rozporządzenia (UE) 2016/399 w sprawie unijnego kodeksu zasad regulujących przepływ osób przez granice (Dz.U. L 2024/1717), 20.06.2024.

Dokumenty te stanowią odpowiedź na narastające wyzwania stojące przez Unią Europejską. Dzięki nim powołano szereg instytucji i wprowadzono wiele rozwiązań, których celem jest wsparcie zarówno państw UE, jak i tych spoza niej w opracowywaniu skutecznych form rozwiązywania problemu migracyjnego.

Podsumowanie

Instytucjonalny wymiar polityki migracyjnej Unii Europejskiej odzwierciedla dążenie do zbalansowanego podejścia w obliczu dynamicznych wyzwań migracyjnych. UE rozwija mechanizmy kontroli granic, procedur azylowych i integracji migrantów, uwzględniając kwestie bezpieczeństwa, solidarności i poszanowania praw człowieka. Wspólna polityka migracyjna wymaga nie tylko skutecznej współpracy między państwami członkowskimi, lecz także elastycznego dostosowywania się do globalnych zmian, takich jak kryzysy humanitarne czy zmiany klimatyczne. Jednocześnie różnice zdań w najważniejszych sprawach politycznych pomiędzy przedstawicielami państw członkowskimi, a także odmienności wynikające z uwarunkowań geopolitycznych, a przede wszystkim legislacyjnych pokazują, że niezbędne są dalsze reformy, aby zapewnić „sprawiedliwy" podział odpowiedzialności pomiędzy państwami członkowskimi UE. Kluczowym wyzwaniem pozostaje znalezienie równowagi między zapewnieniem bezpieczeństwa wewnętrznego (narodowego) danego państwa a zewnętrznego UE. Drugim aspektem, o jakim nie należy zapominać, a wynika o wprost z art. 6 TFUE, jest ochrona praw człowieka wraz z ochroną wartości i zobowiązań humanitarnych, co jest powiązane wprost z art. 4 i 77 TFUE oraz wpłynie na przyszłość zarówno polityki wewnętrznej, migracyjnej, jak i spójności całej Unii Europejskiej.

Bibliografia

Chlebny J., *Postępowanie w sprawie o nadanie statusu uchodźcy*, Warszawa 2011.

Gruszczak A., *Historia współpracy w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych: od TREVI do Tampere* [w:] *Obszar wolności, bezpieczeństwa i sprawiedliwości Unii Europejskiej. Geneza, stan i perspektywy rozwoju*, red. F. Jasiński, K. Smoter, Warszawa 2005.

Heinrich-Hamera D., *Międzynarodowa ochrona uchodźców wewnętrznych. Aspekty prawne i praktyka*, Warszawa 2005.

Jagielski J., *Status cudzoziemca w Polsce*, Warszawa 1997.

Kolbusz P., *Kryzys migracyjny 2015 roku w Europie i sytuacja uchodźców w czasie pandemii – czy kryzys skończył się na dobre i jaki wpływ na migrantów ma epidemia wirusa COVID-19?*, „Acta Erasmiana", red. M. Sadowski, K. Gaweł, M. Popielarski, K. Strużyński, t. 20, Wrocław 2021.

Kowalski M., *Znaczenie art. 14 Powszechnej Deklaracji Praw Człowieka dla międzynarodowego prawa uchodźczego* [w:] *70 lat Powszechnej Deklaracji Praw Człowieka*, red. M. Florczak-Wątor, M. Kowalski, Kraków 2019.

Nickel A., Nowak A., *Trendy migracyjne w XXI wieku*, „Roczniki Studenckie Akademii Wojsk Lądowych" 2017, nr 1.

Oleksiewicz I., Stachurska-Szczesiak K., *Polityka wobec uchodźców i zintegrowana polityka morska a bezpieczeństwo Unii Europejskiej*, Lublin 2017.

Pacek M., *Polska polityka migracyjna na tle rozwiązań i doświadczeń Unii Europejskiej*, „Studia Europejskie" 2005, nr 4.

Potyrała A., *Kryzys uchodźczy a przyszłość unijnego systemu azylowego* [w:] *Uchodźcy w Europie – uwarunkowania, istota, następstwa*, red. K.A. Wojtaszczyk, J. Szymańska, Wydawnictwo ASPRA-JR, Warszawa 2016.

Powszechna encyklopedia PWN, t. 21, Warszawa 2009.

Akty normatywne

Traktat o Unii Europejskiej (Dz.U. C 191 z 29.07.1992 r.).

Traktat z Amsterdamu zmieniający Traktat o Unii Europejskiej, traktaty ustanawiające Wspólnoty Europejskie i niektóre związane z nimi akty (Dz.U. C 340 z 10.11.1997 r.).

Traktat o funkcjonowaniu Unii Europejskiej (TFUE) (Dz.U. C 306 z 17.12.2007 r.).

Dyrektywa Rady 2003/109/WE z dnia 25 listopada 2003 r. dotycząca statusu obywateli państw trzecich będących rezydentami długoterminowymi (Dz.U. L 16 z 23.01.2004 r.).

Dyrektywa Rady 2009/50/WE z dnia 25 maja 2009 r. w sprawie warunków wjazdu i pobytu obywateli państw trzecich w celu podjęcia pracy w zawodzie wymagającym wysokich kwalifikacji (Dz.U. L 155 z 18.06.2009 r.).

Dyrektywa Parlamentu Europejskiego i Rady 2013/33/UE z dnia 26 czerwca 2013 r. w sprawie ustanowienia norm dotyczących przyjmowania wnioskodawców ubiegających się o ochronę międzynarodową (Dz.U. L 180 z 29.06.2013 r.).

Rozporządzenie Rady (WE) nr 2007/2004 z dnia 26 października 2004 r. ustanawiające Europejską Agencję Zarządzania Współpracą Operacyjną na Zewnętrznych Granicach Państw Członkowskich Unii Europejskiej (Dz.U. L 349 z 25.11.2004 r.).

Rozporządzenie (WE) nr 1987/2006 – utworzenie, funkcjonowanie i użytkowanie Systemu Informacyjnego Schengen drugiej generacji (SIS II) (Dz.U. L 381 z 28.12.2006 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 439/2010 z dnia 19 maja 2010 r. w sprawie utworzenia Europejskiego Urzędu Wsparcia w dziedzinie Azylu (Dz.U. L 132 z 29.05.2010 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 604/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca (Dz.U. L 180 z 29.06.2013 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 656/2014 z dnia 15 maja 2014 r. ustanawiające zasady ochrony zewnętrznych granic morskich w kontekście współpracy operacyjnej koordynowanej przez Europejską Agencję Zarządzania Współpracą Operacyjną na Granicach Zewnętrznych państw członkowskich Unii Europejskiej (Dz.U. L 189 z 27.06.2014 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz.U. L 135 z 24.05.2016.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1896 z dnia 13 listopada 2019 r. w sprawie Europejskiej Straży Granicznej i Przybrzeżnej oraz uchylenia rozporządzeń (UE) nr 1052/2013 i (UE) 2016/1624 (Dz.U. L 295 z 14.11.2019 r.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1717 z dnia 13 czerwca 2024 r. dotyczące zmiany rozporządzenia (UE) 2016/399 w sprawie unijnego kodeksu zasad regulujących przepływ osób przez granice (Dz.U. L, 2024/1717, 20.06.2024 r.).

Rozporządzenie Rady (WE) nr 168/2007 z dnia 15 lutego 2007 r. ustanawiające Agencję Praw Podstawowych Unii Europejskiej (Dz.U. L 53 z 22.02.2007 r.).

Netografia

https://historia.dorzeczy.pl/historia-wspolczesna/199495/zamach-na-world-trade-center-11-wrzesnia-2001-trauma-usa-trwa-do-dzis.html.

https://hist.pl/rewolucyjny-kryzys-naftowy-1973-jak-ropa-naftowa-pokonala-swiat/.

Seweryn WALAS[1]

INSPEKCJA TRANSPORTU DROGOWEGO JAKO INSTYTUCJA W WYMIARZE BEZPIECZEŃSTWA PAŃSTWA

Wstęp

Inspekcja Transportu Drogowego (ITD) jako umundurowana, wyspecjalizowana i uzbrojona formacja została powołana ustawą z dnia 6 września 2001 roku o transporcie drogowym[2]. Główną przesłanką jej utworzenia była chęć poprawy bezpieczeństwa ruchu drogowego, zapewnienie uczciwej konkurencji, ochrona środowiska oraz zapewnienie odpowiedniej jednostki uprawionej do kontroli przestrzegania przepisów w zakresie przewozu drogowego. Aby zapewnić skuteczne wykonywanie kontroli, ITD wyposażono w odpowiedni sprzęt i uprawnienia, które pozwalają na sprawne monitorowanie przestrzegania przepisów dotyczących przewozów drogowych. Przy tworzeniu jej struktur w ramach programu bliźniaczego PHARE PL 9908.01 – „Przygotowanie podstaw prawnych i utworzenie Inspekcji Transportu Drogowego" brali udział eksperci z Niemiec oraz Francji.

W procesie tworzenia Inspekcji, kluczowe było opracowanie precyzyjnego zakresu jej działalności oraz struktur, co miało na celu zapewnienie efektywności jej funkcjonowania. Doradcy skupili się na zdefiniowaniu roli ITD w systemie administracji publicznej, wskazując na konieczność określenia odpowiednich kompetencji i odpowiedzialności, które powinny zostać przypisane jej przyszłym pracownikom. Ważnym elementem była także organizacja strukturalna – zapewnienie, że ITD będzie w stanie skutecznie realizować swoje zadania w ramach odpowiednich procedur administracyjnych oraz w koordynacji z innymi organami i instytucjami państwa.

Równocześnie istotną częścią procesu było zaplanowanie kompleksowego programu szkoleń dla kandydatów na odpowiednie stanowiska służbowe. Szkolenia miały na celu przygotowanie pracowników do realizacji zadań związanych

[1] Politechnika Rzeszowska, Wydział Zarządzania. ORCID: 0009-0009-2488-0333.

[2] Ustawa z dnia 6 września 2001 r. o transporcie drogowym (t.j. Dz.U. z 2024 r., poz. 1539). Za kierownictwo Inspekcji Transportu Drogowego odpowiada Główny Inspektor Transportu Drogowego, mając do pomocy podległy mu Główny Inspektorat Transportu Drogowego oraz delegatury terenowe. Delegaturami kierują naczelnicy delegatur, a ich obsługę zapewnia wojewódzki inspektorat transportu drogowego na obszarze funkcjonowania, gdzie znajduje się siedziba delegatury.

z kontrolą i nadzorem nad przestrzeganiem przepisów, jak również do efektywnej reakcji na nieprawidłowości, w tym także zdobycie odpowiednich kompetencji merytorycznych, praktycznych oraz technicznych. Uwzględniono przy tym specyfikę pracy, kładąc szczególny nacisk na znajomość przepisów prawnych, kompetencje miękkie, umiejętność analizy danych oraz znajomość narzędzi informatycznych.

W trakcie tworzenia ITD uwzględniono doświadczenia i najlepsze praktyki formacji o podobnym charakterze działających w innych krajach Unii Europejskiej. Podobne instytucje funkcjonują w takich państwach jak Francja, Niemcy, Belgia czy Wielka Brytania, gdzie zostały już opracowane sprawdzone modele organizacyjne, szkoleniowe i operacyjne. Zebrane doświadczenia z tych państw stanowiły cenne źródło informacji, inspiracji i wskazówek, które pomogły w opracowaniu optymalnych rozwiązań dostosowanych do krajowych realiów transportu.

Działalność Inspekcji Transportu Drogowego

Zadania[3], jakimi zajmuje się Inspekcja Transportu Drogowego, są wyszczególnione w omawianej ustawie[4] i można podzielić je na kilka aspektów. Jednym z nich jest kontrola i powiązane z nią czynności takie jak:

- sprawdzanie dokumentów transportowych. Kluczowy problem, który reguluje ta kompetencja jest kontrola wymaganych uprawnień przewoźników i kierowców, tj. posiadane licencje transportowe, zaświadczenia o dopuszczeniu pojazdów do ruchu, a także dokumenty przewozowe CMR[5],
- kontrola przestrzegania przepisów ruchu drogowego, w tym przestrzeganie prędkości, odpowiednie zabezpieczenie i oznaczenie ładunku, jak i samego pojazdu oraz innych norm związanych z transportem drogowym, a także sprawdzanie, czy przewoźnicy realizują transport zgodnie z określonymi w umowach, licencjach i pozwoleniach warunkami,
- regularne kontrole techniczne pojazdów uczestniczących w transporcie drogowym, w tym sprawdzanie stanu technicznego pojazdów, takich jak

[3] Ustawa z dnia 6 września 2001 r. o transporcie drogowym.

[4] https://www.krakow.witd.gov.pl/wazne-informacje/zadania-inspekcji/ [dostęp: 10.11.2024 r.].

[5] CMR jest to Międzynarodowy List Przewozowy, jeden z najważniejszy dokumentów w transporcie międzynarodowym. Umożliwiający przewóz towarów przez granice państwowe i określający warunki takiego przewozu. CMR powinien być stosowany w przypadku przewozu towarów drogą lądową między państwami, które są stronami umowy o przewozie drogowym międzynarodowym (TIR), jak również ma zastosowanie w przypadku przewozu towarów dla państw z poza tej umowy, ale respektujących zastosowanie CMR. Sama forma jest ściśle określona. Dokument ten musi zawierać podstawowe informacje, takie jak: nazwę i adres przewoźnika, nazwę i adres nadawcy oraz odbiorcy towaru, opis towaru, wagę i objętość ładunku, a także warunki dostawy. Powinien być wypełniony zgodnie z zasadami określonymi w Konwencji o umowie międzynarodowego przewozu drogowego (CMR), która określa również standardowe klauzule stosowane w CMR, https://licencjetransportowe.com/cmr-miedzynarodowy-list-przewozowy.html#CMR_%E2%80%93_podsumowanie [dostęp: 10.11.2024 r.].

ciężarówki, autobusy, pojazdy dostawcze oraz inne pojazdy użytkowane do celów transportowych,

- kontrola przestrzegania norm dotyczących czasu pracy i odpoczynku kierowców[6], a także obowiązkowych przerw podczas wykonywania transportu drogowego. Choć ITD skutecznie monitoruje przestrzeganie norm dotyczących czasu pracy, zmęczenie kierowców pozostaje poważnym problemem, zwłaszcza w kontekście nasilającego się zjawiska pracy w szarej strefie, szczególnie w dużych zagranicznych firmach[7], co może utrudniać egzekwowanie przepisów,
- sprawdzanie, czy przewożone są towary niebezpieczne zgodnie z obowiązującymi przepisami, w tym przepisami ADR[8]. Inspekcja kontroluje odpowiednie oznakowanie pojazdów, zabezpieczenie ładunku oraz inne wymagania związane z transportem materiałów niebezpiecznych,
- nadzór nad transportem zwierząt, a w tym kontrola przestrzegania wymagań związanych z dobrostanem zwierząt, zapewnienia odpowiednich warunków transportu (np. temperatura, wentylacja, odpowiednia przestrzeń), a także dokumentacji związanej z ich przewozem,
- przestrzeganie przepisów dotyczących transportu na potrzeby własne, gdzie transport nie jest wykonywany w celach zarobkowych, ale nadal musi spełniać określone wymagania dotyczące dokumentacji, stanu technicznego pojazdów i przestrzegania przepisów,
- prowadzenie postępowań administracyjnych[9] w zakresie naruszeń przepisów prawa transportowego. ITD ma kompetencje do nakładania kar administracyjnych, w tym mandatów, oraz wydawania decyzji administracyjnych, np. w sprawach związanych z cofnięciem licencji transportowej. Współpracuje również z sądami i innymi organami ścigania, aby zmusić przewoźników do przestrzegania prawa, co pozwala na jeszcze skuteczną jego egzekucję,
- sprawdzanie, czy pojazdy poruszające się po drogach publicznych przestrzegają dopuszczalnych norm masy i wymiarów określonych w przepisach prawa. Inspekcja przeprowadza kontrolę masy pojazdów, zarówno podczas rutynowych kontroli na drogach, jak i na punktach ważących standardowych pojazdów a w szczególności przewożących ładunki ponadgabarytowe[10]. W ostatnich latach ITD wprowadziła systemy automatyczne

[6] Ustawa z dnia 16 kwietnia 2004 r. o czasie pracy kierowców (t.j. Dz.U. z 2024 r., poz. 220).

[7] P. Ciszak, *Niewolnicza praca kierowców z Filipin. Polska pośrednikiem w procederze,* http.money.pl [dostęp: 11.11.2024 r.].

[8] Umowa europejska dotycząca międzynarodowego przewozu drogowego towarów niebezpiecznych (ADR), sporządzona w Genewie dnia 30 września 1957 r. Jest jedną z ważniejszych umów dotyczących transportu (Dz.U. z 1975 r., nr 35, poz. 189).

[9] Ustawa z dnia 6 września 2001 r. o transporcie drogowym.

[10] Ładunek ponadgabarytowy to towar o masie przekraczającej 42 t, szerokości 2,5 m i wysokości ponad 4 m. Do jego przewozu wymagane są specjalne zezwolenia, a także wcześniejsze

do kontroli masy pojazdów, a także wykorzystuje dane z tachografów w czasie rzeczywistym, co pozwala na szybsze i bardziej precyzyjne sprawdzanie przestrzegania przepisów przez kierowców i przewoźników,

- Współpraca międzynarodowa w ramach członkostwa w Euro Contrôle Route (ECR) z organami kontrolnymi innych państw europejskich. Do tej organizacji obecnie należy 14 państw (Holandia, Belgia, Luksemburg, Francja, Irlandia, Królestwo Wielkiej Brytanii i Irlandii Północnej, Niemcy, Polska, Rumunia, Chorwacja, Bułgaria, Węgry, Austria, Hiszpania). W ramach tej współpracy funkcjonują trzy grupy: ECR-Training, ECR-Harmonie oraz ECR-TWG (*Tacho Web Group*), a każda ma inne zadania.

ECR-Training zajmuje się realizacją zadań szkoleniowych z zakresu działalności służb poprzez organizowanie szkoleń inspektorów w ramach różnorodnych programów wymiany oraz warsztatów tematycznych. Celem działalności jest zwiększenie bezpieczeństwa na europejskich drogach poprzez wprowadzanie spójnych procedur kontroli, które usprawniają pracę inspektorów.

ECR-Harmonie jest odpowiedzialna za planowanie i przeprowadzanie skoordynowanych działań kontrolnych między państwami członkowskimi i zainteresowanymi stronami w celu efektywnego wykorzystania dostępnych technologii. Koordynuje regularną wymianę informacji między państwami członkowskimi ECR i innymi. Grupa Harmonie również przykłada dużą wagę do procedur stosowanych podczas kontroli drogowych, interpretacji europejskich przepisów prawa oraz wysokości kar w państwach członkowskich ECR. Dąży ona do wprowadzania najlepszych praktyk w dziedzinie działań kontrolnych w transporcie drogowym, aby zapewnić identyczne podejście.

ECR-TWG tworzą przedstawiciele ECR oraz ROADPOL (*European Roads Policing Network*). Działają oni w obszarze współpracy i zagadnień związanych ze stosowanymi współcześnie urządzeniami rejestrującymi (m.in. nieuprawniona ingerencja w urządzenie rejestrujące).W ramach prac także podejmowane są inicjatywy, które mają na celu poprawę współpracy z sektorem transportowym.

Działania edukacyjne i informacyjne[11] o przepisach transportowych, w tym organizowanie szkoleń i kampanii informacyjnych dla przedsiębiorców, kierowców i innych podmiotów związanych z transportem drogowym w celu poprawy świadomości na temat obowiązujących przepisów i najlepszych praktyk w zakresie transportu drogowego. W tym celu został nawet stworzony „Poradnik dla

zaplanowanie trasy przejazdu. G. Kurpeta, *Jak przewozić i chronić ładunki ponadgabarytowe?*, https://inrel.pl/jak-przewozic-i-chronic-ladunki-ponadgabarytowe/ [dostęp: 10.11.2024 r.].

[11] https://www.gov.pl/web/gitd/ruszyla-kampania-twoje-swiatla--nasze-bezpieczenstwo [dostęp: 10.11.2024 r.]. B. Raźny, K. Domagała, *Działania edukacyjne Inspekcji Transportu Drogowego*, wyd. Apeiron, Kraków 2021, s. 44-66

kierowców”[12], który posiada zestaw odpowiedzi na najistotniejsze pytania związane z zasadami wykonywania przewozu drogowego osób i rzeczy.

Celem wszystkich działań jest zapewnienie bezpieczeństwa na drogach oraz zapobieganie zmęczeniu kierowców, co finalnie przyczynia się do redukcji liczby wypadków, kolizji i wykroczeń.

Wyzwania dla ITD

Z roku na rok w Polsce i Europie przybywa samochodów[13] oraz sposobów obejścia przepisów i żeby nadążyć z zapewnieniem bezpieczeństwa Inspekcja Transportu Drogowego musi posiadać odpowiednie zaplecze kadrowe i sprzętowe. Jednymi z kilku wyzwań jest np. szkolenie inspektorów z obsługi nowych urządzeń i sprzętu pozyskanego z projektów takich jak np. „Wzmocnienie potencjału Inspekcji Transportu Drogowego”[14], aby potrafili biegle obsługiwać i wykrywać nieprawidłowości w trakcie kontroli, a wszystkie narzędzia technologiczne były wykorzystywane w pełni, szczególnie w mniejszych punktach kontrolnych. Część przewoźników może starać się unikać kontroli, korzystając z różnych trików logistycznych, takich jak stosowanie fałszywych dokumentów, przejazdy po mniej kontrolowanych drogach czy zmiana rejestracji pojazdów, co może utrudniać wykrycie naruszeń. Zjawisko nielegalnego transportu osób i towarów (tj. „przewóz na czarno”) jest trudne do wykrycia, szczególnie w kontekście rosnącego rynku transportu międzynarodowego, gdzie często niełatwo jest prześledzić nielegalne działania, a niestabilna sytuacja migracyjna ludności uciekającej przed konfliktami militarnymi pogłębia dodatkowo ten problem.

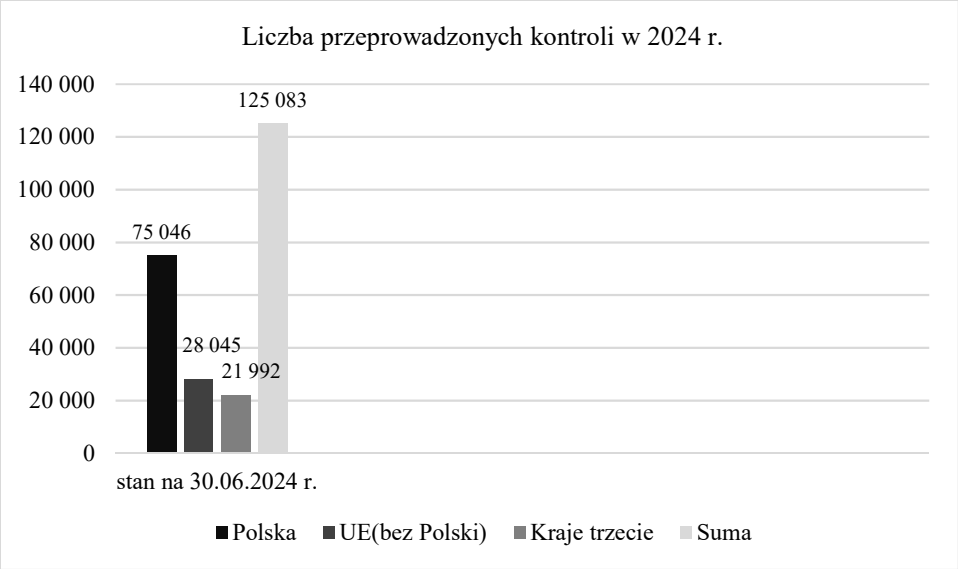
Pozyskanie nowych funkcjonariuszy eliminuje braki kadrowe i umożliwia sprawne okresowe prowadzenie działań kontrolnych na szerszą skalę. Spójne i skuteczne egzekwowanie przepisów mających wpływ na poprawę warunków pracy, bezpieczeństwa na drodze i uczciwej konkurencji jest bardzo ważne. W przypadku powtarzających się wykroczeń lub ciężkich naruszeń, system kar może być niewystarczający, aby zapobiec dalszym nieprawidłowościom. W takich przypadkach konieczne jest wypracowanie bardziej skutecznych sankcji. Problemy z wymianą danych w przypadku współpracy z organami innych krajów, czy nawet trudności w komunikacji podczas prowadzenia kontroli z racji różnych narodowości kierowców. Współpraca międzynarodowa w zakresie wymiany informacji o naruszeniach przepisów wciąż napotyka bariery związane z różnicami w przepisach, a także z opóźnieniami w wymianie danych między krajami. Przekłada się to na wydajność i efektywność samych inspektorów redukując możliwości kontrolne, a wręcz spowalniając znacznie cały proces.

[12] http://gitd.gov.pl [dostęp 11.11.2024 r.].
[13] https://www.acea.auto/publication/report-vehicles-on-european-roads/ [dostęp: 10.11.2024 r.]
[14] S. Rummel, *ITD gotowe na wyzwania. Nowoczesne furgony i Mobilne Jednostki Diagnostyczne*, „Ciężarówki i Logistyka” z dnia 2.10.2024 r.

Ocena efektywności działania ITD

Mimo wielu wyzwań i obowiązków, z jakimi na co dzień muszą mierzyć się funkcjonariusze Inspekcji Transportu Drogowego możemy ocenić ich starania o poprawę bezpieczeństwa uczestników ruchu drogowego na bardzo wysokim poziomie. Poparte jest to statystykami z przeprowadzonych kontroli, których w ciągu roku są tysiące. Dzięki intensyfikacji tych działań w zakresie kontroli czasu pracy kierowców, stanu technicznego pojazdów oraz przewozu towarów niebezpiecznych, ITD przyczynia się do poprawy bezpieczeństwa na drogach. Mimo wzrostu przekroczeń prędkości w sezonie wakacyjnym, liczba naruszeń jest mniejsza z roku na rok. Dzięki nowym technologiom i sprzętowi wykrycie różnych nadużyć jest skuteczne, efektywne oraz zapewnia lepszą ochronę środowiska przez eliminację pojazdów niespełniających norm technicznych i emisyjnych, co ma pozytywny wpływ na jakość powietrza i zdrowie mieszkańców.

Mimo to należy pamiętać o kampaniach edukacyjno-informacyjnych zwiększających świadomość, a to ma też znaczny wpływ na całość działalności i bezpieczeństwo.



Rys. 1. Liczba kontroli w roku 2024

Źródło: Gov.pl, https://dane.gov.pl/pl/dataset/4365,gitd-kontrole-drogowe/resource/59160/table?page=1&per_page=20&q=&sort= [dostęp: 10.11.2024 r.].

Rysunek 1. przedstawia liczbę kontroli przeprowadzonych w Polsce, w pozostałych państwach członkowskich Unii Europejskiej (bez Polski) oraz w krajach trzecich w pierwszej połowie 2024 roku, do dnia 30 czerwca. Z analizy danych wynika, że największą liczbę kontroli przeprowadzono w Polsce – wynosi ona

około 80 000. Kolejną kategorią są kraje Unii Europejskiej (bez Polski), gdzie liczba kontroli jest znacznie niższa i oscyluje wokół 20 000. Najmniej kontroli odnotowano w krajach trzecich, które przeprowadziły około 15 000 kontroli. Łączna suma kontroli wynosi około 130 000, co wskazuje na dużą aktywność kontrolną w regionie, z dominującym udziałem Polski.

Wyraźna przewaga liczby kontroli przeprowadzonych w Polsce w porównaniu do pozostałych kategorii może wynikać z kilku czynników. Po pierwsze, Polska może prowadzić intensywną politykę kontroli w odpowiedzi na lokalne przepisy, które wymagają częstych inspekcji w określonych gałęziach transportu lub obszarach. Może to być związane z próbą podniesienia standardów bezpieczeństwa, ochrony konsumentów lub też wdrażaniem nowych regulacji, które wymagają bardziej rygorystycznego monitorowania. Ponadto, wysoka liczba kontroli może być efektem wzmożonych działań prewencyjnych w Polsce, mających na celu zapobieganie naruszeniom prawa oraz wspieranie zgodności z regulacjami unijnymi i krajowymi.

Niska liczba kontroli w krajach Unii Europejskiej (bez Polski) oraz w krajach trzecich sugeruje, że podejście do polityki kontrolnej jest tam bardziej umiarkowane. W krajach UE (bez Polski) może to wynikać z bardziej zharmonizowanego systemu regulacyjnego, który zakłada mniej kontroli przy wyższej zgodności z przepisami. Z kolei w krajach trzecich, niższa liczba kontroli może być rezultatem ograniczonych zasobów, innego podejścia do regulacji lub mniejszego nacisku na egzekwowanie przepisów w porównaniu do państw unijnych.

Wnioski końcowe

Rozdział ukazuje rolę Inspekcji Transportu Drogowego w Polsce jako instytucji odpowiedzialnej za poprawę bezpieczeństwa na drogach. ITD powołana w 2001 roku, pełni kluczowe funkcje nadzorcze i prewencyjne, monitorując przestrzeganie przepisów transportowych, takich jak czas pracy kierowców, stan techniczny pojazdów, kontrola ładunków oraz uprawnienia przewoźników. Wprowadzono również nowoczesne technologie jak np. zestawy do zdalnego odczytu tachografu czy kamery nowego typu, które pomagają w szybszym wykrywaniu naruszeń. ITD aktywnie współpracuje międzynarodowo z organami kontrolnymi w innych państwach, co umożliwia skuteczną kontrolę międzynarodowego transportu drogowego. Działania te są szczególnie ważne w kontekście krajowego oraz międzynarodowego transportu towarów i osób, ale napotykają wyzwania, m.in. kadrowe, prawne, techniczne i w zakresie wymiany danych z innymi krajami.

Efektywność ITD jest wysoka, co przekłada się na redukcję liczby wypadków drogowych, choć istnieje potrzeba zwiększenia liczby kontroli, bo wciąż występuje problem z dotarciem do wszystkich pojazdów i przewoźników. Skala transportu drogowego w Polsce jest ogromna, a kontrolowanie każdego pojazdu w sposób efektywny jest praktycznie niemożliwe, co stwarza ryzyko, że niektóre nieprawidłowości umykają inspektorom.

Podsumowując, Polska odgrywa kluczową rolę w ogólnej liczbie przeprowadzonych kontroli, co może świadczyć o dużej dbałości o przestrzeganie regulacji na szczeblu państwowym. Powyższe dane oraz ich analiza wskazują na potencjalne różnice w podejściu do kontroli między Polską, państwami członkowskimi UE oraz krajami trzecimi. To z kolei może być niezmiernie istotne patrząc przez pryzmat skuteczności oraz intensywności polityki kontrolnej w poszczególnych regionach Europy i nie tylko.

Bibliografia

Brylak J., *Ochrona prawna bezpieczeństwa w ruchu drogowym*, Warszawa 2018.

Razny B., Domagała K, *Działania edukacyjne Inspekcji Transportu Drogowego*, Wyższa Szkoła Bezpieczeństwa Publicznego i Indywidualnego, wyd. Apeiron, Kraków 2021.

Bujak M., Dudek T., Hrycak A., Janus A., Kapica A., Krawczyk M., Miklis P., Piórkowski K, Radomski M., *Kontrola Inspekcji Transportu Drogowego*, „Wiedza i Praktyka" 2023.

Goniewicz M., Goniewicz K., *Wypadki drogowe w Polsce – czynniki sprawcze i zapobieganie*, „Bezpieczeństwo Pracy: Nauka i Praktyka" 2010, nr 9.

Karczmarczyk P., *ITD ma nowe urządzenia do zdalnej kontroli tachografów*, „Auto Świat", 22 listopada 2021.

Rummel S., *ITD gotowe na wyzwania. Nowoczesne furgony i Mobilne Jednostki Diagnostyczne*, „Ciężarówki i logistyka", 2 października 2023 r.

Jamróz K., *Koncepcje kształtowania bezpieczeństwa ruchu drogowego. Część 1. Przegląd koncepcji kształtowania bezpieczeństwa ruchu drogowego*, „Drogownictwo" 2012, nr 12.

Wojewódzka-Król K., Rolbiecki R., *Infrastruktura transportu*, Wydawnictwo Naukowe PWN, Warszawa 2018.

Wojewódzka-Król K., Załoga E., *Transport. Tendencje zmian*, Wydawnictwo Naukowe PWN, Warszawa 2022.

Akty normatywne

Ustawa z dnia 6 września 2001 r. o transporcie drogowym (tj. Dz.U. z 2024 r ., poz. 1539).

Ustawa z dnia 16 kwietnia 2004 r. o czasie pracy kierowców (t.j. Dz.U. z 2024 r., poz. 220).

Umowa europejska dotycząca międzynarodowego przewozu drogowego towarów niebezpiecznych (ADR), sporządzona w Genewie dnia 30 września 1957 r. (Dz.U. z 1975 r., nr 35, poz. 189).

Netografia

https://dane.gov.pl/pl/dataset/4365,gitd-kontrole-drogowe.

https://inelo.pl/inspekcja-transportu-drogowego-rola-zadania/.

https://inrel.pl/jak-przewozic-i-chronic-ladunki-ponadgabarytowe/.

https://licencjetransportowe.com/cmr-miedzynarodowy-list-przewozowy.html.

https://mapadotacji.gov.pl/projekty/781736/.

https://warszawa.tvp.pl/42611192/bezpieczenstwo-na-drodze-wyjatkowa-lekcja-z-inspekcja-transportudrogowego.

https://www.acea.auto/publication/report-vehicles-on-european-roads/.

https://www.krakow.witd.gov.pl/wazne-informacje/zadania-inspekcji/.

https://www.money.pl/gospodarka/niewolnicza-praca-kierowcow-z-filipin-polska-posrednikiem-w-procederze-6419726481888897a.html.
https://www.tirsped.com.pl/blog/propozycje-zmian-w-funkcjonowaniu-inspekcji-transportu-drogowego.

Kinga MATUSZ[1], Maciej ŻEBRAKOWSKI[2], Filip FERENC[3]

WYKORZYSTANIE BADAŃ DNA W KRYMINALISTYCE PRZEZ POLICJĘ

Wstęp

Dynamiczny rozwój technologii genetycznych w ostatnich dekadach zrewolucjonizował kryminalistykę, wprowadzając nowe narzędzia pozwalające na precyzyjne wykrywanie, analizowanie i interpretowanie dowodów biologicznych. Badania DNA (*deoxyribonucleic acid*) stały się jednym z kluczowych elementów śledztw kryminalnych, oferując możliwości, które jeszcze niedawno były nieosiągalne. Techniki takie jak profilowanie genetyczne umożliwiają identyfikację sprawców przestępstw nawet na podstawie minimalnych ilości materiału biologicznego, co ma szczególne znaczenie w sprawach dotyczących zbrodni popełnianych przed wieloma laty. Powszechne stosowanie analizy DNA otwiera nowe perspektywy nie tylko dla organów ścigania, lecz także dla wymiaru sprawiedliwości, umożliwiając wykluczenie osób niewinnych i potwierdzenie tożsamości sprawców. W rozdziale zostaną omówione takie tematy jak zarys historyczny tych badań i jak radzono sobie bez nich oraz opisana zostanie definicja genetyki i dna. Opisane zostaną podziały śladów biologicznych i czynniki je niszczące, profil dna, analiza pokrewieństwa oraz znaczenie materiału porównawczego oraz fenotypowania. Praca podsumowana zostanie analizą tematu baz danych DNA.

Wprowadzenie do tematu

Genetyka, jako nauka zajmująca się dziedziczeniem cech i zmiennością organizmów, stanowi jedno z fundamentalnych pól badawczych biologii. W jej ramach badane są m.in. struktura i funkcje DNA (kwasu deoksyrybonukleinowego) – materiału genetycznego, który determinuje unikalne właściwości każdego organizmu. DNA, odkryte po raz pierwszy w 1869 roku przez Friedricha Mieschera, przeszło długą drogę badań, zanim stało się w pełni rozpoznane jako kluczowy nośnik informacji genetycznej[4]. Przełomowe prace Jamesa Watsona i Francisa Cricka

[1] Politechnika Rzeszowska, Wydział Zarządzania.
[2] Politechnika Rzeszowska, Wydział Zarządzania.
[3] Politechnika Rzeszowska, Wydział Zarządzania.
[4] D. Myśliwiec, *Przepis na człowieka,* Altenberg, Warszawa 2020, s. 101-108.

z 1953 roku, w których opisali oni podwójną helisę DNA[5], otworzyły nowy rozdział w nauce, kładąc podwaliny pod rozwój współczesnej genetyki. Zanim jednak technologia pozwoliła na bezpośrednią analizę DNA, identyfikacja osób oraz ustalanie tożsamości w kryminalistyce opierały się na analizie fizycznych dowodów, takich jak odciski palców, ślady krwi czy charakterystyka pisma. Choć te metody miały swoje zastosowania, ich skuteczność była ograniczona, a możliwość pomyłek – znacząca. Wprowadzenie analizy DNA do kryminalistyki w latach 80. XX wieku przyniosło prawdziwą rewolucję w identyfikacji osób. Obecnie DNA jest wykorzystywane w kryminalistyce na wiele sposobów: do identyfikacji sprawców przestępstw, do wykluczania podejrzanych, w dochodzeniach genealogicznych oraz do rozwiązywania spraw dotyczących ofiar katastrof masowych. Rola analizy DNA stała się nieoceniona, szczególnie w kontekście tzw. spraw zimnych (*cold cases*), czyli nierozwiązanych przypadków sprzed wielu lat.

Kryminalne historie zapisane w genach

Historia badań w tej dziedzinie kryminalistyki sięga początków XX wieku, gdy ze względu na niską wiedzę i nikłe zaawansowanie, była ona skupiona tylko wokół badań serologicznych. W 1900 roku austriackiemu lekarzowi Karlowi Landsteinerowi udało się odkryć grupy krwi. Pozwoliło to na dalszy rozwój zrozumienia budowy oraz funkcjonowania człowieka i były to m. in.: odkrycia układów białek osocza czy grup enzymów. Warto zaznaczyć, że klasyczne badania krwi opierały się na analizie polimorfizmu (odmienne sekwencje nici DNA w tych samych miejscach w genomie) białek i enzymów, obecności lub braku antygenów powierzchniowych. To właśnie po takich odkryciach i w miarę coraz szerszego poznawania charakterystyk grup krwi, wiedzę tą zaczęto wykorzystywać w laboratoriach na potrzeby organów ścigania. Możliwości pierwszych metod analiz porównawczych były jednak mocno ograniczone. W przypadku posiadania pobranego śladu krwi podejrzanego i śladów krwi na miejscu przestępstwa, możliwe było jedynie określenie czy są one tożsame z pewnym jedynie prawdopodobieństwem. W takim przypadku, pewność zapewniała tylko sytuacja, gdy grupy krwi śladu i podejrzanego różniły się, co pozwalało na jednoznaczne wykluczenie danej osoby. Ponadto, do uzyskania profilu serologicznego potrzebna była duża ilość materiału biologicznego, co współcześnie nie jest już problemem. Co więcej, warto zaznaczyć, że ślady biologiczne, a zwłaszcza ich czynniki serologiczne, są podatne na degradację, szczególnie w niekorzystnych warunkach środowiskowych. Niewłaściwe zabezpieczenie śladów mogło przyspieszyć ten proces, dlatego wprowadzenie badań genetycznych w stosunku do serologii było tak wielkim przełomem. Umożliwiło ono izolację materiału genetycznego nawet bardzo małych śladów i pozwoliło na niemal stuprocentowe dopasowanie śladu do konkretnej

[5] J.D Watson, F.H.C. Crick, *Molecular Structure of Nucleic Acids – A Structure for Deoxyribose Nucleic Acid*, „Nature" 1953, nr 171, s. 737-738.

osoby przy wykorzystaniu materiału porównawczego[6]. Główne czynniki degradujące DNA to wilgoć, wysoka temperatura i bezpośrednie nasłonecznienie. Innymi substancjami mogącymi niszczyć DNA są metale ciężkie, kwasy, zasady oraz detergenty, przy czym warto zauważyć, że materiał biologiczny obecny w glebie podlega szczególnie szybkiemu rozkładowi. Podczas zabezpieczania materiału biologicznego do analizy należy podjąć kroki mające na celu eliminację tych czynników, aby uniknąć zniszczenia DNA[7]. Każdy próbka powinna być dokładnie osuszona, a następnie zapakowana w przepuszczające powietrze opakowanie, najlepiej gdy jest ono papierowe. Należy unikać opakowań, które blokują przepływ powietrza, takich jak woreczki foliowe lub szkło, chyba że materiał nie będzie suszony, lecz zamrożony. Często podczas oględzin natrafia się na wilgotne przedmioty z potencjalnymi śladami biologicznymi, na przykład zakrwawioną, wilgotną odzież należącą do ofiary lub sprawcy. Takie przedmioty należy osuszyć w odpowiednio przygotowanym pomieszczeniu, przeznaczonym do przechowywania lub suszenia materiałów dowodowych. Umieszczenie wilgotnej, zakrwawionej odzieży w papierowym opakowaniu i niewłaściwe obchodzenie się z nią może prowadzić do zanieczyszczenia próbki, co bezpośrednio poprowadzi techników do niewłaściwych wyników badania. Należy pamiętać, że policyjne pojazdy przewożą różne osoby i przedmioty, co skutkuje obecnością licznych nabłonków i potencjalnych profili DNA, gdzie Policja, a w szczególności technicy kryminalistyczni, mają obowiązek chronić dowody przed kontaminacją.

Ślady biologiczne

Aby właściwie zdefiniować pojęcie biologicznego śladu kryminalistycznego, należy najpierw zrozumieć, czym jest ślad kryminalistyczny w kontekście kryminalistyki. Brunon Hołyst definiuje ślad kryminalistyczny jako materialny ślad czynu zabronionego pozostawiony na miejscu przestępstwa lub związany z osobą sprawcy, stanowiący świadectwo jego działania i umożliwiający identyfikację sprawcy, narzędzia lub przebiegu zdarzenia[8]. Ślady kryminalistyczne mają kluczowe znaczenie, ponieważ pozwalają na odtworzenie zdarzeń przestępczych i stanowią podstawę dowodową w procesie wykrywczym. Jan Sehn opisał ślad kryminalistyczny jako zmianę w rzeczywistości obiektywnej, która stanowi widoczną pozostałość po przestępczym zdarzeniu. Ślad jest odbiciem czynności przestępczej i służy jako środek do rekonstrukcji zdarzenia z dużą dokładnością[9]. Według Sehna, ślad kryminalistyczny to każda zmiana, która jako efekt działania przestępczego jest spostrzegalna i stanowi podstawę dowodową. Z kolei Tadeusz Hanausek opisuje ślad kryminalistyczny jako każdy obiekt lub zmiana w stanie rzeczy,

[6] I. Kołakowska, *Kryminalne historie zapisane w genach* https://www.wum.edu.pl/node/17278 [dostęp: 15.10. 2024 r.].
[7] J. Mazepa, *Vademecum technika kryminalistyki,* Wolters Kluwer, Warszawa 2009.
[8] B. Hołyst, *Kryminalistyka. Nowe ujęcie,* Wydawnictwo Naukowe PWN, Warszawa 2009.
[9] J. Sehn, *Kryminalistyka: zarys systematyczny,* Wydawnictwo Naukowe PWN, Kraków 1965.

która może być obserwowana, zidentyfikowana lub zarejestrowana i która pozostaje po zdarzeniu przestępczym[10]. Hanausek wskazuje, że ślady są świadectwem istnienia przestępczego działania i mogą dostarczać informacji o sprawcy, ofierze, narzędziach oraz sposobie popełnienia czynu.

Zmiany będące kryminalistycznymi śladami biologicznymi, którym brak jednak jednolitej, spójnej definicji, będą miały więc ścisły związek z funkcjami życiowymi organizmu (najczęściej badany będzie organizm ludzki), z którego różnymi substancjami możemy spotkać się na miejscu zdarzenia zarówno na ofierze jak i pozostawionymi po sprawcy. Podział śladów biologicznych dzielony jest na:

- Tkanki – krew, tkanki miękkie (mięśniowa, tłuszczowa, nerwowa, łączna), tkanki twarde (zęby i kości), skóra i naskórek, paznokcie, włosy. Tkanki występują na miejscach tych zdarzeń, na których doszło do uszkodzenia ciała. Oprócz szeroko pojętych przestępstw przeciwko zdrowiu i życiu ludzkiemu są to wypadki drogowe oraz, co może dziwić, kradzieże z włamaniem, gdzie sprawca pokonuje przeszkodę w postaci okna lub oszklonych drzwi (sprawca kaleczy się, wybijając szybę).
- Wydzieliny – ślina, nasienie (sperma), wydzielina pochwowa, pot, łzy, wydzielina potowo-tłuszczowa. Wydzieliny są to substancje produkowane przez organizm w ściśle określonym celu. Śliny można spodziewać się na ustnikach niedopałków papierosów, w zużytej gumie do żucia, w miejscach sklejenia koperty do listu lub znaczka pocztowego. Spermy wewnątrz prezerwatywy, w kroczu majtek lub na ciele ofiary zgwałcenia. Wydzielina pochwowa może być na zewnętrznej powierzchni prezerwatywy, odzieży lub ciele sprawcy zgwałcenia. Pot występuje na kominiarkach, zwłaszcza w części czołowej, rękawiczkach i innej odzieży. Łzy jako ślad kryminalistyczny występują jedynie teoretycznie – niezmiernie rzadko się zdarza, by na miejscu zdarzenia ujawnić łzy sprawcy. Natomiast wydzielina potowo-tłuszczowa jest najczęściej zabezpieczanym śladem z tej kategorii – może wystąpić w każdym miejscu, do którego sprawca dotykał.
- Wydaliny – kał, mocz, wymiociny, smółka płodowa (pierwszy stolec, kał w życiu noworodka – wystąpienie smółki płodowej świadczy o tym, że dziecko urodziło się żywe) to substancje usuwane z organizmu, ponieważ są niepotrzebne lub wręcz szkodliwe. We współczesnej biologii kryminalistycznej czynnikiem badanym w śladzie jest DNA, który jest łatwo podatny na uszkodzenia i tym samym na zniszczenie. Kał, i w mniejszym zakresie także smółka płodowa, zawiera ogromne ilości bakterii gnilnych i enzymy trawienne, a wymiociny zawierają enzymy i trucizny, które wymioty spowodowały. Ponieważ DNA w wydalinach jest bardzo mało i działają na niego liczne czynniki niszczące, jako ślad biologiczny mają one znaczenie znikome, żeby nie powiedzieć żadne. Tylko w skrajnych przypadkach zabezpiecza się wydaliny jako ślad biologiczny na miejscu

[10] T. Hanausek, *Kryminalistyka: zarys wykładu,* Wydawnictwo Naukowe PWN, Warszawa 2000.

zdarzenia. Można natomiast wydaliny poddać badaniom toksykologicznym (wymiociny na obecność trucizn), czy np. w celu określenia, co dana osoba jadła dnia poprzedniego[11].

Profil DNA w kryminalistyce

Profilowanie DNA to jedna z kluczowych metod wykrywania sprawców przestępstw, jakimi dysponuje współczesna kryminalistyka. Charakteryzuje się ona jednym z najwyższych poziomów wiarygodności porównywalnym z dowodami badań daktyloskopijnych. Wysoką wartość dowodową ekspertyzy genetycznej niejednokrotnie podkreślał Sąd Najwyższy w swoim orzecznictwie. W wyroku Sądu Najwyższego z dnia 13 grudnia 2000 r., Sąd Najwyższy podniósł, iż: „Moc dowodowa z badań kwasu dezoksyrybonukleinowego [...] jest w takim stopniu duża, że jej kwestionowanie prowadziłoby do przekroczenia granic swobodnej sędziowskiej oceny dowodów"[12].

Przełomowym wydarzeniem, które doprowadziło do rozwoju i wykorzystania badań DNA w kryminalistce, było odkrycie przez Aleca Jeffreysa techniki analizy DNA opartej o zjawisko polimorfizmu (DNA), pozwalającej na wykrywanie powtarzających się sekwencji kodu genetycznego w ludzkim genomie (sekwencje powtórzeń tandemowych)[13]. Jeffreys swoje odkrycie określił mianem „DNA fingerprints", ponieważ krótkie, powtarzające się fragmenty DNA są unikalne oraz niezmienne dla każdego człowieka, a na ich podstawie możliwa jest zatem identyfikacja indywidualna człowieka. Możliwość powiązania danych śladów biologicznych z konkretnymi jednostkami zrewolucjonizowała dotychczasowe metody dowodowe kryminalistyki oraz medycyny sądowej. Już w 1988 roku pierwszy raz wykorzystano profilowanie DNA do wydania wyroku skazującego Collina Pitchforka w sprawie gwałtu i zabójstwa dwóch dziewcząt w Wielkiej Brytanii[14], a analiza DNA pozwoliła wtedy także na uniewinnienie innego mężczyzny, który został niesłusznie oskarżony. Gdy w 1991 roku Edwards (i wspólnicy) odkryli występujące kolejno (tandemowo) krótkie sekwencje DNA (ang. *short tandem repeat* – STR) zwane także sekwencjami mikrosatelitarnymi, które umożliwiały efektywniejsze profilowanie DNA, nastąpił bardzo intensywny rozwój tejże dziedziny kryminalistyki. Technika oparta na wykorzystaniu elektronicznej aparatury badającej materiał biologiczny poprzez elektroforezę kapilarną, fluorescencję i światło lasera, pozwalała na uzyskanie szybkich, wiarygodnych, mocno zróżnicowanych

[11] I. Bogusz, M. Bogusz, *Ślady kryminalistyczne dla słuchaczy szkolenia zawodowego podstawowego – Centrum Szkolenia Policji,* Legionowo 2015.

[12] Wyrok SN z dnia 13 grudnia 2000 r. (III CKN 1422/00), OSNC 2001/7–8, poz. 106.

[13] M. Szczepaniec, *Badania genetyczne DNA na użytek procesu karnego,* „Zeszyty Prawnicze" 2013, nr 13.1, s. 171.

[14] A. Tucholska-Lenart, *Genetyczna identyfikacja człowieka – zarys historii kryminalistycznych badań DNA,* „Kwartalnik Historii Nauki i Techniki" 2016, nr 3, s. 9.

wyników przy niskim koszcie badań[15]. Obecnie profilowanie DNA w kryminalistyce wykorzystywane jest w szczególności do:

- wykrywania sprawców przestępstw poprzez analizę śladów biologicznych (w tym krwi, nasienia, włosów, śliny, innych płynów ustrojowych) pozostawionych np. na miejscu zbrodni, na ciele denata,
- identyfikacji NN ofiar, zwłok i szczątków (*nomen nescio* – osoby o nieustalonej tożsamości),
- ustalania tożsamości osób (o tożsamości nieustalonej lub próbujących ją ukryć),
- analizy pokrewieństwa,
- predykcji cech fizycznych dawcy materiału biologicznego,
- ustalenia regionu geograficznego lub grupy etnicznej dawcy materiału biologicznego,
- identyfikacji gatunkowej zwierząt.

Niezaprzeczalnie kluczową rolę w kryminalistyce odgrywa możliwość przypisania śladów biologicznych pozostawionych na ofierze lub na miejscu zbrodni konkretnej osobie. Pozwala to nie tylko na wskazanie potencjalnego sprawcy czynu zabronionego, ale także na wykluczenie z kręgu podejrzanych osób o innym genotypie. Jest to wysoce użyteczne w sprawach o przestępstwa na tle seksualnym, ze względu na częstotliwość wykrywania męskiego nasienia na lub w ciele ofiary lub na miejscu zbrodni. Analiza DNA pozwala także np. na ujawnienie więcej niż jednego sprawcy przestępstwa zgwałcenia.

Analiza pokrewieństwa

Analiza porównawcza profili genetycznych służących ustaleniu pokrewieństwa pomiędzy dwoma osobami najczęściej powiązywana jest z ustaleniami rodzicielstwa, zazwyczaj ojcostwa. Badania takie (poza zleceniami prywatnymi) znajdują się w domenie prawa cywilnego. Jednakże sporządzanie i porównywanie profili genetycznych ma zastosowanie także w kryminalistyce. Najczęściej spotykanym jest porównanie profili genetycznych ofiar (zwłok, szczątków) o niezidentyfikowanej tożsamości z profilami członków rodziny biologicznej. Przydatne jest to zwłaszcza, gdy ciało ofiary jest w stanie rozkładu bądź nie jest możliwa identyfikacja wizualna ze względu na np. rozległe uszkodzenia skóry. Profile genetyczne do analizy porównawczej można pozyskać z baz danych DNA lub pobrać od domniemanej rodziny denata. Analiza pokrewieństwa nie znajduje zatem zastosowania, w przypadku, gdy brak jest hipotez śledczych wskazujących na powiązania ofiary z innymi osobami[16].

Analiza ta pozwala także na zawężenie kręgu podejrzanych, gdy w bazie danych DNA figuruje już osoba o profilu genetycznym wskazującym na pokre-

[15] M. Szczepaniec, *Badania genetyczne..., op.cit.,* s. 175-176.

[16] B. Speichert-Zalewska, M. Zubańska, K. Bielawska, *cenne dla postępowania karnego informacje z kodowanych regionów genomu,* „Przegląd Policyjny" 2017, nr 2(126), s. 162-163.

wieństwo z osobą, której ślady biologiczne zabezpieczono na miejscu zbrodni lub na ofierze. Mechanizm dziedziczenia sprawia, że potomek z pierwszego pokolenia posiada w swoim genotypie dokładnie po jednym chromosomie rodzica. Oznacza to, że w przypadku pokrewieństwa rodzic – dziecko, wszystkie 15 markerów STR musi być zgodne co najmniej jednym allelem[17]. W przypadku kolejnych pokoleń lub rodzeństwa, prawdopodobieństwo wystąpienia tej zależności jest duże, jednak nie musi występować. Im dalsze pokrewieństwo między dwoma osobami, tym odsetek występowania jednakowych alleli dla danego markera jest mniejsze. Jeśli prawdopodobieństwo to jest niższe niż prawdopodobieństwo wynikające ze statystyki wystąpienia poszczególnych alleli, nie można ustalić pokrewieństwa za pomocą tej metody. Wyjątek dla analizy porównawczej stanowią bliźnięta, lecz tylko jednojajowe z uwagi na identyczne DNA, w przypadku bliźniąt dwujajowych, kod genetyczny różni się między sobą[18].

Materiał porównawczy

Materiałem porównawczym do identyfikacji profilu DNA pozyskanego z zabezpieczonych na miejscu zdarzenia śladów (materiał dowodowy), określa się materiał pobrany najczęściej od osoby lub osób typowanych w danej sprawie – podejrzanych lub oskarżonych. Zazwyczaj przybiera on formę wymazu ze śluzówki policzków, pobranego przez przeszklonego policjanta na specjalny pakiet do wymazów[19]. Popularność tej metody wynika m.in. z niskiej inwazyjności procesu pobierania materiału w porównaniu np. do próbek krwi żylnej, czy próbek wyrwanych włosów (z cebulkami) oraz efektywności w tworzeniu profilu DNA. W przypadku badań identyfikacyjnych, które mają na celu ustalenie tożsamości osoby zaginionej, pobiera się materiał porównawczy z przedmiotów codziennego użytku typowanego zaginionego (szczoteczka do mycia zębów, maszynka do golenia, grzebień) lub pozyskuje materiał biologiczny (wymaz ze śluzówki policzka, próbki krwi, włosy wyrwane) od członków rodziny[20].

Najbardziej efektywne jest pobieranie materiału od dzieci lub rodziców z uwagi na największe pokrewieństwo genetyczne. W przypadku ujawnienia zwłok, materiał porównawczy pobiera się tak jak w przypadku osób zaginionych – z rzeczy codziennego użytku lub od rodziny. Technika ta jest zatem efektywna tylko w określonych przypadkach, takich jak przypuszczenia co do tożsamości sprawcy, ofiary, zaginionego lub posiadanie w bazie DNA identycznego profilu lub profilu wskazującego na pokrewieństwo, a także możliwość wyeliminowanie określonej osoby osób z kręgu podejrzanych. Istotną wadą analizy DNA materiału

[17] W. Olchowik, *Wysoko wiarygodne metody identyfikacji osób,* „Biuletyn WAT" 2013, nr 4, s. 183.
[18] P. Kowalczyk, *Badania DNA w orzecznictwie sądowym w sprawach karnych,* „Prokuratura i Prawo" 2011, nr 3, s. 14-15.
[19] I. Bogusz, M. Bogusz*, Technika kryminalistyczna. Ślady biologiczne,* Wydawnictwo Centrum Szkolenia Policji w Legionowie, Legionowo 2013, s. 14.
[20] *Ibidem*, s. 16.

biologicznego, związaną z materiałem porównawczym jest możliwość kontaminacji próbek materiału porównawczego, która może wyeliminować wartość dowodową badania[21]. Kontaminacja próbki z materiałem biologicznym może bowiem prowadzić do niewłaściwego dopasowania profilu DNA, czyli w konsekwencji wskazać na niewłaściwą osobę. Z tego względu konieczne jest przestrzeganie wszystkich niezbędnych procedur mających na celu zabezpieczenie próbki przed kontaminacją zarówno podczas pobierania, jak i przechowywania materiału porównawczego. Rzadziej występującym błędem, niemniej jednak spotykanym, jest uzyskanie nieprawidłowych wyników dopasowania profilów DNA ze względu na niewłaściwe oznaczenie próbek. Materiał porównawczy może być wtedy analizowany w innej sprawie lub w innym charakterze, na przykład materiał pobrany od oskarżonego może występować jako materiał dowodowy pobrany od ofiary.

Fenotypowanie DNA

Fenotypowanie DNA to technika genetyczna, która polega na analizie DNA w celu przewidzenia cech fenotypowych danej osoby, takich jak kolor oczu, skóry, włosów czy struktura twarzy. W kryminalistyce zastosowanie tej technologii jest szczególnie przydatne w przypadkach, gdy nie ma bezpośredniego dostępu do podejrzanych lub gdy dostępne są jedynie ślady biologiczne niezidentyfikowanej osoby. O ile klasyczne profilowanie DNA umożliwia porównanie materiału biologicznego z bazą danych, o tyle fenotypowanie DNA pozwala na stworzenie „portretu" osoby bez konieczności posiadania próbki do porównania. Fenotypowanie opiera się na identyfikacji specyficznych wariantów genetycznych związanych z wybranymi cechami fizycznymi[22]. Dla przykładu, geny, takie jak *OCA2* i *HERC2* dla koloru oczu, czy *MC1R* dla koloru włosów, mają kluczowy wpływ na cechy zewnętrzne, które można przewidzieć na podstawie analizy DNA.

Postęp w sekwencjonowaniu genomów i zrozumieniu genomiki populacyjnej pozwala na dokładniejsze przewidywanie fenotypów, jednakże dokładność tych przewidywań różni się w zależności od cechy i populacji[23]. Nowoczesne techniki fenotypowania DNA korzystają z różnych metod analizy, takich jak sekwencjonowanie całego genomu, analiza SNP (polimorfizm pojedynczego nukleotydu), oraz bioinformatyczne modelowanie danych genetycznych[24]. Fenotypowanie DNA w kryminalistyce ma szerokie zastosowanie w przypadkach, gdzie tradycyjne metody analizy nie przynoszą rezultatów. Może ono pomóc w identyfikacji cech fizycznych potencjalnych sprawców lub ofiar przestępstw, tworzeniu profili sprawców w przypadkach seryjnych przestępstw oraz wyjaśnianiu zaginięć poprzez

[21] A. Gałęska-Śliwka, *Ocena kompetencji laboratoriów genetyki sądowe,* „Prokuratura i Prawo" 2013, nr 6, s. 115-116.

[22] I. Surożyńska-Godzina, *Kryminalistyczne fenotypowanie DNA – możliwości, ograniczenia oraz stan prawny*, „Problemy Współczesnej Kryminalistyki" 2017, nr 21, s. 210.

[23] L.A. Marano, C. Fridman, *DNA phenotyping: current application in forensic science*, „Research and Reports in Forensic Medical Science" 2019, nr 9, s. 2-3.

[24] S. Matheson, *DNA Phenotyping: Snapshot of a Criminal*, „Cell" 2016, nr 166, s. 1061.

przewidywanie wyglądu na podstawie materiału genetycznego. Fenotypowanie jest szczególnie przydatne, gdy próbki DNA nie pasują do żadnych profili w bazach danych, pozwalając organom ścigania na stworzenie obrazu poszukiwanej osoby na podstawie samych danych genetycznych.

Choć fenotypowanie DNA ma duży potencjał, niesie za sobą pewne ograniczenia techniczne oraz wyzwania etyczne i prawne. Pierwszym problemem jest dokładność i niepewność wyników. Przewidywania fenotypowe nie zawsze są w pełni precyzyjne, a cechy takie jak struktura twarzy są nadal trudne do dokładnego odwzorowania. Dodatkowo, zróżnicowanie populacyjne wpływa na dokładność wyników, co może prowadzić do błędnych interpretacji. Drugim problemem jest etyczne wykorzystanie tej techniki. Tworzenie „portretów" na podstawie DNA wiąże się z pytaniami o prywatność genetyczną i prawo do anonimowości. W niektórych krajach pojawiają się wątpliwości co do stosowania tej technologii, zwłaszcza że fenotypowanie może wpływać na stereotypy lub uprzedzenia.

Innym z problemów jest częsty brak odpowiednich regulacji prawnych pozwalających na wykorzystanie tej techniki. Wykorzystanie techniki może prowadzić do nadużyć lub podważenia takiego dowodu w procesie sądowym[25]. Wraz z rozwojem nauki przewiduje się, że możliwe będzie uzyskanie coraz dokładniejszych wyników, które obejmą nie tylko cechy fizyczne, ale również predyspozycje do pewnych chorób czy cechy behawioralne. Istotnym kierunkiem rozwoju będzie również stworzenie bardziej zaawansowanych algorytmów uwzględniających zróżnicowanie populacyjne, aby zwiększyć dokładność fenotypowania dla różnych grup etnicznych. Fenotypowanie DNA jest obiecującym narzędziem, które może wspierać śledczych w przypadkach, gdzie brak jest innych możliwości identyfikacji. Choć technologia ta wciąż wymaga udoskonaleń, w szczególności w zakresie dokładności i niezależności od zróżnicowania populacyjnego, już teraz stanowi wartościowe uzupełnienie tradycyjnych metod kryminalistycznych. Kluczowe pozostaje jednak wypracowanie odpowiednich ram prawnych oraz przestrzeganie zasad etycznych, aby zapobiec potencjalnym nadużyciom i zapewnić ochronę prywatności osób, których dane genetyczne są analizowane. Fenotypowanie DNA ma potencjał, by zrewolucjonizować kryminalistykę, pod warunkiem że będzie wykorzystywane odpowiedzialnie i z poszanowaniem praw człowieka.

Baza danych DNA

Wprowadzenie baz danych DNA do systemów ścigania stanowiło przełom w kryminalistyce, umożliwiając szybką i skuteczną identyfikację podejrzanych, nawet w przypadkach, gdy inne dowody są ograniczone lub niepewne. Przechowywanie profili DNA osób skazanych, podejrzanych, a także nieidentyfikowanych próbek znalezionych na miejscach przestępstw, pozwala na bardziej efektywną identyfikację sprawców i zwiększa zdolność do łączenia przestępstw o podobnym

[25] T. Tomaszewski, B. Foremniak-Szadura, K. Figaszewska, *Kryminalistyczne fenotypowanie..., op.cit.,* s. 8-10.

charakterze. Bazy te są obecnie stosowane w wielu krajach na świecie, przy czym ich zakres i zasady funkcjonowania różnią się w zależności od jurysdykcji. Bazy danych DNA w kryminalistyce wykorzystują zbiory profili genetycznych, które składają się z markerów genetycznych specyficznych dla każdego człowieka. Proces ten obejmuje analizę wybranych loci DNA, w szczególności krótkich tandemowych powtórzeń (STR), które są wystarczająco zróżnicowane, aby umożliwić indywidualne identyfikacje[26]. Systemy takie jak CODIS (*Combined DNA Index System*) w Stanach Zjednoczonych czy NDNAD (*National DNA Database*) w Wielkiej Brytanii są przykładem zaawansowanych narzędzi kryminalistycznych, które przechowują i porównują profile DNA w celu identyfikacji osób oraz wykrywania przestępców recydywistów[27]. W Polsce nie mamy specjalnej nazwy dla omawianej bazy, która zgodnie z ustawą o Policji nazywana jest po prostu zbiorem danych DNA[28]. W zależności od regulacji prawnej państwa, w bazach danych przechowuje się informacje o osobach skazanych, podejrzanych, śladach biologicznych z miejsca przestępstwa oraz próbki referencyjne[29].

Bazy danych DNA przyczyniają się do wzrostu efektywności postępowań kryminalnych, szczególnie w zakresie identyfikacji sprawców oraz ofiar, uniewinnienia niesłusznie oskarżonych oraz łączenia spraw. Skuteczność baz danych DNA zależna jest jednak od kilku czynników. Pierwszym z nich jest jej rozmiar – im więcej próbek zawiera tym większa szansa na wytypowanie sprawcy. Również jakość pobieranych próbek oraz sposób ich przechowywania jest istotny, bowiem DNA może ulec degradacji, a ze zniszczonej próbki nie da się dopasować osoby ze stuprocentową pewnością[30]. W miarę postępu technologicznego przyszłość baz danych DNA może obejmować rozwój systemów bardziej precyzyjnych, zautomatyzowanych oraz umożliwiających analizę z coraz mniejszych ilości DNA. Możliwość analizy złożonych markerów genetycznych otwiera nowe ścieżki do identyfikacji sprawców, nawet w przypadkach częściowo zdegradowanych próbek.

Zadania i rola Policji w procesie analizy DNA

Instytucjami odpowiedzialnymi za pobieranie i zabezpieczanie materiału źródłowego i materiału porównawczego w Polsce są w szczególności Policja oraz technicy kryminalistyczni. Wynika to bezpośrednio z ustawy o Policji z dnia 6 kwietnia 1990 roku oraz art. 205 §1 k.p.k. Ślady biologiczne ujawnione na

[26] A. Jurga, J. Mondzelewski, *Funkcjonowanie bazy danych DNA w Polsce,* „Problemy Kryminalistyki" 2017, nr 297, s. 15-16.

[27] A.O. Amankwaa, *Trends in forensic DNA database: transnational exchange of DNA data,* „Forensic Sciences Research" 2020, nr 5, s. 10-11.

[28] Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz.U. z 2024 r. poz. 1562).

[29] K. Ćwik, *Eliminacyjna Baza Danych DNA – szansa czy zagrożenie? Przegląd funkcjonowania baz eliminacyjnych na przykładzie wybranych państw,* „Problemy Kryminalistyki" 2017, nr 295, s. 3-4.

[30] A. Jurga, J. Mondzelewski, *Funkcjonowanie bazy…, op.cit.,* s. 19.

miejscu zdarzenia zazwyczaj są pobierane i zabezpieczane przez techników kryminalistycznych na miejscu popełnienia przestępstwa lub w laboratorium kryminalistycznym, gdzie pobieraniem materiału biologicznego zajmują się biegli oraz personel techniczny.

W przypadku pobierania i zabezpieczania materiału od osób (zazwyczaj jest to wymaz z błony śluzowej jamy ustnej), czynności te przeprowadzają wykwalifikowani funkcjonariusze Policji, uprawnieni pracownicy służby zdrowia lub innej instytucji. Wymaz ze śluzówki jamy ustanej pobiera się najczęściej w przypadku osób oskarżonych, podejrzanych, o nieustalonej tożsamości, usiłujących ukryć tożsamość czy stwarzających zagrożenie. Istotną rolę w procesie tworzenia i porównywania profili genetycznych ma Centralne Laboratorium Kryminalistyczne Policji (CLKP), które na mocy ustawy o Policji z dnia 6 kwietnia 1990 r. realizuje zadania z zakresu kryminalistyki oraz technik kryminalistycznych, w których skład wchodzą właśnie analizy materiałów dowodowych i porównawczych[31].

Biegli z określonych specjalizacji identyfikują materiał biologiczny, oznaczają profil DNA, a następnie przeprowadzają analizę porównawczą w zakresie układów typu STR wykorzystując do tego materiał porównawczy lub korzystając z baz danych DNA. Priorytetem dla takich instytucji jest również odpowiednie przechowywanie takich próbek. Warto zauważyć, że dobrze przechowywane ślady biologiczne można badać po kilkudziesięciu latach, dlatego najkorzystniejszym przypadkiem przechowywania materiału biologicznego jest zaciemnione, ciepłe, a przede wszystkim suche pomieszczenia. To wilgoć prowadzi do rozwoju mikroorganizmów, a te z kolei niszczą materiał biologiczny, w tym DNA. Występują także przypadki, gdzie odpowiednie zabezpieczenie śladu jest kluczowe i dostępne wyłącznie w krótkim czasie od wystąpienia zdarzenia. W przypadku ofiar przestępstw na tle seksualnym wymazy z dróg rodnych należy pobierać najszybciej jak to możliwe, bo czas, który upłynął od zdarzenia do pobrania próbek ma znaczący wpływ na wyniki badań DNA.

W literaturze można spotkać informację, że maksymalny czas, który upłynął od zdarzenia do pobrania wymazów z dróg rodnych pokrzywdzonej, z których uzyskano pozytywny wynik badań genetycznych określany jest na nie dłuższy niż 5 dni[32]. Z pobieraniem oraz zabezpieczaniem materiału genetycznego, nierozerwalnie związane jest zjawisko kontaminacji, która wyklucza całkowicie możliwość prawidłowej interpretacji wyników. Z tego właśnie powodu konieczne jest, aby wszyscy funkcjonariusze Policji, technicy kryminalistyczni oraz biegli zaangażowani w proces badań DNA wykazywali się pełną znajomością procedur zabezpieczających materiał przed kontaminacją. Historia pokazuje, iż błędne pobranie lub przechowywanie śladów biologicznych potrafiło zupełnie zmienić oblicze danej prowadzonej sprawy. Interesującym przypadkiem kontaminacji była głośna sprawa „Fantoma z Heilbronn", który powiązany był z 40 różnorodnymi

[31] Art. 5e ustawy o Policji.

[32] A. Ruszczyk, *Badania genetyczne w służbie wymiaru sprawiedliwości,* 2016, https://gazetasledcza.pl/2016/04/badania-genetyczne-sluzbie-wymiaru-sprawiedliwosci/ [dostęp: 11.11.2024 r.].

przestępstwami, w tym 7 morderstwami[33]. Sprawca przez kilkanaście lat pozostawał nieuchwytny, a dowody w jego sprawie pełne były wątpliwości i sprzeczności. Fantom zaangażowany był bowiem w sprawy zarówno drobnych kradzieży, jak i brutalnych morderstw. Dopiero powtórzenie analizy DNA na nowych próbkach ujawniło tajemnicę słynnego Fantoma, jaką było zanieczyszczenie wykorzystywanych przez Policję patyczków zakończonych wacikiem (do zabezpieczania materiału dowodowego), przez pracownicę fabryki, która je produkowała[34].

Wnioski końcowe

Badania DNA stanowią jedno z najważniejszych narzędzi współczesnej kryminalistyki, znacznie zwiększając precyzję i niezawodność dowodów stosowanych w postępowaniach sądowych. W rozdziale omówiono wykorzystanie badań DNA w kryminalistyce, podkreślając ich znaczenie jako narzędzia identyfikacji i rozwiązywania spraw przestępczych. Badania DNA, wprowadzone do kryminalistyki w latach 80. XX wieku, rewolucjonizowały sposób analizowania śladów biologicznych, umożliwiając precyzyjną identyfikację sprawców nawet na podstawie minimalnych ilości materiału biologicznego. Przedstawiono techniki izolacji DNA z różnych próbek, takich jak włosy, ślina, krew czy inne tkanki oraz omówiono metody analiz, w tym sekwencjonowanie i profilowanie DNA. Opisano rozwój technik takich jak PCR i STR, które pozwalają na szybkie i dokładne tworzenie profili genetycznych wykorzystywanych w śledztwach. Przedstawione są także podział śladów biologicznych (tkanki, wydzieliny, wydaliny) oraz procedury ich zabezpieczania, aby uniknąć degradacji i kontaminacji, co może wpływać na wyniki analizy. Omówiono także rolę materiału porównawczego i zasady jego pobierania, jak również wyzwania związane z ochroną prywatności.

Zasygnalizowana została praca instytucji odpowiedzialnych za jego pobieranie i zabezpieczanie, która jest oparta na działalności Policji i techników kryminalistycznych. W Polsce kompetencje tych jednostek opisane są bezpośrednio w ustawie o Policji z dnia 6 kwietnia 1990 roku. Ponadto, poruszono temat baz danych DNA, które przyczyniają się do zwiększenia efektywności działań organów ścigania poprzez umożliwienie szybkiego dopasowania profili genetycznych do osób już notowanych lub próbek znalezionych na miejscu przestępstwa. Jednakże, rosnąca popularność badań DNA niesie za sobą wyzwania prawne i etyczne, takie jak kwestia ochrony prywatności i ryzyko błędnej interpretacji wyników, które przedstawione zostały na podstawie spraw kryminalnych z dawnych lat.

[33] C. Himmelreich, *Deutschlands Phantom-Serienmörder: Ein DNA-Fehler*, 2009, https://time.com/archive/6946145/germanys-phantom-serial-killer-a-dna-blunder/ [dostęp: 12.10.2024 r.].

[34] U. Rogalla, *Ostrożności nigdy za wiele,* „Genetyka i Prawo" 2009, nr 3, s. 15.

Bibliografia

Amankwaa A.O., *Trends in forensic DNA database: transnational exchange of DNA data*, „Forensic Sciences Research" 2020, nr 5.

Bogusz I., Bogusz M., *Ślady kryminalistyczne dla słuchaczy szkolenia zawodowego podstawowego – Centrum Szkolenia Policji*, Legionowo 2015.

Bogusz I., Bogusz M., *Technika kryminalistyczna. Ślady biologiczne,* Wydawnictwo Centrum Szkolenia Policji w Legionowie, Legionowo 2013.

Ćwik K., *Eliminacyjna Baza Danych DNA – szansa czy zagrożenie? Przegląd funkcjonowania baz eliminacyjnych na przykładzie wybranych państw*, „Problemy Kryminalistyki" 2017, nr 295.

Gałęska-Śliwka A., *Ocena kompetencji laboratoriów genetyki sądowe*, „Prokuratura i Prawo" 2013, nr 6.

Hanausek T., *Kryminalistyka: zarys wykładu*, PWN, Warszawa 2000.

Hołyst, B., *Kryminalistyka. Nowe ujęcie*, PWN, Warszawa 2020.

Jurga A., Mondzelewski J., *Funkcjonowanie bazy danych DNA w Polsce*, „Problemy Kryminalistyki" 2017, nr 297.

Kowalczyk P., *Badania DNA w orzecznictwie sądowym w sprawach karnych,* „Prokuratura i Prawo" 2011, nr 3.

Marano L.A., Fridman C., *DNA phenotyping: current application in forensic science*, „Research and Reports in Forensic Medical Science" 2019, nr 9.

Matheson S., *DNA Phenotyping: Snapshot of a Criminal*, „Cell" 2016, nr 166.

Mazepa J., *Vademecum technika kryminalistyki,* Wydawnictwo Wolters Kluwer, Warszawa 2009.

Myśliwiec D., *Przepis na człowieka*, Wydawnictwo Altenberg, Warszawa 2020.

Watson J.D., Crick F.H.C., *Molecular Structure of Nucleic Acids – A Structure for Deoxyribose Nucleic Acid*, „Nature" 1953, nr 171.

Olchowik W., *Wysoko wiarygodne metody identyfikacji osób,* „Biuletyn WAT" 2013, nr 4.

Sehn J., *Kryminalistyka: zarys systematyczny*, PWN, Kraków 1965.

Speichert-Zalewska B., Zubańska M,, Bielawska K., *cenne dla postępowania karnego informacje z kodowanych regionów genomu*, „Przegląd Policyjny" 2017, nr 2(126).

Surożyńska-Godzina I., *Kryminalistyczne fenotypowanie DNA – możliwości, ograniczenia oraz stan prawny*, „Problemy Współczesnej Kryminalistyki" 2017, nr 21.

Szczepaniec M, *Badania genetyczna DNA na użytek procesu karnego, „*Zeszyty Prawnicze" 2013, nr 1.

Tomaszewski T., Foremniak-Szadura B., Figaszewska K., *Kryminalistyczne fenotypowanie DNA – wybrane problemy prawne*, „Problemy Kryminalistyki" 2019, nr 303.

Tucholska-Lenart A., *Genetyczna identyfikacja człowieka – zarys historii kryminalistycznych badań DNA*, „Kwartalnik Historii Nauki i Techniki" 2016, nr 3.

Akty normatywne

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j. Dz.U. z 2024 r., poz. 1562).

Orzecznictwo

Wyrok SN z dnia 13 grudnia 2000 r. (III CKN 1422/00), OSNC 2001/7–8, poz. 106.

ZAKOŃCZENIE

Chociaż obecnie bezpieczeństwo stanowi zasadniczą koncepcją dla stosunków wewnętrznych i międzynarodowych, to można się zastanawiać, czy bezpieczeństwo jest zjawiskiem obiektywnym czy subiektywnym. A. Wolfers nazwał nawet bezpieczeństwo narodowe symbolem[1], który może nie mieć żadnego unikalnego znaczenia. Z kolei bezpieczeństwo w ujęciu R.J. Arta bezpieczeństwo jest sprawą stopnia mniejszego lub większego poczucia bycia bezpiecznym[2], a dla Th. Trouta, J. Harfa, bezpieczeństwo oznacza nieobecność zagrożeń dla istnienia[3].

Tytuł monografii wyraźnie wskazuje na problematykę bezpieczeństwa w wymiarze instytucjonalnym, która bezpośrednio lub pośrednio dotyczy państw, organizacji międzynarodowych, a także jednostki w XXI wieku. Na przestrzeni ostatnich tygodni, a nawet dni ujawniło się wiele nowych napięć i konfliktów o charakterze informacyjnym, które nie są pozbawione szerszych implikacji w skali międzynarodowej. Często podłożem tych konfliktów są kryzysy gospodarcze, polityczne czy militarne, które w niektórych przypadkach zostają umiędzynarodowione prowadząc często do destabilizacji państw ościennych, jak w obecnym konflikcie zbrojnym Rosja – Ukraina, czy Izrael – Palestyna, albo jeszcze wcześniej w pandemii COVID-19, która miała wymiar globalny.

XXI wiek charakteryzuje się licznymi konfliktami zbrojnymi, sporami i kryzysami oraz napięciami przede wszystkim o charakterze regionalnym. Mają one charakter lokalny oraz są długotrwałe i dotkliwe dla obecnego społeczeństwa i władz państwowych.

Najczęstszymi źródłami napięć, konfliktów i kryzysów są: zadawnione spory terytorialne z tendencjami nacjonalistycznymi, rozpad i powstanie nowych państw, napięcia etniczne i religijne, nielegalna migracja, a obecnie przede wszystkim cyberterroryzm i inne formy zorganizowanej przestępczości.

Należy jednak zauważyć, że to cyberprzestrzeń stała się w ostatniej dekadzie dzięki rozwojowi technologii i postępowi cyfryzacji głównym obszarem zagrożenia i postępu. Z jednej strony należy uznać ją jako „miejsce", gdzie dokonywane są transnarodowe transakcje, a jej konstrukcja i rozwój tylko przyśpiesza i ułatwia komunikację w sferze zarówno publicznej, jak i prywatnej. To dzięki niej organy sądowe lub Policja mogą usprawnić postępowanie dowodowe w sprawach karnych

---

[1] A. Wolfers, *Discord and Collaboration*, Baltimore 1962, s. 147.
[2] R.J. Art, *Security* [w:] *Oxford Companion to Politics in the World*, Oxford 1993, s. 822.
[3] Patrz szerzej: M. Pietraś, *Dylematy bezpieczeństwa państwa w postzimnowojemnym świecie*, „Annales Universitatis Mariae Curie-Skłodowska". Sectio K, Politologia 1994, nr 1, s. 47-50.

czy cywilnych. Z drugiej jednak strony należy nie zapominać, że nadmierny udział AI w różnych obszarach życia codziennego człowieka, nie koniecznie jest dla nas tylko skróceniem czasu pracy, wzrostu wynagrodzenia, uproszczeniem rozpoznawania sprawy na etapie przyznawania kredytu, liczenia głosów wyborczych, ale co raz częściej stanowi jedną z przyczyn zastąpienia osoby przez świetnie wyszkolony sztuczny mechanizm.

Od wielu lat traktuje się bezpieczeństwo jako najwyższą wartość ludzką, która gwarantuje stabilność, rozwój i szczęście. Ta wartość nie jest niczym pewnym, danym człowiekowi raz na zawsze. Wymaga ona ogromnego wysiłku państw, sojuszy i organizacji międzynarodowych w budowaniu trwałego pokoju wobec zagrożeń i dylematów dzisiejszego świata. Mając na względzie złożoność i jego nieprzewidywalność oraz wyzwania i zagrożenia wywoływane przez naturę i człowieka, funkcją tej monografii jest umożliwienie identyfikacji problemów wynikających zakresu bezpieczeństwa i samodzielne opracowywanie scenariuszy wobec prawdopodobnych zagrożeń i dylematów.

Izabela Oleksiewicz[4]
Małgorzata Polinceusz[5]

[4] dr hab. Izabela Oleksiewicz, prof. PRz, Politechnika Rzeszowska, Wydział Zarządzania. ORCID: 0000-0002-1622-7467.
[5] dr Małgorzata Polinceusz, Politechnika Rzeszowska, Wydział Zarządzania. ORCID: 0000-0002--1179-6628.

Streszczenie

Celem monografii była analiza i przedstawienie wybranych instytucji bezpieczeństwa wewnętrznego państwa działających zarówno w Polsce, jak i na świecie w XXI w. Autorzy skupili się na zagadnieniach bezpieczeństwa informacyjnego oraz roli i zadaniach takich organów, formacji czy instytucji jak: sądy, Policja, Centralne Biuro Zwalczania Cyberprzestępczości, chcąc w ten sposób ukazać ewolucję zjawiska specjalizacji kompetencji państwa w ściśle wybranych płaszczyznach życia codziennego. Z drugiej strony, starli się ukazać efekty cyfryzacji, jakie następują w różnych instytucjach i na różnym poziomie. Jako przykłady omówiono UE wraz z polityką migracyjną, USA i wybory na prezydenta oraz Polskę na tle UE w kontekście bezpieczeństwa drogowego.

Pokazanie znaczenia poszczególnych instytucji w XXI w. przy jednoczesnym podkreśleniu zmian, jakie w nich nastąpiły od strony materialnoprawnej lub proceduralnej ma ukazać Czytelnikom następstwo rozwoju technologii, cyfryzacji i postępu, które jest rzeczą konieczną.

Summary

The aim of the monograph was to analyse and present selected state internal security institutions operating both in Poland and worldwide in the 21st century. The authors focused on the issues of information security and the role and tasks of such bodies, formations or institutions as the courts, the Police, the Central Office for Combating Cybercrime, thus wishing to show the evolution of the phenomenon of specialisation of state competences in strictly selected areas. On the other hand, they attempted to show the effects of digitisation taking place in different institutions and at different levels. As examples, the EU with its migration policy, the USA and the presidential election and Poland against the background of the EU in the context of road safety were discussed.

Showing the relevance of individual institutions in the 21st century while highlighting the changes that have occurred in them from a substantive or procedural point of view is intended to show readers the corollary of technological development, digitalisation and progress, which is a necessary thing.

DOCUMENT CREATED WITH

PDF COMBINER

PDF Combiner is a free application that you can use to combine multiple PDF documents into one.

Three simple steps are needed to merge several PDF documents. First, we must add files to the program. This can be done using the Add files button or by dragging files to the list via the Drag and Drop mechanism. Then you need to adjust the order of files if list order is not suitable. The last step is joining files. To do this, click button Combine PDFs.

Main features:

secure PDF merging - everything is done on your computer and documents are not sent anywhere

simplicity - you need to follow three steps to merge documents

possibility to rearrange document - change the order of merged documents and page selection

reliability - application is not modifying a content of merged documents.

Visit the homepage to download the application:

www.jankowskimichal.pl/pdf-combiner

To remove this page from your document, please donate a project.