

WYMIAR BEZPIECZEŃSTWA W XXI WIEKU:

Redakcja naukowa
Adrian Pachciarz
Daniel Nowakowski



Integracja perspektyw
w kontekście
współczesnych zagrożeń

Wymiar bezpieczeństwa w XXI wieku:

Integracja perspektyw
w kontekście współczesnych zagrożeń

Wymiar bezpieczeństwa w XXI wieku:

Integracja perspektyw
w kontekście współczesnych zagrożeń

REDAKCJA NAUKOWA

Adrian Pachciarz, Daniel Nowakowski

Poznań 2026

Wydawnictwo Naukowe Kontekst

Wymiar bezpieczeństwa w XXI wieku: Integracja perspektyw w kontekście współczesnych zagrożeń, red. Adrian Pachciarz, Daniel Nowakowski, 210 s., Wydawnictwo Naukowe Kontekst, Poznań 2026.

Redaktor

Adrian Pachciarz, Daniel Nowakowski

Projekt okładki

Michał Łacny

Korekta

Bartosz Sobański

Streszczenie

Przedmiotowa monografia naukowa podejmuje problematykę wymiaru bezpieczeństwa w XXI wieku w kontekście współczesnych zagrożeń. Głównym celem publikacji jest konsolidacja perspektyw oraz badania nad różnymi aspektami bezpieczeństwa poprzez interdyscyplinarne podejście, czerpiące z dorobku prawa, socjologii, kryminologii i nauk o zarządzaniu. Analiza opiera się na założeniu, że istotę bezpieczeństwa stanowi proces nieliniowy i dynamiczny, stale negocjujący granice ryzyka.

Słowa kluczowe

Bezpieczeństwo, zagrożenia hybrydowe, resocjalizacja, prawa człowieka, penitencjarystyka

Recenzenci

Dr hab. Samanta Kowalska, Uniwersytet Kaliski

Dr Jarosław Rychlik, Uniwersytet Opolski

Por. dr inż. Iwona Szkudlarek, Karkonoska Akademia Nauk Stosowanych

© Copyright by Redaktorzy i Autorzy wystąpień

Wydawnictwo Naukowe Kontekst, Poznań 2026

ISBN 978-83-68332-24-7

Druk

Zakład Poligraficzny Moś & Łuczak, Poznań

Wydawca

Wydawnictwo Naukowe Kontekst

www.wkn.com.pl

kontekst2@o2.pl

 **Kontekst**
Wydawnictwo

WYDAWNICTWO NAUKOWE

Spis treści

Wprowadzenie	6
Wstęp	7

CZĘŚĆ I.

Nowe oblicza bezpieczeństwa publicznego w erze globalizacji

Wojciech KONWERSKI: Problematyka ochrony informacji niejawnych na gruncie prawa krajowego	9
Agata DYBIOCH: Rola rejonowej straży miejskiej w zapewnieniu bezpieczeństwa przestrzeni publicznej	27
Ewelina Patrycja ZIELIŃSKA: Nowoczesne technologie i strategie w zwalczaniu przestępczości zorganizowanej oraz cyberprzestępczości. Wykorzystanie i ochrona danych publicznych	43
Daniel MATWIEJCZUK: Uwarunkowania prawne monitoringu przestrzeni publicznej	61
Alicja ZAWORSKA: Bezpieczeństwo w cyberprzestrzeni: Nowe technologie a cyberprzestępczość	83
Patryk MANOWIECKI: Cyberprzestępczość – rodzaje, zapobieganie, zwalczanie	97

CZĘŚĆ II.

Bezpieczeństwo penitencjarne w ujęciu holistycznym

Angelika MARUSZEWSKA: Warunki życia osadzonych a bezpieczeństwo jednostek penitencjarnych	115
Sebastian KĄKOL: Prawo osób osadzonych w zakładach karnych do praktykowania wiary zgodnie z normami prawa kanonicznego, wyznaniowego i konstytucyjnego oraz wpływ praktyk religijnych na resocjalizację osadzonych	129
Adrianna IWAŃSKA: Zagrożenia wynikające z konwojowania osadzonych a bezpieczeństwo funkcjonariuszy i osób postronnych	143
Anna PŁOMIŃSKA: Alternatywny system wykonywania kary pozbawienia wolności	157
Kornelia BREJDAK: Multidyscyplinarna rola psów służbowych w kontekście działań antyterrorystycznych w wybranych służbach mundurowych	173
Tomasz STRZYŻ: Zasadność stosowania środków przymusu bezpośredniego przez funkcjonariuszy Służby Więziennej podczas konwojowania osób pozbawionych wolności	185
Podsumowanie	203
Streszczenie	205
Summary	207

Wprowadzenie

Z wielką radością oddajemy w ręce Szanownych Czytelników monografię naukową pod tytułem „Wymiar bezpieczeństwa w XXI wieku: integracja perspektyw w kontekście współczesnych zagrożeń”. Publikacja ta składa się z dwóch, wielce interesujących w mojej opinii, autonomicznych, aczkolwiek uzupełniających się, części. Pierwsza z nich zatytułowana została „Nowe oblicza bezpieczeństwa publicznego w erze globalizacji”, z kolei część druga nosi nazwę: „Bezpieczeństwo penitencjarne w ujęciu holistycznym”.

Celem publikacji była konsolidacja perspektyw oraz stworzenie zbioru artykułów, w których Autorzy podjąć się mieli badań nad różnymi aspektami bezpieczeństwa w kontekście wyzwań współczesnego świata. Interdyscyplinarne podejście do problematyki doprowadziło Badaczy do interesujących wniosków. Uważam, że cel udało się zrealizować, a Czytelnika czeka ciekawa lektura.

Pragnę wyrazić nadzieję, że niniejsza monografia okaże się przydatna zarówno teoretykom, ale i praktykom związanym z naukami o bezpieczeństwie, naukami prawnymi, penitencjarystyką oraz innym. Krąg odbiorców jest więc szeroki. Szczęśliwy bym był, gdyby owa publikacja trafiła nie tylko do „obrotu naukowego”, ale również do domów. Tak, aby wartości w niej zawarte, mogły zainteresować każdego, kto poszukuje wiedzy związanej z omawianą problematyką.

Wielkim zaszczytem jest, że poproszono mnie, aby to również pod moim naukowym patronatem, publikacja przedmiotowa została wydana. To honor, ale

i odpowiedzialność, jednakże efekt końcowy cieszy i napawa dumą. W tym miejscu pragnę szczerze podziękować oraz pogratulować wszystkim Autorom, którzy napisali ciekawe artykuły. Taka inicjatywa, ambicja oraz pracowitość na rzecz nauki są godne pochwały. Z radością odnotowuję, że artykuły te zawierają w sobie pierwiastek praw człowieka. Praw człowieka, które są moim naukowym życiem i pasją. Gałęzi prawa, która działając w duchu poszanowania praworządności, pokoju, tolerancji, ma na celu sprawianie, aby świat stawał się lepszym.

dr Adrian Pachciarz

Wstęp

Pojęcie bezpieczeństwa, pomimo swej pozornej oczywistości, pozostaje jedną z najbardziej złożonych i dynamicznych kategorii współczesnych nauk społecznych. Jego istota nie sprowadza się już wyłącznie do ochrony przed zewnętrznymi zagrożeniami, definiowanymi w tradycyjnym, westfalskim paradygmacie, lecz obejmuje także aspekt pozytywny: tworzenie trwałych warunków umożliwiających jednostkom i wspólnotom nieskrępowany rozwój, stabilność oraz poczucie ładu. W tym sensie bezpieczeństwo jawi się nie tylko jako stan, lecz przede wszystkim jako proces – nieliniowy i dynamiczny, stale negocjujący granice ryzyka.

Ewolucja ta doprowadziła do przesunięcia punktu ciężkości z bezpieczeństwa państwa na bezpieczeństwo podmiotowe, które za swój ostateczny cel uznaje „wolność od strachu i niedostatku” dla każdego człowieka, która odnosi się do zagrożeń bezpośrednich, takich jak konflikty zbrojne, przemoc, terroryzm i przestępczość, kwestie socjoekonomiczne i strukturalne. Zatem bezpieczeństwo jest osiąganym wtedy, gdy zabezpieczone są podstawowe prawa człowieka, a nie tylko integralność terytorialna państwa. Ten holistyczny wymiar natury bezpieczeństwa wymaga ścisłej integracji wiedzy z różnych dyscyplin. Współczesna nauka o bezpieczeństwie musi zatem badać wzajemne oddziaływanie tych płaszczyzn, ponieważ naruszenie stabilności w jednym sektorze natychmiast przekłada się na zagrożenia w innym. Ta wielowymiarowość jest kluczowa dla zrozumienia dynamiki współczesnych zagrożeń. Interdyscyplinarność w badaniach – czerpiąca

z prawa, socjologii, kryminologii i nauk o zarządzaniu – staje się więc koniecznością, pozwalającą na skuteczną diagnozę złożonych, często hybrydowych źródeł niestabilności.

W dobie płynnej nowoczesności wyzwaniem jest nie tylko obiektywna ocena zagrożeń, ale także sam proces ich definiowania. Koncepcja sekurytyzacji dowodzi, że to, co uznajemy za problem bezpieczeństwa, często jest wynikiem aktu mowy i konsensusu politycznego. Jednocześnie zmagamy się z zagrożeniami asymetrycznymi oraz nowymi formami konfrontacji, takimi jak wojna hybrydowa, która celowo zaciera granice między czasem pokoju a konfliktu, wykorzystując dezinformację, ataki w cyberprzestrzeni i presję ekonomiczną. W tle tych działań utrzymuje się wysoki poziom lęku społecznego, wynikający z poczucia niekontrolowanego ryzyka i niemożności przewidzenia kolejnych „Czarnych Łabędzi”.

Niniejsza monografia – „Wymiar bezpieczeństwa w XXI wieku: integracja perspektyw w kontekście współczesnych zagrożeń” – wpisuje się w potrzebę interdyscyplinarnego namysłu nad tą złożonością. Część pierwsza koncentruje się na strategii neutralizacji tych globalnych i transgranicznych wyzwań, analizując konieczność wzmocnienia odporności społecznej wobec zmian technologicznych i geopolitycznych. Natomiast część druga akcentuje humanistyczny wymiar bezpieczeństwa, ujmując system wykonywania kar nie tylko jako narzędzie ochrony społeczeństwa, lecz przede wszystkim jako przestrzeń realizacji godności człowieka. Kluczowa teza tej części brzmi: stabilność i bezpieczeństwo społeczne może zostać osiągnięte jedynie poprzez skuteczną resocjalizację, gdzie zabezpieczenie zewnętrzne jest nierozdzielnie związane z interioryzacją norm przez jednostkę.

Wierzę, że publikacja ta wzbogaci dorobek nauk o bezpieczeństwie i stanie się inspiracją do poszukiwania równowagi między porządkiem a wolnością, między ochroną a zaufaniem. Właśnie w tej delikatnej równowadze – pomiędzy obiektywną potrzebą ochrony a subiektywnym poczuciem bezpieczeństwa – tkwi istota i największe wyzwanie współczesnych systemów bezpieczeństwa.

mgr Daniel Nowakowski

Część I.

Nowe oblicza
bezpieczeństwa
publicznego
w erze globalizacji

Problematyka ochrony informacji niejawnych na gruncie prawa krajowego

Wojciech KONWERSKI¹

Akademia Wymiaru Sprawiedliwości w Warszawie

ORCID: 0009-0001-6594-2766

Streszczenie. Kilukrotnie nowelizowana Ustawa o ochronie informacji niejawnych w dalszym ciągu budzi wątpliwości wśród gremium prawniczego. Ich usunięcie wymagałoby korekt oraz doprecyzowania przepisów w celu zwiększenia przejrzystości procedur oraz zapewnienia lepszej ochrony informacji niejawnych. W praktyce stosowania ustawy pojawiają się trudności, które wpływają na efektywność systemu ochrony informacji oraz poziom ochrony danych niejawnych. Wśród głównych problemów można wskazać niejasności w interpretacji przepisów, prowadzące do niejednolitości procedur w różnych instytucjach, nadmierną arbitralność w procedurze nadawania klauzul tajności oraz zbyt niskie sankcje za naruszenie przepisów o ochronie informacji, co przekłada się na spadek skuteczności systemu ochrony. Doprecyzowanie oraz skorygowanie niektórych zapisów ustawy poskutkowałoby większym zabezpieczeniem tajemnic państwowych, a w efekcie wzrostem bezpieczeństwa państwa.

Słowa kluczowe: informacje niejawne, bezpieczeństwo, ochrona informacji, bezpieczeństwo publiczne

Wstęp

Ochrona informacji niejawnych stanowi istotny element bezpieczeństwa narodowego każdego państwa. Zapewnienie bezpieczeństwa danych, zarówno na poziomie krajowym, jak i międzynarodowym, zyskuje coraz większe znaczenie

¹ Wojciech Konwerski – student IV roku na kierunku Prawo, Akademia Wymiaru Sprawiedliwości w Warszawie.

w obliczu rosnącej liczby cyberataków. Informacje niejawne, mające szczególną wartość dla państwa, muszą podlegać należytej ochronie, gdyż ich ujawnienie może wiązać się z poważnymi konsekwencjami, zarówno o charakterze wewnętrznym jak i zewnętrznym, prowadząc do zagrożenia integralności terytorialnej, suwerenności oraz stabilności systemu politycznego. Mimo, iż jawność życia publicznego stanowi podstawę funkcjonowania ustroju demokratycznego i jest istotną gwarancją praworządności, nie ma charakteru absolutnego i musi podlegać pewnym ograniczeniom, ze względu na wyższe dobro, jakim jest chociażby ochrona porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa. Konstytucja Rzeczypospolitej Polskiej w art. 61 ust. 3 wskazuje na istnienie takiej kategorii informacji, które ze względu na swój szczególny charakter i potencjalne niebezpieczeństwo wywołane ich nieuprawnionym ujawnieniem muszą znajdować się pod szczególną ochroną państwa. Istnieją zatem sytuacje, w których sam ustawodawca jest zobligowany do ograniczenia praw obywateli ze względu na interes państwa i jego obywateli. W Polsce, podobnie jak w innych krajach członkowskich NATO i Unii Europejskiej, zasady dotyczące ochrony informacji niejawnych zostały ściśle określone przez ustawodawcę. Podstawowym aktem regulującym tę materię na gruncie prawa polskiego jest Ustawa o ochronie informacji niejawnych z dnia 5 sierpnia 2010 r. (u.o.i.n.). Definiuje ona rodzaje informacji, które wymagają szczególnej ochrony, a także procedury ich zabezpieczenia, przetwarzania oraz dostępu. Kluczowym elementem tego systemu jest podział informacji na cztery klauzule tajności: „ściśle tajne”, „tajne”, „poufne” oraz „zastrzeżone”, co pozwala na precyzyjne dopasowanie środków ochrony do stopnia ryzyka związanego z ich ujawnieniem. Nadzór nad szczelnością tego systemu sprawują wyspecjalizowane służby ochrony państwa – Agencja Bezpieczeństwa Wewnętrznego oraz Służba Kontrwywiadu Wojskowego, pełniące funkcję krajowych władz bezpieczeństwa. Obowiązująca ustawa o ochronie informacji niejawnych była kilkakrotnie nowelizowana, jednak w dalszym ciągu istnieją pewne kwestie, które wymagają korekty oraz doprecyzowania, w celu zwiększenia przejrzystości procedur oraz zapewnienia lepszej ochrony informacji.

Krajowa Władza Bezpieczeństwa

Do celów ochrony informacji niejawnych oraz nadzorowania funkcjonowania systemu ochrony tych informacji zostały powołane następujące komórki: Agencja Bezpieczeństwa Wewnętrznego (ABW) – w odniesieniu do podmiotów cywilnych oraz Służba Kontrwywiadu Wojskowego (SKW) – w odniesieniu do Ministerstwa Obrony Narodowej oraz jednostek organizacyjnych podległych Ministrowi Obro-

ny Narodowej lub przez niego nadzorowanych. Podmioty te zgodnie z ustawą prowadzą kontrolę ochrony informacji niejawnych i przestrzegania przepisów obowiązujących w tym zakresie, realizują zadania w zakresie bezpieczeństwa systemów teleinformatycznych, prowadzą postępowania sprawdzające, kontrolne postępowania sprawdzające oraz postępowania bezpieczeństwa przemysłowego². Ponadto w ramach współpracy międzynarodowej oraz konieczności zapewnienia jednolitego stopnia ochrony informacji niejawnych szef ABW pełni funkcję Krajowej Władzy Bezpieczeństwa zapewniając ochronę informacji niejawnych wymienianych między Rzeczpospolitą Polską a innymi państwami lub organizacjami międzynarodowymi³. Odpowiada również za wdrażanie uzgodnionych zasad i środków ochrony informacji niejawnych. W sferze wojskowej Szef ABW sprawuje swoją funkcję za pośrednictwem Szefa SKW.

Zasady przyznawania dostępu do informacji niejawnych

Ustawa o ochronie informacji niejawnych wprowadza szczegółowe zasady oraz procedury przyznawania dostępu do informacji niejawnych. Jedną z naczelných reguł dotyczących ochrony informacji niejawnych, unormowaną w art. 4 u.o.i.n. jest „zasada ograniczonego dostępu”, zwana również zasadą „*need to know*”, zgodnie z którą dostęp do informacji niejawnych może zostać udzielony wyłącznie osobie dającej rękojmię zachowania tajemnicy oraz w zakresie niezbędnym do pełnienia obowiązków lub służby na danym stanowisku⁴. W myśl przepisów rękojmi to zdolność osoby do spełnienia narzuconych przez ustawę wymogów zapewnienia ochrony informacji niejawnych przed nieuprawnionym ujawnieniem⁵. Co ważne zdolność ta musi zostać stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego. Zakres takiego postępowania zależy od kategorii informacji niejawnych, do których dostęp jest zainteresowanemu niezbędny. Na gruncie obowiązującej ustawy wyróżnia się cztery klauzule informacji niejawnych – „ściśle tajne”, „tajne”, „poufne” oraz „zastrzeżone”. Nadanie konkretnym informacjom poszczególnych klauzul zależy od stopnia potencjalnej szkody, jaka mogłaby powstać w razie ich nieuprawnionego ujawnienia. Osoby ubiegające się o dostęp do informacji niejawnych o klauzuli „tajne”, „ściśle tajne” oraz „poufne”, w związku z pełnionymi obowiązkami muszą przejść tzw.

² Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, art. 10 ust. 1 (t.j. Dz.U. z 2024 r. poz. 632).

³ Ustawa z dnia 5 sierpnia 2010 r. o ochronie..., art. 11 ust. 2.

⁴ Ustawa z dnia 5 sierpnia 2010 r. o ochronie..., art. 4 ust. 1.

⁵ Ustawa z dnia 5 sierpnia 2010 r. o ochronie..., art. 2 pkt 2.

postępowanie sprawdzające, które ma na celu ustalenie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy. Ponadto dodatkowym warunkiem uzyskania dostępu jest odbycie szkolenia w zakresie ochrony informacji niejawnych. Na podstawie ustawy, można wyróżnić dwa rodzaje postępowania sprawdzającego. Zwykle postępowanie sprawdzające, które przeprowadzane jest przez pełnomocnika ds. ochrony informacji niejawnych, na pisemne polecenie kierownika jednostki organizacyjnej⁶, przy stanowiskach i pracach związanych z dostępem do informacji niejawnych o klauzuli „poufne”⁷. Postępowanie to polega na sprawdzeniu w niezbędnym zakresie, w ewidencjach, rejestrach i kartotekach, w szczególności w Krajowym Rejestrze Karnym, danych zawartych w wypełnionej i podpisanej przez osobę sprawdzaną ankiecie, a także sprawdzenie innych informacji uzyskanych w toku postępowania sprawdzającego, w zakresie niezbędnym do ustalenia, czy osoba sprawdzana daje rękojmię zachowania tajemnicy⁸. Drugim rodzajem jest tzw. poszerzone postępowanie sprawdzające. Przeprowadzane jest ono przez ABW lub SKW, na pisemny wniosek kierownika jednostki organizacyjnej lub osoby uprawnionej do obsady stanowiska lub zlecenia prac⁹. Obejmuje ono czynności dokonywane przy zwykłym postępowaniu sprawdzającym, a ponadto, jeżeli jest to konieczne – rozmowę z przełożonymi osoby sprawdzanej oraz z innymi osobami, przeprowadzenie wywiadu w miejscu zamieszkania osoby sprawdzanej oraz sprawdzenie stanu i obrotów na rachunku bankowym oraz zadłużenia osoby sprawdzanej, w szczególności wobec Skarbu Państwa¹⁰. W przypadku osób ubiegających się o uzyskanie dostępu do informacji o klauzuli „ściśle tajne” poszerzone postępowanie sprawdzające obejmuje także (jeżeli jest to konieczne w wyniku uzyskanych wcześniej informacji), rozmowę z trzema osobami wskazanymi przez osobę sprawdzaną w celu uzyskania innych informacji mogących mieć znaczenie dla oceny rękojmi zachowania tajemnicy¹¹. Zwieńczeniem każdego pozytywnie zakończonego postępowania sprawdzającego jest wydanie przez organ prowadzący postępowanie poświadczenia bezpieczeństwa – dokumentu, który oficjalnie stwierdza, że dana osoba spełnia wymogi uzyskania dostępu do informacji niejawnych i daje rękojmię zachowania tajemnicy. Postępowania sprawdzających nie stosuje się w przypadku osób, które otrzymują dostęp do informacji niejawnych z mocy prawa.

⁶ Ustawa z dnia 5 sierpnia 2010 r. o ochronie..., art. 23 ust. 1.

⁷ Ustawa z dnia 5 sierpnia 2010 r. o ochronie..., art. 22 ust. 1 pkt 1.

⁸ Ustawa z dnia 5 sierpnia 2010 r. o ochronie..., art. 25 ust. 1 pkt 1.

⁹ Ustawa z dnia 5 sierpnia 2010 r. o ochronie..., art. 23 ust. 2 pkt 1.

¹⁰ Ustawa z dnia 5 sierpnia 2010 r. o ochronie..., art. 26 ust. 1 pkt 1-3.

¹¹ Ustawa z dnia 5 sierpnia 2010 r. o ochronie..., art. 26 ust. 1 pkt 1.

Kryteria klasyfikacji informacji niejawnych

Ustawa z dnia 5 sierpnia 2010 roku wprowadza podział informacji niejawnych na 4 kategorie oraz wyznacza kryteria, jakimi powinna kierować się przy nadawaniu informacjom klauzuli tajności osoba do tego upoważniona. Na tej podstawie ustawodawca dokonał klasyfikacji informacji niejawnych na zastrzeżone, poufne, tajne oraz ściśle tajne, uzależniając nadanie poszczególnych klauzul od stopnia potencjalnej szkody, jaka mogłaby powstać w razie ich nieuprawnionego ujawnienia. W ujęciu art. 5 u.o.i.n. informacjom niejawnym nadaje się klauzulę:

- „ściśle tajne”, jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej;
- „tajne”, jeżeli ich nieuprawnione ujawnienie spowoduje poważną szkodę dla Rzeczypospolitej Polskiej;
- „poufne”, jeżeli ich nieuprawnione ujawnienie spowoduje szkodę dla Rzeczypospolitej Polskiej;
- „zastrzeżone”, jeżeli nie nadano im wyższej klauzuli tajności, a ich nieuprawnione ujawnienie może mieć szkodliwy wpływ na wykonywanie przez organy władzy publicznej lub inne jednostki organizacyjne zadań w zakresie obrony narodowej, polityki zagranicznej, bezpieczeństwa publicznego, przestrzegania praw i wolności obywateli, wymiaru sprawiedliwości albo interesów Rzeczypospolitej Polskiej.

Ustawa nie definiuje jednak różnicy między szkodą, szkodą poważną i wyjątkowo poważną, pozostawiając wybór osobie nadającej klauzulę. Tego typu prognozowanie wystąpienia konkretnej szkody może mieć charakter stricte abstrakcyjny, a tym samym prowadzić do nadinterpretacji i niejednolitego stosowania prawa¹². Posłużenie się przez ustawodawcę pojęciami niedookreślonymi o charakterze wartościującym może prowadzić do nadinterpretacji przepisów na korzyść dysponenta informacji¹³. W związku z brakiem ustawowej definicji szkody i klasyfikowania różnic między jej rodzajami, a co za tym idzie w pełni uznaniowym nadawaniem klauzul tajności istnieje możliwość utajniania dokumentów lub materiałów, które wcześniej nie zostały opatrzone klauzulą tajności w celu wyłączenia konieczności informowania opinii publicznej o sprawach niewygodnych dla rządzących. Co może budzić istotne zastrzeżenia z punktu widzenia konstytucyjnych praw i wolności jednostki¹⁴. Kryteria podziału informacji są nieostre

¹² M. Leciak, *Prawnokarne aspekty nowej ustawy o ochronie informacji niejawnych*, „Studia Iuridica Toruniensia” 2011/9, s. 198.

¹³ Tamże, s. 205.

¹⁴ Tamże.

i uzależnione wyłącznie od swobodnej oceny osoby nadającej klauzulę tajności, nie zaś od obiektywnych przesłanek. Zatem to osoba upoważniona do podpisania dokumentu będzie każdorazowo, subiektywnie dokonywać klasyfikacji informacji. Może to wiązać się z możliwością nadinterpretacji i różnych decyzji, co do nadawania tym samym kategoriom informacji¹⁵ w różnych podmiotach innych klauzul niejawności. W skrajnych i nieodosobnionych niestety przypadkach, informacje tego samego typu w zależności od organizacji mogą być jawne lub chronione¹⁶. Sytuacja, gdy dane o podobnej treści, wytworzone w dwóch jednostkach, różnią się stopniem ochrony ze względu na opatrzenie ich innymi klauzulami tajności może negatywnie wpływać na bezpieczeństwo państwa. Takie rozwiązanie jest niekorzystne, zarówno z punktu widzenia ochrony praw i wolności jednostki, jak i interesów i bezpieczeństwa samego państwa, skoro stwarza realną możliwość np. nadawania informacjom niższych niż przewidziane klauzul tajności¹⁷. Klauzula tajności determinuje bowiem stopień ochrony informacji – procedurę weryfikacji osób mających do niej dostęp, zasady udzielania dostępu oraz stopień użytych środków bezpieczeństwa fizycznego, w tym parametry urządzeń wykorzystywanych do ochrony. Różnicę w standardach ochrony widać szczególnie między informacjami „zastrzeżonymi”, gdzie minimalny wymóg ochrony stanowi zamknięty na klucz mebel biurowy¹⁸, a informacjami „poufnymi”, gdzie minimalną ochronę ma zapewnić szafa metalowa lub pomieszczenie wzmocnione¹⁹. Ponadto uzyskanie dostępu do informacji „zastrzeżonych” może nastąpić po pisemnym upoważnieniu przez kierownika jednostki organizacyjnej oraz odbyciu szkolenia w zakresie ochrony informacji niejawnych²⁰. Dostęp do informacji „poufnych” natomiast obwarowany jest już koniecznością pomyślnego przejścia procedury zwykłego postępowania sprawdzającego, zakończonego wydaniem poświadczenia bezpieczeństwa oraz odbycia szkolenia w zakresie ochrony informacji niejawnych²¹. Zatem prawidłowe klasyfikowanie informacji jest o tyle ważne, że przesądza o zasadach ochrony. Wyłącznie uznaniowe nadawanie klauzul tajności może prowadzić do sytuacji, gdy dostęp do informacji o takiej samej lub podobnej treści będzie mniej rygorystyczny, a więc zapoznanie się z nimi będzie łatwiejsze. Co za

¹⁵ Tamże, s. 198.

¹⁶ R. Zapała, *Teoria i praktyka ochrony informacji niejawnych – wybrane zagadnienia dotyczące bezpieczeństwa informacji*, „Polityka i Społeczeństwo” 2020/ 3(18), s. 115.

¹⁷ M. Leciak, dz. cyt., s. 198.

¹⁸ Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych §7 ust. 4 (Dz.U. poz. 683 z późn. zm.).

¹⁹ Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa... §7 ust. 3 pkt 2.

²⁰ Ustawa z dnia 5 sierpnia 2010 r. o ochronie..., art. 21 ust. 4 pkt 1 i 2.

²¹ Tamże.

tym idzie będą one gorzej chronione. Pozostając w sferze rozważań dotyczących stopnia ochrony informacji, należy wskazać, że ustawodawca z niedostateczną starannością podszedł do ochrony informacji „zastrzeżonych” traktując je nieco marginalnie, mimo że jest to kategoria informacji niejawnych, których ujawnienie może mieć szkodliwy wpływ na funkcjonowanie administracji publicznej²², skoro przyznanie dostępu do materiałów zastrzeżonych opiera się wyłącznie na opisanej powyżej subiektywnej decyzji kierownika jednostki i jest stosunkowo łatwe w pozyskaniu w porównaniu z innymi typami informacji. W przypadku wyższych stopni tajności, oprócz szkolenia, wymagane jest przejście procedury sprawdzającej zakończonej wydaniem poświadczenia bezpieczeństwa²³, która stanowi formę weryfikacji i daje pewność, że osoba ubiegająca się o dostęp daje rękojmię zachowania tajemnicy. Decyzję o przyznaniu dostępu do klauzuli „zastrzeżone” każdorazowo podejmuje kierownik jednostki. Ustawa nie wprowadza w tym zakresie żadnych obiektywnych przesłanek w postaci konkretnych wytycznych pozostawiając kierownikowi jednostki szeroki zakres decyzyjności. W związku z powyższym należałoby rozważyć wprowadzenie sposobu weryfikacji również dla osób ubiegających się o dostęp do danych o najniższej klauzuli tajności. Zastosowanie obiektywnej przesłanki niekaralności i wymóg sprawdzenia osoby w krajowym rejestrze karnym mogłyby stanowić formę kontroli i przyczynić się do zwiększenia ochrony informacji o klauzuli „zastrzeżone”. Jednocześnie przyznanie dostępu nie opierałoby się wyłącznie na uznaniowości i dałoby pewien stopień pewności, że dana osoba spełnia wymóg ochrony informacji.

Dostęp do informacji niejawnych z mocy prawa

Ustawa z dnia 5 sierpnia 2010 roku przewiduje dość rozbudowane i skomplikowane procedury dotyczące uzyskania dostępu do informacji niejawnych. Jednym z warunków uzyskania dostępu do informacji opatrzonej klauzulą „poufne” i wyższą, jest poddanie się postępowaniu sprawdzającemu, którego celem jest zdeterminowanie, czy osoba sprawdzana daje rękojmię zachowania tajemnicy²⁴. Jednak ustawa w art. 34 ust. 10 wprowadza katalog podmiotów, wobec których nie stosuje się standardowych procedur weryfikacyjnych i odstępuje się od przeprowadzenia postępowania sprawdzającego²⁵, tzn. przyznanie dostępu do informacji niejawnych nie wymaga przeprowadzenia takiego postępowania. Między

²² Ustawa z dnia 5 sierpnia 2010 r. o ochronie..., art. 5 ust. 4.

²³ Ustawa z dnia 5 sierpnia 2010 r. o ochronie..., art. 21.

²⁴ Ustawa z dnia 5 sierpnia 2010 r. o ochronie..., art. 24 ust. 1.

²⁵ Ustawa z dnia 5 sierpnia 2010 r. o ochronie..., art. 34 ust. 1.

innymi dotyczy to Prezydenta, Prezesa Rady Ministrów, ministrów, posłów i senatorów oraz sędziów. Osoby te *ex lege*, z racji zajmowanego stanowiska otrzymują dostęp, do najpilniej strzeżonych tajemnic państwowych bez konieczności przejścia procedury sprawdzającej. Jedynym wymogiem jaki ustawa nakłada na osoby zajmujące wyżej wymienione stanowiska jest zapoznanie się z przepisami dotyczącymi ochrony informacji niejawnych i podpisanie oświadczenia o znajomości tych przepisów²⁶. Z uwagi na fakt, iż wskazanym podmiotom nie wydaje się poświadczenia bezpieczeństwa, pojawiają się wątpliwości i problemy w przypadku naruszenia przepisów o ochronie informacji niejawnych przez te osoby. Ustawa w art. 33 ust. 1 mówi jasno, że w przypadku gdy o osobie, której wydano poświadczenie bezpieczeństwa, zostaną ujawnione nowe informacje wskazujące, że nie daje ona rękojmi zachowania tajemnicy, przeprowadza się kontrolne postępowanie sprawdzające²⁷. A zatem z przepisu wprost wynika, że kontrolne postępowanie sprawdzające można przeprowadzić wyłącznie wobec osoby, która uzyskała poświadczenie bezpieczeństwa. Skoro podmioty wymienione w art. 34 ust. 10 uzyskują dostęp do informacji niejawnych z mocy prawa i nie jest wobec nich przeprowadzane postępowanie sprawdzające, zakończone wydaniem poświadczenia bezpieczeństwa, nie można przeprowadzić wobec nich kontrolnego postępowania sprawdzającego. *De facto* nie ma żadnych ustawowych mechanizmów kontroli oraz weryfikacji przestrzegania przepisów przez osoby posiadające dostęp do informacji niejawnych z mocy prawa. Ma to istotne konsekwencje w kontekście ochrony informacji i ewentualnego zapobiegania ich nieuprawnionemu ujawnieniu. Katalog osób, które otrzymują dostęp do informacji niejawnych z mocy prawa jest dość rozbudowany i obejmuje wiele stanowisk, których objęcie wiąże się z przyznaniem dostępu do informacji bez konieczności przejścia postępowania sprawdzającego. Wszystkie te podmioty otrzymują dostęp do danych objętych najwyższymi klauzulami tajności. Należałoby zastanowić się nad zmniejszeniem tego katalogu osób i instytucji w celu minimalizacji ryzyka nieuprawnionego dostępu i wycieków, a co za tym idzie zwiększenia bezpieczeństwa danych. Im węższa lista podmiotów z dostępem z mocy prawa do informacji niejawnych tym łatwiej zapobiegać ewentualnemu nieumyślnemu ujawnieniu i zachować wyższy poziom ochrony informacji. Jednocześnie w przypadku niektórych podmiotów warto zastanowić się nad zawężeniem poziomu dostępu, *ex lege* z klauzuli „ściśle tajne” lub „tajne” pozostawiając zakres dostępu jedynie do informacji o klauzuli „poufne”. Zmniejszenie zakresu dostępu pozwoliłoby na dalszą realizację codziennych zadań i miałyby korzystny wpływ na ochronę informacji. Dostęp do klauzuli „poufne”

²⁶ Tamże.

²⁷ Ustawa z dnia 5 sierpnia 2010 r. o ochronie..., art. 33 ust. 1.

wymaga jedynie zwykłego postępowania sprawdzającego, a w przypadku dostępu do informacji „tajnych” i „ściśle tajnych” wymagane jest przejście poszerzonego postępowania sprawdzającego. Zatem ustawodawca zdecydowanie zróżnicował stopień ochrony interesu informacji niejawnych „tajnych” i „ściśle tajnych” wprowadzając wyższy wymóg postępowania poszerzonego. Poszerzone postępowanie sprawdzające przeprowadzane jest przez profesjonalne podmioty powołane do ochrony informacji niejawnych jak Agencja Bezpieczeństwa Wewnętrznego czy Służba Kontrwywiadu Wojskowego i gwarantuje, że osoba sprawdzana daje rękojmię zachowania tajemnicy, a zatem szczególnie w przypadku wyższych stanowisk nie powinno się go zastępować dostępem z mocy prawa. Wiele podmiotów byłoby w stanie funkcjonować i wykonywać swoje codzienne obowiązki posiadając dostęp do danych „poufnych” bez konieczności dostępu do najbardziej wrażliwych informacji. Zmniejszenie zakresu dostępu poprawiłoby przejrzystość oraz bezpieczeństwo a także pozwoliło na bardziej efektywne zarządzanie dostępem do informacji.

Zgoda na jednorazowe udostępnienie informacji niejawnych

Uzyskanie dostępu do informacji niejawnych wiąże się z koniecznością posiadania poświadczenia bezpieczeństwa lub przejścia postępowania sprawdzającego, co ma niezwykle istotne znaczenie dla zapewnienia prawidłowego funkcjonowania systemu ochrony tych informacji. Jednak Ustawa z 5 sierpnia 2010 roku w art. 34 ust. 5 pkt 1 i 2 upoważnia niektóre podmioty, w szczególnie uzasadnionych przypadkach do wyrażenia pisemnej zgody na jednorazowe udostępnienie określonych informacji niejawnych osobie nieposiadającej odpowiedniego poświadczenia bezpieczeństwa oraz udostępnienie informacji niejawnych o klauzuli „tajne” lub „ściśle tajne” osobie, wobec której wszczęto poszerzone postępowanie sprawdzające. Ustawa nie definiuje jednak, co można uznać za szczególnie uzasadniony przypadek. Ponadto, w ustępie siódmym stwierdza, że kopię zgody na udostępnienie informacji niejawnych lub odstąpienie od przeprowadzenia postępowania sprawdzającego przekazuje się odpowiednio do ABW lub SKW²⁸. Ustawa nie określa konkretnego terminu, w jakim należy powiadomić służby o wyrażeniu zgody na jednorazowe udostępnienie informacji, jednak skoro przepis mówi o kopii zgody, należy przypuszczać, że powiadomienie następuje już po udostępnieniu informacji. O ile udostępnienie informacji osobie, wobec której wszczęto

²⁸ Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, art. 34 ust. 7 (Dz.U. z 2024 r. poz. 632).

poszerzone postępowanie sprawdzające stwarza mniejsze zagrożenie, ponieważ znajduje się ona w trakcie procedury weryfikacyjnej, o tyle udostępnienie takich danych osobie nieposiadającej odpowiedniego poświadczenia bezpieczeństwa, która nie przeszła ani nawet nie jest w trakcie procedury sprawdzającej jest problematyczne. Co prawda zapoznanie z informacją następuje w ściśle kontrolowanych warunkach, jednak nie ma pewności, czy osoba zapoznająca się jest zdolna do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem. Nie powinno się udostępniać informacji osobie, która nie została w pełni zweryfikowana przez wyznaczone do tego służby, gdyż określony interes państwa może zostać poważnie zagrożony w drodze tego typu działań. Cała procedura postępowania sprawdzającego ma przecież zweryfikować, czy osoba sprawdzana daje rękojmię zachowania tajemnicy. Już samo nadanie podmiotom niewyspecjalizowanym w ochronie informacji kompetencji do ich udostępniania stanowi zagrożenie. Należy również zwrócić uwagę na fakt, iż kompetencje te nadano podmiotom, które otrzymują dostęp z mocy prawa, a więc same nie zostały sprawdzone w procedurze weryfikacyjnej. Ponadto Agencja Bezpieczeństwa Wewnętrznego lub Służba Kontrwywiadu Wojskowego informowane są dopiero po fakcie, a zatem po wyrażeniu zgody na udostępnienie informacji, co budzi poważne obawy w kontekście zapewnienia skutecznej ochrony informacji niejawnych. Aby uniknąć niejasności i nadużyć związanych z nadinterpretacją pojęcia „szczególnie uzasadniony przypadek”, należałoby zastanowić się nad wprowadzeniem precyzyjnych wytycznych, które pozwolą jednoznacznie ocenić, kiedy możliwe jest jednorazowe udostępnienie informacji niejawnych. Ponadto warto rozważyć wprowadzenie obowiązku konsultacji z Agencją Bezpieczeństwa Wewnętrznego lub Służbą Kontrwywiadu Wojskowego przed wyrażeniem zgody na jednorazowe udostępnienie informacji niejawnych. Zwiększyłoby to efektywność ochrony informacji niejawnych oraz zapewniło lepszą kontrolę nad ich obiegiem.

Zasady szkolenia kierownika kancelarii tajnej

Ustawa o ochronie informacji niejawnych z 2010 roku w art. 42 nakłada na kierownika jednostki organizacyjnej, w której przetwarzane są informacje niejawne o klauzuli „tajne” lub „ściśle tajne” obowiązek utworzenia kancelarii tajnej oraz zatrudnienia jej kierownika. Kierownik kancelarii tajnej jest jedną z kluczowych osób odpowiadających za bezpieczeństwo informacji niejawnych w jednostce organizacyjnej. Zgodnie z rozporządzeniem, osoba zatrudniona na tym stanowisku odpowiedzialna jest między innymi za bezpośredni nadzór nad obie-

giem materiałów, udostępnianie materiałów osobom do tego uprawnionym, wydawanie materiałów osobom do tego uprawnionym, które zapewniają odpowiednie warunki do ich przechowywania, egzekwowanie zwrotu materiałów, kontrola przestrzegania właściwego oznaczania i rejestrowania materiałów w kancelarii oraz jednostce organizacyjnej, nadzór nad pracą oddziałów kancelarii²⁹. Kierownik kancelarii zatem odpowiada za organizację pracy kancelarii tajnej i zapewnienie fizycznej kontroli obiegu informacji oraz ich ochrony. Działanie kancelarii jest docelowo ukierunkowane na właściwe sposoby operacji dokonywane na informacjach niejawnych. Podsumowując: jest to bezpieczne rejestrowanie, wydawanie oraz przechowywanie materiałów³⁰. *De facto*, kierownik kancelarii ma największą styczność ze wszystkimi materiałami i dokumentami objętymi klauzulą tajności przetwarzanymi w danej jednostce organizacyjnej. Kierownik kancelarii, jak każdy pracownik posiadający dostęp do danych niejawnych, powinien przejść szkolenie w zakresie ochrony tych informacji. Zasadnym jest, aby w związku z pełnieniem tak odpowiedzialnej funkcji jaką jest stanowisko kierownika kancelarii tajnej, ustawa nakładała obowiązek przeszkolenia przez ABW lub SKW, tymczasem zgodnie z art. 19 ust. 2 pkt 3 szkolenie w zakresie ochrony informacji niejawnych dla szefa kancelarii przeprowadza jedynie pełnomocnik ochrony. Kierownik kancelarii tajnej w największym stopniu ma styczność z informacjami niejawnymi, ponieważ odpowiada za zapewnienie ich fizycznej ochrony oraz ewidencji, dlatego szkolenie przeprowadzone jedynie przez pełnomocnika ochrony może budzić zastrzeżenia. Pamiętać należy, iż pełnomocnik ochrony jest w stosunku do Agencji Bezpieczeństwa Wewnętrznego oraz Służby Kontrwywiadu Wojskowego jedynie wtórnym podmiotem odpowiedzialnym za ochronę informacji, ponieważ pełni funkcję wykonawczą polityki i procedur wyznaczonych przez te pierwsze. ABW oraz SKW pełnią nadrzędne funkcje nadzorcze i kontrolne w zakresie ochrony informacji niejawnych, podczas gdy pełnomocnik ds. ochrony informacji niejawnych pełni rolę wykonawczą na poziomie danej jednostki organizacyjnej, odpowiadając jedynie za zapewnienie stosowania przepisów oraz wdrożenie procedur. W związku z tym wydaje się, iż bardziej odpowiednio byłoby przeszkolenie kierownika kancelarii przez służby, co minimalizowałoby ryzyko błędów i luk w procedurach.

²⁹ Rozporządzenie Rady Ministrów z dnia 7 grudnia 2011 r. w sprawie organizacji i funkcjonowania kancelarii tajnych oraz sposobu i trybu przetwarzania informacji niejawnych, par. 4, (t.j. Dz.U. z 2017 r., poz. 1558).

³⁰ P. Budzyń, *Ochrona informacji niejawnych w świetle krajowych aktów prawnych*, „Bezpieczeństwo. Teoria i Praktyka” 2015/3, s. 19.

Sankcje za naruszenie przepisów o ochronie informacji niejawnych

Istotny element systemu ochrony informacji niejawnych stanowią sankcje przewidziane za naruszenie przepisów obowiązujących w tym zakresie. Kwestie odpowiedzialności karnej za pogwałcenie ustawy zostały określone w art. 265 oraz art. 266 § 2 Kodeksu Karnego. Zgodnie z art. 265 „Kto ujawnia lub wbrew przepisom ustawy wykorzystuje informacje niejawne o klauzuli „tajne” lub „ściśle tajne”, podlega karze pozbawienia wolności od 3 miesięcy do lat 5³¹, natomiast jeżeli informację „ujawniono osobie działającej w imieniu lub na rzecz podmiotu zagranicznego, sprawca podlega karze pozbawienia wolności od 6 miesięcy do lat 8”³². Ustawodawca zakwalifikował więc ujawnienie informacji niejawnych o klauzulach „ściśle tajne” oraz „tajne” jako występki, nie zaś jako zbrodnie. Jest to niezrozumiałe z uwagi na fakt potencjalnej szkody oraz zagrożenia mogącego wynikać z nieuprawnionego ujawnienia tych informacji. Informacjom niejawnym nadaje się klauzulę „ściśle tajne”, jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że zagrozi niepodległości, suwerenności, integralności terytorialnej, bezpieczeństwu wewnętrznemu, porządkowi konstytucyjnemu, sojuszom, pozycji międzynarodowej lub osłabi gotowość obronną RP³³. Na gruncie zasad klasyfikacji konkretnych informacji i nadawania im klauzul tajności, minimalna kara za ujawnienie wynosząca 3 miesiące oraz 6 miesięcy w przypadku działania na rzecz podmiotu zagranicznego wydaje się co najmniej niedostateczna. Należałoby zastanowić się nad zwiększeniem wymiaru kary i zakwalifikowaniu przestępstwa ujawnienia informacji jako zbrodni. Ponadto konstrukcja przepisów ustawy uzależnia objęcie sankcją działania polegającego na ujawnieniu informacji od konieczności opatrzenia jej klauzulą tajności. Przyjęte bowiem założenie, że przestępstwem z art. 265 k.k. lub art. 266 § 2 k.k. jest ujawnienie wyłącznie takiej informacji, którą opatrzone jedną z klauzul tajności, prowadzi do wniosku, iż nie dojdzie do realizacji znamion tych przestępstw w sytuacji, w której urzędnik doprowadza do ujawnienia poufnej informacji niezaopatrzonej w taki gryf, np. gdy bezprawnie odmawia jego nadania³⁴. W myśl kodeksu, karze podlega bowiem jedynie osoba, która ujawnia lub wykorzystuje informacje niejawne o określonej klauzuli. Zatem w sytuacji, gdy

³¹ Ustawa z dnia 6 czerwca 1997 r. Kodeks karny art. 265 §1, (t.j. Dz.U. z 2024 r. poz. 17 z późn. zm.).

³² Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, art. 265 §2.

³³ Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, art. 5 ust. 1, (t.j. Dz.U. z 2024 r., poz. 632).

³⁴ M. Leciak, *Prawnokarne aspekty nowej ustawy o ochronie informacji niejawnych*, „Studia Iuridica Toruniensia” 2011/9, s. 206.

informacji nie nadano jeszcze atrybutu tajności, nie korzysta ona z przywileju ochrony na gruncie prawa karnego, co w gruncie rzeczy prowadzi do ograniczenia możliwości ścigania sprawców zachowań skierowanych przeciwko poufności informacji niejawnych³⁵. Jest to wysoce niepożądane, ponieważ prowadzi do trudności w stosowaniu przedmiotowych przepisów oraz osłabienia systemu ochrony informacji niejawnych.

Podsumowanie

Obowiązująca ustawa o ochronie informacji niejawnych była kilkukrotnie nowelizowana, jednak w dalszym ciągu istnieją pewne kwestie, które wymagałyby korekt oraz doprecyzowania w celu zwiększenia przejrzystości procedur oraz zapewnienia lepszej ochrony informacji. Brak jasnych kryteriów klasyfikacji informacji może mieć negatywne skutki na gruncie ochrony informacji i prowadzić do rozbieżności w standardach ochrony. Ponadto wyłącznie uznaniowe nadawanie klauzul może wiązać się z nadużyciami, ze strony rządzących i w efekcie prowadzić do ograniczania konstytucyjnych praw i wolności obywateli, a w szczególności prawa do informacji. Zbyt szeroki katalog stanowisk wiążących się z dostępem do informacji niejawnych z mocy prawa oraz brak mechanizmów pozwalających na weryfikację oraz kontrolę tych podmiotów może budzić kontrowersje. Ponadto uznaniowe prawo do jednorazowego udostępnienia informacji osobom niedającym rękojmi zachowania tajemnicy oraz fakt, iż służby odpowiedzialne za ochronę informacji informowane są po udzieleniu takiego zezwolenia może stwarzać zagrożenie dla interesu państwa oraz utrudniać kontrolę dostępu do tajemnic państwowych. Wreszcie niskie sankcje przewidziane za naruszenie przepisów o ochronie informacji niejawnych oraz uzależnienie objęcia karą przestępstwa przeciwko informacjom od nadania klauzuli tajności może prowadzić do ograniczenia możliwości ścigania sprawców. Mając na uwadze fakt, że w obecnym świecie informacja zyskuje coraz większe znaczenie i staje się pożądanym towarem³⁶, należałoby rozważyć doprecyzowanie obowiązującej ustawy o ochronie informacji niejawnych oraz wprowadzenie korekt w celu zapewnienia lepszej ochrony informacji oraz zwiększenia przejrzystości procedur.

³⁵ M. Leciak, dz. cyt., s. 205.

³⁶ I. Szkudlarek, *Rola środków masowego przekazu w wojnach i konfliktach zbrojnych na wybranych przykładach*, [w]: J. Lasota, M. Palczewska (red. nauk.), *Polemologia: wielowymiarowość wojny i konfliktu zbrojnego*, Akademia Sztuki Wojennej, Warszawa 2017.

Bibliografia

- Budzyń P., *Ochrona informacji niejawnych w świetle krajowych aktów prawnych*, „Bezpieczeństwo. Teoria i Praktyka” 2015/3.
- Leciak M., *Prawnokarne aspekty nowej ustawy o ochronie informacji niejawnych*, „Studia Iuridica Toruniensia” 2011/9.
- Szkudlarek I., *Rola środków masowego przekazu w wojnach i konfliktach zbrojnych na wybranych przykładach*, [w:] Palczewska M., Lasota J., Animus Belli, *Polemologia: wielowymiarowość wojny i konfliktu zbrojnego*, Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2017.
- Zapała R., *Teoria i praktyka ochrony informacji niejawnych – wybrane zagadnienia dotyczące bezpieczeństwa informacji*, „Polityka i Społeczeństwo” 2020/3(18).
- Rozporządzenie Rady Ministrów z dnia 29 maja 2012 r. w sprawie środków bezpieczeństwa fizycznego stosowanych do zabezpieczania informacji niejawnych (Dz. U. poz. 683 z późn. zm.).
- Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (tj. Dz. U. z 2024 r. poz. 632).
- Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (tj. Dz. U. z 2024 r. poz. 17 z późn. zm.).

Rola rejonowej Straży Miejskiej w zapewnieniu bezpieczeństwa przestrzeni publicznej

Agata DYBIOCH¹

Akademia Wymiaru Sprawiedliwości

ORCID: 0009-0003-2228-784X

Streszczenie. Bezpieczeństwo przestrzeni publicznej ma podstawowe znaczenie dla prawidłowego funkcjonowania społeczeństwa. Jest bowiem jednym z podstawowych filarów rozwoju gospodarczego i społecznego danego obszaru, w tym również miejskiego. Celem niniejszego artykułu jest przedstawienie znaczącej roli funkcjonariuszy do spraw rejonowo-patrolowych Straży Miejskiej na szczeblu lokalnym w kontekście zapewnienia bezpieczeństwa. W artykule opisano działalność i sposoby zapewniania bezpieczeństwa na terenie wybranego miasta. Analiza zdobytych materiałów, pozwoliła uzyskać informacje potwierdzające skuteczność działań Straży Miejskiej. Sprawnie działająca straż miejska może bowiem znacząco wpłynąć na stan poczucia bezpieczeństwa w przestrzeni publicznej.

Słowa kluczowe: straż miejska, bezpieczeństwo, rejonowy, miasto

Wstęp

Bezpieczeństwo jest pojęciem coraz częściej używanym w dzisiejszym życiu. Na przestrzeni lat definicja ulegała zmianie i była ciągle uaktualniana. Wynikać mogło to między innymi z faktu, iż bezpieczeństwo rozumiane przez osoby żyjące w czasach prehistorycznych postrzegane było inaczej niż przez współczesnego obywatela.

¹ Agata Dybioch – Adiunkt w Instytucie Nauk o Zarządzaniu i Jakości Akademii Wymiaru Sprawiedliwości, funkcjonariuszka Straży Miejskiej, zainteresowania badawcze: zarządzanie, bezpieczeństwo, administracja samorządowa.

Bezpieczeństwo przestrzeni publicznej jest obszarem priorytetowym w kontekście prawidłowego funkcjonowania państwa. Zapewnienie bezpieczeństwa w przestrzeni publicznej to zadania realizowane przez większość organów administracji publicznej.

Jednym z podstawowych zadań administracji samorządowej, będącej częścią administracji publicznej, jest ochrona porządku publicznego w zakresie wynikającym z ustaw i prawa miejscowego².

W celu zapewnienia bezpieczeństwa w ujęciu lokalnym rada gminy może utworzyć samorządową umundurowaną formację, zwaną strażą gminną, w przypadku miast strażą miejską. Organem wykonawczym w obu przypadkach jest burmistrz lub prezydent miasta.

W zakresie zadań z zakresu zapewnienia bezpieczeństwa w przestrzeni publicznej wiele samorządów zdecydowało się na utworzenie wyżej wymienionych formacji³.

W ostatnich latach można zauważyć tendencję wzrostową, jeśli chodzi o zapewnienie bezpieczeństwa w bezpośrednim otoczeniu człowieka.

Jak można zauważyć bezpieczeństwo przestrzeni publicznej to tak na prawdę wszystko, co nas otacza. Ponadto są to istotne aspekty, bez których człowiek nie byłby w stanie spokojnie funkcjonować⁴.

Trzeba podkreślić jednak fakt, że instytucje, ministerstwa są po to, żeby tworzyć plany dla służby, które zadbają o to bezpieczeństwo.

Na uwagę zasługuje to, że przez wiele lat bezpieczeństwo było wszelako postrzegane. Jednakże ostatecznie chodziło o to, aby zapewnić spokój i możliwość normalnej egzystencji w aktualnie postrzeganej rzeczywistości⁵.

W gruncie rzeczy wszystko zależy od jednostki i postrzegania przez nią pojęcia *bezpieczeństwo*.

² Leśniak I., *Straż miejska jako determinanta bezpieczeństwa i porządku publicznego*, <https://www.wydawnictwo.edu.pl/pdf-136-82?filename=Straż%20miejska%20jako.pdf> [dostęp: 12.08.2024 r.].

³ B. Bonisławska, *Zadania administracji samorządowej w zakresie bezpieczeństwa i porządku publicznego – wybrane zagadnienia*, <https://journals.umcs.pl/teka/article/view/13644> [dostęp: 01.09.2024 r.].

⁴ S. Krizoskvy, A. Urbanek, D. Zbroszczyk, *Zagrożenia bezpieczeństwa w publicznej przestrzeni*, https://eduka.cjaustawicznadoroslych.eu/images/2018/2/10_2_2018.pdf [dostęp: 01.09.2024 r.].

⁵ M. Wiśniewska, *Bezpieczeństwo – pojęcie, istota, typologia*, https://www.researchgate.net/publication/31412_9234_Bezpieczenstwo_-_pojecie_istota_typologia [dostęp: 01.09.2024 r.].

Działalność straży miejskich (gminnych) w świetle przepisów prawa

Dbanie o bezpieczeństwo i jego zapewnienie to podstawowe zadanie państwa według najważniejszego dokumentu w Polsce, którym jest Konstytucja Rzeczypospolitej Polskiej. Odpowiedzialność za wykonywanie tych działań spoczywa na wielu służbach, państwowych oraz prywatnych. Wraz z kolejnymi latami tworzą się nowe zagrożenia i potrzeba przygotowania⁶ się na ochronę przed nimi jest bardzo ważna. Stworzenie wspólnego systemu i reakcji powiązanych między instytucjami i służbami przyczyni się na pewno do powiększenia odczuwalnego bezpieczeństwa, ale także do lepszego życia obywateli.

Jedną z najważniejszych instytucji samorządowych dbających o bezpieczeństwo na danym terenie jest Straż Gminna (Miejska), w którą w 1997 r. przeistoczyła się Policja Muncypalna. Jest to samorządowa, umundurowana formacja służąca zapewnieniu bezpieczeństwa i porządku publicznego w granicach swoich gmin lub miast. Bardzo istotnym walorem straży miejskich (gminnych) jest szczególna znajomość potrzeb występujących na danym terenie, mieszkańców oraz sytuacji mogących stanowić zagrożenie dla bezpieczeństwa i porządku⁷.

„Zasadniczym aktem prawnym regulującym działalność straży miejskich (gminnych) w Polsce jest ustawa z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U. z 1997 r. Nr 123, poz. 779 ze zm.). Straż miejską (gminną) powołuje rada miasta. Utworzenie tej jednostki organizacyjnej gminy jest prawem, a nie obowiązkiem rady gminy, do której też należy wyłączna kompetencja w podjęciu takiej decyzji”⁸. „Bezpośredni nadzór ogólny nad działalnością tej formacji sprawuje organ wykonawczy miasta (gminy), a mianowicie prezydent (burmistrz, wójt), natomiast nadzór fachowy nad strażami miejskimi (gminnymi) sprawowany jest przez właściwego terytorialnie komendanta wojewódzkiego Policji”⁹. „Zakres tego nadzoru określa Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 12 sierpnia 2004 r. w sprawie zakresu i sposobu współpracy

⁶ Zob. I. Szkudlarek, *Zarys ewolucji koncepcji bezpieczeństwa narodowego Rzeczypospolitej w latach 1999-2014* [w:] S. Krysiński, A. Wikarczyk, J. Żylińska (red. nauk.), *Nauki społeczne w dobie innowacji*, Instytut Wydawniczy EuroPrawo, Warszawa 2019, s. 320-327.

⁷ I. Leśniak, *Straż miejska jako determinanta bezpieczeństwa i porządku publicznego*, <https://www.wydawnictwo.edu.pl/pdf-1-6202?filename=Straz%20miejska%20jako.pdf> [dostęp: 01.09.2024 r.].

⁸ J. Bodio, G. Borkowski, T. Demendecki, *Ustrój organów ochrony prawnej*, Oficyna Wolters Kluwer Polska Sp. z o.o., Warszawa 2007, s. 266.

⁹ B. Szmulik, M. Żmigrodzki, *Ustrój organów ochrony prawnej*, Wyd. Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2005, s. 547.

Policji ze Strażami Gminnymi oraz zakresu sprawowania przez Komendanta Głównego Policji nadzoru nad działalnością straży”¹⁰.

„W art. 11 ustawy o strażach gminnych ustawodawca określił otwarty katalog typowych zadań realizowanych przez strażę, do zadań których należy w szczególności”:¹¹

- „ochrona spokoju i porządku w miejscach publicznych;
- czuwanie nad porządkiem i kontrola ruchu drogowego w zakresie określonym w przepisach o ruchu drogowym;
- współdziałanie z właściwymi podmiotami w zakresie ratowania życia i zdrowia obywateli, pomocy w usuwaniu awarii technicznych i skutków klęsk żywiołowych oraz innych miejscowych zagrożeń;
- zabezpieczenie miejsca przestępstwa, katastrofy lub innego podobnego zdarzenia albo miejsc zagrożonych takim zdarzeniem przed dostępem osób postronnych lub zniszczeniem śladów i dowodów, do momentu przybycia właściwych służb, a także ustalenie, w miarę możliwości, świadków zdarzenia;
- ochrona obiektów komunalnych i urządzeń użyteczności publicznej;
- współdziałanie z organizatorami i innymi służbami w ochronie porządku podczas zgromadzeń i imprez publicznych;
- doprowadzanie osób nietrzeźwych do izby wytrzeźwień lub miejsca ich zamieszkania, jeżeli osoby te zachowaniem swoim dają powód do zgorzienia w miejscu publicznym, znajdują się w okolicznościach zagrażających ich życiu lub zdrowiu albo zagrażają życiu i zdrowiu innych osób;
- informowanie społeczności lokalnej o stanie i rodzajach zagrożeń, a także inicjowanie i uczestnictwo w działaniach mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz zjawiskom kryminogennym i współdziałanie w tym zakresie z organami państwowymi, samorządowymi i organizacjami społecznymi;
- konwojowanie dokumentów, przedmiotów wartościowych lub wartości pieniężnych dla potrzeb gminy”¹².

„Warto zauważyć, że spośród dziewięciu wyszczególnionych przez ustawodawcę głównych zadań straży miejskich (gminnych), aż siedem odnosi się do

¹⁰ A. Babiński, P. Bogdalski, *Policja w strukturach administracji publicznej*, Wydział Wydawnictw i Poligrafii Wyższej Szkoły Policji w Szczytnie, Szczytno 2005, s. 76-77.

¹¹ I. Leśniak, dz. cyt.

¹² Ustawa z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz.U. z 1997, Nr 123, poz. 779).

możliwych form udziału tej jednostki w systemie zapewnienia bezpieczeństwa aglomeracji”¹³.

Funkcje Rejonowego Straży Miejskiej w kontekście zapewnienia bezpieczeństwa przestrzeni publicznej

Istotną rolę w dbaniu o bezpieczeństwo przestrzeni publicznej odgrywają strażnicy do spraw rejonowo-patrolowych. To właśnie oni każdego dnia starają się pomóc lokalnej społeczności przez szereg różnych działań. Strażnikiem – rejonowym jest funkcjonariusz, który został mianowany na to stanowisko i w głównej mierze wykonuje służbę patrolową. Bezpośrednim przełożonym Rejonowego jest jego Kierownik Referatu do spraw rejonowo-patrolowych, którego głównym zadaniem jest sprawowanie nadzoru nad Rejonowymi.

Podstawowe zadania wskazanych funkcjonariuszy to m.in.:

- „prowadzenie rozpoznania przydzielonego mu rejonu służbowego pod kątem naruszeń mających wpływ na stan bezpieczeństwa i porządku publicznego;
- realizowanie zadań z zakresu ścigania sprawców wykroczeń;
- podejmowanie działań o charakterze prewencyjnym, interwencyjnym i ochronnym;
- kontrolowanie przestrzegania prawa powszechnie obowiązującego oraz przepisów prawa miejscowego”¹⁴.

Autorka stwierdza, że od cech rejonowego zależy czy obywatele będą czuli się bezpiecznie w miejscu, w którym mieszkają, pracują, lub funkcjonują w inny sposób. To właśnie funkcjonariusz rejonowy jest osobą, do której mieszkańcy gminy lub miasta zwracają się w każdej sprawie. Dzięki rozmowom, zaangażowaniu, umiejętności słuchania i obserwacji powinien móc wyciągnąć wnioski, udzielić wsparcia mieszkańcowi oraz wychwycić i ujawnić zjawiska, które nie rzucają się od razu w oczy. Należy podkreślić, że wskazany funkcjonariusz jest osobą, która posiada ogromną wiedzę o mieszkańcach, rzeczach, instytucjach, firmach, które prowadzą działalność na jego terenie.

¹³ I. Leśniak, dz. cyt.

¹⁴ §29.1 Zarządzenia nr 5 Komendanta Głównego Policji z dnia 20 czerwca 2016 r. w sprawie metod i form wykonywania zadań przez dzielnicowych i kierownika dzielnicowych, Dz.Urz. KGP, poz. 26.

Na uwagę zasługuje fakt, że każdy z funkcjonariuszy ma przydzielony konkretny rejon służbowy. Wszelkie uwagi i wątpliwości czy też propozycje społeczeństwa mogą być zgłaszane osobiście rejonowemu, telefonicznie na numer służbowy lub na elektroniczną skrzynkę pocztową.

Jak już wcześniej zauważono, ważną rolę odgrywa także rozpoznanie terenowe, gdyż wpływa ono również na poziom bezpieczeństwa lokalnego. Można je podzielić na ogólne, które dotyczy położenia geograficznego, aktywności wszelkiego rodzaju spółdzielni i zakresu ich działalności. Natomiast rozpoznanie szczegółowe dotyczy obiektów będących w zainteresowaniu lokalnej administracji i służb mundurowych w związku z ewentualną przestępczością na tym terenie oraz obiekty wymagające ochrony. Do grupy miejsc, na które rejonowy powinien zwrócić uwagę należą: targowiska – miejsca, gdzie może dochodzić do wszelkiego rodzaju zakłóceń; miejsca gromadzenia się osób, które stwarzają realne zagrożenie dla bezpieczeństwa i porządku publicznego, opuszczone obiekty, infrastruktura krytyczna, przedsiębiorstwa, zakłady pracy, linie komunikacyjne. Na podstawie odpowiedniego i szczegółowego rozpoznania funkcjonariusz do spraw rejonowo-patrolowych może skutecznie oddziaływać na bezpieczeństwo lokalne i współpracować w tym zakresie z innymi służbami i instytucjami. Wskazane działania i odpowiednie zaangażowanie rejonowego wpływa znacząco na stan bezpieczeństwa w danym rejonie i zminimalizowanie pojawiania się zjawisk niepożądanych.

Funkcjonariusz do spraw rejonowo-patrolowych na bieżąco uzyskuje informacje na temat zagrożeń istniejących w jego rejonie służbowym. Stara się również prowadzić rozpoznanie swojego rejonu służbowego pod kątem miejsc, gdzie może dochodzić do gromadzenia się osób zagrażających bezpieczeństwu i porządkowi publicznemu, grupowania się nieletnich, lokalizacji obiektów narażonych na popełnianie wykroczeń i przestępstw.

Odczuwalny i faktyczny poziom bezpieczeństwa w danym rejonie służbowym rejonowego w większości zależy także od współpracy ze społecznością lokalną. Ponadto na stan bezpieczeństwa przestrzeni publicznej składa się także wskazane rozpoznanie osobowe i terenowe prowadzone przez dzielnicowego. „Funkcjonariusz na podstawie otrzymywanych informacji o osobach, ale także aktualnych wskazuje ewentualne osoby, które mogą mieć negatywny wpływ na odczuwalny poziom bezpieczeństwa w danej przestrzeni”¹⁵. Osoby, które w szczególnie sposób mogą zagrażać bezpieczeństwu przestrzeni publicznej. Wielokrotnie zdarza się, że to właśnie wskazane wyżej osoby w głównej mierze oddziałują negatywnie na

¹⁵ W. Deńca, *Rola Dzielnicowego w kształtowaniu bezpieczeństwa społeczności lokalnej*, Security, Economy & Law Nr 2/2019 (XXIII), (24-45), DOI: 10.24356/SEL/23/2.

bezpieczeństwo w danym rejonie. Dlatego tak bardzo ważne jest posiadanie aktualnych informacji odnośnie swojego rejonu służbowego. Pomaga to często w ustaleniu sprawców danego zdarzenia lub osób, które mogą ich znać.

„We współczesnym świecie następuje ciągła dynamika działań zakłócających spokój, bezpieczeństwo i porządek publiczny”¹⁶. Podstawowe zadania, które Rejonowy Straży Miejskiej podejmuje wobec wskazanych osób, to wszelkiego rodzaju rozmowy profilaktyczne, stosowanie środków oddziaływania wychowawczego, pomoc w umieszczeniu osoby w konkretnym ośrodku leczenia uzależnień czy wskazanie drogi, która pomoże uniknąć zagrożeń.

Bezpieczeństwo przestrzeni publicznej w kontekście działań funkcjonariuszy Straży Miejskiej Kalisza – analiza *desk research*

Na potrzeby dopełnienia artykułu w tej części wykorzystano metodę analizy *desk reserach*. Zgodnie z Encyklopedią Zarządzania:

desk research to metoda badawcza polegająca na kompilacji, analizowaniu oraz przetwarzaniu danych i informacji pochodzących z istniejących źródeł, a następnie formułowaniu na ich podstawie wniosków dotyczących badanego problemu. Źródła danych mogą obejmować statystyki, dokumenty urzędowe, wyniki badań społecznych i badania marketingowe. Badania desk research można podzielić na wewnętrzne (wykorzystujące zasoby organizacji) i zewnętrzne (wykorzystujące dane i informacje z Internetu i innych źródeł¹⁷.

Punktem wyjścia przy wprowadzaniu przedsięwzięć mających na celu poprawę stanu bezpieczeństwa w aglomeracjach jest analiza sprawozdań z realizowanych działań. Stąd też Autorka podjęła się przeprowadzenia analizy takiego sprawozdania. Na potrzeby tej części artykułu przeanalizowano sprawozdanie z działalności Straży Miejskiej za rok 2022 i 2023 pod kątem działań funkcjonariuszy do spraw rejonowo-patrolowych. W przeprowadzonej analizie dokumentu udało się uzyskać odpowiedź na pytanie pozwalające dokonać oceny bezpieczeństwa w miejscu zamieszkania, określić jakie czynniki mają decydujący wpływ oraz jakie zjawiska przestępcze i patologiczne najczęściej są zauważane przez funkcjonariuszy do spraw rejonowo-patrolowych.

¹⁶ M. Pomykała, *Bezpieczeństwo wewnętrzne państwa wobec współczesnych zagrożeń*, <https://repozytoriumka.edu.pl/server/api/core/bitstreams/877aeb70-e2b3-46cf-bf8d-4ab8b55d0a7a/content> [dostęp: 01.09.2024 r.].

¹⁷ M. Sygut, *Desk research*, https://mfiles.pl/pl/index.php/Desk_research [dostęp: 24.08.2024 r.].

W Kaliszu władze miasta powołały formację mundurową – funkcjonującą początkowo pod nazwą Policja Muncypalna – w czerwcu 1991 roku. Do 2005 roku muncypalni działali jako wyodrębniona komórka w strukturach Urzędu Miejskiego a następnie jako samodzielna jednostka budżetowa:

Straż Miejska Kalisza działa przede wszystkim na zasadach określonych w Ustawie z dnia 29 sierpnia 1997 r. o strażach gminnych i wykonuje zadania w zakresie ochrony porządku publicznego wynikające z ww. aktu prawnego oraz innych ustaw, rozporządzeń jak również aktów prawa miejscowego¹⁸.

Realizuje nadto inne czynności i zadania określone przez Prezydenta Miasta Kalisza w sprawach, które nie zostały zastrzeżone prawem do wyłącznej kompetencji innych organów administracji rządowej i samorządowej. Straż Miejska Kalisza poprzez wyznaczone jej zadania spełnia wiele funkcji w zakresie utrzymania porządku i bezpieczeństwa publicznego, a są to:

- „funkcja ochronna – utrzymanie porządku na terenie gminy;
- funkcja porządkowa – egzekwowanie przestrzegania przez społeczność lokalną przepisów prawa w zakresie porządku publicznego;
- funkcja prewencyjna – stałe patrołowanie osiedli i ulic oraz reagowanie na zgłaszane potrzeby interwencji w zakresie ochrony porządku publicznego;
- funkcja profilaktyczna – zapobieganie przestępstwom, wykroczeniom i zjawiskom kryminogennym, prowadzenie profilaktyki wychowawczej wśród dzieci i młodzieży;
- funkcja informacyjna – informowanie służb i instytucji o zaobserwowanych zagrożeniach, informowanie społeczności lokalnej o stanie i rodzajach zagrożeń na danym terenie oraz sposobach ich eliminacji;
- funkcja społeczno-administracyjna – współdziałanie w zakresie bezpieczeństwa oraz porządku publicznego z zainteresowanymi organami państwowymi, samorządowymi i organizacjami społecznymi;
- funkcja integrująca społeczność lokalną – udział w imprezach sportowych, kulturalnych, charytatywnych, które są organizowane przez gminę, organizacje społeczne, szkoły”¹⁹.

¹⁸ Statut Straży Miejskiej Kalisza, Załącznik Nr 1 do uchwały Nr XXIV/400/2004 Rady Miejskiej Kalisza z dnia 25 listopada 2004.

¹⁹ B. Kraśniewski, D. Słowikowska, P. Sobiech, A. Zatorska, *Rola i postrzeganie Straży Miejskiej w Toruniu*, file:///C:/Users/MSI/Downloads/31-106-1-PB.pdf [dostęp 25.08.2024 r.].

Wybrane działania Rejonowych Straży Miejskiej w kontekście zapewnienia bezpieczeństwa przestrzeni publicznej

„Na dzień 1 stycznia 2024 roku Straż Miejska Kalisza zatrudniała 45 osób. W swojej strukturze posiada część administracyjną, składającą się z 9 pracowników cywilnych oraz Wydział Prewencji, w którym służy 36 strażników.

W ramach tegoż wydziału wyodrębnione zostały dwa Referaty Rejonowo-Patrolowe oraz Referat Dyżurnych i Wykroczeń wraz z zespołami, zgodnie z niżej przedstawionym schematem.

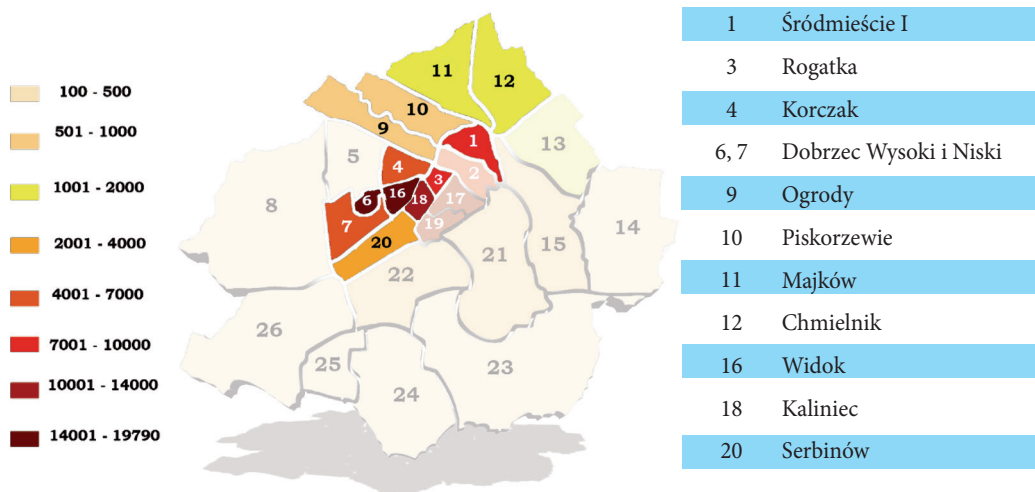


Ryc. 1. Struktura organizacyjna Wydziału Prewencji Straży Miejskiej Kalisza

Źródło: www.sm.kalisz.pl

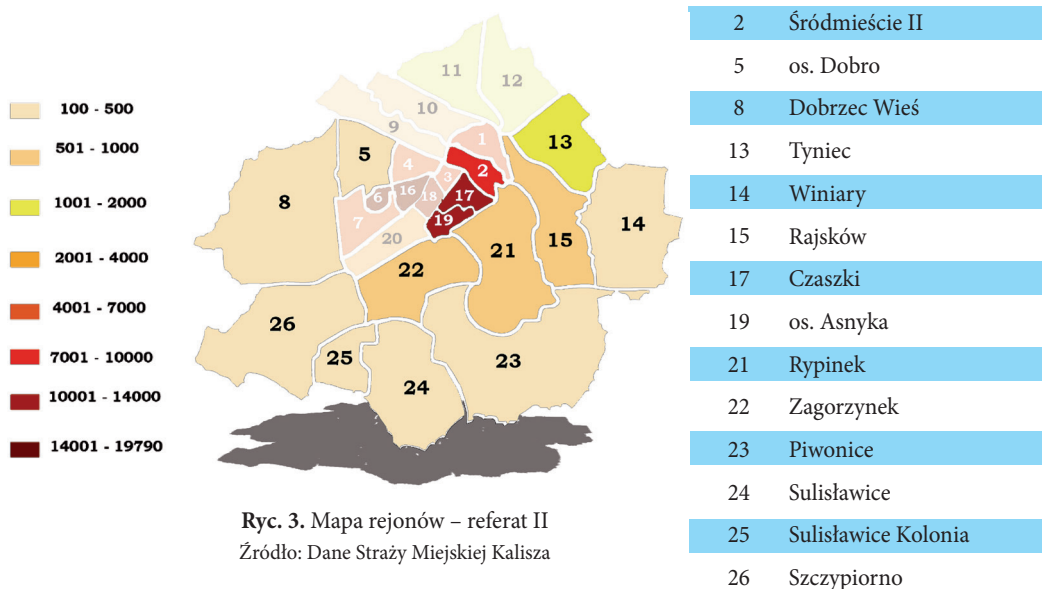
Straż Miejska Kalisza działa wyłącznie na terenie miasta Kalisz, które zajmuje powierzchnię 69,42 km² a jego liczba mieszkańców na początku 2024 roku wynosiła 90.774. W celu zapewnienia prawidłowej organizacji pracy strażników miasto zostało poddane rejonizacji, poprzez wyznaczenie dwóch sektorów przypisanych do poszczególnych referatów rejonowo-patrolowych a następnie przypisanie strażnikom rejonów służbowych, których granice tożsame są z zasięgiem terytorialnym jednostek pomocniczych Miasta Kalisza (23 rady osiedla oraz 3 sołectwa)²⁰.

²⁰ Aktualności, www.sm.kalisz.pl [dostęp 01.09.2024 r.].



Ryc. 2. Mapa rejonów – referat I

Źródło: Dane Straży Miejskiej Kalisza



Ryc. 3. Mapa rejonów – referat II

Źródło: Dane Straży Miejskiej Kalisza

Referaty rejonowo-patrołowe – to dwie odrębne komórki w ramach Wydziału Prewencji, w których służbę na początku 2024 roku łącznie pełniło 23 strażników – 19 rejonowych oraz po 2 w wyspecjalizowanych zespołach ds. profilaktyki i promocji i ds. ochrony środowiska. Ich głównym zadaniem jest codzienne realizowa-

nie służb patrolowych na terenie miasta z uwagą na porządek i bezpieczeństwo publiczne, nieprawidłowe parkowanie jak również uczestniczenie w zabezpieczeniach, wartach i innych wydarzeniach oraz działaniach prewencyjnych i profilaktycznych²¹.

Funkcjonariusze do spraw rejonowo-patrolowych operują na terenie o wysokim stopniu zurbanizowania oraz w przeważającej większości o dużej gęstości zaludnienia. Jest to o tyle istotne, że występuje tutaj oczywista korelacja pomiędzy gęstością zaludnienia a ilością podejmowanych przez strażników interwencji – duże zagęszczenie ludności determinuje wzrost obsługiwanych przez strażników spraw. W rejonach znajdujących się w centrum miasta dominują zdarzenia związane z nieprawidłowym parkowaniem oraz naruszeniem porządku i bezpieczeństwa w miejscach publicznych. Natomiast w rejonach, które znajdują się na jego obrzeżach, przeważają interwencje związane z szeroko rozumianą ochroną środowiska.



Ryc. 4. Akcja usuwania „wraków”

Źródło: www.strazmiejska.kalisz.pl

I Referat Rejonowo-Patrolowy – wyniki działań

W 2023 roku strażnicy z przedmiotowego zespołu zrealizowali 4092 czynności służbowych, które przedstawiają się w sposób następujący:

²¹ Oprac. własne.

Tabela 1. Wyniki działań pracy rejonowych – referat I

Nazwa kategorii	2023 rok
Porządek w komunikacji	2728
Inne zdarzenia wymagające podjęcia interwencji	797
Porządek i bezpieczeństwo w miejscach publicznych	485
Ochrona środowiska i gospodarka odpadami	82
Razem	4092

Źródło: Dane pochodzące ze źródeł SMK

**Ryc. 5.** Wyniki działań pracy rejonowych – referat I

Źródło: Dane pochodzące ze źródeł SMK

II Referat Rejonowo-Patrolowy – wyniki działań

W skład zespołu wchodzi Rejonowi, którym przydzielono przede wszystkim rejony peryferyjne o dużej powierzchni, ale zasiedlone przez relatywnie niewielką liczbę mieszkańców, gdzie dominują interwencje z zakresu ochrony środowiska oraz te związane *sensu stricto* z porządkiem. Odmienny obraz jawi się w przypadku 3 rejonów zlokalizowanych bliżej centrum miasta, gdzie znaczna ilość osób zamieszkuje niewielki obszar. Przeważają tutaj zdarzenia, których charakter zbliżony jest do tych, z którymi mierzą się strażnicy z I Referatu, tj. związane głównie z nieprawidłowym parkowaniem oraz naruszeniem porządku i bezpieczeństwa w miejscach publicznych²².

²² Oprac. własne.

Tabela 2. Wyniki działań pracy rejonowych – referat II

Nazwa kategorii	2023 rok
Porządek w komunikacji	2136
Inne zdarzenia wymagające podjęcia interwencji	1059
Porządek i bezpieczeństwo w miejscach publicznych	524
Ochrona środowiska i gospodarka odpadami	29
Razem	3748

Źródło: Dane pochodzące ze źródeł SMK

**Ryc. 6.** Wyniki działań pracy rejonowych – referat II

Źródło: Dane pochodzące ze źródeł SMK

Diagnoza działań realizowanych przez funkcjonariuszy do spraw rejonowo-patrolowych Straży Miejskiej Kalisza w kontekście bezpieczeństwa przestrzeni publicznej

„76% zrealizowanych w 2023 roku przez kaliskich Rejonowych zadań, związanych było z jakąś formą naruszenia obowiązujących norm prawnych, z czego najwyższy udział mają wykroczenia drogowe. Na kolejne 18% składają się zdarzenia obojętne z punktu widzenia prawa wykroczeń, takie jak konwoje, zabezpieczenia, ochrona obiektów, asysty udzielane innym podmiotom, udział w wartach i sztandarach. Struktura zrealizowanych w 2023 roku przez Rejonowych zadań jest prawidłowa, zarówno z punktu widzenia stawianych wcześniej celów jak i realizacji podstawowej misji, jaką jest stanie na straży ładu prawnego i szeroko rozumianego porządku publicznego. W zestawieniu ujawnionych naruszeń

prawa dominują wykroczenia związane z nieprawidłowym parkowaniem (64%), ale wynika to z obiektywnych względów. Są to przede wszystkim najbardziej powszechne i najczęściej popełniane wykroczenia, co ma również swoje odzwierciedlenie w architekturze zgłoszeń od mieszkańców Kalisza – ponad 39% dotyczy właśnie nieprawidłowego parkowania. Analizując profil zgłoszeń na nr alarmowy 986 widać dużą liczbę interwencji dotyczących wykroczeń przeciwko środowisku (17,2%) – dominują tutaj zdarzenia umownie definiowane jako zadymienie. W bardzo wielu przypadkach takie interwencje nie są potwierdzone: dym wydobywający się z komina jest efektem spalania dozwolonego paliwa; zgłoszenie ma charakter ogólny bez wskazania konkretnego adresu zdarzenia; nie występuje podstawa faktyczna do kontroli (brak oznak zadymienia). W kolejnych latach należy spodziewać się wzrostu tego typu zgłoszeń. Mieszkańcy Kalisza mają bowiem coraz większą świadomość w zakresie właściwych postaw proekologicznych i wykazują się znaczną wrażliwością na tym polu. Prawidłowa ocena wyników pracy Rejonowych za rok 2023 nie byłaby możliwa bez odniesienia się do wcześniejszego równoważnego okresu. W porównaniu z 2022 rokiem odnotowano nieznaczny spadek w łącznie zrealizowanych czynnościach służbowych (-2%). Jest to niewątpliwie związane z fluktuacją kadr. Pogłębiona analiza raportu wskazuje jednak, że w kwestiach najbardziej istotnych z punktu widzenia realizowanych przez Rejonowych zadań, wykazano co najmniej zadowalające rezultaty²³.

Podsumowanie

Istotną rolę, jeśli chodzi o odczuwalny poziom bezpieczeństwa przestrzeni publicznej odgrywa praca funkcjonariuszy do spraw rejonowo-patrolowych, jak i współpraca ze społeczeństwem. Przeprowadzane są analizy i porównania, dzięki czemu można określić stopień bezpieczeństwa. Funkcjonariusze do spraw rejonowo-patrolowych aktywnie zmniejszają ilość czynów zagrażających bezpieczeństwu, porządkowi publicznemu lub życiu²⁴.

Z przeanalizowanych sprawozdań wynika, że funkcjonariusze Straży Miejskiej Kalisza powinni zwrócić szczególną uwagę na zadania takie jak:

- zwiększenie efektywności działań w obszarze współpracy ze społeczeństwem;

²³ Sprawozdanie z działalności Straży Miejskiej Kalisza za rok 2022 i 2023.

²⁴ S. Koziej, *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, file:///C:/Users/MSI/Downloads/Bezpieczenstwo_istota_podstawowe_kategorie_ewolucja%20(1).pdf [dostęp: 01.09.2024 r.].

- podniesienie skuteczności działań funkcjonariuszy w zwalczaniu i identyfikacji największych zagrożeń lokalnych;
- wzrost skuteczności w działaniach skierowanych przeciwko najbardziej uciążliwym społecznie wykroczeniom;
- działania skierowane na podniesienie poziomu bezpieczeństwa na lokalnych drogach;
- zapewnienie optymalnych warunków pełnienia służby strażników miejskich;
- wszelako rozumiana działalność strażników miejskich podczas zabezpieczania imprez masowych.

Jak można zauważyć wskazane wytyczne zawierają podstawowe, ale i bardzo ważne aspekty, które w znaczący sposób oddziałują na jakość wykonywanych działań, jak również na odczuwalny poziom bezpieczeństwa w przestrzeni publicznej.

Wyniki analizy metodą *desk research* pokazują, iż w Kaliszu niezbędna jest formacja dbająca z jednej strony o bezpieczeństwo mieszkańców, a z drugiej strony pilnująca interesów gminy i społeczności lokalnej. Otrzymany wynik badania z pewnością posłuży określaniu kierunków i strategii działań straży miejskich i gminnych w Polsce, mających na celu doskonalenie relacji ze społeczeństwem oraz podnoszenia poziomu poczucia bezpieczeństwa mieszkańców w przestrzeni publicznej.

Bibliografia

- Babiński A., Bogdalski P., *Policja w strukturach administracji publicznej*, Wydział Wydawnictw i Poligrafii Wyższej Szkoły Policji w Szczytnie, Szczytno 2005.
- Bodio J., Borkowski G., Demendecki T., *Ustrój organów ochrony prawnej*, Oficyna Wolters Kluwer Polska Sp. z o.o., Warszawa 2007.
- Boniśławska B., *Zadania administracji samorządowej w zakresie bezpieczeństwa i porządku publicznego – wybrane zagadnienia*, <https://journals.umcs.pl/teka/article/view/13644>
- Deńca W., *Rola Dzielnicowego w kształtowaniu bezpieczeństwa społeczności lokalnej*, Security, Economy & Law Nr 2/2019 (XXIII), (24-45), DOI: 10.24356/SEL/23/2
- Koziej S., *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, file:///C:/Users/MSI/Downloads/Bezpieczenstwo_istota_podstawowe_kategorie_i_historyczna_ewolucja%20(1).pdf
- Krizosky S., Urbanek A., Zbroszczyk D., *Zagrożenia bezpieczeństwa w publicznej przestrzeni*, https://edukacjaustawicznadoroslych.eu/images/2018/2/10_2_2018.pdf

- Leśniak I., *Straż miejska jako determinanta bezpieczeństwa i porządku publicznego*, <https://www.wydawnictwo.wsge.edu.pl/pdf134402?filename=Straz%20miejska%20jako.pdf>
- Pomykała M., *Bezpieczeństwo wewnętrzne państwa wobec współczesnych zagrożeń*, <https://repozytorium.ka.edu.pl/server/api/core/bitstreams/877aeb70-e2b3-46cf-bf8d-4ab8b-55d0a7a/content>
- Statut Straży Miejskiej Kalisza, Załącznik Nr 1 do uchwały Nr XXIV/400/2004 Rady Miejskiej Kalisza z dnia 25 listopada 2004.
- Sygut M., *Desk research*, https://mfiles.pl/pl/index.php/Desk_research
- Szkudlarek I., Zarys ewolucji koncepcji bezpieczeństwa narodowego Rzeczypospolitej w latach 1999-2014 [w:] Krysiński S., Wikarczyk A., Żylińska J. (red. nauk.), *Nauki społeczne w dobie innowacji*, Instytut Wydawniczy EuroPrawo, Warszawa 2019.
- Szmulik B., Żmigrodzki M., *Ustrój organów ochrony prawnej*, Wyd. Uniwersytetu Marii Curie-Skłodowskiej, Lublin 2005.
- Ustawa z dnia 29 sierpnia 1997r. o strażach gminnych (Dz.U. z 1997 Nr 123, poz. 779).
- Wiśniewska M., *Bezpieczeństwo – pojęcie, istota, typologia*, https://www.researchgate.net/publication/314129234_Bezpieczenstwo_-_pojecie_istota_typologia
- Zarządzenie nr 5 Komendanta Głównego Policji z dnia 20 czerwca 2016 w sprawie metod i form wykonywania zadań przez dzielnicowych i kierownika dzielnicowych, Dz. Urz. KGP, poz. 26.

Nowoczesne technologie i strategie w zwalczaniu przestępczości zorganizowanej oraz cyberprzestępczości. Wykorzystanie i ochrona danych publicznych

Ewelina Patrycja ZIELIŃSKA¹

Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego w Warszawie
ORCID: 0009-0006-8590-0738

Streszczenie. Szybki rozwój technologii doprowadził do znacznego wzrostu przestępczości zorganizowanej i cyberprzestępczości, stanowiąc poważne zagrożenie dla bezpieczeństwa narodowego i publicznego. Celem niniejszej pracy jest zbadanie nowoczesnych technologii i strategii stosowanych w zwalczaniu przestępczości zorganizowanej i cyberprzestępczości, ze szczególnym uwzględnieniem wykorzystania i ochrony danych publicznych. Praca ta będzie badać obecny stan przestępczości zorganizowanej i cyberprzestępczości, rolę danych publicznych w ułatwianiu lub utrudnianiu działalności przestępczej oraz różne technologie i strategie stosowane przez organy ścigania w zwalczaniu tych przestępstw. Praca ta będzie również omawiać znaczenie ochrony danych publicznych i środki podjęte w celu zapewnienia ich bezpieczeństwa.

Słowa kluczowe: szybki rozwój technologii, przestępczość zorganizowana, cyberprzestępczość, bezpieczeństwo narodowe i publiczne

Wstęp

W dzisiejszych czasach, w obliczu szybkiego rozwoju technologii, przestępczość przybiera coraz bardziej złożone formy. Przestępczość zorganizowana

¹ Ewelina Zielińska – studentka Wojskowej Akademii Technicznej na kierunku bezpieczeństwo narodowe, na III roku studiów stacjonarnych, na Wydziale Bezpieczeństwa, Logistyki i Zarządzania.

i cyberprzestępczość stają się poważnymi zagrożeniami dla bezpieczeństwa narodowego i stabilności ekonomicznej. Agencje ścigania oraz rządy na całym świecie muszą stawiać czoła nowym wyzwaniom, aby skutecznie walczyć z tymi dynamicznie rozwijającymi się zjawiskami. Aby sprostać tym trudnościom, niezwykle istotne jest wykorzystanie nowoczesnych technologii oraz strategii, które pozwalają na lepsze zrozumienie i zwalczanie przestępczości. W tym kontekście dane publiczne, takie jak informacje z mediów społecznościowych czy raporty agencji, odgrywają kluczową rolę. Dają one wgląd w działania grup przestępczych oraz ich wzorce, co z kolei pozwala na bardziej efektywne reagowanie².

Warto zacząć od tego, czym jest bezpieczeństwo informacyjne, ponieważ jest to taka dziedzina działalności człowieka, której znaczenie w ostatnim czasie gwałtownie rośnie. Jest to jednocześnie dziedzina chyba tak stara, jak sam człowiek, który od zarania swojego istnienia był skazany na zdobywanie informacji (np. gdzie znajdują się zasoby pożywienia i wody), jej ocenę (czy członek plemienia, który podał taką informację, jest wiarygodny i czy ta informacja może być przydatna) oraz jej ochronę (przez tworzenie kręgów „wtajemniczonych” wojowników i szamanów, jej utrwalenie najpierw w przekazach ustnych, a potem także pisemnych itd.). A zatem informacja i działania mające na celu jej wykorzystanie i ochronę towarzyszyły człowiekowi od zawsze, ale w ostatnich latach wraz z coraz szybszym rozwojem techniki i związanymi z tym zmianami cywilizacyjnymi nabrały szczególnego znaczenia. Po pierwsze, rozwój elektroniki spowodował, że pojawiła się „elektroniczna postać informacji”, która może być łatwo i szybko przetwarzana, przesyłana i przechowywana. Do przesyłania takiej informacji służą sieci teleinformacyjne ewoluujące obecnie w kierunku jednej homogenicznej sieci obejmującej cały glob – Internetu, do przetwarzania i przechowywania – węzły sieci z ulokowanymi w nich zasobami przechowującymi i przetwarzającymi informację (od pojedynczych domowych komputerów po centra danych). Po drugie, z powodu wymienionego wyżej, ilość dostępnej informacji gwałtownie rośnie i niezbędna staje się jej selekcja i ocena pod względem szeroko rozumianej jakości³.

Jednym z elementów tych strategii jest wykorzystanie danych publicznych. Dane te, odpowiednio analizowane i chronione, mogą stanowić potężne na-

² I. Szkudlarek, *Środowisko wielokulturowe jako determinant współczesnych operacji reagowania kryzysowego* [w:] M. Drewniak, S. Ejdyś, D. Becker-Pestka, A. Zawadzka (red. nauk.), *Interdyscyplinarność, czyli wyzwanie dla naukowców cz. 7*, Wyd. Naukowe INTELECT, Waleńców 2021, s. 27-37.

³ K. Liderman, *Bezpieczeństwo Informacyjne. Nowe Wyzwania*, PWN, Warszawa 2017, s.15.

rzędzie w walce z przestępczością. Współczesne technologie, takie jak sztuczna inteligencja (AI), analiza *big data*, *blockchain* oraz Internet Rzeczy (IoT), umożliwiają nie tylko identyfikację i śledzenie działań przestępczych, ale też przewidywanie potencjalnych zagrożeń i zapobieganie im. Sztuczna inteligencja (AI) jest wykorzystywana do analizowania ogromnych ilości danych w celu wykrywania wzorców i anomalii, które mogą wskazywać na działalność przestępczą⁴. Algorytmy uczenia maszynowego mogą przewidywać miejsca i czas potencjalnych przestępstw, co pozwala na bardziej efektywne rozmieszczenie zasobów policyjnych⁵.

Celem niniejszej pracy jest analiza nowoczesnych technologii stosowanych w zwalczaniu przestępczości zorganizowanej oraz cyberprzestępczości, takich jak sztuczna inteligencja, uczenie maszynowe, *big data* oraz zaawansowane narzędzia do monitorowania i analizy danych. Praca ta skupi się również na strategiach ochrony danych publicznych, które są potrzebne, aby zapewnić bezpieczeństwo obywateli oraz integralności systemów informacyjnych. Przedstawione zostaną zarówno korzyści, jak i wyzwania związane z wdrażaniem tych technologii, co pozwoli na lepsze zrozumienie ich roli w nowoczesnych działaniach prewencyjnych i operacyjnych.

Przestępczość zorganizowana i cyberprzestępczość jako zagrożenie dla społeczeństwa

W dzisiejszym, zaawansowanym technologicznie społeczeństwie, informacja odgrywa kluczową rolę w funkcjonowaniu zarówno państw, jak i firm oraz jednostek. Przetwarzana, przechowywana i przesyłana za pomocą systemów teleinformatycznych, informacja stała się jednym z najważniejszych towarów, często o strategicznym znaczeniu. Historia pokazuje, że ci, którzy mieli dostęp do właściwych informacji we właściwym czasie, odnosili sukcesy zarówno na polu bitwy, jak i w biznesie. Współczesne podejście do informacji porównuje ją do surowców naturalnych czy nowoczesnych technologii, co podkreśla konieczność jej ochrony. Zakłócenie przepływu informacji lub jej sfałszowanie prowadzi do strat, które dla firm mogą oznaczać bankructwo, a dla państw – niepokoje społeczne, zaburzenia gospodarcze i negatywne postrzeganie na arenie międzynarodowej. Informacja

⁴ Zwalczanie Przestępczości Zorganizowanej, <https://www.abw.gov.pl/pl/zadania/zwalczanie-przestepczo/9Zwalczanie-przestepczosci-zorganizowanej.html> [dostęp: 24.11.2024 r.].

⁵ E. W. Pływaczewski, W. Filipkowski, Z. Rau, *Przestępczość w XXI wieku – Zapobieganie i zwalczanie* [w:] *Problemy prawnokryminologiczne*, s. 31-34.

odgrywa kluczową rolę w zautomatyzowanych procesach produkcyjnych i usługowych, które są nieodzowne dla gospodarki i społeczeństwa⁶. Może występować w postaci informacji sterującej urządzeniami, takimi jak czujniki i mechanizmy wykonawcze. Błędne sterowanie tymi systemami może prowadzić do katastrof, takich jak kryzysy ekologiczne, i wywoływać kryzysy na skalę lokalną, krajową lub międzynarodową. W związku z jej znaczeniem oraz ochroną dóbr osobistych obywateli, wszystkie cywilizowane kraje wprowadziły przepisy prawne nakazujące ochronę informacji przed nieuprawnionym dostępem, zapewniając właściwe przetwarzanie, przechowywanie i przesyłanie danych oraz określając zasady zbierania określonych kategorii informacji.

Przestępczość zorganizowana i cyberprzestępczość stanowią poważne zagrożenie dla współczesnego społeczeństwa, mając szeroki wpływ na bezpieczeństwo obywateli, stabilność gospodarki oraz funkcjonowanie instytucji publicznych i prywatnych. Przestępczość zorganizowana obejmuje działalność grup przestępczych, zaangażowanych w różnorodne nielegalne działania, takie jak handel narkotykami, przemyt ludzi, pranie brudnych pieniędzy czy korupcję⁷. Działania te często mają charakter międzynarodowy, co utrudnia ich zwalczanie. Prowadzą one do destabilizacji społeczności lokalnych, wzrostu przemocy oraz korupcji, co osłabia zaufanie obywateli do instytucji państwowych. Z kolei cyberprzestępczość, obejmująca przestępstwa popełniane przy użyciu technologii informacyjnych i komunikacyjnych, wiąże się z takimi działaniami jak kradzież danych, oszustwa internetowe, ataki *ransomware* czy cyberterroryzm. Stanowi ona zagrożenie dla prywatności obywateli, bezpieczeństwa finansowego firm oraz integralności systemów informatycznych instytucji publicznych. Wzrost liczby cyberataków, zwłaszcza w kontekście pandemii COVID-19, ukazuje, jak ważne jest zabezpieczenie infrastruktury cyfrowej. Oba te rodzaje przestępczości mają negatywny wpływ na społeczeństwo – przestępczość zorganizowana prowadzi do wzrostu przestępczości pospolitej, zwiększając poczucie niepewności wśród obywateli, natomiast cyberprzestępczość może skutkować poważnymi stratami finansowymi oraz utratą zaufania do technologii cyfrowych. W odpowiedzi na te zagrożenia, konieczne jest wzmocnienie współpracy międzynarodowej oraz rozwój nowoczesnych technologii zabezpieczających.

⁶ K. Liderman, dz. cyt.

⁷ Organy ścigania z państw członkowskich UE i unijne agencje wspólnie walczą z przestępczością poważną i zorganizowaną, <https://www.consilium.europa.eu/pl/policies/eu-fight-against-crime/> [dostęp: 30.10.2024 r.].

Nowoczesne technologie w zwalczaniu przestępczości zorganizowanej i cyberprzestępczości

Nowoczesne technologie odgrywają istotną rolę w zwalczaniu przestępczości zorganizowanej i cyberprzestępczości, umożliwiając organom ścigania skuteczniejsze monitorowanie, analizowanie i przeciwdziałanie działalności przestępczej. Wśród najważniejszych technologii, które przyczyniają się do tych działań, znajdują się sztuczna inteligencja (AI), *blockchain* oraz Internet Rzeczy (IoT). Sztuczna inteligencja jest wykorzystywana do analizy ogromnych ilości danych, co pozwala na identyfikację wzorców przestępczych i przewidywanie przyszłych działań przestępców. Algorytmy AI mogą przetwarzać dane z różnych źródeł, takich jak kamery monitoringu, media społecznościowe czy bazy danych policyjnych, w celu wykrywania podejrzanych zachowań. Na przykład, systemy rozpoznawania twarzy oparte na AI mogą identyfikować w tłumie osoby poszukiwane, co znacznie ułatwia ich zatrzymanie. Technologia *blockchain* zapewnia transparentność i bezpieczeństwo transakcji finansowych, co jest kluczowe w walce z praniem pieniędzy i finansowaniem terroryzmu. Dzięki *blockchainowi* możliwe jest śledzenie przepływu środków finansowych w sposób niezmienny i przejrzysty, co utrudnia przestępcom ukrywanie swoich działań. Ponadto, *blockchain* może być wykorzystywany do zabezpieczenia dowodów cyfrowych, co zapewnia ich integralność i autentyczność w procesach sądowych.

W dzisiejszych czasach dane publiczne odgrywają istotną rolę w zwalczaniu przestępczości zorganizowanej i cyberprzestępczości. Dzięki zaawansowanym technologiom i narzędziom analitycznym, organy ścigania mogą skuteczniej identyfikować, monitorować i neutralizować zagrożenia. Wykorzystując dane publiczne, organy ścigania tworzą profile przestępców, identyfikują wzorce przestępczości oraz przewidują przyszłe zagrożenia. Na przykład, analiza danych z mediów społecznościowych może pomóc w wykrywaniu sieci przestępczych i ich działań. Wymiana informacji między krajami jest ważna w walce z przestępczością zorganizowaną, która często ma charakter transgraniczny. Inicjatywy takie jak EMPACT (Europejska Multidyscyplinarna Platforma Przeciwko Zagrożeniom Przestępczym) umożliwiają skuteczną współpracę i wymianę danych między państwami członkowskimi UE. Wykorzystanie technologii, takich jak sztuczna inteligencja i uczenie maszynowe pozwala na szybsze i bardziej precyzyjne przetwarzanie ogromnych ilości danych, co umożliwia wykrywanie skomplikowanych schematów przestępczych i cyberataków. Przepisy takie jak RODO (Rozporządzenie o Ochronie Danych Osobowych) oraz krajowe ustawy o ochronie danych osobowych zapewniają, że dane są przetwarzane zgodnie z prawem i z poszanowaniem prywatności obywateli. Wdrażanie zaawansowanych środków

bezpieczeństwa, takich jak szyfrowanie danych i systemy wykrywania włamań, jest niezbędne do ochrony danych przed nieautoryzowanym dostępem i cyberatakami. Regularne szkolenia i kampanie informacyjne pomagają w zrozumieniu znaczenia ochrony danych i stosowania najlepszych praktyk w tym zakresie. Wykorzystanie i ochrona danych publicznych w walce z przestępczością zorganizowaną i cyberprzestępczością to złożone, ale niezbędne zadanie. Dzięki odpowiednim narzędziom, regulacjom i współpracy międzynarodowej możliwe jest skuteczne przeciwdziałanie zagrożeniom i zapewnienie bezpieczeństwa obywatelom.

Przykłady wykorzystania nowoczesnych technologii w zwalczaniu przestępczości zorganizowanej i cyberprzestępczości

Dzięki współczesnym technologiom organy ścigania mogą skuteczniej identyfikować, śledzić i neutralizować zagrożenia. Jednym z najważniejszych narzędzi w walce z przestępczością jest analiza danych. Dzięki zaawansowanym algorytmom sztucznej inteligencji (AI), możliwe jest przetwarzanie ogromnych ilości danych w celu wykrywania wzorców i anomalii, które mogą wskazywać na działalność przestępczą. Na przykład, systemy AI są wykorzystywane do monitorowania transakcji finansowych w celu wykrywania prania pieniędzy i oszustw finansowych. Technologie biometryczne, takie jak rozpoznawanie twarzy, odcisków palców i skanowanie tęczówki oka, są coraz częściej stosowane w identyfikacji przestępców. Systemy te są wykorzystywane na lotniskach, w bankach oraz przez organy ścigania do szybkiej i dokładnej identyfikacji osób podejrzanych o działalność przestępczą. Rzeczywistość wirtualna (VR) i rozszerzona (AR) znajdują zastosowanie w szkoleniu śledczych oraz w symulacjach operacji policyjnych. Dzięki tym technologiom, funkcjonariusze mogą przećwiczyć różne scenariusze i przygotować się na realne sytuacje, co zwiększa ich skuteczność w działaniach operacyjnych. Inteligentne czujniki i urządzenia IoT są wykorzystywane do monitorowania i zabezpieczania miejsc publicznych oraz infrastruktury krytycznej. Na przykład, czujniki mogą wykrywać nieautoryzowane próby dostępu do budynków, a systemy IoT mogą monitorować ruch i zachowanie osób w czasie rzeczywistym, co pozwala na szybszą reakcję na potencjalne zagrożenia. Oprogramowanie do analizy wizualnej, takie jak systemy rozpoznawania obrazu i wideo, jest wykorzystywane do monitorowania miejsc publicznych i identyfikacji podejrzanych działań. Dzięki tym technologiom, organy ścigania mogą szybko reagować na incydenty i zapobiegać przestępstwom. Nowoczesne narzędzia cyfrowe, takie jak zaawansowane oprogramowanie do analizy danych,

są wykorzystywane w dochodzeniach kryminalnych. Przykładem może być analiza komunikacji elektronicznej, która pozwala na śledzenie i identyfikację sieci przestępczych działających w Internecie. Nowoczesne technologie odgrywają istotną rolę w zwalczaniu przestępczości zorganizowanej i cyberprzestępczości. Dzięki nim organy ścigania mogą skutecznie identyfikować, śledzić i neutralizować zagrożenia, co przyczynia się do zwiększenia bezpieczeństwa publicznego. Technologia *blockchain* jest wykorzystywana do zabezpieczania danych i transakcji, co utrudnia fałszowanie dokumentów i pranie pieniędzy. Dzięki transparentności i niezmienności zapisów, *blockchain* może pomóc w śledzeniu przepływów finansowych i identyfikacji nielegalnych działań. Drony są używane do monitorowania dużych obszarów, prowadzenia obserwacji z powietrza oraz wsparcia operacji policyjnych. Mogą być wyposażone w kamery termowizyjne i inne sensory, co pozwala na skuteczne śledzenie podejrzanych osób i pojazdów. Narzędzia do analizy cyfrowej są kluczowe w badaniu dowodów elektronicznych, takie jak e-maile, pliki i dane z urządzeń mobilnych. Forensyka cyfrowa pozwala na odzyskiwanie usuniętych danych i analizę śladów cyfrowych pozostawionych przez przestępców. Zaawansowane systemy komunikacyjne, takie jak szyfrowane kanały komunikacji, są wykorzystywane przez organy ścigania do bezpiecznego przekazywania informacji i koordynacji działań operacyjnych. Analiza dużych zbiorów danych (*Big Data*) pozwala na identyfikację wzorców przestępczych i prognozowanie przyszłych zagrożeń. Dzięki temu organy ścigania mogą podejmować bardziej świadome decyzje i planować działania prewencyjne.

Współczesne technologie oraz rosnąca ilość dostępnych danych publicznych stwarzają nowe możliwości w walce z przestępczością zorganizowaną i cyberprzestępczością. Wykorzystanie danych publicznych, takich jak rejestry administracyjne, dane finansowe czy informacje z mediów społecznościowych, pozwala na bardziej efektywne monitorowanie i zwalczanie działalności przestępczej. Przestępczość zorganizowana stanowi jedno z największych zagrożeń dla bezpieczeństwa publicznego. Grupy przestępcze działają na szeroką skalę, często przekraczając granice państwowe, co utrudnia ich ściganie. Wykorzystanie danych publicznych może znacząco poprawić skuteczność działań organów ścigania. Na przykład, analiza danych finansowych może pomóc w identyfikacji podejrzanych transakcji i śledzeniu przepływów finansowych, co jest ważne w kontekście walki z praniem brudnych pieniędzy. Cyberprzestępczość to kolejny obszar, w którym dane publiczne odgrywają istotną rolę. Przestępcy coraz częściej wykorzystują Internet do prowadzenia swojej działalności, co wymaga nowoczesnych narzędzi do ich zwalczania. Analiza danych z mediów społecznościowych, forów internetowych oraz innych źródeł *online* może pomóc w identyfikacji i śledzeniu

cyberprzestępców⁸. Przykładem może być przypadek EncroChat, gdzie zaawansowane technologie pozwoliły na rozbicie międzynarodowej sieci przestępczej.

Wykorzystanie danych publicznych w walce z przestępczością napotyka również na wyzwania. Jednym z głównych problemów jest ochrona prywatności obywateli oraz zgodność z przepisami o ochronie danych osobowych. Konieczne jest znalezienie równowagi między skutecznością działań a poszanowaniem praw jednostki. W przyszłości można spodziewać się dalszego rozwoju technologii analitycznych oraz większej integracji danych z różnych źródeł. Współpraca międzynarodowa oraz wymiana informacji między państwami będą kluczowe w skutecznej walce z przestępczością zorganizowaną i cyberprzestępczością.

Strategie wykorzystania i ochrony danych publicznych

Dzisiejsze szybko zmieniające się środowisko techniczne wymaga od podmiotów publicznych przyjęcia minimalnego zestawu zabezpieczeń w celu ochrony swoich informacji i systemów teleinformatycznych. Narodowy standard przetwarzania informacji NSC 200, określa minimalne wymagania bezpieczeństwa w siedemnastu obszarach związanych z bezpieczeństwem. Podmioty publiczne powinny spełniać minimalne wymagania bezpieczeństwa określone w NSC 200 poprzez zastosowanie zabezpieczeń znajdujących się w publikacji NSC 800-53. NSC 800-53 zawiera zabezpieczenia zarządcze, operacyjne i techniczne lub środki zaradcze przewidziane dla systemu teleinformatycznego. Wybrane lub zaplanowane zabezpieczenia muszą być udokumentowane w planie bezpieczeństwa systemu. Europejska strategia w zakresie wykorzystania danych publicznych zakłada: jednolity rynek danych oraz innowacje oparte na danych. Umożliwia to swobodny przepływ danych w UE i między sektorami, co przynosi korzyści przedsiębiorstwom, naukowcom i administracjom publicznym⁹. W przyszłości zabezpieczenia te mogą przynieść korzyści w medycynie, mobilności, polityce oraz modernizacji usług publicznych. Ponowne wykorzystywanie informacji sektora publicznego: Ustawa o otwartych danych, portal dane.gov.pl. Reguluje zasady ponownego wykorzystywania informacji sektora publicznego w celach komercyjnych i niekomercyjnych. Zwiększa dostępność danych, poprawia ich jakość i interopera-

⁸ I. Szkudlarek, M. Błachut, *Bezpieczeństwo informatyczne a portale społecznościowe wykorzystywane na potrzeby przestępstw internetowych* [w:] A. Baryłka, K. Konopka (red. nauk.), *Prawo a bezpieczeństwo*, Oficyna Wydawnicza Centrum Rzecznawstwa Budowlanego, Warszawa 2021, s. 55-77.

⁹ EUROPEJSKA STRATEGIA W ZAKRESIE DANYCH, Europejska strategia w zakresie danych – Komisja Europejska (europa.eu).

cyjność. Ochrona danych publicznych: Europejski akt w sprawie danych oraz bezpieczeństwo danych. Przepisy dotyczące dostępu i wykorzystywania danych zapewniają uczciwe, praktyczne i zrozumiałe zasady, które chronią prywatność i dane osobowe. Kontrola nad danymi, przez co obywatele mają większą kontrolę nad swoimi danymi, co zwiększa zaufanie do przedsiębiorstw. Co więcej, stosowanie standardowych i kompatybilnych formatów oraz protokołów dla gromadzenia i przetwarzania danych w sposób spójny i interpretacyjny¹⁰. Celem planowania bezpieczeństwa systemu teleinformatycznego jest poprawa ochrony zasobów tego systemu. Wszystkie systemy podmiotów publicznych mają pewien poziom wrażliwości i wymagają ochrony w ramach dobrej praktyki zarządzania. Ochrona systemu musi być udokumentowana w planie bezpieczeństwa systemu. Opracowanie planów bezpieczeństwa systemu jest wymagane przepisem § 20 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych¹¹. Celem planu bezpieczeństwa systemu jest przedstawienie przeglądu wymagań bezpieczeństwa systemu i opisanie zabezpieczeń, które zostały wprowadzone lub zaplanowane do wprowadzenia w celu spełnienia tych wymagań. Plan bezpieczeństwa systemu określa również obowiązki i oczekiwane zachowanie wszystkich osób uzyskujących dostęp do systemu. Plan bezpieczeństwa systemu powinien być postrzegany jako dokumentacja ustrukturyzowanego procesu planowania odpowiedniej, kosztowo racjonalnej, ochrony bezpieczeństwa systemu. Powinien odzwierciedlać wkład różnych menedżerów odpowiedzialnych za system, w tym właścicieli informacji, właściciela systemu. W celu odpowiedniego odzwierciedlenia przez plany ochrony zasobów, właściwy członek kierownictwa organizacji musi upoważnić system do działania. Upoważnienie systemu do przetwarzania informacji, udzielone przez członka kierownictwa, zapewnia istotne zabezpieczenie organizacyjne. Autoryzacja przez członka kierownictwa powinna opierać się na ocenie zabezpieczeń zarządczych, operacyjnych i technicznych. Ponieważ plan bezpieczeństwa systemu ustanawia i dokumentuje zabezpieczenia, powinien stanowić podstawę autoryzacji, uzupełniony raportem z oceny (audytu) bezpieczeństwa. Ponadto niezbędny jest okresowy przegląd zabezpieczeń na potrzeby przyszłych autoryzacji. Ponowna autoryzacja powinna nastąpić za każdym razem, gdy nastąpi znacząca zmiana w przetwarzaniu, ale nie rzadziej, niż co trzy lata.

¹⁰ Nowy Program Otwierania Danych na lata 2021-2027 – Otwarte Dane.

¹¹ Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, (Dz.U. 2012 poz. 526).

Bezpieczeństwo informacyjne oraz wykorzystanie danych publicznych w walce z przestępczością zorganizowaną i cyberprzestępczością

Nowoczesne technologie informacyjno-komunikacyjne umożliwiają stałą komunikację i wymianę danych na odległość, bez potrzeby jednoczesnej obecności stron. Rynek teleinformatyczny obecnie odpowiada na potrzeby społeczeństwa informacyjnego. W efekcie, powszechne stało się korzystanie z e-usług i e-informacji, a także gromadzenie, upowszechnianie, uzupełnianie, aktualizowanie oraz przekazywanie danych. Informacja elektroniczna stała się produktem, którego nie można traktować w oderwaniu od poszanowania i ochrony jawności oraz prywatności danych szczególnie chronionych¹². Wykorzystanie danych publicznych w walce z przestępczością zorganizowaną i cyberbezpieczeństwem obejmuje kilka istotnych elementów. Analiza dużych zbiorów danych publicznych przy użyciu algorytmów może pomóc w identyfikacji nietypowych wzorców, które wskazują na działalność przestępczą. Współpraca międzynarodowa jest nieodzowna dla skutecznego zwalczania przestępczości zorganizowanej, ponieważ umożliwia lepsze zrozumienie globalnych trendów przestępczych i wspiera dochodzenia międzynarodowe. Technologie cyfrowe, takie jak sztuczna inteligencja, uczenie maszynowe oraz analiza *big data*, znacznie zwiększają skuteczność działań antyprzestępczych, pozwalając na szybkie wykrywanie i reagowanie na zagrożenia.

W kontekście cyberbezpieczeństwa istotne jest wprowadzenie zaawansowanych technologii ochrony, takich jak kryptografia i systemy wykrywania włamań, aby zapewnić bezpieczeństwo danych publicznych. Edukacja i zwiększanie świadomości społecznej na temat zagrożeń związanych z przestępczością zorganizowaną i cyberprzestrzenią również odgrywa ważną rolę w skutecznych zwalczaniu tych zagrożeń. Programy edukacyjne oraz kampanie informacyjne pomagają w podniesieniu świadomości i zrozumienia zagrożeń.

Wykorzystanie danych publicznych w walce z przestępczością zorganizowaną i cyberprzestępczością jest istotnym elementem współczesnych strategii i bezpieczeństwa. Przede wszystkim analiza *big data* pozwala na identyfikację wzorców i trendów wskazujących na działalność przestępczą, co umożliwia szybszą i skuteczniejszą reakcję na zagrożenia. Współpraca międzynarodowa między różnymi instytucjami i krajami, jak w ramach Unii Europejskiej, jest również istotna w wymianie informacji i wspólnym działaniu przeciwko przestępczości zorganizowanej i cyberprzestępczości. Technologia *blockchain* odgrywa kluczową rolę w zabezpieczaniu danych, zapewniając ich niezawodność i zapobiegając fałszer-

¹² M. Gołka, *Czym jest społeczeństwo informacyjne?*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny” 2005/67(4), s. 254.

stwom. Zwiększenie świadomości społecznej na temat zagrożeń związanych z cyberprzestępczością oraz promowanie bezpiecznych praktyk *online* mogą znacząco zmniejszyć ryzyko stania się ofiarą cyberataków. Sztuczna inteligencja (AI) jest wykorzystywana do automatycznej analizy dużych zbiorów danych i identyfikacji potencjalnych zagrożeń, co umożliwia proaktywne działania prewencyjne. Monitorowanie treści w mediach społecznościowych pomaga w wykryciu podejrzanych działań i potencjalnych zagrożeń. Ograniczenie dostępności danych publicznych, które mogą być wykorzystane przez przestępców, również ma istotne znaczenie. Każda z tych strategii, znacząco przyczynia się do skuteczniejszej walki z przestępczością zorganizowaną i cyberprzestępczością.

Ochrona danych publicznych przed nieuprawnionym dostępem i wykorzystaniem jest istotnym elementem współczesnych strategii bezpieczeństwa. Podstawowym krokiem jest tworzenie silnych, regularnie aktualizowanych haseł i zabezpieczeń dla każdego konta *online* oraz systematyczne aktualizacje oprogramowania, obejmujące m.in. systemy operacyjne i aplikacje, są niezbędne dla eliminowania znalezionych usterek. Ważne jest również korzystanie z technologii kryptograficznych do szyfrowania danych, co utrudnia nieuprawniony dostęp do nieprawidłowo zabezpieczonych informacji. Kolejnym istotnym elementem jest monitorowanie i analiza danych w poszukiwaniu podejrzanych działań, z wykorzystaniem algorytmów AI do wykrywania nietypowych wzorców. Zastosowanie zasady najmniejszych uprawnień, aby upewnić się, że tylko upoważnione osoby mają dostęp do danych publicznych, oraz regularne przeglądanie uprawnień użytkowników i usuwanie tych, które nie są już potrzebne, to kluczowe działania. Bardzo istotne jest zwiększenie świadomości pracowników na temat zagrożeń związanych z bezpieczeństwem danych oraz szkolenia w zakresie najlepszych praktyk bezpieczeństwa. Regularne przeprowadzanie testów bezpieczeństwa, w tym testów penetracyjnych i analiz ryzyka, pomaga identyfikować potencjalne słabości w systemach zabezpieczających dane. Wreszcie, opracowanie planu zarządzania ryzykiem, który obejmuje identyfikację, ocenę i minimalizację ryzyka związanego z nieuprawnionym dostępem do danych publicznych, jest kluczowym elementem ochrony danych.

Jednym z najistotniejszych celów RODO jest harmonizacja zasad przetwarzania i ochrony danych osobowych w państwach członkowskich UE. W styczniu 2022 roku Europejska Rada Ochrony danych (EROD) opublikowała treść wytycznych dotyczących prawa dostępu do danych osobowych. Wytyczne zostaną poddane teraz publicznym konsultacjom, a następnie zostaną zatwierdzone przez EROD i opublikowana zostanie ich ostateczna treść. Prawo dostępu do danych to jedno z najważniejszych praw przyznanych przez RODO osobom fizycznym w kontekście przetwarzania ich danych osobowych. Wiedza o tym jakie dane

i w jaki sposób są przetwarzane oraz prawo uzyskania dostępu do nich, pozwala podmiotowi danych na odpowiednie zarządzanie ich danymi i może stanowić podstawę do wykonywania innych praw przyznanych przez RODO. Najważniejszymi aspektami prawa dostępu do danych osobowych to: prawo do potwierdzenia faktu przetwarzania danych, prawo do kopii danych oraz obowiązku weryfikacji tożsamości osoby wnioskującej. W myśl art. 15 RODO prawo dostępu obejmuje m.in. prawo do uzyskania od administratora potwierdzenia, że przetwarza on dane osobowe konkretnej osoby fizycznej oraz prawo do uzyskania od administratora konkretnych informacji dotyczących przetwarzania jej danych. Pierwszym elementem prawa dostępu do danych jest zatem zobowiązanie administratora do potwierdzenia osobie, której dane dotyczą, faktu przetwarzania jej danych osobowych lub potwierdzenia ich nieprzetwarzania. Osoba może zatem najpierw zapytać, czy administrator posiada (przetwarza) jej dane osobowe, a po uzyskaniu takiego potwierdzenia podjąć dalsze kroki (np. prosić o kopię danych). Jednocześnie podmiot danych ma prawo do uzyskania konkretnych informacji o przetwarzaniu danych osobowych, takich jak cel, kategorie i odbiorcy danych, czas przetwarzania, prawa osób, których dane dotyczą, czy wreszcie odpowiednie zabezpieczenia w przypadku przekazywania danych do państw trzecich. Wytyczne wskazują, że potwierdzenie faktu przetwarzania danych osobowych może zostać dokonane w sposób odrębny, ale też może być połączone z udzieleniem podmiotowi danych informacji o samym procesie przetwarzania. W praktyce często bowiem zdarza się, że zainteresowana osoba formułuje swoje żądanie w sposób warunkowy (np. „proszę o potwierdzenie”).

Głównym celem strategii jest poprawa jakości procedur związanych ze ściganiem przestępstw i usprawnienie współpracy sądowej: ze względu na fakt, że 65% grup przestępczych działających na terenie UE tworzą osoby różnych narodowości, skuteczna wymiana informacji między organami ścigania i organami sądowymi w całej UE ma kluczowe znaczenie dla skutecznego zwalczania przestępczości zorganizowanej. Komisja rozszerzy i zmodernizuje europejską multidyscyplinarną platformę przeciwko zagrożeniom przestępstwami (EMPACT) oraz zwiększy przeznaczane na nią nakłady. EMPACT to struktura, która od 2010 roku skupia wszystkie właściwe organy europejskie i krajowe w celu określania priorytetowych zagrożeń przestępczością i wspólnego przeciwdziałania im. Aby zapewnić lepszą współpracę organów ścigania w całej UE w oparciu o nowoczesny pakiet zasad, Komisja zaproponowała utworzenie unijnego kodeksu współpracy policyjnej, który zastąpi obecną mozaikę różnych narzędzi UE i wielostronnych umów o współpracy. Osiągnięcie celu, jakim jest zapewnienie interoperacyjności systemów informacyjnych na potrzeby bezpieczeństwa, zarządzania granicami i migracją, pozwoli organom ścigania lepiej wykrywać i zwalczać sieci przestępcze

działające na skalę międzynarodową. Co więcej, umożliwi zwiększanie skuteczności prowadzonych postępowań w celu rozbijania struktur przestępczości zorganizowanej i koncentrowanie się na konkretnych, wysoce priorytetowych rodzajach przestępczości: należy zacieśnić współpracę na szczeblu UE w celu likwidacji struktur przestępczości zorganizowanej, aby zapewnić skuteczne reagowanie na konkretne formy przestępczości¹³. Zapewnienie, aby przestępstwa nie mogły się opłacać. Ponad 60 proc. sieci przestępczych działających w UE angażuje się w korupcję, a ponad 80 proc. wykorzystuje legalne przedsiębiorstwa jako złudzenie dla swojej działalności, podczas gdy konfiskacie podlega jedynie 1 proc. mienia pochodzącego z działalności przestępczej.

Ściganie przestępstw i sądownictwo na miarę ery cyfrowej: przestępcy komunikują się i popełniają przestępstwa w Internecie, pozostawiając tam cyfrowe ślady. Ponieważ 80% przestępstw ma komponent cyfrowy, organy ścigania i sądownictwo potrzebują szybkiego dostępu do śladów i dowodów cyfrowych. Muszą one być w stanie korzystać z nowoczesnych technologii i dysponować narzędziami i umiejętnościami umożliwiającymi dotrzymanie kroku nowoczesnym sposobom działania przestępców.

Cyberbezpieczeństwo w ujęciu kluczowych kompetencji technicznych przedsiębiorstw

Cyberbezpieczeństwo w ujęciu kluczowych kompetencji technicznych przedsiębiorstw staje się coraz bardziej istotnym elementem strategii organizacyjnych, wynikającym z dynamicznych procesów związanych z informatyzacją i cyfryzacją. W kontekście cyberbezpieczeństwa kluczowe kompetencje techniczne przedsiębiorstwa wynikają z dynamizmu procesów związanych z informatyzacją i cyfryzacją. Te procesy są napędzane głównie przez globalizację oraz e-rozwoju gospodarki i społeczeństwa. Aleksandra Monarcha-Matlak zauważa, że intensywne wdrażanie nowych technologii informacyjnych jako narzędzi komunikacji elektronicznej prowadzi do istotnych zmian w strukturach państwa i sposobach jego funkcjonowania. Cyberbezpieczeństwo zatem staje się nieodzownym elementem strategii przedsiębiorstw, które muszą rozwijać kompetencje techniczne w celu skutecznej ochrony swoich zasobów informacyjnych przed zagrożeniami w cyfrowym świecie¹⁴. W ślad

¹³ *Walka z przestępczością*, <https://www.riskcompliance.pl/news/walka-z-przestepczoscia-zorganizowana-nowa-strategia-na-rzecz-pobudzenia-wspolpracy-w-ue-i-lepszego-wykorzystania-narzedzi-cyfrowych-w-dochodzeniach/> [dostęp: 24.11.2024 r.].

¹⁴ A. Monarcha-Matlak, *Pojęcie komunikacji elektronicznej w doktrynie i aktach prawnych*, „Lingwistyka Stosowana. Applied Linguistics. Angewandte Linguistik” 2017/24, s. 143.

za autorką należy dodać, że globalny rozwój nowych technologii wpłynął nie tylko na zmiany w administracji publicznej (e-administracja, digitalizacja dokumentacji), ale również na organizację przedsiębiorstw i zachowania użytkowników końcowych. Przedsiębiorstwa w Polsce mają przed sobą bardzo ważny i wymagający okres cyfryzacji, który jest jednym z elementów idei przemysłu przyszłości – Przemysłu 4.0. Proces cyfryzacji szeroko rozumianych danych jest nieuniknioną konsekwencją rozwoju technologicznego, a co za tym idzie niesie ze sobą ryzyka, które często są lekceważone przez właścicieli przedsiębiorstw. Przeprowadzone w styczniu 2022 roku badania Monitora Transformacji Cyfrowej Biznesu pokazały, że aż 21% przedsiębiorstw w Polsce planowało zwiększenie wydatków na cyfryzację w ciągu najbliższego roku. W 2021 roku aż 70% przedsiębiorstw działających w Polsce odnotowało przynajmniej jeden cyberincydent.

Współczesne uwarunkowania rozwoju państwa i społeczeństwa, takie jak interoperacyjność, cyfrowość oraz transgraniczność mają kluczowy wpływ na wzrost wirtualnej mobilności oraz postęp technologiczny, w tym rozwój technologii cyfrowych nowej generacji, takich jak sztuczna inteligencja¹⁵. Te zmiany stawiają przed nami nowe wyzwania w zakresie bezpieczeństwa, a cyberbezpieczeństwo staje się globalnym celem. Narodowe Standardy Cyberbezpieczeństwa (NSC) to zestaw zaleceń mających na celu standaryzację rozwiązań zabezpieczających w sieciach i systemach informacyjnych, opracowany dla podmiotów pragnących efektywnie zarządzać systemami bezpieczeństwa informacji. NSC bazują na standardach amerykańskiego National Institute of Standards and Technology (NIST) i są dostosowane do polskiego systemu prawnego. Normy te są stosowane przez podmioty krajowego systemu cyberbezpieczeństwa, w tym instytucje publiczne, operatorów usług kluczowych i dostawców usług cyfrowych¹⁶. NSC pełnią rolę przewodników metodycznych, ułatwiając budowanie efektywnego systemu zarządzania bezpieczeństwem informacji zgodnie z praktykami administracji federalnej USA¹⁷. Narodowe Standardy Cyberbezpieczeństwa realizują inwestycje

¹⁵ D. Skoczylas, *Interoperacyjność, cyfrowość, transgraniczność technologii informacyjno-komunikacyjnych jako determinanty zrównoważonego rozwoju w XXI wieku*, [w:] *Zrównoważony rozwój i europejski zielony ład wektorami na drodze doskonalenia warsztatu naukowca*, red. M. Stanisławski, H.E. Kretek, Gliwice 2021, s. 238.

¹⁶ [https://www.gov.pl/web/bazawiedzy/narodowestandardcyberbezpieczenstwa#:~:text=Departament%20Cyberbezpieczenstwa%20Kancelarii%20Prezesa%20Rady%20Ministrów%20opracował%20Narodowe,przez%20podmioty%20chcące%20efektywnie%20zarządzać%20systemami%](https://www.gov.pl/web/bazawiedzy/narodowestandardcyberbezpieczenstwa#:~:text=Departament%20Cyberbezpieczenstwa%20Kancelarii%20Prezesa%20Rady%20Ministrów%20opracował%20Narodowe,przez%20podmioty%20chcące%20efektywnie%20zarządzać%20systemami%20) [dostęp: 04.11.2024 r.].

¹⁷ Kancelaria Prezesa Rady Ministrów, *Narodowy Standard Cyberbezpieczeństwa NSC 800-18 wer. 1.1, Przewodnik do opracowywania planów bezpieczeństwa systemów informacyjnych w podmiotach publicznych*, s. 20-21.

2.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 w zakresie opracowania i wdrożenia NSC¹⁸. Ponadto, NSC stanowią fundament nowoczesnych technologii i strategii w zwalczaniu przestępczości zorganizowanej w cyberprzestępczości. Wykorzystanie danych publicznych wspiera współpracę międzynarodową w zwalczaniu przestępczości zorganizowanej umożliwiając lepsze zrozumienie globalnych trendów przestępczych i wspierając dochodzenia międzynarodowe¹⁹. Analiza dużych zbiorów danych i wykorzystanie zaawansowanych technologii, takich jak sztuczna inteligencja i uczenie maszynowe, umożliwiają szybkie wykrywanie zagrożeń oraz skuteczną reakcję na incydenty²⁰. Ochrona danych publicznych przed nieuprawnionym dostępem i ich wykorzystaniem jest nieodzowna dla zapewnienia bezpieczeństwa w cyberprzestrzeni. Implementacja zaawansowanych mechanizmów zabezpieczających, takich jak kryptografia i systemy wykrywania włamań, jest kluczowa. Ważna jest również edukacja i zwiększanie świadomości społecznej na temat zagrożeń związanych z cyberprzestrzenią, a także współpraca międzynarodowa i ciągłe doskonalenie standardów oraz praktyk w zakresie cyberbezpieczeństwa. Przy naruszeniu ochrony danych osobowych należy przeprowadzić analizę czy nastąpiło wysokie czy niskie naruszenie ochrony praw lub wolności osób fizycznych. Zgłoszenie musi co najmniej: opisywać charakter naruszenia ochrony danych osobowych, w miarę możliwości wskazywać kategorie. Zgłoszenie można dokonać elektronicznie na 3 sposoby oraz tradycyjną pocztą wysyłając wypełniony formularz na adres Urzędu²¹.

Cyberbezpieczeństwo w ujęciu kluczowych kompetencji technicznych przedsiębiorstw staje się coraz bardziej istotnym elementem strategii organizacyjnych, wynikającym z dynamicznych procesów związanych z informatyzacją i cyfryzacją. Te procesy są napędzane głównie przez globalizację oraz rozwój e-gospodarki i e-społeczeństwa. Aleksandra Monarcha-Matlak zauważa, że intensywne wdrażanie nowych technologii informacyjnych jako narzędzi komunikacji elektronicznej prowadzi do istotnych zmian w strukturach państwa oraz sposobach jego funkcjonowania²². Te procesy są napędzane głównie przez globalizację oraz

¹⁸ Ministerstwo Cyfryzacji, Narodowy Standard Cyberbezpieczeństwa NSC 800-12, Bezpieczeństwo informacji – wprowadzenie, 2023, s. 105-106.

¹⁹ <https://www.gov.pl/web/mswia/zwalczanie-przestepczosci-zorganizowanej-raz-walka/> [dostęp: 04.11.2024 r.].

²⁰ <https://cyrekdigital.com/pl/baza-wiedzy/analiza-danych-big-data/> [dostęp: 04.11.2024 r.].

²¹ <https://gdpr.pl/baza-wiedzy/aktyprawne/interaktywny-tekst-gdpr/arttykul-33-zglaszanie-naruszenia-ochrony-danych-osobowych-organowi-nadzorcemu> [dostęp: 04.11.2024 r.].

²² A. Monarcha-Matlak, *Obowiązki administracji w komunikacji elektronicznej*, Oficyna Wolters Kluwer Polska, Warszawa 2008, s. 5.

rozwój e-gospodarki i e-społeczeństwa. W związku z tym cyberbezpieczeństwo staje się nieodłącznym elementem strategii przedsiębiorstw, które muszą rozwijać kompetencje techniczne w celu skutecznej ochrony swoich zasobów informacyjnych przed zagrożeniami cyfrowymi na świecie. Globalny rozwój nowych technologii wpływa nie tylko na zmiany w administracji publicznej, takie jak e-administracja i digitalizacja dokumentacji, ale również na organizację przedsiębiorstw oraz zachowania użytkowników końcowych. W Polsce przedsiębiorstwa stoją przed ważnym i wymagającym okresem cyfryzacji, który jest jednym z kluczowych elementów idei Przemysłu 4.0. Proces cyfryzacji danych jest nieuniknioną konsekwencją postępu technologicznego i niesie ze sobą ryzyka, które często są lekceważone przez właścicieli firm. Badania przeprowadzone w styczniu 2022 roku przez Monitor Transformacji Cyfrowej Biznesu pokazały, że aż 21% przedsiębiorstw w Polsce planowało zwiększenie wydatków na cyfryzację w ciągu najbliższego roku, podczas gdy w 2021 roku aż 70% przedsiębiorstw odnotowało przynajmniej jeden cyberincydent²³. Współczesne uwarunkowania rozwoju państwa i społeczeństwa, takie jak interoperacyjność, cyfrowość oraz transgraniczność, mają kluczowy wpływ na wzrost wirtualnej mobilności oraz postęp technologiczny, w tym rozwój technologii cyfrowych nowej generacji, takich jak sztuczna inteligencja. Te zmiany stawiają przed nami nowe wyzwania w zakresie bezpieczeństwa, a cyberbezpieczeństwo staje się globalnym dobrem publicznym. Narodowe Standardy Cyberbezpieczeństwa (NSC) to zestaw zaleceń mających na celu standaryzację rozwiązań zabezpieczających w sieciach i systemach informacyjnych, opracowany dla podmiotów pragnących efektywnie zarządzać systemami bezpieczeństwa informacji. NSC bazują na standardach amerykańskiego National Institute of Standards and Technology (NIST) i są dostosowane do polskiego systemu prawnego. Normy te są stosowane przez podmioty krajowego systemu cyberbezpieczeństwa, w tym instytucje publiczne, operatorów usług kluczowych i dostawców usług cyfrowych. NSC pełni rolę przewodników metodycznych, ułatwiając budowanie efektywnego systemu zarządzania bezpieczeństwem informacji zgodnie z praktykami administracji federalnej USA. Realizują one interwencję 2.1 celu szczegółowego 2 Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, dotyczącego opracowania i wdrożenia NSC. Ponadto, NSC stanowią fundament nowoczesnych technologii i strategii w zwalczaniu przestępczości zorganizowanej oraz cyberprzestępczości. Wykorzystanie danych publicznych wspiera współpracę międzynarodową w zwalczaniu przestępczości zorganizowanej, umożliwiając lepsze zrozumienie globalnych trendów przestępczych

²³ <https://kpmg.com/pl/pl/home/insights/2024/04/monitor-transformacji-cyfrowej-biznesu-edycja-2024.html> [dostęp: 04.11.2024 r.].

i wspierając dochodzenia międzynarodowe. Analiza dużych zbiorów danych i zaawansowane technologie, takie jak sztuczna inteligencja i uczenie maszynowe, umożliwiają szybkie wykrywanie zagrożeń oraz skuteczną reakcję na incydenty.

Ochrona danych publicznych przed nieuprawnionym dostępem i ich wykorzystaniem jest nieodzowna dla zapewnienia bezpieczeństwa w cyberprzestrzeni. Implementacja zaawansowanych mechanizmów zabezpieczających, takich jak kryptografia i systemy wykrywania włamań jest kluczowa. Ważna jest również edukacja i zwiększenie świadomości społecznej na temat zagrożeń związanych z cyberprzestrzenią, a także współpraca międzynarodowa i ciągłe doskonalenie standardów oraz praktyk w zakresie cyberbezpieczeństwa. W praktyce, w przypadku naruszenia ochrony danych osobowych, należy przeprowadzić analizę, czy nastąpiło wysokie czy niskie naruszenie ochrony praw lub wolności osób fizycznych. Zgłoszenie musi co najmniej opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie. Zgłoszenia można dokonać elektronicznie na 3 sposoby, a także tradycyjną pocztą, wysyłając wypełniony formularz na adres Urzędu.

Bibliografia

- Albanese J.S., *Organized Crime and Cybercrime: A Study of the Intersection*, Routledge, 2018.
- Chmielarz P., *Cyberprzestępczość. Zagrożenia i sposoby przeciwdziałania*, Wydawnictwo Uniwersytetu Jagiellońskiego, 2019.
- Fidos J., *Zwalczanie cyberprzestępczości. Strategie i taktyki*, wyd. C.H. Beck, 2019.
- Gołka M., Czym jest społeczeństwo informacyjne?, „Ruch Prawniczy, Ekonomiczny i Socjologiczny” 2005/67(4).
- Kelley B.D., *Cybercrime and the Darknet*, CRC Press, 2020.
- Liderman K., *Bezpieczeństwo Informacyjne Nowe Wyzwania*, PWN, Warszawa 2017.
- Ministerstwo Cyfryzacji, *Narodowy Standard Cyberbezpieczeństwa NSC 800-12, Bezpieczeństwo informacji – wprowadzenie*, 2023.
- Monarcha-Matlak A., *Obowiązki administracji w komunikacji elektronicznej*, Oficyna Wolters Kluwer Polska, Warszawa 2008.
- Monarcha-Matlak A., *Pojęcie komunikacji elektronicznej w doktrynie i aktach prawnych*, „Lingwistyka Stosowana. Applied Linguistics. Angewandte Linguistik” 2017/24.
- Pływaczewski E.W., Filipkowski W., Rau Z., *Przestępczość w XXI wieku – Zapobieganie i zwalczanie [w:] Problemy prawno-kryminologiczne*.
- Skoczyła D., *Interoperacyjność, cyfrowość, transgraniczność technologii informacyjno-komunikacyjnych jako determinanty zrównoważonego rozwoju w XXI wieku [w:] Staniszewski M., Kretek H.E. (red.), Zrównoważony rozwój i europejski zielony ład wektorami na drodze doskonalenia warsztatu naukowca*, Gliwice 2021.

- Solve D.J., *Data Protection and Privacy in the Age of Surveillance*, Cambridge University Press, 2019.
- Szkudlarek I., *Środowisko wielokulturowe jako determinant współczesnych operacji reagowania kryzysowego* [w:] Drewniak M., Ejdys S., Becker-Pestka D., Zawadzka A. (red.), *Interdyscyplinarność, czyli wyzwanie dla naukowców cz. 7*, Wydawnictwo Naukowe INTELECT, Wałęńczów 2021.
- Szkudlarek I., Błachut M., *Bezpieczeństwo informatyczne a portale społecznościowe wykorzystywane na potrzeby przestępstw internetowych* [w:] Baryłka A., Konopka K. (red.), *Prawo a bezpieczeństwo*, Oficyna Wydawnicza Centrum Rzeczoznawstwa Budowlanego, Warszawa 2021.
- Światłowski A., *Kryminalistyka komputerowa*, Wydawnictwo Naukowe PWN, 2017.
- Władowski M., *Nowoczesne technologie w zwalczaniu przestępczości zorganizowanej*, Wydawnictwo Wolters Kluwer, 2018.
- Wojciechowski K., *Bezpieczeństwo danych publicznych w erze cyfrowej*, Wydawnictwo Naukowe Scholar, 2020.

Strony internetowe: [dostęp: 04.11.2024 r.]

- <https://abw.gov.pl/pl/zadania/zwalczanie-przestepczo/9,Zwalczanie-przestepczosci-zorganizowanej.html>
- <https://cyrekdigital.com/pl/baza-wiedzy/analiza-danych-big/data/>
- <https://gdpr.pl/baza-wiedzy/aktyprawne/interaktywnytekstgdpr/arttykul33zgloszenie-naruszenia-ochrony-ndanych-osobowych-organowi-nadzorcemu>
- <https://gov.pl/web/baza-wiedzy/narodowe-standardy-cyberbezpieczenstwa>
- <https://gov.pl/web/mswia/zwalczanie-przestepczosci-zorganizowanej-oraz-walka-z-terroryzmem>
- <https://kpmg.com/pl/pl/home/insights/2024/04/monitor-transformacji-cyfrowej-biznesu-edycja-2024.html>
- <https://riskcompliance.pl/news/walka-z-przestepczoscia-zorganizowana-nowa-strategia-na-rzecz-pobudzenia-wspolpracy-w-ue-i-lepszego-wykorzystania-narzedzi-cyfrowych-w-dochodzeniach/>

Uwarunkowania prawne monitoringu przestrzeni publicznej

Daniel MATWIEJCZUK

Uniwersytet w Białymstoku
ORCID: 0009-0000-3893-8959

Streszczenie. Niniejsza praca ma na celu analizę prawną monitoringu wizyjnego w Polsce, skupiając się na aspektach ochrony prywatności i bezpieczeństwa publicznego. W kontekście dynamicznego rozwoju technologii monitoringu, takich jak systemy rozpoznawania twarzy i analityka wideo, konieczne staje się wypracowanie przepisów, które zrównoważą potrzeby bezpieczeństwa z ochroną praw obywateli. Problemy badawcze koncentrują się na aktualności obowiązujących przepisów w kontekście ochrony danych osobowych oraz na praktycznych wyzwaniach, jakie napotykają sądy w orzekaniu o przypadkach związanych z naruszeniem prywatności. Kluczowe hipotezy pracy zakładają, że obecne przepisy prawne są niewystarczające wobec rozwoju technologii nadzoru, że orzecznictwo sądowe sygnalizuje potrzebę regulacji, a stosowanie technologii biometrycznych powinno być ograniczone do wyjątkowych przypadków. Ponadto założono, że obowiązek przeprowadzania analizy wpływu na prywatność (DPIA) przed wdrożeniem monitoringu publicznego jest konieczny dla zapewnienia bezpieczeństwa danych obywateli. Zastosowano analizę dogmatyczno-prawną, która pozwala na szczegółowe omówienie aktów prawnych dotyczących monitoringu, takich jak Konstytucja RP, RODO, Kodeks karny, prawo telekomunikacyjne oraz wyroki sądów polskich i ETPC. Analiza literatury przedmiotu dostarcza teoretycznych ram zrozumienia wpływu monitoringu na społeczeństwo. Praca kończy się postulatem *de lege ferenda*, które przyczynią się do efektywnej ochrony prywatności obywateli, zapewniając jednocześnie funkcjonalność systemów monitoringu w przestrzeniach publicznych i prywatnych oraz podsumowaniem.

Słowa kluczowe: monitoring, monitoring wizyjny, ochrona prywatności, przepisy prawne, bezpieczeństwo, DPIA

Wprowadzenie

Rozwój nowoczesnych technologii monitoringu przynosi korzyści w zakresie poprawy bezpieczeństwa publicznego, zapobiegania przestępczości oraz efektywnego

zarządzania ruchem w przestrzeni miejskiej. Jednakże wzrastająca liczba systemów monitorujących oraz ich coraz bardziej zaawansowane funkcje, takie jak automatyczne rozpoznawanie twarzy czy numerów rejestracyjnych, rodzą pytania dotyczące granic ingerencji w prywatność jednostki. Obserwacja i nadzór prowadzone zarówno przez władze publiczne, jak i podmioty prywatne (osoby fizyczne, firmy) wywołują potrzebę opracowania jasnych i szczegółowych przepisów regulujących zakres, cele i zasady przetwarzania danych osobowych gromadzonych za pomocą kamer. W Polsce monitoring wizyjny jest stosowany coraz częściej. Systemy te są powszechnie używane przez jednostki administracji samorządowej, instytucje publiczne, a także przez właścicieli firm i posesji prywatnych, którzy dążą do zabezpieczenia swoich nieruchomości i ochrony przed aktami wandalizmu. Jednakże, jak wskazuje literatura przedmiotu, monitoring może prowadzić do naruszeń prawa do prywatności oraz odbierać jednostkom poczucie wolności w przestrzeni publicznej¹.

Praca ma na celu kompleksową analizę regulacji prawnych dotyczących monitoringu w Polsce, ze szczególnym uwzględnieniem ochrony prywatności jednostki, prawa do swobodnego przemieszczania się oraz prawa do ochrony danych osobowych. W pracy podjęto próbę oceny aktualnych przepisów prawnych, zidentyfikowania kluczowych wyzwań i problemów oraz sformułowania postulatów *de lege ferenda*, które mogą przyczynić się do ochrony praw obywateli przy jednoczesnym utrzymaniu skuteczności systemów monitoringu. Badanie to ma zatem charakter teoretyczno-empiryczny, oparty na analizie przepisów prawa, orzecznictwa sądowego oraz literatury przedmiotu. Dodatkowo, przeprowadzono analizę wybranych wyroków polskich sądów oraz Europejskiego Trybunału Praw Człowieka, aby zidentyfikować najważniejsze zagadnienia prawne związane z monitorowaniem przestrzeni publicznej i prywatnej oraz ochroną prywatności. Wśród podstawowych źródeł wykorzystywanych znajdują się zarówno polskie, jak i międzynarodowe akty prawne. Główne regulacje prawne obejmują Konstytucję Rzeczypospolitej Polskiej, w szczególności art. 47 zapewniający prawo do prywatności oraz art. 51, który określa ograniczenia dotyczące zbierania i przetwarzania informacji o obywatelach. Oprócz Konstytucji, niezwykle istotne są przepisy RODO (Rozporządzenie Ogólne o Ochronie Danych), które wprowadzają zasady dotyczące przetwarzania danych osobowych, w tym danych pozyskiwanych w wyniku monitoringu wizyjnego. Przytoczono także Kodeks karny, a zwłaszcza art. 267, który przewiduje sankcje za bezprawne uzyskanie informacji. Kluczowym źródłem są także krajowe przepisy, takie jak Prawo telekomunikacyj-

¹ D. Lyon, *Surveillance Studies: An Overview*, Wyd. Polity Press, Cambridge 2007, s. 139-158.

ne, które dotyczy korzystania z urządzeń rejestrujących w przestrzeniach publicznych, oraz rozporządzenie Prezesa Rady Ministrów dotyczące monitoringu wizyjnego. Dopełnieniem analizy prawnej są wyroki polskich sądów oraz orzeczenia Europejskiego Trybunału Praw Człowieka, które stanowią praktyczne wskazówki interpretacyjne dotyczące stosowania monitoringu oraz ochrony prywatności. Celem jest dostarczenie odpowiedzi na pytanie, na ile obecne przepisy prawne są adekwatne do zmieniającej się rzeczywistości technologicznej oraz jakie zmiany legislacyjne mogą być niezbędne w przyszłości, aby skutecznie chronić prywatność jednostek.

Wyznaczonymi celami w pracy są:

1. Analiza obecnie obowiązujących przepisów prawnych, które regulują stosowanie monitoringu, zwłaszcza w kontekście ochrony prywatności i ochrony danych osobowych.
2. Przedstawienie wybranych wyroków sądowych, aby ukazać praktyczne wyzwania związane z interpretacją przepisów dotyczących monitoringu.
3. Zidentyfikowanie i omówienie najważniejszych problemów wynikających z rosnącego zastosowania monitoringu wizyjnego, takich jak stosowanie technologii biometrycznych, monitoring pojazdów oraz kwestia retencji danych z monitoringu.
4. Opracowanie propozycji legislacyjnych *de lege ferenda*, które będą służyły ochronie prywatności obywateli przy jednoczesnym zachowaniu funkcjonalności systemów monitoringu.

W kontekście założonych celów badania sformułowano również hipotezy, które będą weryfikowane w toku analizy. Pierwsza hipoteza zakłada, że aktualne przepisy dotyczące monitoringu wizyjnego są niewystarczające i nieadekwatne do nowych technologii monitoringu, co może prowadzić do naruszenia prywatności obywateli. Druga hipoteza opiera się na założeniu, że orzecznictwo sądowe wyraźnie wskazuje na konieczność ograniczenia monitoringu w sytuacjach, w których może on naruszać prawa obywateli. Trzecia hipoteza dotyczy konieczności ograniczenia stosowania technologii biometrycznych, które powinny być wykorzystywane jedynie w wyjątkowych przypadkach, aby nie prowadziły do nadmiernej ingerencji w prywatność jednostki. Czwarta hipoteza zakłada, że wprowadzenie obowiązku przeprowadzania analizy wpływu na prywatność (DPIA) przed wdrożeniem systemów monitoringu w przestrzeni publicznej jest niezbędne, aby zminimalizować ryzyko naruszenia danych osobowych.

W realizacji celów niniejszej pracy zastosowano różnorodne metody badawcze, które pozwalają na szczegółową analizę problematyki uwarunkowań prawnych

monitoringu przestrzeni publicznej. Wybór odpowiednich metod był kluczowy, aby zapewnić pełne zrozumienie tematu uwarunkowań prawnych, wyzwań wynikających z rosnącego stosowania technologii nadzoru oraz kierunków zmian legislacyjnych. Główną metodą zastosowaną w pracy jest analiza dogmatyczno-prawna, której celem jest zbadanie obowiązujących przepisów prawa w zakresie monitoringu wizyjnego². Analiza ta pozwoliła na szczegółowe omówienie aktów prawnych, takich jak Konstytucja Rzeczypospolitej Polskiej, Ustawa o ochronie danych osobowych (RODO), Kodeks karny oraz przepisy prawa telekomunikacyjnego. Dogmatyczna analiza przepisów umożliwiła wyjaśnienie, jak polskie i unijne prawo odnoszą się do ochrony prywatności jednostek w kontekście monitoringu, a także określenie podstawowych obowiązków i ograniczeń nałożonych na podmioty stosujące monitoring.

Orzecznictwo polskich sądów oraz Europejskiego Trybunału Praw Człowieka stanowi ważne źródło informacji o praktycznej interpretacji przepisów prawnych dotyczących monitoringu. W ramach pracy przeanalizowano wybrane wyroki sądowe, które dotyczyły stosowania monitoringu w przestrzeni publicznej, w miejscach pracy oraz na posesjach prywatnych. Analiza orzecznictwa³ pozwoliła na identyfikację kluczowych problemów związanych z interpretacją przepisów, a także na zrozumienie, w jaki sposób sądy oceniają równowagę między prawem do prywatności a potrzebą zapewnienia bezpieczeństwa. Orzeczenia te dostarczają praktycznych wskazówek na temat ograniczeń w stosowaniu monitoringu i wyznaczają standardy ochrony prywatności jednostek. W celu zrozumienia teoretycznych aspektów monitoringu oraz wpływu technologii nadzoru na społeczeństwo zastosowano metodę analizy literatury przedmiotu⁴. Literatura naukowa, w tym prace autorów takich jak David Lyon, Gary T. Marx czy Katja Koskela, dostarczyła cennych informacji na temat koncepcji „społeczeństwa nadzorowanego” oraz zagrożeń wynikających z masowego nadzoru. Analiza literatury umożliwiła wyciągnięcie wniosków dotyczących społecznych konsekwencji rozwoju technologii monitoringu oraz była podstawą do sformułowania postulatów dotyczących przyszłych regulacji. Dobór powyższych metod badawczych umożliwił szczegółową analizę problematyki monitoringu wizyjnego w Polsce oraz zapewnił kompleksowe podejście do kwestii ochrony prywatności i potrzeb bezpieczeństwa publicznego. Dzięki zastosowaniu metod analizy dogmatyczno-prawnej, prawno-

² A.B. Zimny, *Analiza dogmatyczno-prawna jako metoda badawcza w prawie*, [w:] J. Kowalski (red.), *Metody badawcze w naukach prawnych*, Wyd. Prawnicze, Warszawa 2020, s. 45-58.

³ M. Zieliński, *Wykładnia prawa i analiza orzecznictwa jako metody badawcze w naukach prawnych*, Wyd. Wolters Kluwer, Warszawa 2018, s. 73-85.

⁴ K. Wojciechowski, *Metodologia badań prawnych: analiza literatury przedmiotu*, Wyd. C.H. Beck, Warszawa 2019, s. 102-115.

porównawczej, orzecznictwa, literatury przedmiotu, praca dostarcza pełniejszego obrazu uwarunkowań prawnych i społecznych, które determinują kształt i przyszłość uwarunkowań prawnych monitoringu w Polsce.

Ramy prawne monitoringu w Polsce

Monitoring wizyjny w przestrzeniach publicznych jest regulowany przez różne akty prawne, które wyznaczają zasady instalacji, funkcjonowania oraz przetwarzania danych osobowych gromadzonych przez kamery. Poniżej przedstawiono główne źródła prawa, które mają zastosowanie do monitoringu w Polsce:

1. Konstytucja Rzeczypospolitej Polskiej, jako najwyższy akt prawny, ustanawia fundamentalne prawa i wolności obywatelskie, w tym prawo do ochrony prywatności oraz ograniczenia w przetwarzaniu informacji na temat obywateli. Art. 47 Konstytucji RP: stanowi, że „każdy ma prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym”. W kontekście monitoringu miejskiego oznacza to, że obywatele mają prawo oczekiwać, że ich prywatność nie będzie naruszona przez nadmierne lub nieuzasadnione monitorowanie przestrzeni publicznej⁵. W świetle tego artykułu monitoring musi być prowadzony w sposób proporcjonalny, z zachowaniem zasady minimalizacji ingerencji w życie prywatne osób, które mogą być objęte nadzorem. Art. 51 Konstytucji RP: określa ograniczenia w gromadzeniu, przechowywaniu i udostępnianiu informacji o obywatelach, wskazując, że „nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby”. Artykuł ten odnosi się do monitoringu w zakresie przechowywania nagrań, co oznacza, że zbieranie i przetwarzanie danych przez systemy monitoringu powinno odbywać się jedynie w przypadkach ściśle określonych przez prawo, a ich przechowywanie powinno być ograniczone czasowo.
2. Rozporządzenie Ogólne o Ochronie Danych Osobowych (RODO), które obowiązuje we wszystkich krajach Unii Europejskiej, w tym w Polsce, reguluje przetwarzanie danych osobowych, również danych pochodzących z monitoringu wizyjnego. Podstawowe zasady przetwarzania danych osobowych: RODO wprowadza zasady dotyczące przetwarzania danych osobowych, takie jak legalność, przejrzystość, celowość, minimalizacja danych

⁵ M. Chmaj, *Wolności i prawa jednostki w Konstytucji RP*, Wyd. Wolters Kluwer, Warszawa 2014, s. 250-255.

oraz ograniczenie retencji. Dane osobowe uzyskane za pomocą monitoringu wizyjnego powinny być przetwarzane jedynie w sposób zgodny z celem, dla którego zostały zebrane⁶.

- a) Podstawa prawna przetwarzania: Przetwarzanie danych osobowych przez monitoring musi mieć uzasadnioną podstawę prawną, co najczęściej wiąże się z uzasadnionym interesem administratora lub potrzebą zapewnienia bezpieczeństwa publicznego⁷. W przypadku monitoringu prowadzonego przez podmioty prywatne, zgodność z RODO oznacza również konieczność uwzględnienia interesów osób, które mogą być objęte monitoringiem, oraz obowiązek informacyjny.
- b) Ochrona danych biometrycznych: RODO traktuje dane biometryczne, takie jak rozpoznawanie twarzy, jako szczególną kategorię danych osobowych, wymagając dodatkowych zabezpieczeń i wyraźnej zgody osoby monitorowanej, chyba że dane są przetwarzane na potrzeby zapobiegania przestępstwom przez uprawnione organy⁸.

Prawa osób monitorowanych: RODO zapewnia osobom monitorowanym szereg praw, takich jak prawo do informacji, prawo dostępu do danych, prawo do ich usunięcia lub ograniczenia przetwarzania. Oznacza to, że osoby mogą domagać się informacji o celach monitoringu oraz o tym, kto jest administratorem ich danych, a także żądać usunięcia danych, jeżeli monitoring nie spełnia wymogów prawnych.

Prawo telekomunikacyjne reguluje między innymi zasady dotyczące urządzeń rejestrujących, w tym kamer monitoringu w przestrzeniach publicznych.

Legalność stosowania urządzeń monitorujących: Prawo telekomunikacyjne określa zasady korzystania z urządzeń rejestrujących w kontekście komunikacji i ochrony danych osobowych. W Polsce obowiązują przepisy, które wymagają odpowiednich zgłoszeń i zezwoleń dla systemów monitoringu wykorzystywanych w określonych celach. Prawo to ma zastosowanie w szczególności do systemów monitoringu, które mogą być wykorzystywane przez władze publiczne, jak również przez operatorów prywatnych⁹.

⁶ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO), art. 5, Dz.Urz. UE L 119 z 4.5.2016, s. 1.

⁷ Tamże.

⁸ Tamże.

⁹ Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, Dz.U. z 2004 r. Nr 171, poz. 1800, z późn. zm., art. 156-159.

Kodeks karny wprowadza sankcje za nielegalne zdobywanie informacji, co obejmuje przypadki nielegalnego stosowania monitoringu wizyjnego. Art. 267 Kodeksu karnego przewiduje sankcje za bezprawne uzyskanie informacji poprzez nieautoryzowany dostęp do systemów informacyjnych, w tym urządzeń monitorujących¹⁰. Oznacza to, że monitoring prowadzony bez wymaganych zezwoleń lub z naruszeniem przepisów prawa może stanowić przestępstwo podlegające karze. Warto również zaznaczyć, że dowody zdobyte niezgodnie z przepisami, np. nagrania z nielegalnego monitoringu, mogą zostać uznane za niedopuszczalne w postępowaniu sądowym, chyba że sąd, kierując się zasadą proporcjonalności, zdecyduje się je dopuścić jako dowód pomocniczy w sytuacjach wyjątkowych – na rozważenie zasługuje kwestia wystawiania mandatów lub rozpoczynania spraw na podstawie nagrań osób prywatnych. Art. 168a Kodeksu postępowania karnego wskazuje, że dowód uzyskany z naruszeniem przepisów nie może być wykorzystany, chyba że wyłączenie takiego dowodu zagrażałoby interesowi wymiaru sprawiedliwości w sposób znaczący, np. w przypadkach poważnych przestępstw¹¹.

Rozporządzenie Prezesa Rady Ministrów z dnia 16 marca 2000 r, a także Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2019 r. w sprawie sposobu prowadzenia monitoringu wizyjnego określają szczegółowe zasady instalacji oraz użytkowania systemów monitoringu wizyjnego w przestrzeni publicznej.

Warunki instalacji kamer: Rozporządzenie określa, że kamery mogą być instalowane jedynie w miejscach, gdzie jest to uzasadnione koniecznością ochrony bezpieczeństwa publicznego, prewencji przestępstw lub ochrony mienia. Wymaga również odpowiedniego oznakowania obszarów objętych monitoringiem, tak aby obywatele mieli świadomość, że są obserwowani¹².

Przepisy dotyczące przechowywania nagrań: W celu ochrony prywatności osób nagranych przez kamery, rozporządzenie przewiduje zasady dotyczące przechowywania danych, nakładając obowiązek minimalizacji okresu ich przechowywania i usuwania nagrań po upływie określonego czasu, o ile nie są one potrzebne w postępowaniach prawnych¹³.

¹⁰ Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz.U. z 1997 r. Nr 88, poz. 553 z późn. zm., art. 267.

¹¹ Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego, Dz.U. z 1997 r. Nr 89, poz. 555 z późn. zm., art. 168a.

¹² Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2019 r. w sprawie sposobu prowadzenia monitoringu wizyjnego, Dz.U. z 2019 r., poz. 819, § 3-5.

¹³ Rozporządzenie Prezesa Rady Ministrów z dnia 16 marca 2000 r. w sprawie sposobu, trybu i form dokumentowania oraz przechowywania nagrań monitoringu wizyjnego, Dz.U. z 2000 r. Nr 25, poz. 309.

W Polsce monitorowanie przestrzeni publicznej jest również regulowane przez szereg innych przepisów i wytycznych, które uzupełniają ogólne ramy prawne. W kontekście monitorowania miejsc pracy przepisy kodeksu pracy przewidują, że pracodawca może stosować monitoring jedynie w celu zapewnienia bezpieczeństwa pracowników i ochrony mienia, a pracownicy muszą być informowani o stosowaniu kamer. Natomiast ustawa o ochronie osób i mienia określa zasady stosowania monitoringu przez firmy ochroniarskie, w tym wymóg posiadania licencji oraz obowiązek informowania osób o zakresie monitoringu.

Podsumowując, uwarunkowania prawne monitoringu w przestrzeni publicznej w Polsce opierają się na zasadach minimalizacji ingerencji w prywatność, transparentności i proporcjonalności działań. Przepisy te mają na celu ochronę praw obywatelskich w dobie coraz bardziej powszechnego monitoringu, zachowując jednocześnie możliwość stosowania technologii monitorujących do zapewnienia bezpieczeństwa publicznego.

Monitoring Miejski

Monitoring miejski jest nieodłącznym elementem współczesnych miast, mającym na celu poprawę bezpieczeństwa publicznego, zapobieganie przestępstwom oraz wspomaganie zarządzania przestrzenią miejską. Zastosowanie kamer w przestrzeniach publicznych wiąże się jednak z szeregiem wyzwań, w tym koniecznością pogodzenia dwóch wartości: zapewnienia bezpieczeństwa oraz ochrony prywatności obywateli. Według raportu Fundacji Panoptykon z 2012 roku, aż 89% spośród 217 badanych miast posiadało kamery finansowane z budżetu miejskiego, a 75% z nich miało zintegrowany system monitoringu miejskiego¹⁴. Ponadto zostały przeprowadzone w ośmiu polskich miastach badania, które wykazały, że monitoring miejski częściowo przyczynia się do zmniejszenia liczby przestępstw w badanych kategoriach, choć jego wpływ na straty spowodowane przestępczością jest mniej wyraźny¹⁵. Zastosowanie systemów monitoringu wizyjnego w przestrzeniach miejskich jest uzasadniane potrzebą ochrony mieszkańców oraz zapewnienia ich bezpieczeństwa. Kamery monitoringu są instalowane w miejscach szczególnie narażonych na przestępczość, takich jak centra miast, dworce kolejowe,

¹⁴ Fundacja Panoptykon, *Monitoring wizyjny w miastach powiatowych w Polsce – Raport z badań*, Warszawa 2012, s. 6-8, dostęp online: <https://panoptykon.org/sites/default/files/text/raport-z-badan-monitoringu-w-miastach-powiatowych.pdf>

¹⁵ K. Zając, M. Wójcik, *Monitoring wizyjny i jego wpływ na straty spowodowane przestępczością. Przykłady z wybranych polskich miast*, „Kwartalnik Studiów nad Przestępczością i Polityką Karną” 2020, nr 4, s. 67-85.

środki komunikacji miejskiej czy obszary o wysokim natężeniu ruchu pieszego. Badania wskazują, że obecność kamer może mieć efekt odstrasżający, zmniejszając skłonność do popełnienia przestępstwa w monitorowanym obszarze¹⁶. Według Davida Lyon'a, monitoring miejski może działać jako narzędzie prewencji, co jest szczególnie istotne w miejscach, gdzie interwencje służb są utrudnione ze względu na ograniczoną widoczność i rozproszenie przestrzenne¹⁷. Monitoring stanowi również narzędzie wsparcia dla służb porządkowych, takich jak policja, umożliwiając szybkie reagowanie na zagrożenia oraz ułatwiając identyfikację sprawców przestępstw. Dzięki integracji kamer z systemami analizy obrazu możliwe jest automatyczne wykrywanie podejrzanych zachowań, co znacznie skraca czas reakcji służb na potencjalne zagrożenia¹⁸.

Pomimo korzyści wynikających z monitoringu miejskiego, jego obecność w przestrzeniach publicznych wzbudza liczne kontrowersje, głównie z powodu potencjalnych naruszeń prywatności obywateli. D. Lyon w swojej pracy zwraca uwagę, że kamery monitoringu miejskiego, mimo że służą prewencji przestępczości, jednocześnie mogą przyczyniać się do erozji prywatności, ponieważ umożliwiają stały nadzór nad życiem codziennym jednostek¹⁹.

Koncepcja „społeczeństwa nadzorowanego” opisana przez Lyon'a zakłada, że obywatel, mając świadomość bycia obserwowanym, stopniowo traci poczucie prywatności, co może prowadzić do zmiany jego zachowań i wewnętrznej autocenzury. Problem ten ilustruje tzw. efekt panoptyczny, zaproponowany przez Michela Foucaulta, który opisuje mechanizm kontroli społecznej opartej na idei ciągłego nadzoru²⁰. W przypadku monitoringu miejskiego, efekt ten polega na tym, że jednostki w przestrzeni publicznej zaczynają dostosowywać swoje zachowanie, wiedząc, że mogą być obserwowane, co prowadzi do podporządkowania się regułom i normom społecznym. Obecność kamer w przestrzeni publicznej powoduje, że ludzie są mniej skłonni do podejmowania działań naruszających przepisy, takich jak przekraczanie prędkości, drobne akty wandalizmu czy kradzieże, ponieważ obawiają się konsekwencji wynikających z bycia nagranych. Jednostki przebywające w monitorowanych miejscach często starają się zachowywać zgodnie z oczekiwaniami społecznymi, unikając działań, które mogłyby zostać

¹⁶ J. Welsh, D. Farrington, *Effects of Closed-Circuit Television on Crime*, „The Annals of the American Academy of Political and Social Science”, vol. 587, Thousand Oaks, CA, SAGE Publications, 2003, s. 110-135.

¹⁷ D. Lyon, *Surveillance Studies: An Overview*, Polity Press, Cambridge 2007, s. 89-92.

¹⁸ K. Haggerty, R. Ericson, *The New Politics of Surveillance and Visibility*, Toronto, University of Toronto Press, 2006, s. 102-105.

¹⁹ D. Lyon, dz. cyt., s. 95-98.

²⁰ M. Foucault, *Nadzorować i karać: narodziny więzienia*, Wyd. Aletheia, Warszawa 1998, s. 207-213.

negatywnie odebrane, nawet jeśli nie są zabronione. Przykładem mogą być młodzi ludzie ograniczający spontaniczne zachowania na skwerach czy w parkach. Ponadto, w miejscach publicznych objętych monitoringiem, ludzie mogą unikać intymnych interakcji, takich jak wyrażanie uczuć czy wymiana poufnych informacji, w obawie przed rejestracją ich zachowań. Kamery monitorujące ruch drogowy, takie jak systemy odcinkowego pomiaru prędkości, również wywołują efekt panoptyczny – kierowcy, wiedząc, że mogą być obserwowani, przestrzegają przepisów i poruszają się zgodnie z ograniczeniami prędkości. Monitoring miejski, formalnie służący bezpieczeństwu, wpływa więc na kształtowanie zachowań społecznych zwiększając samodyscyplinę i autocenzurę jednostek, które w odpowiedzi na obecność kamer podporządkowują się normom społecznym – tym samym ogranicza wolność jednostki. W związku z naruszeniami prywatności, jakie może powodować monitoring miejski, konieczne jest stosowanie odpowiednich ograniczeń prawnych, aby zapewnić równowagę między bezpieczeństwem a ochroną prywatności. RODO nakłada na administratorów monitoringu obowiązek minimalizacji danych osobowych, co oznacza, że monitoring powinien być stosowany tylko w miejscach i w czasie, gdy jest to rzeczywiście niezbędne²¹. Przepisy te mają na celu ograniczenie zakresu monitoringu, tak aby zapewnić zgodność z zasadą proporcjonalności oraz prawnymi wymogami w zakresie ochrony danych osobowych.

W kontekście przestrzeni publicznej przepisy unijne oraz polskie nakładają obowiązek transparentności w stosowaniu kamer monitorujących. W praktyce oznacza to, że obywatele powinni być informowani o obecności kamer za pomocą odpowiednich znaków oraz informacji dostępnych publicznie²². Takie podejście jest zgodne z zaleceniami Europejskiego Trybunału Praw Człowieka, który w kilku swoich wyrokach wskazał na konieczność jasnego określenia celów monitoringu i zapewnienia odpowiednich zabezpieczeń, aby zapobiec nadużyciom.

Przykładem kraju, który podjął istotne kroki w zakresie regulacji monitoringu publicznego, jest Wielka Brytania, gdzie wprowadzono specjalne wytyczne dla organów publicznych dotyczące stosowania monitoringu, zwane *Surveillance Camera Code of Practice*²³. Kodeks ten wymaga, aby każda instalacja kamer była

²¹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO), art. 5 ust. 1 lit. c, Dz.Urz. UE L 119 z 4.05.2016 r., s. 1.

²² Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO), art. 12 oraz art. 13, Dz.Urz. UE L 119 z 4.05.2016 r., s. 1.

²³ *Surveillance Camera Code of Practice*, <https://www.gov.uk/government/publications/surveillance-camera-code-of-practice> [dostęp: 03.08.2024 r.].

uzasadniona, a jej cele jasno określone, co ma na celu ograniczenie nadzoru jedynie do miejsc, gdzie jest to absolutnie konieczne. Podobne standardy są przyjmowane w Stanach Zjednoczonych, gdzie wprowadzono przepisy wymagające, aby instalacja kamer monitorujących była poprzedzona analizą wpływu na prywatność, a ich stosowanie ograniczone do zidentyfikowanych obszarów zagrożenia. W miastach takich jak San Francisco czy Portland wprowadzono nawet zakaz używania technologii rozpoznawania twarzy w przestrzeniach publicznych, aby chronić prywatność obywateli przed potencjalnymi nadużyciami ze strony organów ścigania²⁴.

Monitoring miejski jest skutecznym narzędziem w zapobieganiu przestępczości i poprawie bezpieczeństwa, jednak jego obecność w przestrzeniach publicznych wymaga odpowiednich regulacji prawnych. Zastosowanie kamer monitorujących powinno być ograniczone do miejsc szczególnie narażonych na przestępczość, a obywatele powinni być informowani o ich obecności. Konieczne jest również stosowanie zabezpieczeń technologicznych, które umożliwią anonimowość osób w przypadku, gdy monitoring nie jest wymagany w celach prewencyjnych lub ścigania przestępstw.

Monitoring przestrzeni publicznej przez osoby prywatne

Monitoring wizyjny stosowany przez właścicieli nieruchomości prywatnych staje się coraz bardziej powszechny, zarówno w przypadku posesji prywatnych, jak i firm²⁵. Celem takiego monitoringu jest ochrona mienia, zapewnienie bezpieczeństwa właścicieli oraz prewencja w zakresie kradzieży i wandalizmu. W kontekście prawnym stosowanie monitoringu prywatnego niesie ze sobą szczególne wyzwania, zwłaszcza gdy kamery rejestrują także fragmenty przestrzeni publicznej, takie jak chodniki, ulice czy sąsiednie posesje. W związku z tym istnieje konieczność precyzyjnego uregulowania zasad monitoringu prywatnego, aby zrównoważyć ochronę prywatności osób trzecich z prawem właścicieli do zabezpieczenia swojego mienia.

W Polsce obowiązujące przepisy prawne regulujące monitoring prywatny opierają się przede wszystkim na Ogólnym Rozporządzeniu o Ochronie Danych (RODO) oraz na krajowych przepisach dotyczących ochrony danych osobowych²⁶.

²⁴ *Electronic Frontier Foundation, Surveillance and Privacy Standards in the United States*, <https://www.eff.org/issues/surveillance> [dostęp: 03.08.2024 r.].

²⁵ M. Chmaj, *Wolności i prawa jednostki...*, dz. cyt., s. 260-263.

²⁶ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO), Dz.Urz. UE L 119 z 4.05.2016 r., s. 1.

Według przepisów RODO, nagrania z monitoringu, które mogą pozwolić na identyfikację osób, są uznawane za dane osobowe, co oznacza, że ich przetwarzanie podlega szczególnym ograniczeniom. Administrator danych, czyli właściciel systemu monitoringu, ma obowiązek spełniać wymogi związane z transparentnością, legalnością oraz minimalizacją przetwarzania danych²⁷.

Zgodnie z RODO, właściciel monitoringu musi poinformować osoby znajdujące się w zasięgu kamer o ich działaniu, co najczęściej realizuje się za pomocą tabliczek lub znaków informacyjnych. Oznacza to, że właściciel prywatny, który instaluje kamery w pobliżu przestrzeni publicznej, ma obowiązek jasno komunikować cel monitoringu oraz udostępniać informacje o administratorze danych, czyli osobie odpowiedzialnej za przetwarzanie nagrań. RODO nakłada także obowiązek minimalizacji zakresu monitoringu²⁸, co oznacza, że kamery nie powinny rejestrować więcej przestrzeni, niż jest to konieczne do realizacji celu monitoringu. W praktyce oznacza to, że kamery powinny być skierowane wyłącznie na obszar należący do właściciela, tak aby zminimalizować ryzyko rejestrowania osób postronnych.

Pomimo, że właściciele prywatnych nieruchomości mają prawo do ochrony swojego mienia, monitoring, który obejmuje przestrzeń publiczną lub fragmenty posesji sąsiadów, może naruszać prywatność osób trzecich. Literatura prawnicza oraz badania naukowe wskazują, że monitoring wkraczający w przestrzeń sąsiadów lub przestrzeń publiczną rodzi liczne kontrowersje i wymaga szczególnej uwagi legislacyjnej²⁹. Możliwość rejestrowania osób bez ich zgody, nawet w przestrzeni publicznej, stawia pytania o zakres prawa do prywatności w przestrzeni publicznej oraz o granice, do jakich właściciele prywatnych nieruchomości mogą stosować monitoring³⁰.

Orzecznictwo sądowe wskazuje, że w przypadkach, gdy monitoring prywatny obejmuje przestrzeń publiczną, osoby postronne mogą mieć prawo do ochrony swoich danych. Przykładowo, w orzeczeniu niemieckiego Federalnego Trybunału Konstytucyjnego wskazano, że monitoring prywatny powinien być ograniczony do przestrzeni prywatnej właściciela i nie powinien obejmować miejsc ogólnodostępnych³¹.

²⁷ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679, art. 5 ust. 1 lit. a-c, dotyczący zasad przetwarzania danych osobowych.

²⁸ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679, art. 5 ust. 1 lit. c.

²⁹ A. Mednis, *Prawo do prywatności a nowe technologie*, C.H. Beck, Warszawa 2018, s. 145-150.

³⁰ K. Wojciechowski, *Prawo do prywatności w przestrzeni publicznej: nowe wyzwania*, Wyd. Naukowe UAM, Poznań 2019, s. 78-81.

³¹ Wyrok Federalnego Trybunału Konstytucyjnego Niemiec z dnia 15 grudnia 2011 r., BVerfG, 1 BvR 2027/02, dotyczący zakresu monitoringu prywatnego w przestrzeni publicznej.

Wytyczne RODO oraz krajowe przepisy dotyczące ochrony danych osobowych wskazują na konieczność stosowania monitoringu prywatnego w sposób, który nie narusza prywatności osób trzecich. W związku z tym właściciele systemów monitoringu prywatnego mają obowiązek przestrzegać zasady przetwarzania danych, takiej jak: przechowywanie nagrań z monitoringu tylko przez określony czas. Po jego upływie powinny zostać usunięte lub zanonimizowane, jeśli nie są już potrzebne. Przykładowo, rekomenduje się, aby dane były przechowywane maksymalnie przez 30 dni, chyba że są one niezbędne do celów dowodowych w przypadku zaistnienia incydentu³². Ponadto obywatele powinni być informowani o istnieniu monitoringu oraz celu jego stosowania. RODO wymaga od administratora danych udostępnienia informacji o przetwarzaniu danych, co w kontekście monitoringu oznacza konieczność umieszczenia wyraźnych informacji o kamerach i ich administratorze.

W literaturze przedmiotu wskazuje się, że właściciele nieruchomości prywatnych, stosując monitoring, powinni wykazać szczególną staranność w zakresie przestrzegania przepisów prawa, aby uniknąć potencjalnych nadużyć. Przykładowo, Koskela wskazuje, że monitoring, który obejmuje przestrzeń sąsiadów, powinien być ograniczony do absolutnego minimum, aby uniknąć przypadkowego naruszenia prywatności³³.

Firmy, które prowadzą monitoring na terenie swojej posesji, także muszą spełniać wymogi RODO i polskich przepisów o ochronie danych osobowych³⁴.

Celem takiego monitoringu jest zazwyczaj ochrona mienia i zapewnienie bezpieczeństwa pracownikom oraz klientom. Podobnie jak w przypadku osób prywatnych, monitoring firmowy nie powinien obejmować przestrzeni publicznej, takiej jak ulice, chodniki czy sąsiednie posesje.

Przykłady z literatury wskazują, że firmy, które decydują się na monitoring³⁵, powinny zainstalować kamery w sposób umożliwiający rejestrowanie wyłącznie obszarów znajdujących się na terenie zakładu. Przekroczenie tej granicy może zostać uznane za naruszenie prawa, co znalazło swoje potwierdzenie w orzecznictwie sądowym. W sprawie jednej z niemieckich firm Sąd Najwyższy wskazał, że

³² Urząd Ochrony Danych Osobowych, Wytyczne dotyczące przetwarzania danych z monitoringu wizyjnego, <https://uodo.gov.pl/wytyczne-monitoring> [dostęp: 01.11.2024 r.].

³³ K. Koskela, *Urban Surveillance and Spatial Privacy: Monitoring in the Neighbourhood*, Routledge, London 2009, s. 112-115.

³⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO), Dz.Urz. UE L 119 z 4.05.2016 r., art. 5.

³⁵ K. Koskela, dz. cyt.

monitoring obejmujący parking publiczny przylegający do zakładu narusza prawo do prywatności osób postronnych³⁶.

Firmy odpowiadają za zgodność monitoringu z przepisami RODO, co obejmuje między innymi zapewnienie odpowiednich procedur ochrony danych oraz dostęp do nagrań jedynie dla uprawnionych osób³⁷. W przypadku naruszenia prawa, firmy mogą zostać obciążone karami finansowymi oraz innymi sankcjami administracyjnymi³⁸.

Monitoring prywatny i firmowy stanowi istotny element w zabezpieczeniu mienia i zapewnieniu bezpieczeństwa. Jego stosowanie wiąże się jednak z koniecznością zachowania proporcjonalności oraz poszanowania prywatności osób postronnych. Przepisy RODO i polskie przepisy o ochronie danych osobowych wymagają, aby monitoring prywatny był stosowany w sposób ograniczony, przejrzysty i zgodny z zasadą minimalizacji danych.

W świetle przepisów prawa oraz literatury przedmiotu, stosowanie monitoringu prywatnego powinno być ściśle ograniczone do przestrzeni należącej do właściciela nieruchomości, tak aby uniknąć przypadkowego nagrywania osób trzecich, które mogą poruszać się po przestrzeni publicznej lub po posesjach sąsiadujących. Przestrzeganie tych wymagań jest kluczowe dla zrównoważenia prawa właścicieli do ochrony mienia z prawem obywateli do prywatności.

Podsumowując, monitoring przestrzeni publicznej przez właścicieli prywatnych nieruchomości oraz firmy wymaga szczególnej staranności w zakresie przestrzegania zasad wynikających z prawa ochrony danych osobowych. Właściele systemów monitoringu muszą stosować odpowiednie środki ochrony, aby zminimalizować ryzyko naruszenia prywatności, co oznacza konieczność precyzyjnego ustawienia kamer, aby rejestrowały jedynie niezbędny obszar. W przypadku firm obowiązek ten dodatkowo wiąże się z koniecznością wdrażania polityki zgodności z RODO oraz zapewnienia odpowiednich procedur przechowywania i dostępu do nagrań.

Postulaty legislacyjne

Wraz z rozwojem technologii monitoringu wizyjnego, takich jak kamery o wysokiej rozdzielczości, systemy rozpoznawania twarzy oraz analityka wideo, istnieje rosnące zapotrzebowanie na uregulowanie zasad, na jakich monitoring jest stoso-

³⁶ Wyrok Federalnego Trybunału Konstytucyjnego Niemiec z dnia 23 lutego 2012 r., BVerfG, 1 BvR 249/11.

³⁷ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679, art. 32.

³⁸ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679, art. 83.

wany zarówno w przestrzeniach publicznych, jak i prywatnych³⁹. Regulacje prawne powinny zapewniać równowagę między potrzebą zapewnienia bezpieczeństwa publicznego a ochroną prywatności i praw obywatelskich, szczególnie w kontekście zaostrzającej się debaty wokół wpływu nadzoru na wolność jednostki⁴⁰.

Z uwagi na fakt, że coraz więcej właścicieli prywatnych nieruchomości, takich jak domy jednorodzinne czy firmy, decyduje się na instalację systemów monitoringu, konieczne jest wprowadzenie przepisów, które jasno określą granice prywatnego nadzoru w odniesieniu do przestrzeni publicznej i prywatnej⁴¹. Przykłady z literatury sugerują, że brak jednoznacznych regulacji w tym zakresie może prowadzić do licznych sporów prawnych, a nawet naruszeń praw obywatelskich⁴².

W tym kontekście proponuje się następujące kierunki regulacji:

1. W przypadku monitoringu prywatnego wymagane powinno być stosowanie oznakowania, informującego osoby przebywające na danej posesji o działaniu systemu kamer. Właściciele powinni również udostępniać informacje o administratorze danych oraz celu monitoringu, co jest zgodne z wymogami RODO. Transparentność jest kluczowa, aby zapewnić, że osoby monitorowane są świadome obecności kamer i celów, dla których są one stosowane⁴³.
2. Nagrania z prywatnego monitoringu powinny być przechowywane jedynie przez okres niezbędny do realizacji celów ochrony mienia, np. przez maksymalnie 30 dni, po czym powinny zostać usunięte lub zanonimizowane. Wprowadzenie standardów dotyczących retencji danych pozwoliłoby zminimalizować ryzyko nadużycia danych.
3. W przypadku, gdy nagrania z monitoringu są wykorzystywane w postępowaniach prawnych lub jako dowód w przypadku przestępstw, właściciele systemów monitoringu powinni mieć obowiązek zgłaszania takiego wykorzystania do odpowiednich organów. Taki wymóg zapewni większą kontrolę nad wykorzystywaniem nagrań i pomoże zapobiegać potencjalnym nadużyciom w zakresie ochrony prywatności.
4. Monitoring w przestrzeniach publicznych, zwłaszcza gdy jest stosowany przez władze lokalne, rodzi jeszcze większe wyzwania z punktu widzenia praw obywatelskich i prywatności⁴⁴. Ze względu na szeroki zasięg kamer monitorujących

³⁹ D. Lyon, *Surveillance Studies: An Overview*, Polity Press, Cambridge 2007, s. 138-140.

⁴⁰ M. Chmaj, dz. cyt., s. 260-263.

⁴¹ K. Wojciechowski, dz. cyt., s. 45-48.

⁴² A. Mednis, dz. cyt., s. 145-150.

⁴³ Tamże.

⁴⁴ D. Lyon, dz. cyt., s. 140-143.

przestrzenie publiczne, takie jak parki, ulice czy centra miast, niezbędne jest, aby ustawodawca określił szczegółowe zasady stosowania monitoringu, które uwzględniają najnowsze technologie oraz potrzebę ochrony prywatności⁴⁵. Proponowane kierunki regulacji:

- Systemy rozpoznawania twarzy w przestrzeni publicznej powinny być stosowane tylko w szczególnych przypadkach, takich jak zapobieganie przestępstwom terrorystycznym, i to wyłącznie na podstawie wyraźnej podstawy prawnej oraz zgody odpowiednich organów sądowych⁴⁶. Tego rodzaju systemy mogą w znacznym stopniu ingerować w prywatność obywateli i powinny być stosowane z zachowaniem zasady proporcjonalności oraz minimalizacji danych.
- Organy stosujące monitoring publiczny powinny być zobowiązane do przeprowadzenia analizy wpływu na prywatność (*Data Protection Impact Assessment*, DPIA) przed wdrożeniem systemu monitoringu⁴⁷. Analiza ta powinna uwzględniać potencjalne ryzyko dla prywatności obywateli, a także sugerować środki minimalizujące ewentualne negatywne skutki. Tego rodzaju analizy są już wymagane przez RODO dla systemów o wysokim ryzyku ingerencji w prywatność i powinny być standardem również w przypadku monitoringu publicznego.
- Podobnie jak w przypadku monitoringu prywatnego, monitoring publiczny powinien być realizowany w sposób przejrzysty, z odpowiednimi oznaczeniami oraz dostępem do informacji na temat administratora danych i celu monitoringu⁴⁸. Organy publiczne powinny informować obywateli o lokalizacji kamer, a także umożliwić im dostęp do informacji na temat sposobu przetwarzania ich danych.
- Zaleca się wprowadzenie obowiązku przeprowadzania regularnych audytów systemów monitoringu publicznego przez niezależne organy nadzorcze. Audyty te mogłyby oceniać skuteczność systemów monitoringu, ich zgodność z przepisami o ochronie danych oraz monitorować przestrzeganie zasady minimalizacji⁴⁹. Audyty miałyby również na celu zapewnienie,

⁴⁵ M. Chmaj, op. cit., s. 255-257.

⁴⁶ M. Smith, *Facial Recognition and Privacy: Legal Standards in Public Spaces*, Routledge, London 2021, s. 105-108.

⁴⁷ K. Koskela, *Surveillance and the Right to Privacy: Urban Contexts*, Palgrave Macmillan, New York 2017, s. 120-125.

⁴⁸ D. Lyon, *The Culture of Surveillance: Watching as a Way of Life*, Polity Press, Cambridge 2018, s. 83-87.

⁴⁹ J. Nowak, *Nadzór i kontrola w systemach monitoringu publicznego*, Wyd. Prawnicze, Warszawa 2020, s. 190-195.

że kamery monitorujące nie są wykorzystywane do nieuzasadnionego nadzoru nad obywatelami.

Orzecznictwo

Analiza orzecznictwa sądowego w zakresie monitoringu wizyjnego w przestrzeni publicznej oraz prywatnej dostarcza cennych wskazówek dotyczących interpretacji przepisów prawa w kontekście ochrony prywatności i bezpieczeństwa publicznego. Poniżej przedstawiono wybrane orzeczenia polskich sądów, które ilustrują kluczowe aspekty prawne związane z monitoringiem.

- Wyrok Sądu Apelacyjnego w Warszawie z dnia 6 czerwca 2014 r. (sygn. akt VI ACa 1490/13).

W tej sprawie powódka zarzuciła naruszenie dóbr osobistych przez sąsiada, który zainstalował kamery monitoringu skierowane na jej posesję. Sąd Apelacyjny uznał, że takie działanie stanowi naruszenie prawa do prywatności i nakazał demontaż kamer oraz zapłatę zadośćuczynienia. Orzeczenie to podkreśla, że monitoring prywatny nie może ingerować w sferę prywatności osób trzecich bez ich zgody.

- Wyrok Naczelnego Sądu Administracyjnego w Warszawie z dnia 11 grudnia 2018 r. (sygn. akt I OSK 1825/18).

Sprawa dotyczyła skargi na decyzję organu administracyjnego, który odmówił udostępnienia nagrań z monitoringu miejskiego. NSA stwierdził, że nagrania te stanowią informację publiczną i powinny być udostępniane na wniosek, o ile nie naruszają prywatności osób trzecich. Wyrok ten wskazuje na konieczność wyważenia prawa do informacji publicznej z ochroną danych osobowych.

- Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 17 stycznia 2019 r. (sygn. akt II SA/Wa 1309/18).

W tej sprawie sąd rozpatrywał legalność monitoringu wizyjnego w miejscu pracy. WSA uznał, że pracodawca ma prawo stosować monitoring w celu zapewnienia bezpieczeństwa, jednak musi spełnić określone warunki, takie jak poinformowanie pracowników o jego stosowaniu oraz zapewnienie, że monitoring nie narusza ich prywatności.

- Wyrok Sądu Najwyższego w Warszawie z dnia 25 kwietnia 2019 r. (sygn. akt II CSK 51/18).

Sąd Najwyższy rozpatrywał sprawę dotyczącą monitoringu wizyjnego w budynku mieszkalnym. Stwierdził, że wspólnota mieszkaniowa ma prawo instalować kamery w częściach wspólnych budynku, pod warunkiem że nie narusza to prywatności mieszkańców i służy zapewnieniu bezpieczeństwa. Orzeczenie to podkreśla znaczenie zgody mieszkańców oraz transparentności w stosowaniu monitoringu.

- Wyrok Sądu Apelacyjnego w Gdańsku z dnia 30 października 2019 r. (sygn. akt V ACa 440/19).

W tej sprawie powódka zarzuciła naruszenie dóbr osobistych przez sąsiada, który zainstalował kamery monitoringu obejmujące jej posesję. Sąd Apelacyjny uznał, że takie działanie stanowi naruszenie prawa do prywatności i nakazał demontaż kamer oraz zapłatę zadośćuczynienia. Orzeczenie to podkreśla, że monitoring prywatny nie może ingerować w sferę prywatności osób trzecich bez ich zgody.

- Wyrok Sądu Apelacyjnego w Warszawie z dnia 17 sierpnia 2016 r. (sygn. akt VI ACa 839/15).

Sprawa dotyczyła konfliktu między sąsiadami, gdzie jeden z nich zainstalował kamery monitoringu skierowane na posesję drugiego. Sąd Apelacyjny uznał, że takie działanie narusza prawo do prywatności i nakazał usunięcie kamer. Orzeczenie to wskazuje na konieczność poszanowania prywatności sąsiadów przy instalacji systemów monitoringu.

- Wyrok Naczelnego Sądu Administracyjnego z dnia 11 grudnia 2018 r. (sygn. akt I OSK 1825/18).

Sprawa dotyczyła skargi na decyzję organu administracyjnego, który odmówił udostępnienia nagrań z monitoringu miejskiego. NSA stwierdził, że nagrania te stanowią informację publiczną i powinny być udostępniane na wniosek, o ile nie naruszają prywatności osób trzecich. Wyrok ten wskazuje na konieczność wyważenia prawa do informacji publicznej z ochroną danych osobowych.

- Wyrok Europejskiego Trybunału Praw Człowieka z dnia 28 czerwca 2007 r. w sprawie Vukota-Bojic przeciwko Szwajcarii (skarga nr 61838/10)

Choć nie jest to orzeczenie polskiego sądu, warto przytoczyć wyrok ETPC, który uznał, że potajemne nagrywanie osoby w przestrzeni publicznej przez prywatną firmę ubezpieczeniową stanowi naruszenie prawa do prywatności. Orzeczenie to ma znaczenie również w kontekście polskiego prawa, wskazując na konieczność poszanowania prywatności nawet w przestrzeni publicznej.

Sądy konsekwentnie podkreślają, że monitoring wizyjny nie może naruszać prawa do prywatności osób trzecich. Zarówno w kontekście monitoringu prywatnego, jak i publicznego, istnieje obowiązek informowania osób objętych monitoringiem o jego stosowaniu. Stosowanie monitoringu musi być proporcjonalne do celu, któremu ma służyć, i nie może prowadzić do nadmiernej ingerencji w sferę prywatności. W przypadkach monitoringu w przestrzeniach współdzielonych, takich jak budynki mieszkalne, wymagana jest zgoda osób, których monitoring dotyczy.

Podsumowanie

Monitoring wizyjny w Polsce i na świecie jest coraz szerzej stosowany jako narzędzie zapewniające bezpieczeństwo publiczne, zapobiegające przestępczości oraz wspierające zarządzanie przestrzenią publiczną. Korzyści wynikające z obecności kamer w miejscach publicznych, takich jak parki, ulice, czy centra miast, są jednak obciążone znaczącymi wyzwaniami z zakresu ochrony praw obywatelskich, a zwłaszcza prawa do prywatności. Problematyka monitoringu w przestrzeni publicznej, zarówno tej administrowanej przez organy państwowe, jak i stosowanej przez osoby prywatne, stała się istotnym zagadnieniem badawczym, mającym na celu poszukiwanie równowagi między potrzebami bezpieczeństwa a ochroną prywatności jednostek.

Regulacje prawne monitoringu w Polsce są oparte na przepisach konstytucyjnych, ustawach krajowych oraz aktach prawa Unii Europejskiej, takich jak RODO, które określają obowiązki administratorów danych w zakresie minimalizacji danych, proporcjonalności działań oraz obowiązku informacyjnego. Zgodnie z tymi regulacjami, stosowanie monitoringu powinno być ograniczone do miejsc rzeczywiście wymagających nadzoru. Kamery monitoringu powinny być ustawione tak, aby nie obejmować przestrzeni prywatnej innych osób, a nagrania przechowywane jedynie przez okres niezbędny do realizacji celów bezpieczeństwa.

Orzecznictwo sądowe w Polsce oraz Europejskiego Trybunału Praw Człowieka potwierdza konieczność przestrzegania zasady proporcjonalności i minimalizacji. Wyroki sądowe wielokrotnie wskazywały na naruszenia prywatności wynikające z monitoringu wykraczającego poza przestrzeń należącą do właściciela systemu, czego przykładem są przypadki monitoringu obejmującego posesje sąsiadów lub miejsca publiczne. Decyzje sądów w sprawach dotyczących monitoringu prywatnego i publicznego uwypuklają wymóg zgody osób, których dane mogą być przetwarzane, oraz podkreślają konieczność przejrzystości w informowaniu o monitoringu.

Pomimo uzasadnionych korzyści związanych z monitoringiem, jego obecność w przestrzeni publicznej wiąże się z ryzykiem naruszenia prywatności, co w literaturze przedmiotu bywa porównywane do efektu panoptycznego, czyli stałego nadzoru, który może wpływać na samodyscyplinę i autocenzurę jednostek. Monitoring miejski w szczególności prowadzi do ukształtowania zachowań społecznych poprzez świadomość nadzoru, co w dłuższym okresie może wywoływać negatywne efekty społeczne. W odpowiedzi na te wyzwania postulaty *de lege ferenda* wskazują na potrzebę ustanowienia precyzyjnych zasad monitoringu, zwłaszcza w odniesieniu do systemów rozpoznawania twarzy i analityki wideo, które mają potencjalnie największy wpływ na prywatność jednostek. Zasadnicze znaczenie mają również propozycje dotyczące regularnych audytów, które pozwoliłyby na ocenę zgodności systemów monitoringu z przepisami o ochronie danych osobowych. Podjęcie kroków legislacyjnych mających na celu zapewnienie transparentności, ograniczenia czasu retencji danych oraz uregulowania stosowania systemów monitoringu w określonych sytuacjach może przyczynić się do zwiększenia akceptacji społecznej dla monitoringu oraz utrzymania równowagi między potrzebami bezpieczeństwa a ochroną prywatności.

Bibliografia

- Chmaj M., *Wolności i prawa jednostki w Konstytucji RP*, Wyd. Wolters Kluwer, Warszawa 2014.
- Electronic Frontier Foundation, *Surveillance and Privacy Standards in the United States*, <https://www EFF.org/issues/surveillance> [dostęp: 03.08.2024 r.].
- Fundacja Panoptikon, *Monitoring wizyjny w miastach powiatowych w Polsce – Raport z badań*, Warszawa 2012, dostęp online: <https://panoptikon.org/sites/default/files/text/raport-z-badan-monitoringu-w-miastach-powiatowych.pdf>
- Haggerty K., Ericson R., *The New Politics of Surveillance and Visibility*, University of Toronto Press, Toronto 2006.
- Koskela K., *Urban Surveillance and Spatial Privacy: Monitoring in the Neighbourhood*, Routledge, London 2009.
- Lyon D., *Surveillance Studies: An Overview*, Polity Press, Cambridge 2007.
- Mednis A., *Prawo do prywatności a nowe technologie*, C.H. Beck, Warszawa 2018.
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2019 r. w sprawie sposobu prowadzenia monitoringu wizyjnego, Dz.U. z 2019 r., poz. 819.
- Surveillance Camera Code of Practice*, <https://www.gov.uk/government/publications/surveillance-camera-code-of-practice> [dostęp: 03.08.2024 r.].
- Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne, Dz.U. z 2004 r. Nr 171, poz. 1800, z późn. zm.
- Wyrok Federalnego Trybunału Konstytucyjnego Niemiec z dnia 15 grudnia 2011 r., BVerfG, 1 BvR 2027/02.

Wyrok Naczelnego Sądu Administracyjnego z dnia 11 grudnia 2018 r., sygn. akt I OSK 1825/18, dostęp online w bazie orzeczeń NSA: <https://orzeczenia.nsa.gov.pl>

Wyrok Sądu Apelacyjnego w Gdańsku z dnia 30 października 2019 r., sygn. akt V ACa 440/19.

Wyrok Sądu Apelacyjnego w Warszawie z dnia 6 czerwca 2014 r., sygn. akt VI ACa 1490/13, dostęp w bazie orzeczeń: <https://orzeczenia.ms.gov.pl>

Wyrok Sądu Najwyższego z dnia 25 kwietnia 2019 r., sygn. akt II CSK 51/18.

Bezpieczeństwo w cyberprzestrzeni: nowe technologie a cyberprzestępczość

Alicja ZAWORSKA

Akademia Wymiaru Sprawiedliwości w Warszawie

ORCID: 0009-0000-3935-0268

Streszczenie. Wraz z dynamicznym wzrostem liczby użytkowników Internetu oraz ekspansją nowych technologii cyberprzestrzeń stała się obszarem niosącym wiele potencjalnych zagrożeń. Technologiczne innowacje, mimo swych niezaprzeczalnych korzyści, generują ryzyko m.in. kradzieży danych osobowych, oszustw finansowych, ataków *ransomware*, phishingu oraz innych form cyberprzestępstw, których nieustannie przybywa. W obliczu takich wyzwań konieczne staje się nie tylko stosowanie zaawansowanych technologii ochronnych, ale również opracowanie i implementacja odpowiednich rozwiązań prawnych, które umożliwią skuteczne przeciwdziałanie oraz ściganie przestępców działających w cyberprzestrzeni. Regulacje prawne dotyczące (między innymi) funkcjonowania sztucznej inteligencji oraz coraz bardziej złożonych metod popełniania przestępstw w Internecie, wymagają od prawodawcy ciągłych modyfikacji i udoskonaleń w celu ochrony interesów obywateli. W artykule omówiono najważniejsze wyzwania związane z nowymi technologiami oraz przedstawiono kluczowe zmiany prawne, mające na celu zabezpieczenie użytkowników Internetu przed zagrożeniami związanymi z rosnącą cyberprzestępczością. Ponadto w artykule zaprezentowano informacje na temat nowych jednostek służb państwowych powołanych do przeciwdziałania cyberprzestępczości, ze wskazaniem ich miejsca w strukturach organów bezpieczeństwa państwa. Wzrastająca skala cyberprzestępczości wymaga kompleksowego podejścia do ochrony zarówno w aspekcie technologicznym, jak i prawnym. Wobec tego konieczne staje się również nieustanne dostosowywanie regulacji prawnych, zwłaszcza w kontekście funkcjonowania sztucznej inteligencji oraz nowoczesnych metod cyberataków, aby sprostać złożoności i dynamice współczesnych zagrożeń.

Słowa kluczowe: prawo, cyberprzestrzeń, cyberprzestępczość, nowe technologie, sztuczna inteligencja

Wstęp

W XXI wieku Internet stał się jednym z kluczowych narzędzi, bez którego trudno wyobrazić sobie dziś życie. W 1996 roku Amerykański poeta i eseista John Perry Barlow w swojej „Deklaracji Niepodległości Cyberprzestrzeni” (*A Declaration of the Independence of Cyberspace*) stwierdził:

Tworzymy świat, w którym każdy, niezależnie od miejsca, może wyrażać swoje przekonania, bez względu na to, jak są one odosobnione, bez obawy przed zmuszaniem do milczenia czy konformizmu. Wasze koncepcje prawne dotyczące własności, ekspresji, tożsamości, ruchu i kontekstu nie mają tu zastosowania. Wszystkie są oparte na materii, a w naszym świecie nie ma materii¹.

Narzędzia dostępne w cyberprzestrzeni mają olbrzymi zasięg i potencjał, są dziś istotną częścią życia, a możliwość przeprowadzania za jego pośrednictwem spraw urzędowych, finansowych czy biznesowych pokazuje jego znaczenie. Internet oferuje nieograniczony dostęp do wiedzy, ułatwia komunikowanie się, wspiera rozwój zarówno gospodarczy jak i technologiczny. Jednak mimo korzyści jakie przynosi, stanowi również źródło licznych zagrożeń, takich jak cyberprzestępczość czy dezinformacja. Niesie za sobą również ryzyko uzależnień. Niezbędne jest zrozumienie, jak bezpiecznie korzystać z Internetu oraz jakie wyzwania stoją przed społeczeństwem w erze cyfrowej transformacji i rozwoju technologicznego, a także jakie metody stosowane są wśród cyberprzestępców. Dlatego celem niniejszego opracowania jest analiza aktów prawnych i regulacji a także dyrektyw Unii Europejskiej w zakresie cyberbezpieczeństwa oraz analiza literatury oraz raportów polskich służb działających w cyberprzestrzeni ukazujących identyfikację trendów i ocenę efektywności działań prewencyjnych w sieci.

Spojrzenie na Internet zarówno w kontekście historycznym, jak i współczesnym pokazuje, że narzędzie to stanowi istotny element badań nad wpływem technologii na życie społeczne i na rozwój cyberzagrożeń.

Ramy prawne i definicje pojęć związanych z cyberbezpieczeństwem

W dobie coraz dalej idącego rozwoju Internetu oraz usług świadczonych za jego pomocą rozwój trzech istotnych w tym kontekście pojęć cyberbezpieczeństwa,

¹ *A Declaration of the Independence of Cyberspace* by John Perry Barlow <https://www.eff.org/pl/cyberspace-independence> [dostęp: 10.05.2024 r.].

cyberzagrożeń oraz cyberprzestępczości ma ogromne znaczenie dla społeczeństwa a także prawodawstwa w Polsce. Definicja legalna pojęcia cyberbezpieczeństwo zawarta została w Ustawie o krajowym systemie cyberbezpieczeństwa z dnia 5 lipca 2018 roku² (dalej jako u.k.s.c.). Ustawa ta wdraża do krajowego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z 6 lipca 2016 roku w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii³, zmieniając również niektóre przepisy w ustawie z dnia 7 września 1991 roku. o systemie oświaty⁴, ustawy z dnia 16 lipca 2004 roku – Prawo telekomunikacyjne⁵ oraz ustawy z dnia 26 kwietnia 2007 roku o zarządzaniu kryzysowym⁶. Ustawa powieli materialne i proceduralne postanowienia dyrektywy NIS (*Network and Information Systems Directive*) dostosowując jednocześnie jej regulacje do warunków krajowych⁷. Zgodnie z wyżej wskazanym aktem prawnym definicja pojęcia to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy⁸. Z kolei w punkcie 3 art. 2 u.k.s.c. termin „cyberbezpieczeństwo” został zdefiniowany jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Definicja ta jest podobna do określenia „bezpieczeństwo sieci i systemów informacyjnych”, które zostało wyrażone w art. 4 pkt 2 dyrektywy NIS (red. *Network and Information Systems Directive*)⁹ oraz NIS 2 (red. *Network and Information Systems*

² Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2024 r., poz. 1077).

³ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii.

⁴ Ustawa z dnia 7 września 1991 r. o systemie oświaty (Dz.U. z 2025 r., poz. 881.).

⁵ Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2024 r., poz. 34 z późn. zm.).

⁶ Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz.U. z 2023 r., poz. 122 z późn. zm.).

⁷ C. Banasiński, M. Rojszczak, J.M. Chmielewski, W. Hydzik, J. Łuczak, W. Nowak, K. Waćkowski, 2. *Krajowy system cyberbezpieczeństwa* [w:] C. Banasiński, M. Rojszczak, J. M. Chmielewski, W. Hydzik, J. Łuczak, W. Nowak, K. Waćkowski, *Cyberbezpieczeństwo*, Warszawa 2020, s. 15.

⁸ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2024 r., poz. 1077).

⁹ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2).

Directive 2). Zgodnie z nadmienionym dokumentem będącym pierwszym europejskim aktem prawnym regulującym tę kwestię: bezpieczeństwo sieci i systemów informacyjnych oznacza odporność tych systemów, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność danych przetwarzanych, przechowywanych lub przekazywanych, a także związanych z nimi usług, oferowanych lub dostępnych za pośrednictwem tych sieci i systemów informacyjnych. Ujednolicenie terminów „cyberbezpieczeństwo” oraz „bezpieczeństwo sieci i systemów informacyjnych” mogłoby przynieść korzyści w kontekście transgranicznej współpracy oraz realizacji obowiązków wynikających z dyrektyw NIS i NIS 2.

Celem dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 było zbudowanie zdolności w zakresie cyberbezpieczeństwa w całej Unii, łagodzenie zagrożeń dla sieci i systemów informatycznych wykorzystywanych do celów świadczenia usług kluczowych w sektorach oraz zapewnienie ciągłości takich usług w przypadku wystąpienia incydentów, a tym samym przyczynienie się do bezpieczeństwa Unii oraz do sprawnego funkcjonowania jej gospodarki i społeczeństwa¹⁰. Po wejściu w życie Unijnej dyrektywy poczyniono postępy związane z budowaniem odporności państw Unii w zakresie cyberbezpieczeństwa i zgłaszanych incydentów. W myśl Polskich przepisów ustawa ogranicza zakres ochrony jedynie do „systemów informacyjnych”, podczas gdy dyrektywa odnosi się do „sieci i systemów informacyjnych”. Ta rozbieżność może wpłynąć na interpretację przepisów w zakresie ochrony danych informacyjnych w sieci. W dyrektywie NIS przedmiotem ochrony są dane „przechowywane, przekazywane lub przetwarzane”, natomiast ustawa o KSC odnosi się jedynie do danych „przetwarzanych”. Ograniczenie to może prowadzić do różnic w interpretacji zakresu ochrony danych w przypadku innych operacji na danych, takich jak przechowywanie czy przekazywanie. Te rozbieżności wskazują na istotne różnice między ustawą o KSC a dyrektywą NIS, które mogą mieć wpływ na stosowanie przepisów prawa w praktyce oraz na efektywność transgranicznej współpracy w zakresie cyberbezpieczeństwa¹¹. Wskazany dokument określa w art. 3 również cele krajowego systemu cyberbezpieczeństwa. Ma on na celu zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnię-

¹⁰ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE. L. z 2022 r. Nr 333, s. 80).

¹¹ G. Szpor [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. K. Czaplicki, A. Gryszczyńska, Warszawa 2019, art. 2., <https://sip.lex.pl/#/commentary/587786644/584084?tocHit=1&cm=RELATIONS> [dostęp: 10.05.2024 r.].

cie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów¹². Artykuł 3 *in fine* wskazuje jakie operacje uznawane są za niezbędne do realizacji celu, tj. zadania. Pierwszym z nich jest osiągnięcie „odpowiedniego” poziomu bezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług cyfrowych. Drugim zadaniem jest zapewnienie obsługi incydentów, które mają miejsce w sieci a których zgłoszenie stanowić może nie tylko informacje statystyczne, ale również mogące pomóc w pracach nad dalszymi możliwościami walki z cyberprzestępczością. Pojawia się tutaj również pytanie, czy przez „odpowiedni” poziom bezpieczeństwa należy rozumieć taki system, który gwarantuje „niezakłócone świadczenie usług”, oraz czy każde zakłócenie świadczenia usług oznacza, że dany system należy uznać za niewystarczający. Tego rodzaju interpretacja może rodzić wątpliwości w stosowaniu prawa, zważywszy na fakt, że samo zapewnienie obsługi incydentów stanowi odrębne zadanie. Wynika z tego, że ustawodawca dopuszcza możliwość wystąpienia zakłóceń, co rodzi pytanie, jak rozumieć „odpowiedni” poziom bezpieczeństwa w kontekście nieuniknionych incydentów i cyberataków.

Najpopularniejsze przestępstwa internetowe oraz ich rozwiązania prawne

Cyberprzestrzeń stała się w ostatnich latach miejscem, w którym znacznie wzrosła skala popełniania przestępstw. Coraz częściej mamy do czynienia z nowszymi metodami wyłudzeń finansowych, wyłudzeń danych czy naruszeniami wizerunku. Bardzo istotne w kontekście tego co dzieje się w sieci w ostatnim czasie jest zjawisko dezinformacji, czyli możliwe do zweryfikowania nieprawdziwe lub wprowadzające w błąd informacje, tworzone, przedstawiane i rozpowszechniane w celu uzyskania korzyści gospodarczych lub wprowadzenia w błąd opinii publicznej, które mogą wyrządzić szkodę publiczną¹³. Zjawisko dezinformacji w Polsce znacząco pojawiało się w czasie pandemii Covid-19 czy po wybuchu wojny w Ukrainie. Wówczas pojawiało się wiele fałszywych informacji wprowadzających w błąd opinię publiczną lub skłaniających ją do podejmowania różnych działań mogących wprowadzić chaos. Zjawisko to co jakiś czas nasila się, pojawiając się w mediach społecznościowych czy portalach informacyjnych. Sytuacja taka miała miejsce przy okazji publikacji fałszywej depeszy 31 maja 2024 roku, która ukazała się o godzinie 14:00 a następnie ponownie o 14:20 na stronie Polskiej Agencji

¹² Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2024 r., poz. 1077).

¹³ Wystąpienie Rzecznika do Ministerstwa Cyfryzacji ws. walki z dezinformacją. Odpowiedź ministra <https://bip.brpo.gov.pl/pl/content/rpo-dezinformacja-walka-mc-odpowiedz> [dostęp: 10.05.2024 r.].

Prasowej. Polska Agencja Prasowa doświadczyła dziś (piątek, 31 maja 2024 roku) cyberataku, w efekcie którego w Codziennym Serwisie Informacyjnym PAP dwukrotnie ukazała się nieprawdziwa depesza o rzekomej mobilizacji w Polsce. PAP nie był źródłem tej informacji. Depesza nie powstała w Agencji, nie została napisana ani nadana przez pracowników PAP; została natychmiast anulowana i wycofana z serwisu – podkreślili w oświadczeniu likwidator PAP Marek Błoński i redaktor naczelny PAP Wojciech Tumidalski¹⁴. Informacja ta wywołała niepokój w polskim społeczeństwie. Po tym zdarzeniu władze polskiego rządu zleciły szereg kontroli a także oświadczyły, że sytuacja ta miała na celu destabilizację polskiego społeczeństwa przed wyborami do Parlamentu Europejskiego, które odbywały się w Polsce 9 czerwca 2024 roku, uznając, że był to przykład cyberataku ze strony Rosji. Jednym z narzędzi dezinformacji jest również *deepfake*. Jest to technologia wykorzystująca sztuczną inteligencję do generowania realistycznych filmów lub dźwięków, które są manipulacjami. *Deepfake* wykorzystują techniki uczenia maszynowego i sztucznych sieci neuronowych do naśladowania wyglądu, głosu i manier osoby, tworząc fałszywe materiały wideo lub audio, które mogą wyglądać i brzmieć jak rzeczywiste. Technologia ta jest wykorzystywana w działaniach przestępczych¹⁵. Przypadki dezinformacji za pomocą *deepfaków* bardziej znane są od 2017 roku, kiedy to na portalu o nazwie Reddit mianem *deepfake-ów* nazwano zdjęcia oraz filmy pornograficzne, w których zamiast twarzy autorów umieszczone zostały twarze znanych osobistości. *Deepfake* swoje zastosowanie w przestępczości znalazł bardzo szybko często wykorzystywany jest do realizacji filmów czy zdjęć ze znanymi osobami, które zachęcają np. do wątpliwej inwestycji. W rzeczywistości jest to forma wyłudzenia, najczęściej pieniędzy, które jest przestępstwem. Kolejną formą przestępstw powszechną w cyberprzestrzeni jest *phishing*. Jest to jedna z najczęściej występujących form ataków opartych na wiadomościach e-mail lub SMS, która wykorzystuje techniki inżynierii społecznej. Metodę tę stosują cyberprzestępcy do działania mającego na celu wprowadzenie w błąd odbiorcy, aby ten podjął określone działania zgodne z ich zamierzeniami. Przestępcy podszywając się m.in. pod firmy kurierskie, organy administracji publicznej, operatorów telekomunikacyjnych czy nawet osoby z najbliższego otoczenia ofiary, dążąc do wyłudzenia danych uwierzytelniających, takich jak dane logowania do kont bankowych czy portali społecznościowych, za pomocą których mogą wykorzystać wyżej wymienione informacje. Najczęściej w ramach ataków *phishingowych* cyberprzestępcy próbują wyłudzić pieniądze. Często w wiadomościach pojawiają się również fał-

¹⁴ <https://www.pap.pl/aktualnosci/cyberatak-na-pap-w-serwisie-polskiej-agencji-prasowej-nieprawdziwadepesza> [dostęp: 10.05.2024 r.].

¹⁵ <https://cebrf.knf.gov.pl/encyklopedia/hasla/385-definicje/891-deepfake> [dostęp: 10.05.2024 r.].

szywe linki kierujące do fałszywych stron bankowych. Wiadomości te są przygotowane bardzo precyzyjnie i mają na celu imitować właściwą korespondencję np. bankową, dlatego ciężko odróżnić je od prawdziwej korespondencji. Wiadomości tego rodzaju mają dążyć do wyłudzenia danych oraz pieniędzy, a przygotowane strony do wyłudzeń różnią się od autoryzowanych nieznacznie i mogą zawierać drobne literówki w nazwach czy opisach. Tego typu praktyki stały się bardzo powszechne. Do zgłaszania takich incydentów na mocy ustawy o Krajowym Systemie Cyberbezpieczeństwa (Dz. U. poz. 1560) powołano NASK CSIRT (*Computer Security Incident Response Team*), którego obowiązki od 2018 roku pełni CERT POLSKA. Zestawienie zadań oraz szczegółowy zakres aktywności rzeczonoego zespołu zostały zamieszczone na jego oficjalnej witrynie internetowej¹⁶.

Kolejnym rodzajem popularnych ataków mających miejsce w cyberprzestrzeni są ataki typu *ransomware*. *Ransomware* (ang. *ransom* – okup, ang. *software* – oprogramowanie) to program należący do rodziny szkodliwego oprogramowania. Powoduje blokadę lub zaszyfrowanie plików znajdujących się na urządzeniu¹⁷. Może atakować zarówno systemy operacyjne komputerów, jak i urządzenia mobilne. Atak przebiega zazwyczaj w taki sposób, że urządzenie generuje komunikat lub plik z instrukcjami informujący, że odzyskanie dostępu do danych jest możliwe wyłącznie po dokonaniu wpłaty na wskazane konto cyberprzestępców. Coraz częściej cyberprzestępcy stosują tzw. podwójne wymuszanie (*double extortion*), poprzez które oprócz szyfrowania plików, wykradają również wrażliwe dane, grożąc ich ujawnieniem w przypadku braku zapłaty okupu. Należy podkreślić, że spełnienie żądania finansowego nie gwarantuje odszyfrowania danych ani zapobiegnięcia ich ujawnieniu. Pierwszy publicznie znany atak tego typu miał miejsce w 1989 roku, kiedy to amerykański biolog ewolucyjny Joseph Popp rozesał nośniki danych do uczestników konferencji Światowej Organizacji Zdrowia (WHO) na temat AIDS. Dyskietki oznaczone jako *AIDS Information. Introductory Diskette* trafiły do około 20 000 uczestników i miały zawierać informacje związane z edukacją w zakresie tej choroby. W rzeczywistości dyskietki zawierały złośliwe oprogramowanie, które szyfrowało nazwy i rozszerzenia plików a ofiary tego ataku zmuszone były do zapłaty ok. 189 dolarów w celu odzyskania dostępu do plików. W latach osiemdziesiątych oprogramowanie to wywołało duże zaskoczenie, a metody szyfrowania były stosunkowo prymitywne w porównaniu do dzisiejszych standardów, jednak incydent ten zapoczątkował rozwój *ransomware* jako formy cyberprzestępczości, a atak ten nazwano „AIDS Trojan” lub „PC Cyborg”. Obecnie tego typu ataki zdarzają

¹⁶ <https://incydent.cert.pl/#!/lang=pl> [dostęp: 05.10.2024 r.].

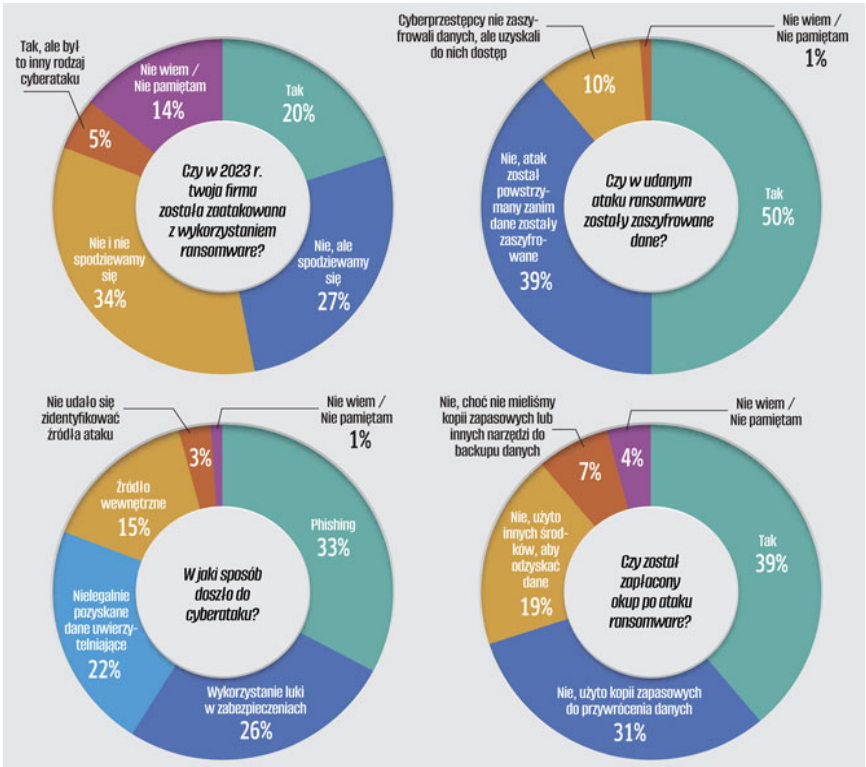
¹⁷ <https://www.gov.pl/web/baza-wiedzy/ransomware-jedno-z-najpoważniejszych-zagrożeń-w-cyberprzestrzeni> [dostęp: 05.10.2024 r.].

się bardzo często a wyłudzone przez cyberprzestępców kwoty są bardzo wysokie. Według danych zawartych w pierwszym w historii raporcie dotyczącym ataków ransomwer zatytułowanym *State of Ransomware* firmy Sophos. Liczba ataków na przestrzeni lat, w 2024 roku zmniejszyła się, co obrazuje poniższa tabela.

Tabela 1. Wskaźnik ataków ransomwere według raportu Sophos

Wskaźnik ataków ransomwere				
2020 rok	2021 rok	2022 rok	2023 rok	2024 rok
51%	37%	66%	66%	59%

Pytanie: Czy w ostatnim roku Państwa organizacja została zaatakowana przez ransomware? Tak. n=5,000 (2024), 3,000 (2023), 5,800 (2022), 5,400 (2021), 5,000 (2020).



Ryc. 1. Grafika przedstawiająca dane związane z atakami ransomwere
Źródło: Badanie Ransomware w Polsce 2024, Sophos.

Według tego samego dokumentu w 2024 roku przedsiębiorstwa związane z sektorem infrastruktury krytycznej (np. branży energetycznej, gazowej, obiektach i instytucjach użyteczności publicznej) aż w 67% padły ofiarami tego typu ataków. Raport ten pokazuje, iż podatność na ataki jest tym wyższa, im wyższe są przychody danej organizacji z wyżej wskazanej branży. Podmioty generujące przychody przekraczające 5 miliardów dolarów odnotowują najwyższy wskaźnik tego typu incydentów, według badań wynosi on aż 67%. Niemniej jednak, także mniejsze firmy, o przychodach poniżej 10 milionów dolarów, pozostają regularnym celem cyberprzestępców – w ubiegłym roku niemal 47% z nich padło ofiarą ataków *ransomware*. Pomimo, że znaczna część tych ataków jest realizowana przez dobrze zorganizowane grupy przestępcze, odnotowuje się wzrost liczby incydentów z użyciem prostych, niedrogich narzędzi *ransomware*, wykorzystywanych przez mniej zaawansowanych sprawców. Z raportu „Ransomware w Polsce 2024” wynika również, że wiele Polskich firm padło ofiarami tego typu ataków. Raport ten wskazuje ponadto, że w Polsce ciągle mamy w tym zakresie lukę związaną z odpowiednimi zabezpieczeniami i ochroną.

Sposoby przeciwdziałania cyberprzestępczości

W erze dynamicznie rozwijającej się cyfryzacji, problem cyberprzestępczości zyskał na znaczeniu. Przestępcy, posługując się coraz bardziej zaawansowanymi technologiami, stosują metody takie jak: *phishing*, *ransomware* czy ataki DDoS, a także liczne metody manipulacyjne, szczególnie na osobach starszych, co prowadzi do poważnych strat finansowych oraz destabilizacji zaufania do systemów cyfrowych. W odpowiedzi na te zagrożenia, rozwój strategii przeciwdziałania cyberprzestępczości staje się kluczowy. Istotne staje się także powstawanie komórek ścigania tego typu przestępstw. Podstawą skutecznej ochrony przed zagrożeniami cyfrowymi jest edukacja użytkowników Internetu. Powszechnie uważa się, że odpowiednio przeszkolony personel jest najważniejszą linią obrony przed cyberatakami. Szkolenia w zakresie tworzenia silnych haseł, a także edukacja i informowanie o zagrożeniach osób starszych, które mniej znają się na technologii, mogą znacznie zmniejszyć liczbę udanych ataków. Wielokrotnie podkreśla się, że świadomość zagrożeń, takich jak e-maile *phishingowe* czy fałszywe strony internetowe może stanowić istotny czynnik zmniejszający skuteczność działań cyberprzestępców. Przykładem może być wdrożenie procedur uwierzytelniania dwuskładnikowego (tzw. 2FA), wprowadzanego między innymi przez portale społecznościowe czy banki, które – choć nie zawsze popularne wśród użytkowników – zwiększają poziom bezpieczeństwa poprzez wymóg dodatkowej weryfikacji.

Jednak ważnym aspektem przeciwdziałania przestępczości w sieci oraz rozwojowi tego obszaru było powołanie odpowiednich organów służb, które mają zajmować się przestępczością w Internecie oraz cyberwojną. Ważną rolę w procesie zwalczania cyberprzestępczości w Polsce ma Centralne Biuro Zwalczania Cyberprzestępczości (CBZC) które zostało powołane w 2021 roku. Do głównych zadań Centralnego Biura Zwalczania Cyberprzestępczości należą:

1. cyberprzestępczość, która stanowi jedno z największych i najbardziej rozwijających się zagrożeń dla bezpieczeństwa obywateli naszego kraju. Jest zjawiskiem narastającym i niebezpiecznym. Skuteczna walka z zagrożeniami płynącymi z sieci możliwa jest wyłącznie w warunkach, gdy organy ścigania nie ustępują cyberprzestępcom zarówno w technologii jak i w umiejętnościach;
2. zwalczanie cyberprzestępczości powinno się opierać na ograniczaniu skutków jej wpływu na społeczeństwo oraz identyfikowaniu zagrożeń pochodzących z sieci. Głównym celem jest tworzenie bezpieczniejszej cyberprzestrzeni.
3. Centralne Biuro Zwalczania Cyberprzestępczości (CBZC) jest jednostką organizacyjną Policji i służy zwalczaniu cyberprzestępczości. CBZC odpowiedzialne jest za realizację na obszarze całego kraju zadań w zakresie rozpoznawania i zwalczania przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej oraz zapobiegania tym przestępstwom, a także wykrywania i ścigania sprawców tych przestępstw oraz wspierania w niezbędnym zakresie jednostek organizacyjnych Policji w rozpoznawaniu, zapobieganiu i zwalczaniu tych przestępstw.

Centralnym Biurem Zwalczania Cyberprzestępczości kieruje Komendant Centralnego Biura Zwalczania Cyberprzestępczości, który podlega Komendantowi Głównemu Policji.

Do służby przyjmowane są przede wszystkim osoby z wiedzą i umiejętnościami z zakresu informatyki i nowoczesnych technologii teleinformatycznych. Funkcjonariusze CBZC mogą prowadzić działania operacyjno-rozpoznawcze oraz dochodzeniowo-śledcze na zasadach wynikających z ustawy o Policji¹⁸.

W Biurze Zwalczania Cyberprzestępczości pracują wykwalifikowani funkcjonariusze odnoszący na tym polu liczne sukcesy. Według danych przedstawionych w raporcie z działalności za rok 2023 roku funkcjonariusze przeprowadzili nie-

¹⁸ <https://cbzc.policja.gov.pl/bzc/o-cbzc/podstawowe-zadania/5,Zadania-Centralnego-Biura-ZwalczaniaCyberprzestepczosci.html> [dostęp: 05.10.2024 r.].

mal 613 postępowań przygotowawczych, wzięli udział w 440 realizacjach wraz z innymi służbami na terenie całego kraju, w wyniku których podejrzanym było 681 osób, zatrzymano 501 osób, 231 z nich zostało tymczasowo aresztowanych. Szacuję się, że policjanci działający w ramach Centralnego Biura Zwalczania Cyberprzestępczości w czasie swojego działania zabezpieczyli mienie łącznej wartości 441 milionów złotych. Udało się także odzyskać ponad 14 milionów złotych¹⁹. Jest to niewątpliwie duży sukces w działalności tej stosunkowo młodej służby oraz jej niezbyt rozbudowanej struktury, przed którą wciąż pojawiają się nowe wyzwania.

Kolejną nową formacją mającą bronić cyberprzestrzeni są Wojska Obrony Cyberprzestrzeni. Wojska Obrony Cyberprzestrzeni powstały w odpowiedzi na dynamicznie rozwijające się zagrożenia w cyfrowej sferze bezpieczeństwa narodowego. Początki tej formacji sięgają przełomu XX i XXI wieku, kiedy to rozwój technologii informacyjno-komunikacyjnych zaczął znacząco wpływać na prowadzenie działań zbrojnych oraz bezpieczeństwo państwowe. Służba ta powstała w 2022 roku jako komponent Sił Zbrojnych odpowiedzialny za zapewnienie bezpieczeństwa w cyberprzestrzeni. Wojska Obrony Cyberprzestrzeni odpowiadają za kluczowe obszary związane z kryptologią, cyberbezpieczeństwem oraz budową i eksploatacją systemów teleinformatycznych. Kluczowymi zadaniami Wojsk Obrony Cyberprzestrzeni jest zapewnienie bezpieczeństwa teleinformatycznego całego resortu, prowadzenie badań, projektowanie, budowa, wdrażanie, użytkowanie oraz ochrona narodowych technologii kryptologicznych czy wytwarzanie nowych produktów dla państwa przez zespolenie potencjału w obszarze zaawansowanych technologii informatycznych i kryptograficznych. Wojska Obrony Cyberprzestrzeni prowadzą też działalność naukowo-edukacyjną, wdrożeniową, badawczo-rozwojową i opiniotwórczą²⁰. W swojej strukturze służba ta posiada 12 podporządkowanych jednostek wojskowych w tym dwie wyspecjalizowane w działaniach w cyberprzestrzeni w Białobrzegach i Gdyni. W 2024 roku rozpoczęło się formowanie kolejnej jednostki „C” we Wrocławiu, a także Jednostki Wsparcia Działań w Legionowie. Zadaniem Wojsk Obrony Cyberprzestrzeni jest również dbanie o to, by zespół CSIRT MON (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego) działał prawidłowo. CSIRT MON pracuje non stop, monitorując sieci resortu obrony narodowej przez całą dobę, 7 dni w tygodniu i zajmuje się ochroną oraz obroną polskiej cyberprzestrzeni. Ich misja to czuwanie nad bezpieczeństwem, szybkie wykrywanie zagrożeń i reagowanie na nie, zanim jeszcze staną się poważnym problemem. Według raportu z działalności

¹⁹ Wyniki Statystyczne Centralnego Biura Zwalczania Cyberprzestępczości za 2023 rok.

²⁰ <https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni> [dostęp: 05.10.2024 r.].

Wojsk Obrony Cyberprzestrzeni formacja ta odnotowała liczne sukcesy takie jak np. „Aplikacja Żołnierz.pl” – mająca na celu dotarcie z rzetelnymi informacjami do Żołnierzy Wojska Polskiego; przygotowany został również raport „Ukraina 2022 – 10 Miesięcy Rosyjskiej Propagandy”. Publikacja ta miała na celu podniesienie świadomości społecznej z zakresu zagrożeń w cyberprzestrzeni oraz elementami walki z dezinformacją, którą stosuje Federacja Rosyjska. Służba organizowała również wiele szkoleń i ćwiczeń z wojskami z innych krajów. Celem takich działań było podniesienie kompetencji żołnierzy oraz zacieśnienie współpracy z sojusznikami²¹. Służby takie jak Wojska Obrony Cyberprzestrzeni a także Centralne Biuro Zwalczenia Cyberprzestępczości to istotne komórki z punktu widzenia bezpieczeństwa Państwa, które mają chronić zarówno obywateli, jak i samą rację stanu Państwa.

Podsumowanie

W dobie dynamicznego rozwoju cyfryzacji, problem cyberprzestępczości stał się jednym z kluczowych zagrożeń dla bezpieczeństwa państw i ich obywateli. W odpowiedzi na nowe wyzwania, takie jak *phishing*, *ransomware*, ataki DDoS czy dezinformację, niezbędne stało się wprowadzenie odpowiednich regulacji prawnych oraz powołanie wyspecjalizowanych służb zajmujących się ochroną cyberprzestrzeni. Ich przykładem jest polska Ustawa o Krajowym Systemie Cyberbezpieczeństwa (KSC) z 2018 roku, wdrażająca dyrektywę NIS (UE) 2016/1148, mającą na celu zapewnienie bezpieczeństwa sieci i systemów informacyjnych w Unii Europejskiej. Pomimo postępów w budowaniu odporności cyfrowej na poziomie unijnym i krajowym, wciąż istnieją rozbieżności między regulacjami KSC a dyrektywą NIS, które mogą wpływać na efektywność współpracy transgranicznej oraz na praktyczne stosowanie przepisów w zakresie ochrony danych. Krajowy System Cyberbezpieczeństwa skupia się na systemach informacyjnych, podczas gdy dyrektywa obejmuje także sieci, co może powodować różnice interpretacyjne, zwłaszcza w kontekście przechowywania i przekazywania danych. Jednak polskie prawo ciągle nie jest dostosowane do wielu norm Europejskich w tym zakresie, co więcej, zmiany polskiego prawodawstwa w tym zakresie wprowadzane są bardzo powoli. W celu przeciwdziałania cyberprzestępczości i ochrony infrastruktury krytycznej powołano w Polsce Centralne Biuro Zwalczenia Cyberprzestępczości

²¹ Podsumowanie z działań Wojsk Obrony Cyberprzestrzeni 2023 r. https://www.wojskopolskie.pl/woc/u/c2/51/c251ce6c-b74f-40dc-8b12-dde8b14144a6/dkwoc_-_podsumowanie_2023_r. [dostęp: 05.10.2024 r.].

(CBZC) oraz Wojska Obrony Cyberprzestrzeni. CBZC, działające od 2021 roku, specjalizuje się w zwalczaniu przestępstw popełnionych przy użyciu systemów informatycznych oraz wspieraniu innych jednostek policji w tego typu działaniach. Biuro to przeprowadza działania operacyjno-rozpoznawcze oraz dochodzeniowo-śledcze, realizując zadania w zakresie monitorowania, identyfikowania i ściągania cyberprzestępców. Dzięki wykwalifikowanym funkcjonariuszom, CBZC odnotowało liczne sukcesy, m.in. zabezpieczenie mienia o wartości setek milionów złotych i odzyskanie części wyłudzonych środków. Z kolei Wojska Obrony Cyberprzestrzeni powstałe w 2022 roku stanowią komponent Sił Zbrojnych RP odpowiedzialny za zapewnienie bezpieczeństwa teleinformatycznego oraz ochronę narodowych technologii kryptograficznych. Formacja ta prowadzi działalność badawczo-rozwojową, edukacyjną oraz współpracuje z innymi państwami w ramach szkoleń i ćwiczeń wojskowych. W jej strukturze działają wyspecjalizowane jednostki, takie jak CSIRT MON, które monitorują sieci resortu obrony narodowej przez całą dobę, zapewniając szybką reakcję na zagrożenia i incydenty.

Zarówno CBZC, jak i Wojska Obrony Cyberprzestrzeni odgrywają kluczową rolę w budowaniu bezpiecznej przestrzeni cyfrowej w Polsce. Zadania obu wskazanych instytucji obejmują ochronę przed cyberprzestępczością, ale również reagowanie na cyberataki i dezinformację, co jest szczególnie istotne w kontekście obecnych zagrożeń geopolitycznych. Ich działania przyczyniają się do wzmacniania bezpieczeństwa narodowego oraz zapewnienia stabilności w erze rosnącej cyfryzacji.

Bibliografia

Akty prawne:

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2024 r., poz. 1077).

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

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz.U. z 2024 r., poz. 1077).

Źródła literaturowe:

- Barlow J. P. „*A Declaration of the Independence of Cyberspace*” <https://www.eff.org/pl/cyberspace-independence> [dostęp: 05.10.2024 r.].
- Banasiński C., Rojszczak M., Chmielewski J. M., Hydzik W., Łuczak J., Nowak W., Waćkowski K., 2. *Krajowy system cyberbezpieczeństwa* [w:] Banasiński C., Rojszczak M., Chmielewski J. M., Hydzik W., Łuczak J., Nowak W., Waćkowski K., *Cyberbezpieczeństwo*, Wyd. Wolters Kluwer, Warszawa 2020.
- <https://sip.lex.pl/#/monograph/369463629/6?tocHit=1&cm=REL> [dostęp: 05.10.2024 r.].
- G. Szpor [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa*. Komentarz, red. K. Czapliski, A. Gryszczyńska, Warszawa 2019, art. 2. <https://sip.lex.pl/#/commentary/587786644/584084?tocHit=1&cm=RELATIONS> [dostęp: 28.09.2024 r.].

Źródła internetowe:

- <https://www.pap.pl/aktualnosci/cyberatak-na-pap-w-serwisie-polskiej-agencji-prasowej-nieprawdziwa-depesza-o>
- <https://cebrf.knf.gov.pl/encyklopedia/hasla/385-definicje/891-deepfake>
- <https://www.gov.pl/web/baza-wiedzy/ransomware--jedno-z-najpowazniejszych-zagrozen-w-cyberprzestrzeni>
- <https://cbzc.policja.gov.pl/bzc/o-cbzc/podstawowe-zadania/5,Zadania-Centralnego-Biura-Zwalczania-Cyberprzestepczosci.html>
- Wyniki Statystyczne Centralnego Biura Zwalczania Cyberprzestępczości za 2023 rok
- <https://www.gov.pl/web/obrona-narodowa/wojska-obrony-cyberprzestrzeni>
- Podsumowanie z działań Wojsk Obrony Cyberprzestrzeni 2023 r. https://www.wojsko-polskie.pl/woc/u/c2/51/c251ce6c-b74f-40dc-8b12-dde8b14144a6/dkwoc_-_podsumowanie_2023_r.pdf
- Wystąpienie Rzecznika do Ministerstwa Cyfryzacji ws. walki z dezinformacją. Odpowiedź ministra <https://bip.brpo.gov.pl/pl/content/rpo-dezinformacja-walka-mc-odpowiedz>

Cyberprzestępczość – rodzaje, zapobieganie, zwalczanie

Patryk MANOWIECKI¹

Uniwersytet Jana Kochanowskiego w Kielcach
ORCID: 0009-0003-2257-0506

Streszczenie. W niniejszym artykule omówiono problem cyberprzestępczości – jednego z bardzo poważnych zagrożeń XXI w. Poza wskazaniem ujęcia definicyjnego tego terminu zostały omówione wybrane rodzaje cyberprzestępstw (w oparciu o dostępną literaturę), z jakimi może mieć styczność użytkownik np. *cyberstalking*. Celem pracy było również wskazanie możliwych sposobów zapobiegania przestępczości w sieci. Ostatnim elementem było nawiązanie do aspektu zwalczania tego zjawiska oraz przedstawienie instytucji CBZC (Centralne Biuro Zwalczania Cyberprzestępczości) jako organu koncentrującego swoje działania w tym obszarze. Opracowanie dowodzi, że cyberprzestępczość jest zjawiskiem bardzo szerokim, gdyż obejmuje szeroki zakres czynów zabronionych.

Słowa kluczowe: cyberprzestępczość, zapobieganie, phishing, cyberstalking, cyberpedofilia

Wstęp

Postęp technologiczny, do którego doszło na przełomie XX i XXI wieku spowodował, iż obecnie znaczna część społeczeństwa coraz więcej czasu spędza w cyberprzestrzeni. Związane jest to z faktem, że Internet stwarza użytkownikowi różne możliwości w sferze pracy, rozrywki, bankowości, kontaktów z innymi itp. Udogodnienia, jakie oferuje dostęp do sieci wpływają na fakt coraz to większej aktywności w niej młodzieży i dzieci. Należy jednak pamiętać, że świat wirtualny niesie ze sobą również wiele zagrożeń dla użytkownika. Przestępcy,

¹ Patryk Manowiecki – student 1 roku studiów magisterskich na kierunku bezpieczeństwo narodowe, zainteresowania badawcze: bezpieczeństwo, cyberbezpieczeństwo.

którzy funkcjonowali w świecie rzeczywistym w znacznej części przenieśli swoje działania do Internetu stając się cyberprzestępcami. Internet kojarzy się z anonimowością, w związku z czym cyberprzestępczość stała się zjawiskiem bardzo powszechnym oraz rozbudowanym. *Phishing*, cyberpedofilia, cyberstalking czy przestępstwa przeciwko poufności i integralności danych komputerowych to tylko niektóre z rodzajów cyberprzestępstw. Na kontakt z cyberprzestępczością narażony jest każdy użytkownik sieci, w tym dzieci i młodzież, bowiem to zazwyczaj te osoby spędzają najwięcej czasu w sferze online. Dlatego bardzo istotne jest umiejętne zapobieganie cyberprzestępczości, aby ograniczyć jej występowanie i niepożądane skutki. Niestety nie każdej sytuacji uda się zapobiec, dlatego równie ważną rzeczą jest zwalczanie cyberprzestępczości. W tym celu w Polsce powstało Centralne Biuro Zwalczania Cyberprzestępczości (CBZC).

Celem artykułu będzie omówienie zjawiska cyberprzestępczości oraz ukazanie i zdefiniowanie podstawowych rodzajów przestępstw w sieci, na które narażony jest użytkownik. W treści całej pracy chciałbym przedstawić sposoby zapobiegania przestępczości w sieci. Rzeczą ostatnią będzie zwrócenie uwagi czytelnika na kwestię zwalczania cyberprzestępczości, w tym scharakteryzowanie instytucji CBZC jako organu działającego w tym zakresie. Niniejsza praca została przygotowana w oparciu o literaturę przedmiotu, dostępne statystyki oraz inne materiały źródłowe skupiające się na analizowanej tematyce.

Cyberprzestępczość – ujęcie definicyjne

Termin „cyberprzestępstwo” jest aktualnie jednym z najszerzej komentowanych i używanych pojęć używanych do określania różnego rodzajów przestępstw w sieci². Natomiast sama analiza tego pojęcia jest dość złożona, ponieważ zarówno na gruncie krajowym, a także międzynarodowym nie ma wypracowanej jednej, w pełni spójnej definicji cyberprzestępczości. Każda organizacja (np. Rada Europy czy ONZ) jak również dany kraj ujmują to zjawisko inaczej. Problem z dokładnym zdefiniowaniem omawianego terminu wynika również z faktu, o którym pisze Wojciech Czerski. Autor ten w swoim artykule zwraca uwagę, iż na taką sytuację ma wpływ cytując *tworzenie definicji ad hoc przez autorów dokumentów i opracowań*³.

² J. Wasilewski, *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd Bezpieczeństwa Wewnętrznego” 2016, nr 15, s. 162.

³ W. Czerski, *Cyberprzestępczość wśród nieletnich – charakterystyka zjawiska, jego skala i przeciwdziałanie* [w:] *Dydaktyka Informatyki*, Wydawnictwo Uniwersytetu Rzeszowskiego, Rzeszów 2022, s. 13.

Jednym z podstawowych dokumentów, który odwołuje się do tematu artykułu jest sporządzona w 2001 roku Konwencja Rady Europy o cyberprzestępczości. Natomiast dokument ten w części terminologicznej nie przedstawia odbiorcy definicji terminu cyberprzestępczości czy cyberprzestępstwo, tylko ukazuje na kolejnych jego stronach rodzaje czynów zabronionych. Samo pojęcie *cyberprzestępstwo* (oryginalny zwrot – *cybercrime*) zostało użyte w przytoczonej Konwencji 9 razy, z czego 8 w preambule tekstu⁴.

Podczas X Kongresu ONZ w Sprawie Zapobiegania Przestępczości i Traktowania Przestępców została przyjęta definicja, która określa cyberprzestępstwo w dwóch ujęciach:

- wąskim – *jest to wszelkie nielegalne działanie wykonywane w postaci operacji elektronicznych, wymierzone przeciw bezpieczeństwu systemów komputerowych lub procesowanych przez te systemy danych*⁵;
- szerokim – *wszelkie nielegalne działanie popełnione za pomocą lub dotyczące systemów lub sieci komputerowych, włączając w to między innymi nielegalne posiadanie i udostępnianie lub rozpowszechnianie informacji przy użyciu systemów lub sieci komputerowych*⁶.

Określenie pojęcia *cyberprzestępstwo* odnajdujemy również w przyjętym w 2013 roku dokumencie pt. „Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej”, gdzie widnieje: „cyberprzestępstwo – czyn zabroniony popełniony o obszarze cyberprzestrzeni”⁷. Jest to jedna z najbardziej związanych, z jednocześnie trafnych definicji omawianego terminu. Jej istotną cechą jest odwołanie się do pojęcia cyberprzestrzeni a nie rodzajów czynów zabronionych⁸. Damian Wyglądała w swoim artykule napisał, iż cyberprzestępczość

to czyny zabronione, skierowane przeciwko systemom informatycznym, w których komputer jest celem samym w sobie, oraz czyny dokonane z użyciem komputera, w których stanowi on jedynie narzędzie⁹.

Z definicji tej wyłaniają nam się dwa ujęcia cyberprzestępczości: horyzontalne i wertykalne, o których również w swojej książce napisał Jerzy Kosiński.

⁴ J. Wasilewski, *Cyberprzestępczość – wybrane aspekty prawnokarne i kryminalistyczne*, Białystok 2017, s. 98.

⁵ M. Stefanowicz, *Cyberprzestępczość – próba diagnozy zjawiska*, „Kwartalnik Policyjny” 2017, nr 4, s. 21.

⁶ Tamże.

⁷ *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa 2013, s. 5.

⁸ J. Wasilewski, *Cyberprzestępczość – wybrane aspekty...*, dz. cyt., s. 106.

⁹ D. Wyglądała, *Internet jako źródło cyberprzestępczości*, „Zeszyty Naukowe Pro Publico Bono” 2020, t. 1(1), s. 115.

Przywołany autor wyodrębnił również cechy cyberprzestępczości, do których zaliczył między innymi:

- niewielkie koszty;
- anonimowość sprawcy;
- komputer (urządzenie z dostępem do Internetu) może być przedmiotem, celem lub środkiem ataku;
- globalny zasięg (brak granic);
- mniejszy bufor czasowy potrzebny do popełnienia przestępstwa;
- ofiara może nie być świadoma, że jej urządzenie (system) zostało zaatakowane¹⁰.

Cyberprzestępczość jest zjawiskiem specyficznym ze względu na właściwości miejsca, gdzie jest ona realizowana tj. w cyberprzestrzeni. Przestrzeń wirtualna pozbawiona jest fizycznych cech obecności sprawcy takich jak odciski palców. Znajduje to swoje odzwierciedlenie w dość wysokiej liczbie ofiar, przy coraz to trudniejszym wykrywaniu sprawców cyberprzestępstw¹¹.

Klasyfikacja cyberprzestępstw

Dokonanie dogłębnej klasyfikacji oraz charakterystyki cyberprzestępstw jest rzeczą bardzo skomplikowaną, przez wzgląd na ich charakter oraz specyfikę. Natomiast analizując dostępną literaturę z tego zakresu można wyszczególnić dwie podstawowe kategorie przestępstw w cyberprzestrzeni:

- *charakterystyczne dla cyberprzestępczości, w których przedmiotem ataku jest komputer, jak też szeroko pojęte przetwarzanie danych w systemach informatycznych*¹² – przykładami są *sniffing* (podśluch komputerowy), czy *hacking* (uzyskanie informacji w sposób nieuprawniony);
- *popełniane z wykorzystaniem sieci Internet, w których komputer jest wyłącznikiem środkiem do jego popełnienia*¹³ – np. *propagowanie treści pedofilskich, obraza uczuć religijnych*.

¹⁰ J. Kosiński, *Paradygmaty cyberprzestępczości*, Difin SA, Warszawa 2015, s. 46.

¹¹ M. Jurek, *Cyberprzestępczość w dobie transformacji cyfrowej państwa. Analiza wybranych problemów*, „Transformacje” 2023, t. 1(116), s. 102.

¹² A. Lebedowicz, *Wybrane aspekty prawnokarne, kryminalistyczne i kryminologiczne cyberprzestępczości*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury” 2022, t. 45, z. 1, s. 35.

¹³ Tamże.

Z kolei Wasilewski w swojej rozprawie doktorskiej pt. „Cyberprzestępczość – wybrane aspekty prawnokarne i kryminalistyczne” podzielił cyberprzestępstwa na następujące grupy:

- przeciwko integralności, poufności i dostępności danych;
- związane z używaniem komputerów;
- związane z rozpowszechnianiem treści zakazanych np. pornografii dziecięcej;
- „przestępstwa przeciwko dostępowi warunkowemu do usług informacyjnych”¹⁴.

Analizując kolejne rozdziały książki Kosińskiego pt. „Paradygmaty cyberprzestępczości” możemy wykazać szerszy podział przestępstw w sieci, co zobrazowane zostało poniżej (Tabela 1).

Tabela 1. Klasyfikacja cyberprzestępstw

Przeciw poufności oraz integralności i dostępności danych	• hacking • szpiegostwo komputerowe • ataki DoS, DDoS • podsłuchiwanie użytkowników • nieuprawnione zmienianie czy niszczenie danych • sabotaż komputerowy
Przestępstwa, w których komputer jest narzędziem	• oszustwa (manipulacja fakturami, nielegalne aukcje) • komputerowe podróbki • fałszerstwo komputerowe
Związane z treścią	• rozpowszechnianie nieprawdziwych informacji • molestowanie internetowe • dziecięca pornografia • dostarczanie instrukcji przestępczych • nawoływanie do nienawiści (np. na tle rasowym) • rozsyłanie gróźb karalnych • cyberstalking • kradzież tożsamości • phishing • grooming (uwodzenie dzieci w sieci) • pomówienie, znieważanie danej osoby • wysyłanie fałszywych wiadomości • nielegalna sprzedaż leków • nielegalna sprzedaż organów

¹⁴ J. Wasilewski, *Cyberprzestępczość – wybrane aspekty...*, dz. cyt., s. 111.

Związane z naruszeniem prawa autorskiego i praw pokrewnych	• nielegalne uzyskanie programu komputerowego • nielegalne wykorzystanie cudzych utworów • plagiat • nielegalne rozpowszechnianie cudzego utworu
Inne cyberprzestępstwa	• udostępnianie danych osobowych osobom nieuprawnionym • przetwarzanie danych osobowych bez prawa przetwarzania • naruszenie obowiązku zabezpieczenia danych osobowych np. przed uszkodzeniem • nielegalny hazard internetowy

Źródło: Opracowanie własne na podstawie: J. Kosiński, *Paradygmaty cyberprzestępczości*, Difin SA, Warszawa, 2015.

Biorąc pod uwagę ciągły rozwój nowych technologii oraz sztucznej inteligencji należy mieć na uwadze, że powyższa tabela ma charakter otwarty. Postęp się nie zatrzymuje i wraz z jego rozwojem będą pojawiać się nowe rodzaje cyberprzestępczości. Przekonuje o tym Marcin Konieczny, który podkreśla, że „Cyberprzestępczość to nowa i jedna z najszybciej rozwijających się przestępczości o transgranicznym charakterze”¹⁵. W artykule Małgorzaty Wróbel pt. „Cyberprzestępczość w polskim systemie prawnym” zostały wyodrębnione trzy grupy cyberprzestępstw. Pierwsza z grup – przestępstwa komputerowe – do której zostały zaliczone takie czyny zabronione jak: hacking komputerowy, nieuprawnione niszczenie informacji, szpiegostwo czy oszustwo komputerowe. Druga grupa określona została mianem przestępstw komunikacyjnych wśród której możemy wyodrębnić np. oszustwo telekomunikacyjne czy kradzież impulsów telefonicznych. Ostatnią grupę stanowią przestępstwa internetowe, takie jak: podmiana zawartości stron internetowych, nielegalny handel lekami czy internetowe oszustwa¹⁶. Do tej grupy możemy również zaliczyć gry internetowe, gry hazardowe, jak również nielegalne rozpowszechnianie cudzych utworów.

Analiza rodzajów cyberprzestępstw

Analizując dostępną literaturę przedmiotu można z pełną świadomością stwierdzić, że istnieje wiele rodzajów cyberprzestępstw. Chęć zysku i zaspokojenia

¹⁵ M. Konieczny, *Cyberprzestępczość – krótka historia, współczesne oblicza i trudna do przewidzenia przyszłość*, „Roczniki Administracji i Prawa” 2023, XXIII, z. 1, s. 33.

¹⁶ M. Wróbel, *Cyberprzestępczość w polskim systemie prawnym* [w:] *Wiedza Obronna*, Towarzystwo Wiedzy Obronnej, 2014, s. 77-78.

własnych potrzeb sprawia, iż przestępcy w sieci „sięgają” po coraz to nowsze metody swoich działań. W niniejszym artykule zostaną omówione wybrane rodzaje przestępstw w cyberprzestrzeni.

Phishing

Jednym z najpoważniejszych obecnie rodzajów cyberprzestępstw, na które narażony jest każdy użytkownik sieci jest *phishing*, czyli metoda opierająca się na inżynierii społecznej. Polega ona na podszyciu się pod daną instytucję w celu wykradzenia danych od użytkownika¹⁷. Miron Lakomy charakteryzując to zagrożenie stwierdził, iż jest to:

podsywanie się pod określoną osobę lub instytucję w celu wyłudzenia wrażliwych informacji, takich jak np. loginy i hasła do kont bankowych. Od innych cyberataków różni się on przede wszystkim tym, iż *de facto* omija zabezpieczenia komputerowe, bazując przede wszystkim na psychologii i logice relacji międzyludzkich (...)¹⁸.

Hakerzy, stosując ten rodzaj ataku, wykorzystują różnego rodzaju „zachęty”, takie jak wiadomości e-mail. Celem takiego działania jest chęć wywołania u ofiary chaotycznego i szybkiego podjęcia działania (zazwyczaj kliknięcia w zainfekowany link)¹⁹. O tym, jak poważnym zagrożeniem dla społeczeństwa jest aktualnie *phishing* mogą świadczyć dane publikowane w raportach CERT Polska, w których możemy odnaleźć, że liczba tego typu ataków na przestrzeni kilku ostatnich lat jest bardzo wysoka. W najnowszym, dostępnym aktualnie zestawieniu (za rok 2023) widnieje, że doszło do ponad 95000 zgłoszeń *phishingu* w polskich sieciach²⁰.

Tabela 2 obrazuje cele, pod które najczęściej podszywali się przestępcy w 2023 r. Przedstawione dane ukazują również jak zmieniła się liczba przestępstw w porównaniu z rokiem 2022. Omawiając niniejsze przestępstwo

¹⁷ R. Kołodziejczyk, *Nowa odsłona terroryzmu – cyberterroryzm*, „Rocznik Bezpieczeństwa Międzynarodowego” 2017, tom 11, nr 2, s. 153.

¹⁸ M. Lakomy, *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wyd. Uniwersytetu Śląskiego, Katowice 2015, s. 131.

¹⁹ R. Kołodziejczyk, P. Manowiecki, *Phishing jako zagrożenie cybernetyczne występujące wśród młodzieży*, „Rocznik Świętokrzyski” 2023, t. 4, s. 119..

²⁰ Raport roczny z działalności CERT POLSKA 2023, s. 86 [w:] cert.pl [dostęp: 08.09.2024 r.].

należy zaznaczyć, że istnieje specjalna forma *phishingu*, czyli *spearphishing*, którego charakterystyczną cechą jest ukierunkowanie ataku na konkretną instytucję czy osobę²¹.

Tabela 2. Najczęstsze cele phishingu

Poz.	Cel phishingu	Liczba domen 2023 r.	Liczba domen 2022 r.
1	Inwestycje	20609	2443
2	Allegro	11015	643
3	Baltic Pipe	6971	583
4	Facebook	6638	7186
5	OLX	4564	1656
6	InPost	2770	6728
7	PGNiG	2764	309
8	Tesla	2758	2647
9	Netflix	1495	1231
10	Webmail	1325	562

Źródło: Raport roczny z działalności CERT POLSKA 2023, s. 88 [w:] cert.pl [dostęp: 08.09.2024].

Cyberpedofilia

Kolejnym bardzo istotnym przestępstwem w sieci, na które w bardzo dużym stopniu mogą być narażone osoby młode i dzieci jest *cyberpedofilia*. Według Olgi Jabłonko zjawisko to polega na:

nawiązywaniu przez pedofilów, a także przez osoby posiadające takie skłonności kontaktów z nieletnimi poprzez sieć mające na celu doprowadzenie do spotkania w rzeczywistości oraz seksualne wykorzystanie dziecka²².

²¹ M. Konieczny, *Cyberprzestępczość – krótka historia...*, dz. cyt., s. 37.
²² O. Jabłonko, *W niewoli sieci – współczesne zagrożenia dzieci i młodzieży* [w:] L. Kowalczyk (red.), *Prace Naukowe Wyższej Szkoły Zarządzania i Przedsiębiorczości z siedzibą w Wałbrzychu*, Wałbrzych 2022, s. 50.

Jedną z istotnych cech tego cyberprzestępstwa jest fakt, iż jego sprawcy chcą nawiązać emocjonalną więź z wytypowaną ofiarą oraz zdobyć jej zaufanie. Analizując kwestię *cyberpedofili* zasadnym wydaje się nawiązanie do innego pojęcia *groomingu*. Są to dwa bliskoznaczne stwierdzenia, które funkcjonują w literaturze przedmiotu. Wskazuje na ten fakt Emilia Truskołaska, która w swoim artykule określiła, iż *cyberpedofilia* jest polskim odpowiednikiem *groomingu*²³.

Cyberpedofilia przejawiać się może takimi działaniami jak: wyszukiwanie ofiar za pomocą mediów społecznościowych, tworzenie stron internetowych nawołujących do legalizacji tego zjawiska, nawiązywanie kontaktów z dziećmi oraz wciąganie ich w rozmowy o tematyce seksualnej itp²⁴. Pedofil funkcjonujący w sieci czuje się bezkarnie (za sprawą poczucia jego anonimowości) w związku z czym ośmiela go to do wykonywania czynności, na które nie zdecydowałby się w świecie rzeczywistym.

Cyberstalking

Historia *cyberstalkingu* nie jest dość odległa, bowiem na temat tego problemu zaczęto mówić na początku XXI wieku. To właśnie wtedy Internet bardzo dynamicznie się rozwijał i wiele zjawisk przeniosło się z świata rzeczywistego w przestrzeń wirtualną. Dotyczy to również *cyberstalkingu*, który wywodzi się od zjawiska zwanego *stalking*²⁵. *Cyberstalking* możemy zdefiniować jako „uporczywe i niesprowokowane przez ofiarę działanie, obejmujące wielokrotne groźby oraz zachowania nękające ofiarę, pomimo jej cierpienia i próśb o zaprzestanie, przy użyciu narzędzi komunikacji, jak też informacji, w wyniku którego ofiara obawia się o własne bezpieczeństwo”²⁶. Zjawisko to możemy utożsamiać z uporczywym i zastraszającym śledzeniem ofiary przez sprawcę za pomocą urządzenia (komputer, telefon itp.) z dostępem do sieci. Bardzo zbliżoną definicję *cyberstalkingu* w swoim artykule umieściła Jabłonko, która napisała, cytując: „cyberstalking to intensywne, powtarzające się nękanie ofiary przez groźby i oczernianie jej przy użyciu Internetu i mediów elektronicznych, aby wywołać u niej

²³ E. Truskołaska, *Grooming, czyli uwodzenie małoletnich przez internet – aspekty kryminologiczne oraz prawne* [w:] *Prawo w działaniu. Sprawy karne*, 2021, s. 72.

²⁴ J. Lizut (red.), *Nowa polityka społeczna, Zagrożenia cyberprzestrzeni kompleksowy program dla pracowników służb społecznych*, Wydawnictwo Wyższej Szkoły Pedagogicznej im. Janusza Korczaka, Warszawa 2014, s. 142.

²⁵ M. Konieczny, *Cyberprzestępczość – krótka historia...*, dz. cyt., s. 42.

²⁶ K. Materska, B. Taraszkiewicz (red.), *Ekologia informacji a zasoby informacyjne w bibliotekach i cyberprzestrzeni*, Słupsk 2017, s. 204.

znaczący strach²⁷. Analizując literaturę dotyczącą omawianego zagadnienia możemy wyszczególnić trzy formy nękania, jakie mogą stosować sprawcy stalkingu w cyberprzestrzeni. Są nimi: napastowanie (odbywa się ono tylko w przestrzeni wirtualnej), nękanie (odbywa się zazwyczaj w sieci, ale jest również przenoszone do świata rzeczywistego), oraz dręczenie (dzieje się ono głównie w realnym świecie, a tylko niektóre jego elementy odbywają się w cyberprzestrzeni)²⁸.

Analizując problem *cyberstalkingu* możemy wyodrębnić formy, jakie może przyjąć to zjawisko, np.:

- przeszukiwanie Internetu w celu znalezienia różnych (najlepiej krępujących) informacji o ofierze, które by ją mogły ośmieszyć;
- rozsyłanie nieprawdziwych informacji na temat danej osoby;
- uporczywe komentarze wypisywane przez sprawcę na różnych forach internetowych;
- nagminne wysyłanie obraźliwych wiadomości;
- zachęcanie innych użytkowników sieci do prześladowania bądź znieważania danej osoby²⁹.

Przejawy *cyberstalkingu* mogą być różnorodne, zwłaszcza, że problem ten jest bardzo rozpowszechniony, nie tylko wśród dorosłych, ale również dzieci i młodzieży. Niestety to właśnie poprzez zastraszanie czy nękanie rówieśników młodzi ludzie znajdują sposób na rozwiązywanie własnych problemów. Należy jednak pamiętać, iż uporczywe nękanie jest czynem karalnym, skutkującym pozbawieniem wolności.

Sposoby zapobiegania cyberprzestępczości

Zapobieganie czy też ochrona przez cyberprzestępczością jest rzeczą bardzo istotną, aczkolwiek niekoniecznie prostą. Dlatego podejmowane są różne działania zarówno na szczeblach lokalnych, jak i międzynarodowych, aby ograniczyć występowanie przestępczości w sieci. Utrwalanie odpowiednich reguł oraz kom-

²⁷ O. Jabłonko, *W niewoli sieci...*, dz. cyt., s. 49.

²⁸ J. Lizut (red.), *Nowa polityka społeczna, Zagrożenia cyberprzestrzeni kompleksowy program dla pracowników służb społecznych*, Wyd. Wyższej Szkoły Pedagogicznej im. Janusza Korczaka, Warszawa 2014, s. 175.

²⁹ K. Materska, B. Taraszkiewicz (red.), *Ekologia informacji a zasoby informacyjne w bibliotekach i cyberprzestrzeni*, Słupsk 2017, s. 205.

petencji z zakresu bezpiecznego korzystania z Internetu należy zacząć od najmłodszych lat życia człowieka. Uświadamianie dzieci z zakresu zagrożeń w sieci, rodzajów cyberprzestępstw powinno odbywać się najpierw za sprawą rodziców, potem na zajęciach szkolnych i w dalszej edukacji młodej osoby³⁰. Na ten aspekt zwraca również uwagę Konieczny, który napisał:

Dlatego tak ważne jest edukowanie społeczeństwa i skupienie się na problemie edukacji informatycznej, prowadzonej od najwcześniejszych lat³¹.

Należy od podstaw rozwijać świadomość użytkowników z zakresu cyberbezpieczeństwa, bowiem to właśnie człowiek jest najsłabszym elementem wszystkich zabezpieczeń.

Analizując możliwe sposoby zapobiegania przestępczości w sieci, należy wskazać metody i zasady o jakich zawsze powinni pamiętać użytkownicy Internetu.

Wśród nich możemy wymienić:

- zabezpieczenie dostępu do kont bezpiecznymi i silnymi hasłami;
- korzystanie z weryfikacji dwuetapowej;
- korzystanie oraz bieżąca aktualizacja programów antywirusowych;
- stosowanie zasady ograniczonego zaufania (należy zastanowić się czy np. wiadomość, którą otrzymaliśmy jest spójna, logiczna i prawdziwa);
- dbanie o własną prywatność w sieci (np. korzystanie z trybu incognito)³².

Bardzo istotną rolę w tym procesie odgrywają również działania podejmowane przez różne instytucje z zakresu bezpieczeństwa w sieci. Przykładem mogą być zajęcia edukacyjne z zakresu cyberprofilaktyki prowadzone przez policjantów Centralnego Biura Zwalczania Cyberprzestępczości. Funkcjonariusze podczas prelekcji w szkołach, czy na różnego rodzaju organizowanych konferencjach np. „Chec IT” w Lublinie pogłębiają wiedzę odbiorców z zakresu cyberprzestępczości³³.

³⁰ O. Jabłonko, *W niewoli sieci...*, dz. cyt., s. 55.

³¹ M. Konieczny, *Cyberprzestępczość – krótka historia...*, dz. cyt., s. 47.

³² <https://www.gov.pl/web/baza-wiedzy/jak-chronic-sie-przed-atakami-cyberprzestepcow> [dostęp: 15.09.2024 r.].

³³ *Cyberprofilaktyka – lepiej zapobiegać niż leczyć* [w:] <https://cbzc.policja.gov.pl/bzc/aktualnosci/292,Cyberprofilaktyka-lepiej-zapobiegac-niz-leczyc.html> [dostęp: 15.09.2024 r.].

Działania podejmowane przez rodziców, pedagogów czy przedstawicieli różnych instytucji z zakresu bezpieczeństwa w sieci powinny koncentrować się na ukształtowaniu u odbiorców (dzieci, młodzieży) dwóch bardzo istotnych kompetencji: myślenia krytycznego oraz myślenia przewidującego. Myślenie krytyczne np. pomaga chronić danej osobie swoją prywatność w sieci oraz minimalizuje podatność na przyswajanie manipulacji w niej zawartej. Z kolei myślenie przewidujące to zdolność szybkiego reagowania i podejmowania działania na podstawie aktualnych obserwacji i wiedzy w odniesieniu do zdarzeń mogących wystąpić w przyszłości. Anna Mróz określiła, iż „Myślenie krytyczne to kompetencja niezwykła w czasach wszechobecności nowych mediów w życiu każdego człowieka. Podobnie myślenie przewidujące jest kompetencją determinującą bezpieczeństwo własne i innych użytkowników sieci”³⁴.

Zwalczanie cyberprzestępczości

Wspomniane wyżej działania prewencyjne z zakresu bezpieczeństwa w sieci są konieczne i niewątpliwie skuteczne. Niestety są sytuacje, kiedy to z różnych przyczyn nie uda się zapobiec cyberprzestępstwu i sprawcy „dopadają” swoje ofiary. W takiej sytuacji należy podjąć niezbędne kroki, aby z cyberprzestępczością walczyć, co *de facto* nie jest rzeczą łatwą.

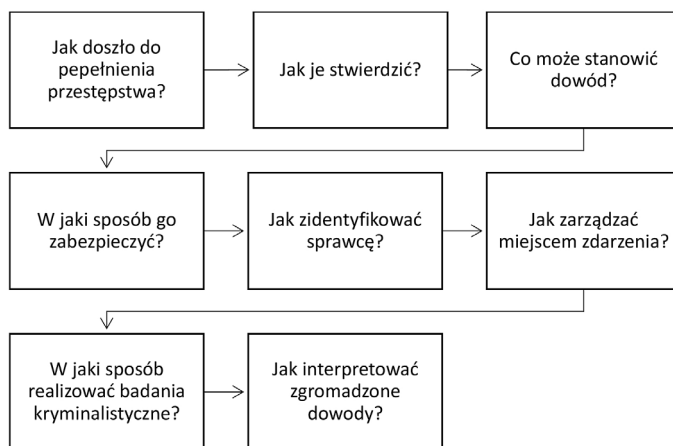
Cyberprzestrzeń jest płaszczyzną posiadającą specyficzną strukturę funkcjonowania, w związku z czym możemy wyodrębnić kilka aspektów, które stanowią trudność w zwalczaniu cyberprzestępczości. Problemy te (sformułowane w postaci pytań) zostały ukazane na schemacie obok (Rycina 1).

Dokonując rozważań na temat problemów związanych ze skutecznym zwalczaniem przestępstw w sieci Kosiński w swojej pozycji opracował model zwalczania cyberprzestępczości, który oparł na trzech filarach: śledztwo sieciowe, zarządzanie miejscem zdarzenia oraz analiza dowodów cyfrowych³⁵. Takie podejście ma sprawić, iż proces zwalczania cyberprzestępczości stanie się mniej skomplikowany oraz będzie bardziej zrozumiały i skuteczny.

W Polsce instytucją, która obecnie jest odpowiedzialna za zwalczanie przestępczości w sieci jest Centralne Biuro Zwalczania Cyberprzestępczości (CBZC).

³⁴ A. Mróz, *Kompetencje kluczowe dla zrównoważonego rozwoju jako determinanta bezpieczeństwa młodych ludzi w sieci* [w:] M. Górka (red.), *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, Wyd. Difin, Warszawa, 2017, s. 269.

³⁵ J. Kosiński, *Paradygmaty cyberprzestępczości*, Wyd. Difin, Warszawa, 2015, s. 214.



Ryc. 1. Problemy w procesie zwalczania cyberprzestępczości

Źródło: Opracowanie własne na podstawie: M. Kozielska (red.), *Przegląd naukowo-metodyczny Edukacja dla Bezpieczeństwa*, Wydawnictwo Wyższej Szkoły Bezpieczeństwa, Poznań, 2019, s. 165.

Biuro jest wyspecjalizowaną jednostką Policji, powołaną na mocy ustawy z dnia 17 grudnia 2021 roku³⁶.

CBZC odpowiedzialne jest za realizację zadań w zakresie:

1. „rozpoznawania i zwalczania przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej oraz zapobiegania przestępstwom, a także wykrywania i ścigania sprawców przestępstw”;
2. „wspierania w niezbędnym zakresie jednostek organizacyjnych Policji w rozpoznawaniu, zapobieganiu i zwalczaniu tych przestępstw”³⁷.

O tym jak istotną rolę odgrywa CBZC mogą świadczyć statystyki dotyczące działalności Biura. Według dostępnych danych w 2023 roku funkcjonariusze tej formacji zatrzymali ponad 500 osób oraz odzyskali mienie o wartości ponad 14,3 mln zł³⁸.

³⁶ K. Pawelec, *Centralne Biuro Zwalczania Cyberprzestępczości i jego wybrane uprawnienia. Kilka refleksji* [w:] *Cybersecurity and Law*, Akademia Sztuki Wojennej, 2022, s. 131.

³⁷ <https://cbzc.policja.gov.pl/bzc/o-cbzc/podstawowe-zadania/5,Zadania-Centralnego-Biura-Zwalczania-Cyberprzestepczosci.html> [dostęp: 24.09.2024 r.].

³⁸ <https://cbzc.policja.gov.pl/bzc/statystyka/raporty-z-dzialalnosci/262,Raporty-z-dzialalnosci.html> [dostęp: 24.09.2024 r.].

Podsumowanie

Rozwój sieci przyniósł epokową zmianę dla społeczeństwa oraz stał się punktem początkowym wielu zmian w jego funkcjonowaniu. Internet stworzył dla ludzi nowe możliwości rozwoju i pracy, a także stał się nieodzownym elementem w codziennym funkcjonowaniu. Szeroki dostęp do informacji, zakupy w sieci, rozrywka czy portale społecznościowe ułatwiające kontakt z innymi, to tylko niektóre z zalet tego wynalazku. Należy jednak pamiętać, że Internet oprócz wielu zalet, ma też wady, w postaci coraz to szerszej puli zagrożeń dla użytkownika. Cyberprzestępczość, jak ukazuje powyższe opracowanie, jest zjawiskiem bardzo trudnym do scharakteryzowania i sklasyfikowania, bowiem powstają coraz to nowe rodzaje przestępstw w sieci. Liczba czynów zabronionych w Internecie na przestrzeni ostatnich kilku lat znacząco wzrosła, przez co temat zapobiegania i zwalczania cyberprzestępczości odgrywa bardzo istotną rolę w narracji społecznej.

Użytkownicy Internetu często nie zdają sobie sprawy na jak wiele niebezpieczeństw są narażeni, dlatego bardzo istotne jest rozwijanie w nich wiedzy i budowanie świadomości z tego obszaru. Uwagę należy tutaj zwrócić w stronę dzieci i młodzieży, bowiem to oni zazwyczaj spędzają w sieci najwięcej czasu przez co są najbardziej narażeni na takie zjawiska jak np. *cyberstalking* czy *cyberpedofilia*. Myślenie krytyczne, oraz myślenie przewidujące, są to dwie kompetencje, które należy kształtować u społeczeństwa od najmłodszych lat.

Istotnym momentem w kwestii zapobiegania, jak i zwalczania cyberprzestępstw w Polsce, było utworzenie Centralnego Biura Zwalczania Cyberprzestępczości. Jest to organ (w ocenie autora opracowania niezbędny) dla obecnych oraz przyszłych pokoleń. Istotne jest, aby CBZC cały czas się rozwijało i zwiększało swój potencjał zarówno osobowy, jak i materialny, bowiem przestępcy w sieci są coraz bardziej wyrafinowani.

Bibliografia

- Czerski W., *Cyberprzestępczość wśród nieletnich – charakterystyka zjawiska, jego skala i przeciwdziałanie* [w:] *Dydaktyka Informatyki*, Wyd. Uniwersytetu Rzeszowskiego, Rzeszów 2022.
- Cyberprofilaktyka – lepiej zapobiegać niż leczyć* [w:] <https://cbzc.policja.gov.pl/bzc/aktualnosci/292,Cyberprofilaktyka-lepiej-zapobiegac-niz-leczyc.html> [dostęp: 15.09.2024 r.].

- <https://www.gov.pl/web/baza-wiedzy/jak-chronic-sie-przed-atakami-cyberprzestepcow> [dostęp: 15.09.2024 r.].
- <https://cbzc.policja.gov.pl/bzc/statystyka/raporty-z-dzialalnosci/262,Raporty-z-dzialalnosci.html> [dostęp: 24.09.2024 r.].
- <https://cbzc.policja.gov.pl/bzc/o-cbzc/podstawowe-zadania/5,Zadania-Centralnego-Biura-Zwalczania-Cyberprzestepczosci.html> [dostęp: 24.09.2024 r.].
- Jabłonko O., *W niewoli sieci – współczesne zagrożenia dzieci i młodzieży* [w:] L. Kowalczyk (red.), *Prace Naukowe Wyższej Szkoły Zarządzania i Przedsiębiorczości z siedzibą w Wałbrzychu*, Wałbrzych 2022.
- Jurek M., *Cyberprzestępczość w dobie transformacji cyfrowej państwa. Analiza wybranych problemów*, „Transformacje” 2023, t. 1(116).
- Kołodziejczyk R., *Nowa odsłona terroryzmu – cyberterroryzm*, „Rocznik Bezpieczeństwa Międzynarodowego”, Wydawnictwo Naukowe Dolnośląskiej Szkoły Wyższej, Wrocław 2017, tom 11, nr 2.
- Kołodziejczyk R., Manowiecki P., *Phishing jako zagrożenie cybernetyczne występujące wśród młodzieży*, „Rocznik Świętokrzyski” 2023, t. 4.
- Konieczny M., *Cyberprzestępczość – krótka historia, współczesne oblicza i trudna do przewidzenia przyszłość*, „Roczniki Administracji i Prawa” 2023, XXIII, z. 1.
- Kosiński J., *Paradygmaty cyberprzestępczości*, Difin SA, Warszawa 2015.
- Lakomy M., *Cyberprzestrzeń jako nowy wymiar rywalizacji i współpracy państw*, Wydawnictwo Uniwersytetu Śląskiego, Katowice 2015.
- Lebiedowicz A., *Wybrane aspekty prawnekarne, kryminalistyczne i kryminologiczne cyberprzestępczości*, „Kwartalnik Krajowej Szkoły Sądownictwa i Prokuratury” 2022, t. 45, z. 1.
- Lizut J. (red.), *Nowa polityka społeczna, Zagrożenia cyberprzestrzeni kompleksowy program dla pracowników służb społecznych*, Wydawnictwo Wyższej Szkoły Pedagogicznej im. Janusza Korczaka, Warszawa 2014.
- Materska K., Taraszkiewicz B. (red.), *Ekologia informacji a zasoby informacyjne w bibliotekach i cyberprzestrzeni*, Słupsk 2017.
- Mróz A., *Kompetencje kluczowe dla zrównoważonego rozwoju jako determinanta bezpieczeństwa młodych ludzi w sieci* [w:] M. Górka (red.), *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, Wyd. Difin, Warszawa 2017.
- Pawelec K., *Centralne Biuro Zwalczania Cyberprzestępczości i jego wybrane uprawnienia. Kilka refleksji* [w:] *Cybersecurity and Law*, Akademia Sztuki Wojennej, Warszawa 2022.
- Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, Warszawa 2013.
- Raport roczny z działalności CERT POLSKA 2023, s. 86 [w:] cert.pl [dostęp: 08.09.2024 r.].
- Stefanowicz M., *Cyberprzestępczość – próba diagnozy zjawiska*, „Kwartalnik Policyjny” 2017, nr 4.
- Truskolaska E., *Grooming, czyli uwodzenie małoletnich przez internet – aspekty kryminologiczne oraz prawne* [w:] *Prawo w działaniu. Sprawy karne*, Warszawa 2021.
- Wasilewski J., *Cyberprzestępczość – wybrane aspekty prawnekarne i kryminalistyczne*, Białystok 2017.
- Wasilewski J., *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd Bezpieczeństwa Wewnętrznego” 2016, nr 15.

- Wróbel M., *Cyberprzestępczość w polskim systemie prawnym* [w:] *Wiedza Obronna*, Towarzystwo Wiedzy Obronnej, Warszawa 2014.
- Wyglądała D., *Internet jako źródło cyberprzestępczości*, „Zeszyty Naukowe Pro Publico Bono” 2020, t. 1(1).

Część II.

Bezpieczeństwo
penitencjarne
w ujęciu
holistycznym

Warunki życia osadzonych a bezpieczeństwo jednostek penitencjarnych

Angelika MARUSZEWSKA¹

Akademia Wymiaru Sprawiedliwości w Warszawie

ORCID: 0000-0001-7328-8453

Streszczenie. Artykuł analizuje złożoną relację między warunkami życia osadzonych a bezpieczeństwem jednostek penitencjarnych. Zwraca uwagę, że bezpieczeństwo w zakładach karnych i aresztach śledczych jest kluczowe nie tylko dla ochrony personelu, ale również dla więźniów oraz całego społeczeństwa. Badanie koncentruje się na aktualnych regulacjach prawnych, w tym na programie „Nowoczesne Więziennictwo”², którego celem jest poprawa warunków życia skazanych poprzez zindywidualizowane podejście oraz zwiększenie dostępu do programów resocjalizacyjnych. Analiza wskazuje na konieczność stworzenia warunków sprzyjających rehabilitacji, co ma pozytywny wpływ na bezpieczeństwo w jednostkach penitencjarnych. W pracy uwzględniono również statystyki dotyczące liczby osadzonych oraz jakości życia w polskich zakładach karnych, co pozwala na sformułowanie wniosków dotyczących skuteczności stosowanych metod resocjalizacji i bezpieczeństwa.

Słowa kluczowe: warunki życia osadzonych, życie w zakładzie karnym, nowoczesne więziennictwo, bezpieczeństwo w jednostce penitencjarnej, prawo karne wykonawcze

Wstęp

Podstawową potrzebą, którą człowiek musi zaspokoić, jest bezpieczeństwo. Izolacja w zakładach karnych wpływa negatywnie na prawa i wolność jednostki,

¹ Angelika Maruszewska – magister prawa, asystent prokuratora przy Prokuraturze Regionalnej w Warszawie, zainteresowania badawcze: penitencjarystyka, psychologia, prawo.

² Program „Nowoczesne Więziennictwo” to inicjatywa w polskim systemie penitencjarnym, mająca na celu poprawę warunków życia osadzonych oraz ich resocjalizację. Skupia się na indywidualnym podejściu do skazanych, dostosowując programy rehabilitacyjne do ich potrzeb. W ramach programu zwiększono dostęp do pracy oraz zajęć edukacyjnych, kulturalnych i sportowych, co ma przygotować osadzonych do powrotu do społeczeństwa. Dodatkowo, program ma na celu zwiększenie bezpieczeństwa w zakładach karnych przez rozwijanie pozytywnych postaw i umiejętności społecznych.

prowadząc do wielu emocjonalnych problemów, które mogą zagrażać bezpieczeństwu osadzonych.

Warunki życia osadzonych stanowią fundamentalny element funkcjonowania systemu sprawiedliwości, który wpływa nie tylko na same osoby odbywające karę, ale również na bezpieczeństwo całego społeczeństwa. Izolacja w zakładach karnych oraz aresztach śledczych wiąże się z wieloma wyzwaniami, które mogą prowadzić do negatywnych konsekwencji zarówno dla osadzonych, jak i dla personelu.

Od 1 stycznia 2023 roku w Polsce wprowadzono nowe przepisy w Kodeksie karnym wykonawczym oraz ustawie o Służbie Więziennej, tworząc program „Nowoczesne Więziennictwo”. Nowe regulacje mają na celu poprawę warunków życia osadzonych, w tym rozszerzenie programu pracy, umożliwienie rozmów telefonicznych oraz czasowe opuszczanie jednostki w celu uczestnictwa w zajęciach sportowych i kulturalnych.

Służba Więzienna, jako kluczowa instytucja w systemie bezpieczeństwa wewnętrznego³, ma za zadanie izolację i resocjalizację skazanych. Przepisy „Nowego Więziennictwa” zwiększają poziom bezpieczeństwa w jednostkach penitencjarnych, co ma ogromne znaczenie dla ochrony całego społeczeństwa (zapobieganie ucieczkom i nieuprawnionym opuszczeniom), bezpieczeństwa personelu więziennego (w tym ochrona przed przestępstwami, takimi jak napaści na funkcjonariuszy) oraz bezpieczeństwa osadzonych (które obejmuje zapobieganie przemocy fizycznej i psychicznej, bójkom czy innym przestępstwom).

Z perspektywy analizy statystyk Służby Więziennej należy zauważyć, że warunki życia blisko 71 tysięcy faktycznie osadzonych⁴ oraz rzeczywiste bezpieczeństwo 175 jednostek penitencjarnych w Polsce⁵ zasługują na dokładniejsze zbadanie. Celem tego opracowania jest analiza relacji między warunkami życia osadzonych a bezpieczeństwem jednostek penitencjarnych. Przeanalizowane zostaną aktualne regulacje prawne oraz praktyki, które wpływają na jakość życia skazanych i ich proces rehabilitacji. W pracy uwzględnione zostaną również dane statystyczne dotyczące liczby osadzonych i ich sytuacji w polskich zakładach karnych, co pozwoli na sformułowanie wniosków dotyczących skuteczności wprowadzonych zmian oraz ich wpływu na bezpieczeństwo w jednostkach penitencjarnych.

³ Zarządzenie Ministra Sprawiedliwości z dnia 5.03.2024 r. w sprawie nadania statutu Centralnemu Zarządowi Służby Więziennej (Dz.Urz.MS.2024.67).

⁴ Informacja o zaludnieniu jednostek penitencjarnych – Centralny Zarząd Służby Więziennej Biuro Ewidencji, z dnia 18.10.2024 r., sygn. BEW.0335.42.2024.JL.

⁵ Dane statystyczne Służby Więziennej – stan na dzień 31.12.2023 r., sygn. BIS.0332.17.2023. MM <https://www.sw.gov.pl/strona/statystyka-roczna> [dostęp: 18.10.2024 r.].

Izolacja penitencjarna, a środki oddziaływania penitencyjnego

Izolacja w zakładzie karnym to forma ograniczenia wolności, która ma na celu nie tylko ukaranie przestępców, ale również ich resocjalizację. Ten proces jest bardzo złożony i oddziałuje na różne aspekty życia osadzonych, ich rodzin oraz społeczeństwa.

W myśl art. 67 §3 k.k.w.⁶, priorytetem w oddziaływaniu na skazanych jest zapewnienie im możliwości pracy oraz zdobywania kwalifikacji zawodowych. Obejmuje to również nauczanie, zajęcia kulturalno-oświatowe, sportowe, a także wspieranie kontaktów z rodziną i światem zewnętrznym oraz stosowanie środków terapeutycznych.

Z kolei zgodnie z art. 67 §1 k.k.w. celem wykonywania kary pozbawienia wolności jest wzbudzenie w skazanym chęci współpracy w kształtowaniu społecznie pożądanых postaw, w szczególności poczucia odpowiedzialności oraz potrzeby przestrzegania prawa. Z treści przywołanej normy wynika, że głównym celem wykonywania kary izolacyjnej jest wprowadzenie w osobowości osadzonego takich zmian, które umożliwią mu zrozumienie popełnionych błędów oraz przyczynią się do zadośćuczynienia innym i moralnego odrodzenia. Podstawą jest osiągnięcie takich zmian, które zapewnią, że osadzony po wyjściu z więzienia będzie przestrzegał prawa⁷.

Umieszczenie osoby w zakładzie karnym lub areszcie śledczym, powinno być uzasadnione nie tylko koniecznością wykonania nałożonej kary, ale także przekonaniem, że skazany, po zakończeniu okresu izolacji, wróci do społeczeństwa jako osoba zmieniona, przystosowana do życia zgodnie z obowiązującymi normami i regułami życia w społeczeństwie. Jednak aby osiągnąć te cele, niezbędne jest właściwe stosowanie odpowiednich, zindywidualizowanych mechanizmów i procedur wobec osadzonych, zgodnie z przepisami prawa.

Osiągnięcie celu kary pozbawienia wolności realizowane jest poprzez zindywidualizowane oddziaływanie na skazanych. W tym celu wykorzystuje się narzędzia określane jako środki oddziaływania penitencyjnego. Jest to zbiór metod i środków stosowanych w zakładzie karnym, mających na celu wzbudzenie w osadzonym chęci współpracy w kształtowaniu społecznie akceptowanych postaw, co przyczynia się do realizacji celu kary. Zakres tych działań zależy od systemu wykonywania kary, a także od rodzaju i typu jednostki penitencyjnej.

⁶ Kodeks karny wykonawczy (Dz.U.2024.706).

⁷ S. Paweła, *Prawo karne wykonawcze. Zarys Wykładu*. Wyd. Zakamycze, Kraków 2003, s. 24-25; S. Paweła, *Kodeks karny wykonawczy. Praktyczny komentarz*, Wyd. ZPP, Warszawa 1999 [dostęp: 18.10.2024].

Ustawodawca nakłada obowiązek prowadzenia oddziaływania penitencjarnego w formie zindywidualizowanych działań, dostosowanych do psychofizycznych cech każdego skazanego, jak i do grupy skazanych. Zindywidualizowanie środków oddziaływania penitencjarnego ma kluczowe znaczenie, ponieważ zwiększa szanse na osiągnięcie pożądaných efektów wychowawczych.

W świetle obowiązującego prawa, do środków oddziaływania na skazanych należą w szczególności zatrudnienie, edukacja, zajęcia sportowe oraz kulturalno-oświatowe, a także nagradzanie i karanie dyscyplinarne⁸, jak również kontakty z rodziną i światem poza jednostką penitencjarną. Można to interpretować jako aktywizację skazanych, właściwe podejście do nich oraz stymulowanie ich do podejmowania własnych działań⁹.

Zatrudnienie

Współcześnie zatrudnienie osadzonych nie jest już jedynie elementem kary, ale przede wszystkim narzędziem resocjalizacji, przynoszącym korzyści zarówno pracodawcom, jak i osadzonym oraz ich rodzinom. Trybunał Konstytucyjny trafnie wskazał, że „dla skazanych praca nadal pozostaje jednym z podstawowych obowiązków, w cieniu którego pozostaje ich prawo do pracy”¹⁰.

Zatrudnienie skazanych w polskim systemie prawnym reguluje głównie Ustawa z 6 czerwca 1997 r. – Kodeks karny wykonawczy, szczególnie w rozdziale X zatytułowanym „Kara pozbawienia wolności”, w oddziale 5 poświęconym „Zatrudnieniu”¹¹. Ponadto, kwestie te porusza również Ustawa z 28 sierpnia 1997 r. o zatrudnieniu osób pozbawionych wolności¹².

Znaczącą rolę odgrywa również Rekomendacja Rec (2006) 2 Komitetu Ministrów do państw członkowskich Rady Europy dotycząca Europejskich Reguł Więziennych, przyjęta przez Komitet Ministrów 11 stycznia 2006 r.¹³. Z Rekomendacji wynika, że wszystkie osoby pozbawione wolności powinny być traktowane z poszanowaniem przysługujących im praw, co nie wyklucza możliwości wykonywa-

⁸ §35. Rozporządzenia Ministra Sprawiedliwości z dnia 23.12.2022 r. w sprawie regulaminu organizacyjno porządkowego wykonywania kary pozbawienia wolności (Dz.U.2022.2847).

⁹ T. Szymanowski, Z. Świda, *Kodeks karny wykonawczy. Komentarz*, Warszawa 1998, s. 148.

¹⁰ Wyrok Trybunału Konstytucyjnego z 13.12.2004 r., sygn. K 20/04, OTK-A 2004/11, poz. 115; LEX 140352.

¹¹ Art. 121-129 k.k.w. (Dz.U.2024.706).

¹² Ustawa z dnia 28 sierpnia 1997 r. o zatrudnieniu osób pozbawionych wolności (Dz.U.2023.1559).

¹³ Zalecenia Rec (2006) 2 Komitetu Ministrów państw członkowskich Rady Europy w sprawie Europejskich Reguł Więziennych (przyjętych przez Komitet Ministrów w dniu 11 stycznia 2006 r. na 952 posiedzeniu delegatów) <https://sw.gov.pl> [dostęp: 18.10.2024 r.].

nia pracy przez skazanych w ramach kary pozbawienia wolności. Rekomendacja Komitetu Ministrów Rady Europy jasno wskazuje na kilka kluczowych zasad dotyczących zatrudnienia skazanych. Po pierwsze, praca osadzonych jest traktowana jako pozytywny element rygoru więziennego i nie może być używana jako forma kary (reg. 26 ust. 1). Władze więzienne są zobowiązane do dążenia do zapewnienia osadzonym pracy, która ma wystarczającą wartość użyteczną (reg. 26 ust. 2). Ponadto, w miarę możliwości, praca przydzielona skazanym powinna wspierać ich umiejętności, aby mogli samodzielnie zarabiać na życie po zwolnieniu (reg. 26 ust. 3). Dodatkowo, rekomendacja podkreśla, że każdy skazany, który wykonuje pracę, powinien otrzymywać sprawiedliwe wynagrodzenie za swoje usługi (reg. 26 ust. 10). Te zasady mają na celu nie tylko resocjalizację osadzonych, ale również ich przygotowanie do życia w społeczeństwie po odbyciu kary¹⁴.

Zatrudnienie osadzonych niesie ze sobą wiele pozytywnych aspektów. Przede wszystkim pozwala im nabywać nowe umiejętności, co znacznie zwiększa ich szanse na znalezienie pracy po odbyciu kary. Dla pracodawców oznacza to z kolei dostęp do zróżnicowanej siły roboczej oraz możliwość korzystania z ulg podatkowych. Praca ma również korzystny wpływ na poczucie własnej wartości osadzonych i sprzyja ich lepszemu reintegracji w społeczeństwie, co pozytywnie oddziałuje na ich rodziny i zmniejsza ryzyko recydywy.

Taki system aktywizacji pozwala osadzonym rozwijać kwalifikacje zawodowe, uczyć się odpowiedzialności, systematyczności oraz współpracy w grupie. Aspekt ekonomiczny zatrudnienia jest równie istotny w kontekście resocjalizacji. Dzięki pracy skazani mogą spłacać długi, takie jak alimenty, oraz wspierać finansowo swoje rodziny na wolności¹⁵.

W Zakładzie Karnym w Warszawie-Białoleśe zatrudnienie osiąga miesięcznie 60-70% wszystkich skazanych, którzy są zdolni do pracy. Codziennie grupy osadzonych wykonują prace na zewnątrz, realizując zlecenia dla różnych firm, takich jak Vendi Service, Bestion Projekt, PPPU Presbet, Kam-Pol, El-Trans, a po zakończeniu pracy wracają do swoich cel mieszkalnych. Inni skazani zajmują się pracami wewnątrz jednostki, wykonując sprzątanie, drobne naprawy, pracując w magazynach oraz wydając posiłki¹⁶.

W 2019 roku Zakład Karny w Raciborzu nawiązał współpracę z firmą Bitron Poland, podpisując porozumienie, które miało na celu zwiększenie zatrudnienia

¹⁴ P. Jaki, *Zatrudnienie skazanych w Polsce na tle porównawczym. Zagadnienia wybrane*, „Przegląd Więziennictwa Polskiego” 2017, nr 95, s. 79-98.

¹⁵ T. Szymanowski, *Funkcje zatrudnienia skazanych w świetle danych empirycznych*, Lublin 1985, s. 53-57.

¹⁶ I. Gradowska, *Oddziaływania penitencjarne – na czym to polega?* <https://sw.gov.pl/jednostka/zatrudnienie-osob-pozbawionych-wolnosci> [dostęp: 18.10.2024 r.].

osób pozbawionych wolności. Dzięki temu liczba osadzonych zatrudnionych w Bitronie wzrosła o ponad 80%. Taka inicjatywa nie tylko sprzyjała resocjalizacji skazanych, ale także pozwalała im zdobyć cenne umiejętności i doświadczenie zawodowe, co zwiększa ich szanse na reintegrację w społeczeństwie po odbyciu kary¹⁷.

Skala wzrostu oraz osiągnięty obecnie poziom zatrudnienia osadzonych w polskich zakładach karnych jest najwyższy od 30 lat. W 2022 roku średnia liczba zatrudnionych skazanych wyniosła 37 468, co przekładało się na powszechność zatrudnienia na poziomie 58,49%. W 2023 roku sytuacja uległa poprawie, a średnie zatrudnienie wzrosło do 41 775 osadzonych, co oznacza wzrost powszechności do 61,62%. Te dane świadczą o coraz większym zaangażowaniu w proces resocjalizacji i integracji osadzonych w życie zawodowe¹⁸.

Warto jednak zauważyć, że sama obecność w pracy nie gwarantuje resocjalizacji – jej efektywność zależy od odpowiednich metod oddziaływania, takich jak system nagród i kar. Aby praca mogła pełnić swoje resocjalizacyjne funkcje, musi być społecznie użyteczna, dobrze zorganizowana, nadzorowana i zgodna z normami bezpieczeństwa oraz higieny pracy. Kluczowe jest także dostosowanie do fizycznych i psychicznych możliwości skazanych oraz ich kwalifikacji i zainteresowań.

Nagrody i kary dyscyplinarne

Wpływ na skazanych odbywających karę pozbawienia wolności opiera się na zastosowaniu różnych środków, które pełnią rolę narzędzi działania. Wśród tych środków znajdują się nagrody oraz kary dyscyplinarne, które mają na celu oddziaływanie na postawy osadzonych.

Analiza art. 138 k.k.w., który określa enumeratywnie katalog nagród, które mogą być przyznane skazanemu w warunkach izolacji penitencjarnej, ujawnia kilka kluczowych aspektów, które mają na celu wspieranie resocjalizacji skazanych oraz ich reintegrację społeczną. Nagrody mają na celu motywowanie skazanych do pozytywnego zachowania oraz przestrzegania regulaminu zakładu karnego. Dają możliwość nagradzania postaw prospołecznych i wspierają proces resocjalizacji¹⁹.

¹⁷ Artykuł zamieszczony na stronie Służby Więziennej w 2019 r., <https://sw.gov.pl/aktualnosc/zaklad-karny-raciborz-rosnie-zatrudnienie-osadzonych-w-zakladzie-karnym> [dostęp: 18.10.2024 r.].

¹⁸ Dane statystyczne Służby Więziennej – stan na dzień 31.12.2023 r., sygn. BIS.0332.17.2023. MM <https://www.sw.gov.pl/strona/statystyka-roczna> [dostęp: 18.10.2024 r.].

¹⁹ A. Gerecka-Żołyńska, *Komentarz Kodeks karny wykonawczy*, Warszawa 2023, s. 468-469.

Nagrody można podzielić na kilka kategorii:

- nagrody związane z kontaktami z bliskimi: zezwolenie na dodatkowe lub dłuższe widzenia oraz widzenia bez dozoru podkreślają znaczenie relacji rodzinnych i społecznych w procesie resocjalizacji;
- nagrody związane z poprawą warunków życia: zezwolenia na opuszczenie zakładu karnego, dodatkowe paczki żywnościowe czy zakupy artykułów codziennego użytku wpływają na komfort życia skazanych;
- nagrody dotyczące edukacji i kultury: umożliwienie uczestnictwa w zajęciach kulturalno-oświatowych sprzyja rozwojowi osobistemu i kulturalnemu skazanych;
- nagrody materialne: nagrody rzeczowe i pieniężne są ważnym elementem motywacyjnym, który może zwiększać zaangażowanie skazanych w programy resocjalizacyjne.

Kary dyscyplinarne definiuje art. 143 k.k.w., mają one na celu utrzymanie porządku i dyscypliny w zakładzie karnym. Stanowią one odpowiedź na niewłaściwe zachowanie skazanych, co jest kluczowe dla zapewnienia bezpieczeństwa i efektywności funkcjonowania instytucji penitencjarnych²⁰.

Kary dyscyplinarne można podzielić na kilka kategorii:

- nagany: stanowią podstawową formę reprimendy, która formalnie potwierdza niewłaściwe zachowanie skazanych;
- pozbawienie nagród lub ulg: ograniczenie dostępu do nagród oraz ulg ma na celu zniechęcenie do nieodpowiednich zachowań poprzez bezpośrednie negatywne konsekwencje;
- ograniczenia w uczestnictwie w zajęciach kulturalno-oświatowych i sportowych: takie kary mogą wpływać na rozwój osobisty skazanych, co czyni je szczególnie dotkliwymi, gdyż ograniczają dostęp do aktywności sprzyjających rehabilitacji;
- pozbawienie możliwości otrzymywania paczek żywnościowych i dokonywania zakupów: te kary mogą znacząco wpływać na codzienne życie skazanych, co sprawia, że są one skuteczną metodą dyscyplinowania;
- udzielanie widzeń w sposób uniemożliwiający bezpośredni kontakt: ograniczenie kontaktu z bliskimi ma poważne konsekwencje emocjonalne i psychiczne, mogąc wpływać na relacje skazanych z ich rodzinami;

²⁰ Tamże, s. 476-477.

- obniżenie wynagrodzenia za pracę: ta kara wpływa na motywację do pracy, co może zniechęcać do działania na rzecz poprawy swojego statusu;
- umieszczenie w celi izolacyjnej: to jedna z najcięższych kar, która może prowadzić do poważnych konsekwencji psychicznych, izolując skazanych od społeczności.

Edukacja i zajęcia sportowe oraz kulturalno-oświatowe

W zakładach karnych stwarza się skazanym warunki do odpowiedniego spędzania czasu – nauczanie, zajęcia sportowe czy kulturalno-oświatowe są istotnym elementem procesu resocjalizacji osadzonych.

Nauczanie jest obowiązkowe w zakładach karnych, szczególnie dla skazanych poniżej 18. roku życia²¹. Art. 130 k.k.w. odnosi się do prawa skazanych do kształcenia i samokształcenia, uznawanego za jedno z podstawowych praw w systemie penitencjarnym. Minister Sprawiedliwości ma możliwość zakładania szkół w jednostkach penitencjarnych, a nadzór nad nauczaniem sprawują dyrektorzy zakładów, a komisje penitencjarne odpowiedzialne są za kwalifikowanie skazanych do nauki. Decyzje komisji dotyczące nauczania nie mogą być zaskarżane do sądu, ale mogą być weryfikowane przez sędziów penitencjarnych i organy nadzoru²². Szczegółowe zasady nauczania określa odpowiednie rozporządzenie Ministra Sprawiedliwości²³.

W jednostkach penitencjarnych organizowane są różnorodne zajęcia kulturalno-oświatowe, które mają na celu rozwijanie zainteresowań oraz umiejętności skazanych²⁴. Programy te obejmują warsztaty artystyczne, wykłady, spotkania z ciekawymi osobami oraz inne formy działalności, które poszerzają horyzonty uczestników. W każdym zakładzie karnym działa wypożyczalnia książek i prasy, a także istnieje możliwość korzystania z urządzeń audiowizualnych w świetlicach oraz celach mieszkalnych. Osadzeni, korzystając z tych urządzeń, muszą jednak przestrzegać ustalonego porządku w zakładzie. Organizowane są także seanse telewizyjne, a także audycje radiowe oraz różne koła zainteresowań²⁵.

Szczególną uwagę przykładą się do wychowania fizycznego i sportu. Zajęcia sportowe, takie jak piłka nożna, siatkówka czy aerobik, nie tylko poprawiają kon-

²¹ T. Szymanowski, *Polityka karna i penitencjarna...*, dz. cyt., s. 184-186.

²² T. Przesławski, W. Sych, *Kodeks karny wykonawczy. Komentarz*, wyd. II. Lex/el 2024.

²³ Rozporządzenie Ministra Sprawiedliwości z 28.11.2016 r. w sprawie sposobu i trybu prowadzenia nauczania w zakładach karnych i aresztach śledczych (Dz.U. poz. 2004).

²⁴ Art. 135-136a k.k.w. (Dz.U.2024.706).

²⁵ A. Gerecka-Żołyńska, *Komentarz...*, dz. cyt., s. 466-468.

dycję fizyczną, ale także uczyć współpracy, dyscypliny oraz wzmacniają więzi społeczne między skazanymi. Regularna aktywność fizyczna ma pozytywny wpływ na zdrowie psychiczne, co jest kluczowe w zamkniętym środowisku. Dodatkowo, w zakładach karnych promuje się aktywność społeczną skazanych, co sprzyja ich integracji oraz budowaniu umiejętności społecznych. Udział w projektach grupowych, wolontariatach czy organizacji wydarzeń wewnętrznych pozwala skazanym na rozwijanie poczucia odpowiedzialności oraz zaangażowania w życie społeczności.

Każdy osadzony, który wykaże choć odrobinę dobrej woli znajdzie dla siebie interesujący program resocjalizacyjny, a wszystkie te działania mają na celu nie tylko umilenie czasu wolnego, ale przede wszystkim przygotowanie do życia po odbyciu kary, poprzez rozwijanie umiejętności, które są niezbędne do funkcjonowania w społeczeństwie²⁶.

Kontakty z rodziną i światem poza jednostką penitencjarną

Kontakty z rodziną i światem zewnętrznym są kluczowe w procesie resocjalizacji osób przebywających w jednostkach penitencjarnych. Utrzymywanie więzi z bliskimi nie tylko wspiera zdrowie psychiczne osadzonych, ale także pomaga im zachować poczucie normalności w trudnym czasie odbywania kary. Regularne rozmowy telefoniczne, wizyty oraz wymiana listów umożliwiają skazanym wyrażanie emocji, dzielenie się przeżyciami i budowanie relacji, co może przynieść ulgę w izolacji²⁷.

Dostęp do informacji o wydarzeniach w świecie zewnętrznym, poprzez prasę czy media, jest równie istotny. Umożliwia to osadzonym śledzenie zmian w społeczeństwie, co ułatwia ich późniejszą adaptację po wyjściu na wolność. Świadomość tego, co dzieje się na zewnątrz, zmniejsza lęk przed nowym otoczeniem i daje poczucie łączności z życiem, które toczy się poza murami zakładu karnego.

²⁶ Dla przykładu: W Zakładzie Karnym w Dębicy prowadzone są programy takie jak: „Mam talent” – realizowany poprzez twórczość własną skazanych, sprzyjający rozwojowi własnych zainteresowań, „Obelisk” – program kształtowania poczucia patriotyzmu i szacunku do historii narodowej poprzez aktywne włączanie się w opiekę nad miejscami pamięci narodowej, czy „Drużyna” – program zespołowej aktywności sportowej. W Zakładzie Karnym w Rawiczu program „Promocja zdrowego trybu życia, nauka akceptowalnych społecznie postaw – Złota Setka 2024”, który odbył się już po raz szósty; <https://www.sw.gov.pl/> [dostęp 20.10.2024 r.].

²⁷ Na terenie jednostki Zakładu Karnego w Garbalinie w ramach programu resocjalizacji w zakresie integracji rodzin odbyło się spotkanie pt. „Mur to nie przeszkoda”; <https://www.sw.gov.pl/> [dostęp: 20.10.2024 r.].

Rodzina odgrywa także kluczową rolę w motywowaniu osadzonych do podejmowania działań resocjalizacyjnych, takich jak nauka czy uczestnictwo w programach terapeutycznych. Wsparcie ze strony bliskich często staje się impulsem do zmiany postaw i zachowań. W związku z tym, jednostki penitencjarne powinny stwarzać sprzyjające warunki do utrzymywania tych kontaktów.

Wprowadzenie programów wspierających komunikację z rodziną oraz organizacja spotkań mogą znacząco wpłynąć na pozytywne rezultaty resocjalizacji. Przez umożliwienie osadzonym aktywnego uczestnictwa w życiu rodzinnym i społecznym, zwiększamy szanse na ich skuteczną reintegrację po zakończeniu kary.

Bezpieczeństwo jednostek penitencjarnych

Bezpieczeństwo jednostek penitencjarnych jest kluczowym aspektem funkcjonowania systemu penitencjarnego. Obejmuje zarówno ochronę skazanych, jak i personelu, a także zapewnienie porządku wewnętrznego w placówkach.

Bezpieczeństwo osób pozbawionych wolności to jeden z kluczowych aspektów, który wpływa na ich zdrowie psychiczne i fizyczne, a także na efektywność procesu resocjalizacji. W trakcie odbywania kary skazani mogą być narażeni na różnorodne zdarzenia, które w znacznym stopniu wpływają na ich codzienne życie.

Wśród najpoważniejszych problemów, z jakimi borykają się osadzeni, należy wymienić znęcanie się psychiczne i fizyczne. Przemoc, zarówno werbalna, jak i fizyczna, może przybierać różne formy, od agresji słownej po brutalne ataki. Takie sytuacje prowadzą do poważnych konsekwencji dla ofiar, w tym do traum, obniżenia poczucia własnej wartości i chronicznego stresu. Osadzeni, którzy doświadczają takich sytuacji, często mają trudności z nawiązywaniem relacji i adaptacją w zamkniętym środowisku.

Bójki i pobicia są kolejnymi aspektami, które wpływają na bezpieczeństwo w jednostkach penitencjarnych. Często wynikają one z napięć między grupami osadzonych, rywalizacji o wpływy lub zasoby, a także z osobistych konfliktów. Takie incydenty nie tylko stwarzają zagrożenie dla zdrowia fizycznego, ale również mogą prowadzić do długotrwałych konsekwencji emocjonalnych i psychicznych²⁸.

Niestety, w niektórych przypadkach dochodzi również do gwałtów. Takie tragiczne zdarzenia mają szczególnie dramatyczny wpływ na życie ofiar, niszcząc ich

²⁸ J. Kowalski, *Bezpieczeństwo w zakładach karnych*, Wyd. Prawnicze, Warszawa 2018, s. 45-50.

poczucie bezpieczeństwa i zaufania. Wiele osób nie zgłasza takich przestępstw z obawy przed odwetem lub z braku wiary w skuteczność działań ochronnych ze strony personelu.

Aby zapewnić bezpieczeństwo osób pozbawionych wolności, niezbędne są działania na wielu frontach. Kluczowe jest wprowadzenie skutecznych procedur monitorowania i reagowania na przypadki przemocy, a także szkolenie personelu w zakresie rozpoznawania i radzenia sobie z sytuacjami konfliktowymi. Ważne jest także stworzenie atmosfery, w której osadzeni czują się bezpieczni, co może być osiągnięte poprzez promowanie działań resocjalizacyjnych oraz edukacyjnych²⁹.

Bezpieczeństwo funkcjonariuszy jednostki penitencjarnej jest kluczowym aspektem skutecznego zarządzania placówkami karnymi. Praca w tych instytucjach wiąże się z wieloma wyzwaniami, a zagrożenia, na które narażeni są pracownicy, mogą mieć poważne konsekwencje zarówno dla ich zdrowia fizycznego, jak i psychicznego.

Jednym z najpoważniejszych problemów są przestępstwa skierowane przeciwko personelowi więziennemu, w tym naruszenie nietykalności cielesnej oraz czynna napaść na funkcjonariuszy. Takie incydenty mogą występować w różnych formach, od agresji werbalnej po brutalne ataki, a ich konsekwencje mogą być tragiczne.

Naruszenie nietykalności cielesnej to nie tylko zagrożenie dla zdrowia fizycznego pracowników, ale także dla ich poczucia bezpieczeństwa. Funkcjonariusze, którzy doświadczają przemocy w miejscu pracy, mogą odczuwać chroniczny stres, co prowadzi do wypalenia zawodowego oraz obniżenia efektywności w wykonywaniu obowiązków. Takie sytuacje mogą również wpływać na atmosferę w całej jednostce, wprowadzając poczucie niepewności i lęku wśród personelu.

Czynna napaść na funkcjonariusza to zjawisko, które może mieć szczególnie poważne skutki. W skrajnych przypadkach może prowadzić do ciężkich obrażeń, a nawet śmierci. Takie ataki często są wynikiem napięć i konfliktów pomiędzy osadzonymi, które mogą eskalować do sytuacji kryzysowych. Właściwe przygotowanie personelu do radzenia sobie z takimi incydentami jest kluczowe dla zapewnienia ich bezpieczeństwa.

Aby zwiększyć bezpieczeństwo funkcjonariuszy, niezbędne są kompleksowe działania. Wprowadzenie odpowiednich procedur monitorowania i zarządzania ryzykiem, a także szkolenie pracowników w zakresie technik deeskalacji konfliktów, może znacząco zmniejszyć liczbę incydentów. Ważne jest również zapewnienie

²⁹ M. Kaczmarek, *Zarządzanie kryzysowe w jednostkach penitencjarnych*, Wyd. Akademickie, Gdańsk 2021, s. 60-65.

funkcjonariuszom dostępu do wsparcia psychologicznego, które pomoże im radzić sobie z konsekwencjami pracy w stresującym środowisku³⁰.

Ponadto, warto zwrócić uwagę na konieczność stworzenia efektywnego systemu raportowania i reagowania na przypadki przemocy. Dzięki temu, personel będzie mógł szybciej interweniować w sytuacjach zagrożenia, co przyczyni się do zwiększenia bezpieczeństwa zarówno funkcjonariuszy, jak i osadzonych³¹.

Bezpieczeństwo całego społeczeństwa jest fundamentalnym celem funkcjonowania jednostek penitencjarnych. Kluczowym aspektem tego zagadnienia jest skuteczne przeciwdziałanie ucieczkom oraz samowolnemu oddaleniu się skazanych z terenu zakładów karnych czy konwojów policyjnych. Takie incydenty nie tylko zagrażają bezpieczeństwu lokalnych społeczności, ale mogą również destabilizować porządek publiczny i prowadzić do poważnych konsekwencji.

Ucieczki skazanych to poważne naruszenia, które mogą wynikać z różnych czynników, w tym niewłaściwego nadzoru, braków w systemie zabezpieczeń, a także z braku programów resocjalizacyjnych. Kiedy osadzeni decydują się na ucieczkę, narażają nie tylko siebie, ale także osoby postronne. Często takie sytuacje mogą prowadzić do konfrontacji z organami ścigania, co stwarza dodatkowe zagrożenie dla życia i zdrowia obywateli.

Aby przeciwdziałać ucieczkom, kluczowe jest wprowadzenie skutecznych środków bezpieczeństwa w jednostkach penitencjarnych. Obejmuje to zarówno monitoring, jak i odpowiednie szkolenie personelu, który powinien być przygotowany na reakcję w sytuacjach kryzysowych. Zastosowanie nowoczesnych technologii, takich jak systemy monitoringu wizyjnego czy elektroniczne urządzenia do śledzenia osadzonych, może znacząco zwiększyć bezpieczeństwo w zakładach karnych.

Samowolne oddalanie się osadzonych z terenu jednostki penitencjarnej, a także z konwojów policyjnych, stanowi kolejny ważny temat. Tego typu incydenty mogą wystąpić podczas transportu skazanych, gdyż są one często związane z rutynowymi operacjami. Dlatego też, kluczowe jest, aby służby mundurowe przestrzegały ściśle określonych procedur bezpieczeństwa oraz korzystały z odpowiednich środków ochrony.

Wzmoczona współpraca między jednostkami penitencjarnymi a służbami mundurowymi, takimi jak policja, jest niezbędna dla zwiększenia efektywności działań prewencyjnych. Wspólne szkolenia, wymiana informacji oraz analiza

³⁰ J. Kowalski, *Bezpieczeństwo funkcjonariuszy w zakładach karnych*, Wyd. Prawnicze, Warszawa 2019, s. 34-38.

³¹ P. Szymański, *Psychologia bezpieczeństwa w jednostkach penitencjarnych*, Wyd. UMCS, Lublin 2017, s. 120-125.

przypadków ucieczek mogą przyczynić się do opracowania lepszych strategii zabezpieczeń.

W kontekście bezpieczeństwa społeczeństwa, niezwykle istotne jest również angażowanie lokalnych społeczności w działania prewencyjne. Informowanie obywateli o działaniach podejmowanych przez służby oraz edukacja na temat zagrożeń związanych z ucieczkami skazanych mogą zwiększyć poczucie bezpieczeństwa wśród mieszkańców³².

Zakończenie

Na kanwie powyższego zauważyć należy, że relacja między warunkami życia skazanych a bezpieczeństwem w placówkach penitencjarnych jest niezwykle złożona. Odpowiednie warunki bytowe, które obejmują dostęp do edukacji, pracy, aktywności sportowych oraz możliwości kontaktu z rodziną, mają kluczowe znaczenie dla resocjalizacji osadzonych. Poprawa tych warunków przyczynia się nie tylko do zmniejszenia napięć i konfliktów w zakładach karnych, ale także wpływa na obniżenie recydywy, co z kolei przekłada się na wyższy poziom bezpieczeństwa w jednostkach. Z drugiej strony, brak odpowiednich warunków może prowadzić do frustracji i agresji, co stwarza zagrożenie zarówno dla osadzonych, jak i personelu. Dlatego tak istotne jest podejmowanie działań na rzecz poprawy jakości życia w zakładach karnych oraz stworzenie systemu, który łączy skuteczną resocjalizację z zapewnieniem bezpieczeństwa. Tylko w ten sposób można dążyć do skutecznego wprowadzenia osadzonych w życie społeczne po odbyciu kary, co przynosi korzyści nie tylko samym skazanym, ale całemu społeczeństwu.

Bibliografia

- Gerecka-Żołyńska A., *Komentarz Kodeks karny wykonawczy*, Warszawa 2023.
Informacja o zaludnieniu jednostek penitencjarnych – Centralny Zarząd Służby Więziennej Biuro Ewidencji, z dnia 18.10.2024 r., sygn. BEW.0335.42.2024.JL.
Jaki P., *Zatrudnienie skazanych w Polsce na tle porównawczym. Zagadnienia wybrane*. „Przegląd Więziennictwa Polskiego” 2017.
Kaczmarek M., *Zarządzanie kryzysowe w jednostkach penitencjarnych*, Wyd. Akademickie, Gdańsk 2021.

³² T. Kowalczyk, *Bezpieczeństwo publiczne w kontekście jednostek penitencjarnych*, Wyd. Prawnicze, Warszawa 2020, s. 67-70.

Kodeks karny wykonawczy (Dz.U.2024.706).

Kowalczyk T., *Bezpieczeństwo publiczne w kontekście jednostek penitencjarnych*, Wyd. Prawnicze, Warszawa 2020.

Kowalski J., *Bezpieczeństwo funkcjonariuszy w zakładach karnych*, Wyd. Prawnicze, Warszawa 2018.

Kowalski J., *Bezpieczeństwo w zakładach karnych*, Wyd. Prawnicze, Warszawa 2018.

Pawela S., *Kodeks karny wykonawczy. Praktyczny komentarz*, Wyd. ZPP, Warszawa 1999.

Pawela S., *Prawo karne wykonawcze. Zarys Wykładu*, Wyd. Zakamycze, Kraków 2003.

Przesławski, T., Sych, W., *Kodeks karny wykonawczy. Komentarz*. wyd. II., el/Lex 2024.

Rozporządzenie Ministra Sprawiedliwości z 28.11.2016 r. w sprawie sposobu i trybu prowadzenia nauczania w zakładach karnych i aresztach śledczych (Dz.U.2004).

Rozporządzenie Ministra Sprawiedliwości z dnia 23.12.2022 r. w sprawie regulaminu organizacyjno-porządkowego wykonywania kary pozbawienia wolności (Dz.U.2022.2847).

Szymanowski T., Świda Z., *Kodeks karny wykonawczy. Komentarz*, Warszawa 1998.

Szymanowski T., *Funkcje zatrudnienia skazanych w świetle danych empirycznych*, Lublin 1985.

Szymański P., *Psychologia bezpieczeństwa w jednostkach penitencjarnych*, Lublin, Wydawnictwo UMCS, Lublin 2017.

Ustawa z dnia 28 sierpnia 1997 r. o zatrudnianiu osób pozbawionych wolności (Dz.U. 2023.1559).

Wyrok Trybunału Konstytucyjnego z 13.12.2004 r., sygn. K 20/04, OTK-A 2004/11, poz. 115; LEX 140352.

Zalecenia Rec (2006) 2 Komitetu Ministrów państw członkowskich Rady Europy w sprawie Europejskich Reguł Więziennych; <https://sw.gov.pl> [dostęp: 18.10.2024 r.].

Zarządzenie Ministra Sprawiedliwości z dnia 5.03.2024 r. w sprawie nadania statutu Centralnemu Zarządowi Służby Więziennej (Dz.Urz.MS.2024.67).

<https://sw.gov.pl/jednostka/zatrudnienie-osob-pozbawionych-wolnosci>

<https://sw.gov.pl/aktualnosc/zaklad-karny-raciborz-rosnie-zatrudnienie-osadzonych-w-zakladzie-karnym> [dostęp: 20.10.2024 r.].

<https://www.sw.gov.pl/> [dostęp: 20.10.2024 r.].

Prawo osób osadzonych w zakładach karnych do praktykowania wiary zgodnie z normami prawa kanonicznego, wyznaniowego i konstytucyjnego oraz wpływ praktyk religijnych na resocjalizację osadzonych

Sebastian KĄKOL¹

Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
ORCID: 0009-0000-5779-3660

Streszczenie. Zgodnie ze współczesnymi normami prawnymi zawartymi w przepisach prawa kanonicznego, wyznaniowego oraz z normami Konstytucji Rzeczypospolitej Polskiej, osadzeni mają prawo korzystać z posługi duszpasterskiej zarówno Kościoła Rzymskokatolickiego oraz innych kościołów i związków wyznaniowych zaaprobowanych przez MSWiA. W Polsce zdecydowana większość społeczeństwa deklaruje wyznanie rzymskokatolickie. Konferencja Biskupów w Polsce oraz poszczególne diecezje w tym Ordynariat Polowy podejmują współpracę z właściwymi organami administracji publicznej, by zapewnić osadzonym ich prawa do sprawiedliwego i godnego odbycia kary oraz przyczynić się do ich resocjalizacji poprzez wiarę. Św. Tomasz z Akwinu pisząc o sprawiedliwości zaznaczył, powołując się na Cyncerona, że oznacza ona pewną równość względem drugich i należyte postępowanie, bowiem postępowanie sprawiedliwe to oddawanie każdemu tego, co się mu należy. Osadzonym w polskich zakładach karnych zarówno państwo, jak i Kościół gwarantuje praktykowanie religii oraz posługę duszpasterską. Za pośrednictwem statystyki praca przedstawi konkretne

¹ Sebastian Kąkol – kapłan Diecezji Kaliskiej. Absolwent Wydziału Teologicznego Uniwersytetu im. Adama Mickiewicza w Poznaniu, gdzie uzyskał stopień magistra teologii. Absolwent Wydziału Prawa Kanonicznego studiów I, II stopnia. Obecnie przygotowuje się do obrony dysertacji doktorskiej. Od 2021 r. Audytor Sądu Biskupiego w Kaliszu. Od 2023 r. Diecezjalny Duszpasterz Akademicki w Kaliszu. Badania naukowe prowadzi z zakresu kościelnego prawa publicznego zwłaszcza dotyczącego wolności religijnej w wyrokach trybunałów UE, Prawa Wyznaniowego oraz Prawa Rzymskiego.

liczby w ilu zakładach karnych znajduje się kaplica, w ilu posługę pełni więzienny kapelan oraz jaki wpływ na resocjalizację ma wiara.

Słowa kluczowe: kapelan, wolność religijna, prawo wyznaniowe, konstytucja

Wstęp

*Oddać każdemu, co mu się należy – oto najwyższa forma sprawiedliwości*², ta starożytna sentencja przypisywana Markowi Tulliuszowi Cynceronowi, stała się dla współczesnego prawodawstwa zasadą sprawiedliwości polegającej na równym traktowaniu każdego człowieka. Należy zaznaczyć, że zasada ta dotyczy również tych, którzy nie stosują się do przestrzegania prawa, bez znaczenia czy jest to prawo ludzkie czy prawo boskie, czy innymi słowy prawo naturalne. Zasada, którą rzymianie określili jako *Suum cuique* Ulpian zamieścił w *Praecepta iuris*, Justynian w wydany przez siebie zbiorze prawa zatytułowanym *Instytucje*, zaznaczył: *Sprawiedliwość jest stałą i niewzruszoną wolą, aby oddać każdemu, co mu się należy*³. Zasadę sprawiedliwości należy odnosić bezpośrednio do każdego człowieka, nawet tego, który sam się do tej zasady nie stosuje i łamie ustalony ład prawny. Stąd należy tę zasadę stosować także do osadzonych w zakładach karnych bowiem w myśl zasady sprawiedliwości mają oni prawo do odbycia kary i resocjalizacji w czym odpowiednie służby, instytucje i wspólnoty powinny im to umożliwić. Osadzeni jako obywatele posiadający konstytucyjne prawo do wolnego wyznawania i praktykowania wiary⁴, mają wynikające z zasady sprawiedliwości prawo do praktykowania swojej wiary we właściwym dla siebie obrządku. Opracowanie to będzie próbą ukazania najistotniejszych praw osadzonych w zakresie wolności religijnej i możliwości praktykowania wiary oraz wpływ wiary na resocjalizację osadzonych, poczynając od okresu dominatu Imperium Romanum, aż po współczesne przepisy prawa cywilnego i kanonicznego regulujące prawo do swobodnego wyznawania i praktykowania wiary przez osadzonych w zakładach karnych w Polsce.

² M. Jońca, *Suum cuique*, <https://www.edukacjaprawnicza.pl/suum-cuique/> [dostęp: 12. 09. 2024 r.].

³ Tamże.

⁴ Art. 53, *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* (Dz.U. 1997 nr 78 poz. 483).

Więziennictwo i prawa osadzonych w czasie kształtowania się prawa

Istotnym dla każdego tematu jest odniesienie się do źródeł. Dla dyscypliny nauki prawa w cywilizacji europejskiej takim źródłem jest wielowiekowy okres funkcjonowania i działania Imperium Romanum. Dla zachowania struktury tematu należy skupić się na okresie dominatu, czyli po reformach ustrojowo prawnych wprowadzonych przez Cesarza Dioklecjana w III w. n.e. Dioklecjan nie służył z wielkoduszności – wręcz przeciwnie – często skłaniał się do stosowania tortur nie tylko wobec rozwijających się gmin chrześcijańskich, ale i wobec obywateli cesarstwa, w tym również więźniów⁵. Okres dominatu w Cesarstwie Rzymskim przyniósł liczne zmiany w systemie prawnym. W imperium jedynym władcą stał się cesarz, który sprawował władzę absolutną. Przestępcy byli nie tylko karani surowiej, niż w czasach wcześniejszych, ale również zmieniło się podejście do ich traktowania. O ile w okresie pryncypatu więzienie było raczej środkiem tymczasowym, w dominacie uzyskało istotną funkcję jako forma represji i kontroli społecznej⁶. Więźniowie rzymskich (w szerokim tego słowa znaczeniu) więzień podczas odbywania kary byli poddawani wyznaczonym karom, które dzielono na: kary cielesne, które najczęściej stosowano wobec niewolników i osób z niskich warstw społeczeństwa. Kary finansowe, które obejmowały nie tylko płacenie grzywny, ale i konfiskatę majątku nakładane na bardziej zamożnych obywateli oraz przymusową pracę⁷. Dalej nakreślając historię i sytuację osadzonych w Cesarstwie Rzymskim należy wskazać na funkcję więzień i ich typy by dojść do roli chrześcijaństwa i jego wpływu na zachodzące tam zmiany. Do głównych funkcji więzienia w pierwszych wiekach należało przetrzymywanie osadzonych do czasu rozpoczęcia się procesu i wymierzenia egzekucji kary. Więzienie nie stanowiło kary samo w sobie, a było środkiem zatrzymania przed wykonaniem właściwej sankcji. Więzienia posiadały także swoją klasyfikację i dzieliły się na *carcer publica* (więzienia publiczne), w których przetrzymywano zarówno skazanych, jak i osoby oczekujące na rozprawę. Więźniów zamykano również w aresztach, a w niektórych przypadkach w lochach zarezerwowanych dla groźnych przestępców⁸.

⁵ K. Chojnicka, *Dominat*, [w:] *Słownik historii doktryn politycznych*, t. 2, red. M. Jaskólski, Warszawa 1999, s. 71.

⁶ C. Kunderewicz, *Traktowanie więźniów w konstytucjach cesarskich z okresu dominatu*, „Prawo Kanoniczne” 1977, 20/3-4, s. 283-291.

⁷ Tamże.

⁸ Tamże.

Okres dominatu i rozwijające się w nim prawo zaczęło regulować warunki w jakich więźniowie mieli przygotowywać się do wymierzenia i odbycia kary. Warunki więzienia były bardzo trudne. Na uwagę zasługuje traktowanie poszczególnych grup społecznych, zwłaszcza cudzoziemców i chrześcijan, którzy najczęściej zostawali skazani za swoją narodowość lub praktykowanie wiary⁹. Warunki w jakich przebywali więźniowie według badań archeologicznych i opisów historycznych były bardzo trudne. Więzienia były często miejscami brudnymi, bez dostępu do świeżego powietrza i światła. Więźniowie przebywali w zatłoczonych pomieszczeniach, co sprzyjało szerzeniu się chorób. Osadzeni otrzymywali minimalne porcje żywności, które były często niewystarczające dla podtrzymania zdrowia. W wielu przypadkach, zwłaszcza gdy wyrok obejmował prace przymusowe, więźniów zmuszano do wyczerpujących zajęć fizycznych, takich jak praca w kamieniołomach czy kopalniach¹⁰. W tych trudnych warunkach nikt nawet nie myślałby umożliwić jakąkolwiek formę pobożności, bez względu na religię, jaką wyznawał osadzony.

Edykt Mediolański ogłoszony w 313 roku przez Konstantyna Wielkiego oraz Dekrety Teodozjusza Wielkiego¹¹ i wartości chrześcijańskie jakie te akty wprowadzały, stały się motywem krytycznego spojrzenia wobec brutalności stosowanej w systemie więziennictwa. Również chrześcijańscy myśliciele, tacy jak Augustyn z Hippony, podnosili kwestię sprawiedliwości i humanitarnego traktowania więźniów. Krytyka ta wpłynęła na system prawny dopiero po upadku Cesarstwa, jednak była ona początkiem debat nad prawami więźniów¹². Upowszechnienie i prawne umocowanie chrześcijaństwa w Cesarstwie Rzymskim miało istotny wpływ na traktowanie więźniów i sposób sprawowania kar. Wśród najważniejszych zmian jakie wprowadzono dzięki rozwojowi chrześcijaństwa była zmiana optyki wartości życia i ładu społecznego. Pojawiają się nowe principia takie jak przebaczenie, miłosierdzie, równość wobec Boga oraz szacunek dla życia i godności człowieka. Te wartości stopniowo wpłynęły na prawo i karę. Chrześcijaństwo nie dążyło do zniesienia kary śmierci, ale wywarło wpływ na zmniejszenie jej stosowania. Kościół nawoływał do większej łagodności i miłosierdzia wobec skazanych. Śmierć zaczęto stosować bardziej selektywnie, co miało swoje odzwierciedlenie w liczbie wyroków oraz w ich interpretacji przez duchownych. Kary cielesne, takie jak bi-

⁹ A. Krawczyk, *Poczet cesarzy rzymskich*, Warszawa 2006, s. 506-520.

¹⁰ C. Kunderewicz, *Traktowanie więźniów...*, op. cit.

¹¹ Z. Jaworski, *Wolność religijna według Edyktu Mediolańskiego – w 1700 rocznicę wydania*, „Biuletyn Stowarzyszenia Absolwentów i Przyjaciół Wydziału Prawa Katolickiego Uniwersytetu Lubelskiego”, t. 9, nr 14, s. 19.

¹² C. Kunderewicz, *Traktowanie więźniów...*, op. cit.

czowanie, były powszechnie stosowane w dominancie, szczególnie wobec niewolników i niższych warstw społecznych. Chrześcijaństwo wpłynęło na ograniczenie ich stosowania. Zamiast brutalnych kar cielesnych zaczęto akcentować potrzebę pokuty i duchowej resocjalizacji. Chrześcijaństwo nie wyeliminowało przymusowej pracy, jednak wpłynęło na poprawę warunków jej wykonywania oraz lepsze traktowanie osób skazanych na pracę w kopalniach czy kamieniołomach¹³. Nastąpiły również duże zmiany w samym systemie więziennictwa. Więzienie, które w okresie dominatu było raczej miejscem tymczasowego przetrzymywania skazanych, niż ośrodkiem resocjalizacji, zaczęło pełnić bardziej znaczącą rolę, jako miejsce odosobnienia i pokuty. Zmiany te wynikały z chrześcijańskiego podejścia do winy i odkupienia. Chrześcijaństwo wprowadziło ideę pokuty jako moralnego obowiązku skazanych. Więzienie miało więc umożliwić osadzonej osobie refleksję nad winą, modlitwę i pracę duchową, co stawało się ważniejsze, niż sama kara cielesna. W okresie po przyjęciu chrześcijaństwa niektóre klasztory i wspólnoty religijne zaczęły zajmować się poprawą warunków w więzieniach, dostarczając więźniom żywność, ubrania czy opiekę duchową. Mimo to warunki bytowe nadal były trudne, lecz chrześcijańscy duchowni starali się oferować pomoc więźniom, promując idee współczucia i pomocy. Interesującą zmianą stało się Prawo do interwencji Kościoła – Kościół zyskał prawo do interwencji na rzecz więźniów i często zabiegał o ułaskawienia czy złagodzenie wyroków, szczególnie w przypadku chrześcijan. Dzięki wsparciu biskupów wielu więźniów, zwłaszcza z grup wykluczonych, mogło liczyć na łagodniejsze traktowanie.

Prawo zaczęło się zmieniać, by uwzględnić zasady chrześcijańskiego miłosierdzia. W V wieku niektóre prawa, w tym Kodeks Teodozjański, zaczęły regulować kwestie ochrony więźniów oraz ograniczania stosowania tortur. Chrześcijaństwo wywierało wpływ na stopniowe ograniczenie tortur w śledztwach. Cesarz Konstantyn Wielki wydał szereg dekretoów ograniczających stosowanie tortur, szczególnie wobec chrześcijan, uznając, że przemoc wobec ciała ludzkiego jest sprzeczna z zasadami wiary¹⁴. Upowszechnienie chrześcijaństwa przyniosło istotne zmiany w systemie karnym Cesarstwa Rzymskiego. Skupienie się na pokucie, resocjalizacji i łagodności wobec więźniów wpłynęło na ograniczenie brutalnych kar oraz powolne humanizowanie traktowania skazanych. Pomimo że więzienia nadal były miejscem odosobnienia o trudnych warunkach, nowe wartości chrześcijańskie wprowadziły szacunek dla życia i godności ludzkiej, co położyło podwaliny pod późniejsze reformy prawa karnego w Europie.

¹³ Tamże.

¹⁴ Z. Jaworski, *Wolność religijna...*, dz. cyt.

Współczesne prawo osób osadzonych w zakładach karnych do praktykowania wiary – prawo cywilne

Przytoczona na wstępie zasada sprawiedliwości Cycerona: *Oddać każdemu, co mu się należy – oto najwyższa forma sprawiedliwości*¹⁵, jest aktualna także w współczesnym systemie prawnym. Konstytucja Rzeczypospolitej Polskiej jako podstawowy akt prawny w Polsce zgodnie z brzemieniem art. 53 Konstytucji RP, każdemu obywatelowi przysługuje prawo do wolności sumienia i religii, w tym możliwości praktykowania jej zarówno prywatnie, jak i publicznie. Przepis ten dotyczy także osób przebywających w zakładach karnych¹⁶. Kodeks karny wykonawczy – Art. 106 i 107 k.k.w¹⁷, jako akt obowiązujący precyzują prawa osadzonych do praktyk religijnych. Kodeks nakłada na administrację więzienną obowiązek umożliwienia skazanym uczestnictwa w nabożeństwach i korzystania z posługi duszpasterskiej, a także umożliwienia im posiadania literatury religijnej. Należy mieć zawsze na uwadze, że prawo osadzonych do praktykowania religii jest nie tylko konstytucyjnym prawem czy wypełnieniem ustawy, ale jest przede wszystkim prawem człowieka. Można tu znów przytoczyć stwierdzenie, że osoba skazana prawomocnym wyrokiem za nieprzestrzeganie obowiązującego prawa nie jest pozbawiana swoich praw, w tym prawa do zadośćuczynienia i odbycia kary zgodnie z współczesnymi normami i standardami. Jeżeli osadzony zostałby pozbawiony prawa do praktykowania religii zostałyby naruszone jego prawa¹⁸. Sprawy duszpasterstwa w jednostkach penitencjarnych uregulowane są w następujących aktach prawnych: (art. 19 ust. 2 pkt 3 w związku z art. 4 ust. 1 pkt 3), jak również w większości ustaw indywidualnych, m.in. w art. 32 ust. 1-4 ustawy z dnia 17 maja 1989 r. o stosunku Państwa do Kościoła Katolickiego w RP¹⁹, art. 28 ust. 1-4 ustawy z dnia 4 lipca 1991 r. o stosunku Państwa do Polskiego Autokefalicznego Kościoła Pra-

¹⁵ M. Jońca, *Suum cuique...*, dz. cyt.

¹⁶ Art. 53, *Konstytucja Rzeczypospolitej Polskiej...*, dz. cyt.

¹⁷ Art. 106. – *Praktyki religijne skazanych – Kodeks karny wykonawczy*. Dz.U.2024.706 t.j. Wersja od: 8 maja 2024 r. do: 31 grudnia 2025 r.

¹⁸ Art. 9 Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności z 1950 r. (Dz.U. z 1993 r., Nr 61, poz. 284); art. 18 Międzynarodowego paktu praw obywatelskich i politycznych z 1966 r. (Dz.U. z 1977 r., Nr 38, poz. 167); orzecznictwo Europejskiego Trybunału Praw Człowieka, np. wyrok ETPC z 3 listopada 2009 r., 30814/06, *Lautsi v. Włochy*, Lex nr 523579; wyrok ETPC(WI) z 18 marca 2011 r., 30814/06, *Lautsi i inni v. Włochy*, Lex nr 784874; art. 53 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r., Nr 78, poz. 483 ze zm.); ustawa z dnia 17 maja 1989 r. o gwarancjach wolności sumienia i wyznania (t.j. Dz.U. z 2017 r., poz. 1153). Zob. także I.C. Kamiński, *Wolność myśli, sumienia i wyznania w orzecznictwie ETPCz za lata 2008-2009*, „Europejski Przegląd Sądowy” 2010, nr 11, s. 33-39; M. Hucal, *Wolność sumienia i wyznania w orzecznictwie Europejskiego Trybunału Praw Człowieka*, Warszawa 2012, ss. 229.

¹⁹ Dz.U. z 2019 r., poz. 1347.

wosławnego²⁰, art. 12 ust. 2-3 ustawy z dnia 13 maja 1994 r. o stosunku Państwa do Kościoła Ewangelicko-Reformowanego w RP²¹, art. 19 ust. 1-4 ustawy z dnia 20 lutego 1997 r. o stosunku Państwa do Kościoła Zielonoświątkowego w RP²², art. 15 ustawy z dnia 20 lutego 1997 r. o stosunku Państwa do Kościoła Katolickiego Mariawitów w RP²³ czy art. 18 ustawy z dnia 30 czerwca 1995 r. o stosunku Państwa do Kościoła Adwentystów Dnia Siódmego w RP²⁴. Zadania w zakresie działalności duszpasterskiej prowadzonej wobec osadzonych koordynuje Rada Duszpasterstwa Więziennego, którą tworzą naczelni kapelani: Kościoła Rzymskokatolickiego, Kościoła Ewangelicko-Augsburskiego oraz Kościoła Prawosławnego.

W Polsce funkcjonuje 81 zakładów karnych, 39 aresztów śledczych oraz 51 oddziałów zewnętrznych²⁵. Po przeprowadzonej kwerendzie wśród wszystkich zakładów karnych należy wskazać, że każdy z nich posiada kaplicę więzienną oraz zatrudnia lub korzysta z posługi kapelana więziennego. Zakłady karne w Polsce działają według procedur wewnętrznych, które pozwalają na realizację praktyk religijnych osadzonych w sposób zgodny z zasadami bezpieczeństwa i porządku jednostki. Zgodnie z wytycznymi ustawodawcy posługa duszpasterska w zakładach karnych jest organizowana i prowadzona przez duchownych Kościołów związków wyznaniowych, zgodnie z zasadą równości wyznań, nie promując dominującego wyznania na terenie kraju. Posługa ta obejmuje spotkania indywidualne i grupowe, rozmowy duchowe, a także wsparcie w problemach osobistych, emocjonalnych czy moralnych. Więźniowie mogą również zwracać się o indywidualne rozmowy z duchownymi, które są przeprowadzane na życzenie osadzonego. Osadzeni w zakładach karnych w myśl art. 6 k.k.w. mają prawo do uczestnictwa w regularnie organizowanych przez zakłady karne nabożeństwach, Mszach świętych i innych obrzędach kultycznych, które powinny znajdować się w wydzielonych i specjalnie przygotowanych do tego celu pomieszczeniach (kaplicach). W Polsce najczęściej spotykanymi są nabożeństwa katolickie, ale w zależności od potrzeb i liczby wyznawców różnych religii, administracja więzienna zapewnia także spotkania dla wyznawców innych religii. Organizowanie nabożeństw w zakładach karnych umożliwia praktykowanie religii przez osadzonych, ale odbywa się zgodnie z harmonogramem i wewnętrznymi regulacjami, by zachować bezpieczeństwo.

Kolejnym prawem jest dostęp do literatury religijnej i przedmiotów kultu religijnego. Każdy osadzony ma prawo posiadać w celi literaturę religijną, jak Biblia,

²⁰ Dz.U. z 2014 r., poz. 1726.

²¹ Dz.U. z 2015 r., poz. 483.

²² Dz.U. z 2015 r., poz. 13.

²³ Dz.U. z 2015 r., poz. 44.

²⁴ Dz.U. z 2014 r., poz. 1889.

²⁵ <https://www.sw.gov.pl/sitemap> [dostęp: 25.09.2021 r.].

Koran, Tora, czy inne święte księgi. Administracja zakładu karnego umożliwia dostarczanie takich materiałów, a także pozwala na ich sprowadzenie z zewnątrz przez rodziny lub organizacje religijne. Literatura ta nie tylko stanowi pomoc duchową, ale i spełnia rolę edukacyjną oraz wspiera proces resocjalizacji osadzonych. Osadzeni mogą posiadać przedmioty związane z ich religią, takie jak różańce, ikony, krzyże czy modlitewniki. Posiadanie przedmiotów religijnych jest jednak uzależnione od specyfiki danego zakładu karnego i oceny ich bezpieczeństwa. Przedmioty te nie mogą stanowić zagrożenia, dlatego administracja więzienna zastrzega sobie prawo do ich kontroli.

Ważnym elementem prowadzącym do resocjalizacji osadzonych jest współpraca z organizacjami religijnymi. Wiele zakładów karnych współpracuje z organizacjami religijnymi, które prowadzą działania duszpasterskie i resocjalizacyjne na terenie więzień. Kościół katolicki prowadzi duszpasterstwo więzienne, ale podobne działania prowadzą także inne wspólnoty, które organizują spotkania, grupy modlitewne oraz akcje wsparcia dla osadzonych. W szczególnych sytuacjach, np. podczas ważnych świąt religijnych, w zakładach karnych organizowane są dodatkowe nabożeństwa oraz obrzędy, co pozwala osadzonym aktywnie uczestniczyć w życiu religijnym. Podstawą oraz podsumowaniem wskazanych ustrojowych zasad jest przepis art. 32 ustawy z 17 maja 1989 r. o stosunku państwa do Kościoła katolickiego w Rzeczypospolitej Polskiej²⁶. Zgodnie z brzmieniem tej ustawy osoby tymczasowo aresztowane mogą wykonywać praktyki religijne i uczestniczyć we mszy św. transmitowanej przez środki masowego przekazywania oraz za zgodą organu, do którego dyspozycji pozostają, korzystać z indywidualnej posługi religijnej. Osadzonym należy zapewnić możliwość praktykowania kultu religijnego, korzystania z posług religijnych oraz uczestniczenia we Mszy św. odprawianej w niedziele i święta w odpowiednio przystosowanym pomieszczeniu w zakładzie, w którym przebywają. Osobom, które nie mogą uczestniczyć we mszy św. odprawianej na terenie zakładu, należy zapewnić możliwość wysłuchania mszy św. transmitowanej przez środki komunikacji społecznej²⁷.

Przy zachowaniu §3 art. 106 k.k.w. *Korzystanie z wolności religijnej nie może naruszać zasad tolerancji ani zakłócać ustalonego porządku w zakładzie karnym.* Należy strzec bezpieczeństwa osadzonych którzy praktykują religię oraz nie dopuścić do żadnej formy dyskryminacji religijnej mogącej zakłócić porządek ustalony w zakładzie karnym.

²⁶ Dz.U. z 2013 r., poz. 1169.

²⁷ O. Sitarz, A. Jaworska-Wieloch, *Prawo do praktyk religijnych osób osadzonych w areszcie śledczym i odbywających karę pozbawienia wolności w teorii i praktyce penitencjarnej*, Archiwum Kryminologii, t. XXXIX/2017, s. 117-148.

Analizując badania z zakresu penitencjarystyki oraz psychologii można założyć duży wpływ na resocjalizację osadzonych zwłaszcza w kontekście ich duchowej, moralnej oraz społecznej przemiany. Włączenie praktyk religijnych oraz wartości wyznaniowych w życie osadzonych może pozytywnie oddziaływać na różne aspekty resocjalizacji, takie jak refleksja nad popełnionymi czynami, rozwój pozytywnych wzorców postępowania oraz integracja społeczna po wyjściu na wolność. Możliwość rozwoju życia religijnego prowadzi również do rozwoju moralnego i wewnętrznej przemiany, ponieważ religia kładzie nacisk na moralność, samoświadomość oraz osobistą odpowiedzialność, co może być korzystne dla osadzonych. Dzięki obcowaniu z wartościami religijnymi, które promują zrozumienie, empatię i szacunek dla innych, więźniowie mogą dokonać refleksji nad swoimi czynami oraz ich konsekwencjami²⁸. Z pastoralnego punktu widzenia właściwe przeżywanie religijności niesie za sobą pragnienie pokuty i przebaczenia. Większość religii podkreśla znaczenie pokuty i przebaczenia, co pozwala osadzonym na podjęcie wysiłku w celu naprawienia swoich błędów. Zrozumienie potrzeby zadośćuczynienia za szkody wyrządzone innym może wzmocnić proces resocjalizacji, ucząc osadzonych odpowiedzialności za swoje czyny²⁹. Konkluzją staje się autorefleksja, która poprzez praktyki, takie jak modlitwa czy medytacja, zachęcają do głębokiej autorefleksji i pracy nad sobą, co sprzyja przemianie wewnętrznej. Ta refleksja nad swoimi wyborami i zachowaniem może wspomóc proces przemiany moralnej oraz motywować do poprawy³⁰.

Badania psychologiczne wskazują również na pozytywny wpływ na poprawę kondycji emocjonalnej więźniów. Osadzeni często zmagają się z trudnymi emocjami, poczuciem izolacji, a także z wysokim poziomem stresu związanym z życiem w więzieniu. Religia może stanowić formę wsparcia emocjonalnego i zapewniać osadzonym poczucie przynależności oraz nadziei na lepsze życie. Religia i wspólnoty religijne tworzą poczucie przynależności, które przeciwdziała samotności i pomaga osadzonym nawiązać zdrowe relacje społeczne. Dzięki wspólnym spotkaniom i nabożeństwom więźniowie mogą czuć się częścią większej wspólnoty, co pozwala im odnaleźć sens w swoim życiu i chęć do zmiany. Praktyki religijne uczą wielu pozytywnych cech, jak dyscyplina, samokontrola czy empatia, które mogą pomóc osadzonym w radzeniu sobie z codziennymi wyzwaniami życia w więzieniu oraz po wyjściu na wolność³¹. Religia może odegrać istotną rolę

²⁸ O. Sitarz, A. Jaworska-Wieloch, *Prawo do praktyk religijnych...*, dz. cyt.

²⁹ Z. Lasocik, *Praktyki religijne więźniów*, Wyd. Naukowe PWN, Warszawa 1993, s. 131.

³⁰ J. Nikołajew, *Wolność sumienia i religii skazanych i tymczasowo aresztowanych*, Wyd. Katolickiego Uniwersytetu Lubelskiego, Lublin 2012, s. 120-146.

³¹ Z. Lasocik, *Praktyki religijne...*, dz. cyt., s. 148.

w procesie przygotowywania osadzonych do życia po wyjściu na wolność, ułatwiając im integrację społeczną oraz odnalezienie się w społeczności. Wartości promowane przez religię mogą być przydatne podczas budowania nowych relacji i znajdowania wsparcia po opuszczeniu zakładu karnego.

Statystyki i badania na temat wpływu religii na resocjalizację, wskazują na pozytywny wpływ religii na proces resocjalizacji. Pokazują one, że osoby aktywnie zaangażowane w praktyki religijne mają niższy wskaźnik recydywy w porównaniu do osadzonych, którzy nie angażują się w życie religijne. Różne studia sugerują, że religia pełni funkcję buforującą wobec negatywnych skutków izolacji więziennej, a także ułatwia integrację społeczną po zakończeniu odbywania kary. Religia, dzięki swoim wartościom i praktykom, wspiera proces resocjalizacji w zakładach karnych, wpływając pozytywnie na rozwój moralny, wsparcie emocjonalne, kształtowanie pozytywnych wzorców zachowania oraz przygotowanie do powrotu do społeczeństwa. Wspólnoty religijne oraz duchowni odgrywają ważną rolę w wspieraniu osadzonych, oferując im narzędzia do refleksji nad własnym życiem oraz pomocy w budowaniu nowej, konstruktywnej ścieżki po wyjściu na wolność. Dzięki temu religia stanowi wartościowe uzupełnienie tradycyjnych metod resocjalizacji.

Troska Kościoła o osadzonych w kontekście Prawa Kanonicznego

Kodeks Prawa Kanonicznego promulgowany przez św. Jana Pawła II w 1983 r. miał stać się pasem transmisyjnym do wprowadzenia reform Soboru Watykańskiego II, który daje nowe spojrzenie na rolę i podmiotowość wiernych oraz wskazuje na niezniszczalną godność osoby ludzkiej, która w kościele realizuje swoje życie³². Ustawodawca kościelny w Kodeksie Prawa Kanonicznego zawarł wszystkie niezbędne normy mające na celu najwłaściwsze prowadzenie misji Kościoła, którą zawarł w ostatnim kanonie Kodeksu *Zbawienie dusz jest najwyższym prawem*³³. Oprócz kodeksu prawa kanonicznego, który jest stałym źródłem prawa dla całego Kościoła, normy pomiędzy poszczególnymi Państwami a Kościołem reguluje umowa międzynarodowa, czyli Konkordat. W tych aktach prawnych należy doszukiwać się norm odnoszących się do sytuacji osób pozbawionych wolności uwzględniając ich prawo do praktykowania religii, a także zapewniając Kościołowi możliwość pełnienia posługi duszpasterskiej w więzieniach.

³² J. Dyduch, *Rola Kodeksu Prawa Kanonicznego 1983 w realizowaniu misji Kościoła*, „Prawo Kanoniczne” 2014, 57/1, s. 23-37.

³³ Por. KPK. Kan. 1752.

Kodeks Prawa Kanonicznego jako zbiór praw obowiązujących w Kościele katolickim, odnosi się ogólnie do kwestii administracji i duszpasterstwa w tym opieki duszpasterskiej nad wiernymi, w tym nad osobami przebywającymi w zakładach karnych. Ustawodawca kościelny w trosce o wiernych przyznaje prawo do posługi sakramentalnej. Osoby pozbawione wolności mają prawo do sakramentów, takich jak spowiedź, Eucharystia czy sakrament namaszczenia chorych³⁴. Prawo kanoniczne podkreśla, że żadna osoba, także przebywająca w więzieniu, nie powinna być pozbawiona dostępu do sakramentów, jeśli jest do tego odpowiednio przygotowana i wyraża taką wolę. Prawo do opieki duszpasterskiej – zgodnie z kan. 747 i kan. 529 §1 Kodeksu, Kościół katolicki ma obowiązek zapewnić wiernym opiekę duszpasterską, niezależnie od ich miejsca pobytu. W przypadku osób pozbawionych wolności oznacza to możliwość wizyt księży, organizowania nabożeństw i zapewnienia literatury religijnej. Duchowni są zobowiązani do prowadzenia działalności duszpasterskiej, która wspiera duchowy rozwój osadzonych oraz umożliwia im powrót na ścieżkę moralności i godności³⁵.

Konkordat podpisany w 1993 roku reguluje kwestie dotyczące współpracy między Kościołem katolickim a polskim państwem, w tym również dostęp do opieki duszpasterskiej w miejscach odosobnienia, takich jak więzienia. Zapewnienie opieki duszpasterskiej – Art. 16 Konkordatu mówi, że: *Kościół katolicki zapewnia opiekę religijną wiernym przebywającym w zakładach karnych oraz w placówkach penitencjarnych*. Duchowni mają zagwarantowaną możliwość regularnych wizyt w zakładach karnych w celu prowadzenia posługi religijnej, co obejmuje udzielanie sakramentów, organizowanie nabożeństw oraz spotkań duszpasterskich³⁶. Konkordat zapewnia osobom przebywającym w więzieniach prawo do praktykowania religii, w tym uczestnictwa w Mszy Świętej i przyjmowania sakramentów. Państwo zobowiązuje się do współpracy z Kościołem w celu stworzenia odpowiednich warunków do sprawowania posługi religijnej w miejscach odosobnienia, co obejmuje dostęp do pomieszczeń na modlitwy i spotkania, a także umożliwienie posiadania literatury religijnej i przedmiotów kultu³⁷. Umowa między Stolicą Apostolską a Rzeczpospolitą Polską podkreśla potrzebę szacunku dla praw i godności wszystkich obywateli, w tym osób osadzonych, szczególnie w kontekście ich wolności religijnej. Duchowni oraz administracja zakładów karnych współpracują

³⁴ Por. KPK. kan. 213, 913-914, 921.

³⁵ *Kodeks Prawa Kanonicznego komentarz*, wyd. 2, Uniwersytet Nawarry w Pampelunie. Wyd. Wolters Kluwer, Warszawa 2023, s. 366-367.

³⁶ Konkordat między Stolicą Apostolską i Rzeczpospolitą Polską, Dz.U. 1998, nr 51, poz. 318.

³⁷ Tamże.

w celu realizacji praw osadzonych do opieki duchowej, co wspiera ich duchowy rozwój i proces resocjalizacji³⁸.

Konkordatowy zapis zobowiązania dotyczący posługi duszpasterskiej jest w Polsce realizowany poprzez obecność kapelanów więziennych, którzy regularnie odwiedzają zakłady karne. Duszpasterstwo więzienne, organizowane głównie przez Kościół katolicki, ale także przez inne wspólnoty wyznaniowe, oferuje osadzonym wsparcie duchowe, co pomaga im radzić sobie z wyzwaniami życia więziennego i sprzyja ich resocjalizacji.

Podsumowując Kodeks Prawa Kanonicznego i Konkordat gwarantują osobom osadzonym prawo do praktykowania religii i korzystania z opieki duszpasterskiej, a duchowni są zobowiązani do wspierania ich rozwoju duchowego i moralnego. Konkordatowe zasady i praktyki Kościoła są wdrażane we współpracy z polskim systemem penitencjarnym, co pozwala osadzonym na korzystanie z pełni praw religijnych i duchowego wsparcia.

Troskę o osadzonych w zakładach karnych możemy zauważyć w ostatnich latach trwającego od 13 marca 2013 roku pontyfikacie papieża Franciszka. Papież Franciszek wielokrotnie przemawiał do więźniów, podkreślając potrzebę szacunku, nadziei oraz możliwości odkupienia dla osób osadzonych. Jego słowa skierowane do więźniów podczas wizyt w zakładach karnych, a także jego homilie i przemówienia, zwracają uwagę na ich godność i możliwość przemiany. Oto kilka fragmentów z jego przemówień:

Wizyta w zakładzie karnym w Filadelfii (2015)

Podczas spotkania z więźniami w zakładzie karnym Curran-Fromhold w Filadelfii w 2015 roku papież Franciszek powiedział:

Jestem tutaj jako pasterz, ale przede wszystkim jako brat, który przychodzi, by podzielić się waszym cierpieniem, które przynosi mi radość i nadzieję. Przebywanie tutaj oznacza dla mnie pokazanie, że żadne miejsce nie jest zbyt dalekie dla Bożej miłości. Nic nie może odgrodzić nas od tej miłości.

Podkreślał, że więzienie nie powinno odbierać osadzonym ich godności i że życie każdego człowieka może się zmienić³⁹.

W Wielki Czwartek w zakładzie karnym w Paliano (2017) papież Franciszek umył nogi więźniom, co symbolizowało pokorę i służbę wobec drugiego człowieka. Mówił wtedy:

³⁸ Tamże.

³⁹ Franciszek, *Viaggio Apostolico del Santo Padre Francesco a Cuba, Negli Stati Uniti D'america e Visita alla Sede Dell'organizzazione delle Nazioni unite (19-28 Settembre 2015)*. https://www.vatican.va/content/francesco/pl/speeches/2015/september/documents/papafrancesco_20150927_usa-detenuiti.html [dostęp: 10.10.2024 r.].

Każdy z nas, każdy człowiek może się zmienić, przejść z ciemności do światła. To jest przesłanie nadziei, które przynoszę wam dzisiaj: Bóg kocha nas, pomimo naszych błędów, i zawsze jest gotowy przyjąć nas z powrotem⁴⁰.

Podczas jednej z audiencji papież Franciszek mówił także o resocjalizacji więźniów i ich godności, wskazując na to, że społeczeństwo nie powinno marginalizować osób osadzonych:

Każdy człowiek, także ten, który dopuścił się błędów, jest dzieckiem Boga. Kara powinna być nadzieją na poprawę, a nie wyrokiem na wykluczenie. Każdy z was ma prawo do nadziei i do życia pełnego godności.

Papież Franciszek nieustannie przypomina, że więzienie nie powinno odbierać więźniom człowieczeństwa, a Kościół i społeczeństwo mają obowiązek wspierać ich duchową i moralną przemianę.

Podsumowanie

Nie ulega wątpliwości, że troska o osadzonych w zakładach penitencjarnych jest zarówno troską Państwa o obywateli, którzy postępując niewłaściwie zasłużyli na stosowną karę a także troską Kościoła, jako o każdego jego członka włączonego sakramentalnymi znakami do wspólnoty wyznawców Chrystusa. Prawodawca kościelny zaznacza, że *Zbawienie dusz jest najwyższym prawem*, więc dostarcza on stosownych środków by takie zbawienie stało się udziałem tych, którzy poprzez zwoje czyny często zaprzeczali godności chrześcijanina. Należy zaznaczyć, że dyplomatyczne relacje pomiędzy państwem a Stolicą Apostolską oraz umowy w formie ustaw z innymi kościołami i związkami wyznaniowymi stają się gwarantem wypełnienia przepisów prawa czy to cywilnego czy religijnego dotyczącego wolności praktykowania religii poprzez osadzonych w zakładach karnych.

Bibliografia

Dyduch J., *Rola Kodeksu Prawa Kanonicznego 1983 w realizowaniu misji Kościoła*, „Prawo Kanoniczne” 2014, 57/1.

⁴⁰ Franciszek, *Przemówienie do Więźniów*, <https://www.vaticannews.va/pl/swiat/news/2021-02/wiezniowie-z-palano-przygotowuja-swiece-wielkanocne.html> [dostęp: 10.10.2024 r.].

- Franciszek, *Przemówienie do Więźniów*, https://www.vaticannews.va/swiat/new_s/2021-02/wiezniowie-z-palano-przygotowuja-wielkanocne.html [dostęp: 10.10.2024 r.].
- Franciszek, *Viaggio Apostolico del Santo Padre Francesco a Cuba, Negli Stati Uniti D'america e Visita alla Sede Dell'organizzazione delle Nazioni unite (19-28 Settembre 2015)*. https://www.vatican.va/content/francesco/pl/speeches/2015/september/documents/papa-francesco_20150927_usa-detenuti.html [dostęp: 10 Października 2024 r.].
- Jaskólski M., *Słownik historii doktryn politycznych*, t. 2, red. Warszawa 1999.
- Jońca M., *Suum cuique*, <https://www.edukacjaprawnicza.pl/suum-cuique/> [dostęp: 12.09.2024 r.].
- Kodeks karny wykonawczy, *Praktyki religijne skazanych* – U.2024.706 t.j. Wersja od: 8 maja 2024 r. do: 31 grudnia 2025 r.
- Kodeks Prawa Kanonicznego, komentarz, wydanie 2, Uniwersytet Nawarry w Pampelunie. Wyd. Wolters Kluwer, Warszawa 2023.
- Konkordat między Stolicą Apostolską i Rzeczpospolitą Polską, Dz.U. 1998 nr 51 poz. 318.
- Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997 nr 78 poz. 483).
- Krawczyk A., *Poczet cesarzy rzymskich*, Warszawa 2006.
- Kunderewicz C., *Traktowanie więźniów w konstytucjach cesarskich z okresu dominatu*, „Prawo Kanoniczne” 1977, 20/3-4.
- Lasocik Z., *Praktyki religijne więźniów*, Wyd. Naukowe PWN, Warszawa 1993.
- Nikołajew J., *Wolność sumienia i religii skazanych i tymczasowo aresztowanych*, Wyd. Katolickiego Uniwersytetu Lubelskiego, Lublin 2012.
- Sitarz, O., Jaworska-Wieloch A., *Prawo do praktyk religijnych osób osadzonych w areszcie śledczym i odbywających karę pozbawienia wolności w teorii i praktyce penitencjarnej*, „Archiwum Kryminologii” 2017, t. XXXIX.

Zagrożenia wynikające z konwojowania osadzonych a bezpieczeństwo funkcjonariuszy i osób postronnych

Adrianna IWAŃSKA¹

Akademia Wymiaru Sprawiedliwości w Warszawie

ORCID: 0009-0003-2005-4575

Streszczenie. Służba Więzienna to formacja uzbrojona, umundurowana i apolityczna, która pełni istotną rolę w zapewnieniu bezpieczeństwa państwa. Jednym z kluczowych jej zadań jest ochrona społeczeństwa przed osobami, które zostały osadzone w Zakładach Karnych lub Aresztach Śledczych. Niezbędnym elementem podczas wykonywania kary pozbawienia wolności, a które wiąże się z dużym ryzykiem naruszenia bezpieczeństwa jest konwojowanie i transport osadzonych. W opracowaniu zostały przedstawione wybrane zagadnienia dotyczące bezpieczeństwa funkcjonariuszy, jak i osób postronnych w trakcie konwojowania osadzonych. Wskazano zagrożenia występujące podczas wykonywania czynności konwojowych, a także zaprezentowano działania, które mają na celu zapobiegnięciu lub zminimalizowaniu ich występowania, oraz rolę, jaką pełnią w nich funkcjonariusze Służby Więziennej. W przedmiotowym artykule podjęto próbę szczegółowej analizy przepisów pragmatycznych, które dotyczą transportu skazanych.

Słowa kluczowe: konwojowanie, bezpieczeństwo, zagrożenia, Służba Więzienna

Wstęp

Bezpieczeństwo jest nadrzędną i podstawową potrzebą każdego człowieka. Umożliwia ono prawidłowe funkcjonowanie, jak i realizację codziennych czynności. Instytucje a także organizacje zajmujące się zapewnieniem bezpieczeństwa

¹ Adrianna Iwańska – funkcjonariusz Służby Więziennej, studentka 3 roku na kierunku penitencjarystka.

ogółu społeczeństwu często sami są narażeni w większym stopniu na jego utratę poprzez pracę w trudnych bądź specyficznych warunkach. Zalicza się między innymi do nich funkcjonariuszy, jak i pracowników Służby Więziennej. Spełniając swoje obowiązki są zmuszeni do zrezygnowania w pewnym stopniu z własnego komfortu psychicznego oraz fizycznego, gdyż przy wielu czynnościach realizowanych przez nich występuje wysokie prawdopodobieństwo wystąpienia zagrożeń lub zdarzeń. Szczególnie dzieje się tak podczas realizowania zadań konwojowych. Wykonywanie obowiązków w czasie transportu osadzonych jest trudne ze względu na dodatkowe czynniki zewnętrzne, które mają znaczny wpływ na bezpieczeństwo ogółu. Celem artykułu jest analiza zagrożeń mogących wystąpić w trakcie realizacji zadań konwojowych, a także przedstawienie czynników oraz sposobów, które mogą zminimalizować prawdopodobieństwo pojawienia się ewentualnych niebezpieczeństw.

Pojęcie bezpieczeństwa

Bezpieczeństwo to stan, w którym dana jednostka nie odczuwa jakiegokolwiek zagrożenia. Pochodzi ono od łacińskiego słowa *sine cura* (*securitas*), tłumaczone jest jako „bez pieczy” i rozumie się je jako stan pewności, spokoju, zabezpieczenia, a także jego poczucia oraz ochronę przed wszelkim zagrożeniem. Piecza sama w sobie oznacza troskliwość, staranność i otaczanie czegoś lub kogoś opieką lub ochroną, natomiast przedrostek „bez” wskazuje na pewien brak cechy, osoby bądź rzeczy. Bezpieczeństwo bez wątpienia jest naczelną potrzebą każdego człowieka oraz instytucji przez niego tworzonych. Daje przede wszystkim poczucie pewności i gwarancję określonego poziomu dobrostanu ograniczając się przy tym jedynie do zaspokajania podstawowych potrzeb duchowych czy materialnych. Bezpieczeństwo jest procesem ciągłym, który obejmuje szereg różnych przedsięwzięć skierowanych przeciwko zagrożeniom². Ponadto jest ono potrzebą podmiotową uczestników, zarówno danych jednostek, jak i wielkich grup społecznych oraz reprezentujących je instytucji. Potrzeba wynikająca z bezpieczeństwa ma charakter niezbywalny (naczelny) i egzystencjalny³. Poszczególne podmioty podejmują więc próby, które mają na celu wpłynąć na otoczenie, aby wyeliminować bądź ograniczyć zagrożenia i jednocześnie usunąć własne obawy, lęki, niepokój oraz niepewność. Działania te mogą mieć charakter wewnętrzny, który jest związany z zapewnieniem stabilności i harmonijności jednostki bądź

² T. Bąk, Z. Ciekanowski, *Teorie bezpieczeństwa*, Wyd. PWSTE, Jarosław 2012, s. 15.

³ J. Zięba, *Treść i zakres pojęcia „bezpieczeństwo Polski”*, Wyd. WNSiH, Poznań 2023, s. 13.

grupy oraz zewnętrzny, polegający na braku zagrożenia. Te dwa rodzaje bezpieczeństwa stanowią składową ogólnego pojęcia bezpieczeństwa. Można stwierdzić, iż podstawowymi składnikami pojęcia bezpieczeństwa jest swoboda jego rozwoju i pewność nienaruszalności podmiotu. Bardzo ważną funkcję spełnia tu zachowanie podmiotów, ponieważ bezpieczeństwo zależy również od nas samych, naszego zdrowia, przygotowania motorycznego w danym zakresie oraz gotowości sprostanienia pojawiającym się zagrożeniom⁴. W identyfikacji i pojmowaniu bezpieczeństwa podstawowe są założenia politologa szwajcarskiego Daniela Freia. Naukowiec ten postrzega bezpieczeństwo jako: stan właściwy bezpieczeństwa – gdy zagrożenie jest niewielkie, a postrzeganie jego jest właściwe; stan fałszywego bezpieczeństwa – polegający na niedoszacowaniu zagrożeń oraz ich lekceważeniu; stan obsesji – gdy niewielkie jest zagrożenie; stan braku bezpieczeństwa wynikający z sytuacji prawidłowego postrzegania zagrożenia rzeczywistego.

Zagłębiając się w tematykę samego bezpieczeństwa można stwierdzić, że bardzo istotnym elementem w życiu człowieka jest bezpieczeństwo narodowe. Definiuje się je jako system wartości oraz środków je zabezpieczających, składających się z następujących elementów: integralności terytorialnej, przetrwania, odpowiedniej jakości życia, oraz politycznej niezależności. Przy czym wydajność struktur, które są odpowiedzialne za bezpieczeństwo państwa jest jednocześnie podstawą jego suwerenności oraz dobrobytu obywateli⁵. Jest ono również definiowane jako stan uzyskany w rezultacie odpowiednio zorganizowanej obrony i ochrony przed wszelkimi zagrożeniami militarnymi i pozamilitarnymi, tj. zewnętrznymi i wewnętrznymi, przy użyciu sił i środków pochodzących z różnych dziedzin działalności państwa. Sposób jego organizacji, został skonkretyzowany oraz określone zostały jego kryteria. Można je rozpatrywać przez bezpieczeństwo indywidualne (unilateralne), które dotyczy działań jednostronnych, podejmowane przez dane państwo, aby zapewnić mu bezpieczeństwo. Zaliczane jest do niego: hegemonizm mocarstwowy, neutralność, izolacjonizm, a także niezaangażowanie. Waldemar Kiltler utożsamia pojęcie bezpieczeństwa narodowego z najważniejszą wartością, potrzebą krajową oraz priorytetowym celem działalności państwa i dzieli je na przedmiotowe, podmiotowe i funkcjonalne. Przedmiotowe polega na niepodważalności jego rozwojowych szans i są to na przykład wizje, wartości bezpieczeństwa oraz środki jego ochrony, które rozpatruje się w kilku płaszczyznach. Bezpieczeństwo polityczne odnoszące się do niezależności politycznej danego państwa,

⁴ A. Szczepiński, *Pojęcie bezpieczeństwa i jego typologia – próba systematyzacji*, „Zeszyty Naukowe Collegium Witelona” 2023, nr 48(3), s. 32.

⁵ K. Śmiałek, *Zarządzanie kryzysowe wobec wyzwań i zagrożeń dla bezpieczeństwa wewnętrznego państwa*, Wyd. WAT, Warszawa 2020, s. 111.

gwarantujące przy tym warunki umożliwiające funkcjonowanie jego politycznego systemu⁶ i składające się z bezpieczeństwa: władzy, państwa i stosunków międzynarodowych. Bezpieczeństwo militarne, którego celem jest przeciwdziałanie zagrożeniom zewnętrznym, jak i wewnętrznym, które mogłyby skutkować groźbą użycia siły wobec państwa oraz jest to stan wynikający z ochrony zorganizowanej i obrony przed zagrożeniami. Bezpieczeństwo ekonomiczne w którym nadrzędny jest czynnik materialny, kształtujący jakość życia i standardy określonego społeczeństwa pod względem indywidualnym, międzynarodowym i lokalnym⁷. Bezpieczeństwo społeczne, które skupia się na zapewnieniu jednostkom godnego życia, a także zapobiega grożącym im niebezpieczeństwem ekonomicznym i naturalnym, jednocześnie gwarantuje podstawowe prawa i wolność obywatelską. Bezpieczeństwo powszechne zapewnia bezpieczeństwo ludności cywilnej przez działania w obszarze prawnym, społecznym, sanitarnym oraz ekologicznym. Bezpieczeństwo publiczne umożliwia funkcjonowanie ogółu instytucji społecznych, państwowych czy prywatnych oraz zachowuje zdrowie, życie i mienie ich mieszkańców. Podmiotowe Kitler definiuje jako pewność przetrwania i istnienia podmiotu i jest to bezpieczeństwo międzynarodowe polegające na braku istniejących obiektywnie zagrożeń, obaw i kompatybilnym dążeniu i działaniu międzynarodowej społeczności w sprawie ochrony wartości państwowych i pozapaństwowych przy użyciu instytucji, norm i instrumentów, które zapewniają bezkonfliktowe rozstrzyganie sporów, a także kreowanie gospodarczych, ekologicznych, społecznych przesłanek stabilności dynamicznej i eliminowania zagrożeń. Natomiast bezpieczeństwo funkcjonalne charakteryzuje się pewnością funkcjonowania oraz rozwoju określonego podmiotu⁸.

Z powyższych założeń wynika, iż fundamentem poprawnego definiowania bezpieczeństwa jest przyjmowanie go w oparciu o naukowe i rzeczywiste przesłanki⁹. Stanisław Sulowski, który jest przekonany o interdyscyplinarności bezpieczeństwa uważa, iż rozpatrywana kategoria jest przedmiotem badań między innymi prawa, politologii, socjologii, ekonomii, psychologii oraz nauk inżyniersko-technicznych. Może być ono analizowane pod kątem braku występujących zagrożeń – w sensie negatywnym, a także tym pozytywnym – w poczuciu pewności ochrony oraz stanu, który został osiągnięty dzięki istnieniu instytucji specjalistycznych i przestrzeganiu wcześniej ustalonych praw. Analizuje on również

⁶ W. Kitler, *Bezpieczeństwo narodowe RP. Podstawowe kategorie, uwarunkowania, system*, Wyd. Akademii Obrony Narodowej, Warszawa 2011, s.46.

⁷ K. Ficoń, *Bezpieczeństwo narodowe i jego typologie*, Wyd. BEL Studio, Warszawa 2020, s. 83.

⁸ T. Bąk, Z. Ciekanowski, *Teorie bezpieczeństwa*, dz. cyt., s. 33.

⁹ A. Czupryński, B. Wiśniewski, J. Zboina, *Bezpieczeństwo. Teoria-badania-praktyka*, Wyd. CN-BOP-PIB, Warszawa 2016, s. 6.

bezpieczeństwo w kontekście obiektywnym – związanym bezpośrednio z statusem materialnym samych jednostek, jak i zbiorowości, a także uzyskanymi przez nie prawnymi gwarancjami, które chronią przed zagrożeniem kryminalnym oraz subiektywnym, dotyczącymi stanów świadomości odczuwania niebezpieczeństw, a także poczucia ich braku. Bezpieczeństwo analizuje się również pod względem normatywnym i uważane jest wtedy za naturalną potrzebę podmiotu, wartości do których powinno się dążyć, mimo iż nigdy nie będzie się w stanie uzyskać ich w pełni, a także pod względem redukcji ryzyka mającego związek z zastosowaniem różnego rodzaju środków zaradczych eliminujących zagrożenia¹⁰. Warto zwrócić uwagę na fakt, iż od początku XXI, a w szczególności po 2001 r., problematyka bezpieczeństwa jest stale poruszana w debatach publicznych i jest przedmiotem badań wielu naukowych dyscyplin. Mając na uwadze jego charakter, cechujący się subiektywnością, stopniowością i dynamicznością ustalenie jednej, poprawnej i powszechnie akceptowalnej definicji wydaje się zadaniem, które nie jest możliwe do wykonania¹¹.

Rola Służby Więziennej w systemie bezpieczeństwa państwa

Służba Więzienna jako formacja uzbrojona i umundurowana jest jednym z kluczowych elementów w systemie bezpieczeństwa państwa. Nie jest ona przeznaczona do bezpośredniej zbrojnej walki, ale do wspomagania wszelkich działań sił zbrojnych oraz zapewnienia wewnętrznego bezpieczeństwa państwa. Jej głównym zadaniem jest zabezpieczenie kraju przed osobami nieprzestrzegającymi obowiązującego porządku prawnego poprzez ich izolację oraz resocjalizację zachowując przy tym wszelkie standardy humanitarne oraz godność ludzką. Do obowiązków Służby Więziennej należy realizacja zadań w taki sposób, aby skutecznie zapewnić bezpieczeństwo nie tylko ogółowi społeczeństwa czy osadzonym przebywającym w warunkach izolacji penitencjarnej, ale także wszystkim funkcjonariuszom oraz pracownikom, którzy realizują swoje zadania w bezpośrednim kontakcie z osobami pozbawionymi wolności. Realizowane jest to poprzez: prowadzenie oddziaływań penitencjarnych oraz resocjalizacyjnych wobec osób osadzonych w zakładach karnych i aresztach śledczych; wykonywanie tymczasowego aresztowania w sposób zabezpieczający prawidłowy tok postępowania karnego; ochronę społeczeństwa przed sprawcami przestępstw osadzonymi w jednostkach

¹⁰ A. Szczepiński, *Pojęcie bezpieczeństwa...*, dz. cyt., s. 30-31.

¹¹ M. Szuniewicz, *Pojęcie i istota bezpieczeństwa państwa*, [w:] *Administracja bezpieczeństwa narodowego*, red. A. Tyburska, Wyd. Wyższej Szkoły Policji w Szczytnie, Szczytno 2011, s.1-2.

penitencjarnych; zapewnienie bezpieczeństwa i porządku w jednostkach penitencjarnych; wykonywanie na terytorium Polski tymczasowego aresztowania oraz kar pozbawienia wolności i środków przymusu skutkujących pozbawieniem wolności. Aby zrealizować wyżej wymienione zadania Służba Więzienna tworzy wyodrębniony podsystem rządowej instytucji, który bezpośrednio jest odpowiedzialny za wewnętrzne bezpieczeństwo państwa. Realizuje politykę kryminalną składającą się z retrybucji, resocjalizacji, odstraszenia, pozytywnej prewencji generalnej, naprawienia szkody oraz zabezpieczania społeczeństwa przez odseparowywanie sprawców¹². Ponadto według M. Kuć rola więziennictwa rozpoczyna się w momencie przejścia wymiaru sprawiedliwości do etapu wykonawczego, który dotyczy bezpośrednio indywidualnego człowieka – podejrzanego lub sprawcy przestępstwa oraz pośrednio ofiary przestępstwa i całego społeczeństwa¹³. Służba Więzienna posiada kilka strategicznych funkcji, które umożliwiają i stanowią podstawę systemu bezpieczeństwa. Pierwszym z nich jest zdolność, jak i prezentacja w społeczeństwie możliwości do nieuchronnego oraz pełnego wyegzekwowania orzeczonej kary. Wykonywanie kary powoduje zapobieganie negatywnym wpływom przestępców i jest tym samym dobrą i skuteczną profilaktyką tego systemu. Jednocześnie spełnia ona funkcję, która polega na zapobieganiu poprzez wskazanie na nieuchronność konsekwencji prawnych wynikających z nieprzestrzegania obowiązującego porządku prawnego. Potencjalni przestępcy mają zrozumieć, iż należy przestrzegać prawa, aby nie zostać odizolowanym od społeczeństwa. W tym celu Służba Więzienna prowadzi programy edukacyjno-profilaktyczne oraz organizuje kampanie społeczne, pozwalające na poznanie jej działalności np. oferują możliwość zapoznania się z formami prowadzonych działań czy prezentacje wykorzystywanych sprzętów i technik. Profilaktyka ta pełni istotną rolę w właściwym funkcjonowaniu systemu, gdyż dzięki niej zmniejszane jest prawdopodobieństwo wystąpienia konfliktu z prawem przez obywateli. Kolejną funkcją charakterystyczną i strategiczną dla tego systemu bezpieczeństwa jest reakcja na zaistniałe zagrożenie. Służba Więzienna realizuje ją poprzez separację skazanych od reszty społeczeństwa, umieszczając skazanych w zakładach karnych bądź aresztach śledczych rozlokowanych na terenie całego kraju. Więziennictwo jest zobowiązane wykonywać to w sposób skuteczny, pewny, bezwzględny, zachowując przy tym wszelkie standardy cywilizacyjne. Ostatnią funkcją związaną z systemem bezpieczeństwa jest powrót do normalnego funkcjonowania po wcześniejszej likwidacji zagrożenia. Służba Więzienna wykonuje to poprzez resocjalizację mającą

¹² B. Stańdo-Kawecka, *Prawne podstawy resocjalizacji*, Wyd. Zakamycze, Kraków 2000, s. 56-58.

¹³ M. Kuć, *Rola służb penitencjarnych w polityce kryminalnej*, [w:] *Autorytet i godność służb penitencjarnych a skuteczność metod resocjalizacji*, (red.) J. Świtek, M. Kuć, I. Niewiadomska, Wyd. KUL, Lublin 2004, s. 39.

na celu przywrócenie osoby do normalnego i zgodnego z obowiązującym porządkiem prawnym funkcjonowania w społeczeństwie¹⁴. Resocjalizacja następuje między innymi przez edukację skazanych. Ukazywanie wartości oraz redukowanie negatywnych zachowań ma doprowadzić do motywacji zmiany życia na bardziej wartościowe, nie tylko dla społeczeństwa, ale także dla samego osadzonego. Działania edukacyjne, które są podejmowane w jednostkach organizacyjnych Służby Więziennej nie tylko prowadzą do uzupełnienia wiedzy przez osoby odbiegające od norm społecznych, pozwalają także na dogłębnierze rozumienie otaczającej rzeczywistości oraz dynamicznych zmian w niej zachodzących¹⁵. Praca podejmowana przez osadzonego wspomaga resocjalizację i stosowane jako narzędzie pełni funkcję adaptacyjną oraz poprawczą. Zatrudnienie osadzonego daje mu szansę na poznanie zgodnego z prawem życia i tym samym możliwość powrotu do właściwego funkcjonowania w społeczeństwie¹⁶. Jednym z ważniejszych czynników readaptacyjnych i umożliwiających resocjalizację jest kontakt osadzonych ze światem zewnętrznym podczas przebywania w jednostkach penitencjarnych. Ważnym elementem wspierającym proces resocjalizacji jest kontakt z rodziną i najbliższymi. Możliwy on jest przez wizyty tych osób na terenie Zakładu czy Aresztu Śledczego, rozmowy telefoniczne oraz korespondencję. Resocjalizacja ta ma na celu powtórne uspołecznienie danej jednostki w powszechnie przyjętych i akceptowanych rolach życiowych i społecznych poprzez profilaktykę, korektę nieodpowiedniego przystosowania oraz wspomaganie indywidualnego rozwoju.

Powyżej omówione działania realizowane przez Służbę Więzienną przyczyniają się do prawidłowej ochrony państwa i tym samym zapewniają społeczeństwu polskiemu bezpieczeństwo. Bez prawidłowego funkcjonowania tej służby eliminacja zagrożeń w państwie byłaby niemożliwa.

Pojęcie konwojowania

Czynności związane z konwojowaniem osadzonych towarzyszą funkcjonariuszom Służby Więziennej każdego dnia i stanowią istotną rolę w prawidłowym funkcjonowaniu wszelkich jednostek penitencjarnych. Jest to złożony proces, określony ścisłymi zasadami, który polega na ochronie skazanego lub mienia

¹⁴ R. Poklek, *Służba więzienna w systemie bezpieczeństwa państwa*, „Securitologia” 2013, nr 1 (17), s. 153-201.

¹⁵ Tamże, s. 255.

¹⁶ J. Kwieciński, B. Waligóra, *Zatrudnienie w strategii readaptacji społecznej skazanych – na przykładzie Zakładu Karnego we Wronkach*, [w:] B. Skafirniak, *Pomoc postpenitencjarna w kontekście działań resocjalizacyjnych*, Wyd. Impuls, Kraków 2007, s. 234.

w trakcie jego przemieszczania się oraz pobytu poza obszarem jednostki organizacyjnej Służby Więziennej. Do przypadków konwojowania zalicza się transportowanie, zatrudnienie poza terenem jednostki organizacyjnej, konwojowanie do placówek służby zdrowia, przemieszczanie oraz ochrona określonych ustawą przedmiotów. W skład konwoju wchodzi podmioty konwojowane, konwojenci oraz dowódca konwoju. Do osób lub mienia, które podlegają konwojowaniu zalicza się:

- osoby pobrane z aresztu śledczego, zakładu karnego, zakładu poprawczego, okręgowego ośrodka dla nieletnich, schroniska dla nieletnich, a także policyjnej izby dziecka,
- osoby przekazywane na podstawie danych umów międzynarodowych, które zostały uprzednio skazane lub tymczasowo aresztowane,
- wartości pieniężne lub inne przedmioty wartościowe,
- broń, amunicję, materiały lub środki niebezpieczne (w tym materiały wybuchowe, chemiczne lub radioaktywne),
- uzbrojenie, urządzenia i sprzęt wojskowy,
- środki odurzające lub substancje psychotropowe,
- dokumenty lub materiały, które zawierają informacje niejawne¹⁷.

Istnieją dwa rodzaje konwojowania do placówki służby zdrowia. Pierwszym jest konwojowanie planowane, organizowane po to, by przeprowadzić zaplanowane wcześniej badania lekarskie bądź czynności lub badania zlecone w wyniku badania lekarskiego. Konwój ten odbywa się wtedy na zasadach ogólnych. Funkcjonariusze służby zdrowia zobowiązani są w tym wypadku przygotować niezbędną dokumentację, ustalić miejsce i godzinę przyjęcia oraz zadbać o załatwienie spraw administracyjnych. Drugim rodzajem jest konwojowanie doraźne, które następuje w momencie wystąpienia nagłych wypadków (np. samouszkodzenie, atak choroby) i organizowane jest w celu udzielenia niezbędnej pomocy lekarskiej. Konwojowanie to organizuje dowódca zmiany, który powinien wykonać niezbędne czynności, które są związane z wyjazdem konwoju¹⁸. Konwojenci podczas wykonywania swoich obowiązków są wyposażeni w broń palną i środki przymusu bezpośredniego (wyposażenie oraz uzbrojenie dostosowuje się do warunków i trasy konwojowania, odległości do miejsca docelowego, klasyfikacji osoby konwojowanej oraz innych przesłanek ustalonych w wyniku podjętych czynności

¹⁷ Zob. szerzej: I. Szkudlarek, K. Szkudlarek, *Bezpieczeństwo przewozu towarów niebezpiecznych – przepisy wewnętrzne na przykładzie Polskich Kolei Państwowych Polskich Linii Kolejowych S.A.*, „Studia Kaliskie – Studia Calisiensia” 2024, t. 12, nr 1/2024, s. 350-351.

¹⁸ P. Jarczewski, K. Jędrzejak, M. Kuświk, K. Setla, *Konwojowanie w służbie więziennej*, Wyd. COSSW, Kalisz 2006, s. 19.

sprawdzających). Funkcjonariusz służby więziennej powinien posiadać niezbędną wiedzę, która umożliwi mu właściwe zachowanie się oraz skuteczne posługiwanie się środkami, w które został wyposażony na czas realizacji czynności konwojowych w momencie wystąpienia zagrożenia. Broni palnej konwojenci używają jedynie w ostateczności (gdy środki przymusu bezpośredniego okazały się niewystarczające) i w celu odparcia bezpośredniego, jak i bezprawnego zamachu na życie lub zdrowie funkcjonariusza lub innej osoby; udaremnieniu ucieczki osoby konwojowanej; bądź w momencie wystąpienia sytuacji, która stanowi zagrożenie dla konwoju. Oprócz wiedzy z zakresu posługiwania się bronią konwojent musi posiadać umiejętność właściwej oceny danej sytuacji, rozpoznania jej i podjęcia w razie potrzeby decyzji o warunkach realizacji wykonywania zadań konwojowych, znać elementy techniki obezwładniania, elementy taktyki konwojowania, a także elementy ratownictwa taktycznego, co umożliwi mu wykonanie powierzonego zadania w sposób zgodny z obowiązującymi przepisami i bezpieczny dla niego i innych osób.

Zagrożenia, które mogą wystąpić podczas konwojowania

Charakterystyczne podczas zadań realizowanych w trakcie konwojowania jest wysokie prawdopodobieństwo wystąpienia zdarzeń, zagrożeń i sytuacji niebezpiecznych, które są zróżnicowane pod względem miejsca, podmiotu oraz okoliczności. Zagrożenia te można podzielić na *zewnętrzne i wewnętrzne*¹⁹. Źródłem zagrożeń wewnętrznych są zachowania osób konwojowanych, natomiast zewnętrzne są ściśle związane z problemami wynikającymi z czynnikami zewnętrznymi (trasy przejazdu konwoju, osób postronnych, warunków terenowych bądź atmosferycznych, itp.). Ustawodawca określa definicję zdarzenia, która brzmi następująco:

Zdarzeniem mogącym wystąpić w Służbie Więziennej jest zagrożenie lub naruszenie bezpieczeństwa jednostki organizacyjnej Służby Więziennej. A także naruszenie prawa przez wymienionych, ścigane z urzędu.

Jest wiele zdarzeń, które mogą wystąpić podczas konwojowania. Zalicza się do nich między innymi: ucieczka osoby konwojowanej, bunt osób konwojowanych, napad na konwój, choroba osób konwojowanych, choroba samych konwojentów, wypadek bądź katastrofa drogowa, utknięcie w korku samochodowym, awaria pojazdu oraz jego unieruchomienie, autoagresja konwojowanych, zaśląbnięcie konwojowanych oraz śmierć osadzonego podczas realizacji konwoju.

¹⁹ W. Gromadzki, *Konwojowanie osadzonych*, Wyd. COSSW, Kalisz 1993, s. 3.

Zagrożenia mogą wystąpić w każdym miejscu, czasie i sytuacji. Kluczowym jest, aby przewidywać następstwa danych wydarzeń i stosować profilaktykę w działaniu, która umożliwi prawidłowe i bezpieczne przeprowadzenie konwoju. W czasie powstania któregośkolwiek z zagrożeń funkcjonariusze powinni podejmować działania adekwatne do jego charakteru. Działania te powinny być przemyślane, jak i zespołowe. Jedynie zespół, który działa w sposób zorganizowany, daje szansę konwojentom na opanowanie i przeciwdziałanie powstałym zagrożeniom.

Minimalizacja zagrożeń, które mogą wystąpić podczas konwojowania

Aby zminimalizować wszelkie zagrożenia związane z transportem osadzonych konwojowanie należy przeprowadzać właściwie i według norm prawnych. Natomiast uczestnicy konwoju powinni wywiązać się z swoich wcześniej określonych obowiązków. Dzięki temu wystąpienie wszelkich niespodziewanych zdarzeń będzie mniej prawdopodobne. Konwojowanie powinno przebiegać bez zakłóceń, gdy zostanie uprzednio zaplanowane i zorganizowane. Niezbędne w tym przypadku jest opracowanie instrukcji przeznaczonej dla funkcjonariuszy (konwojentów, dowódcy konwoju, kierowcy, funkcjonariuszy służby medycznej bądź przewodników psów służbowych) uczestniczących w transporcie. Opracowane instrukcje powinny zawierać ogólne zasady wykonywania czynności związanych z konwojowaniem z uwzględnieniem charakteru danego konwoju (inne dla stale wykonywanych czynności konwojowych np. do miejsca pracy osadzonych a inne dla wykonywania konwoju np. do placówki medycznej). Podstawą do wykonania niezbędnej dokumentacji jest protokół z przeprowadzonego rozpoznania²⁰. Natomiast sam sposób przygotowania konwoju jest uzależniony od tego, czy będzie on planowany, czy doraźny. Przy konwojowaniu planowanym należy zorganizować transport osadzonych w taki sposób, aby zostały spełnione kryteria transportowe (są to niezbędne informacje, które dotyczą skazanego w trakcie podejmowania decyzji w przedmiocie przetransportowania, pozostawienia skazanego w danej jednostce penitencjarnej bądź jego pobytu), a w szczególności należy uwzględnić zasady, które zostały określone w art. 100, §165 i 112 §3 i 4 kodeksu. Jeśli dochodzi do zbiegu przynajmniej dwóch przyczyn przetransportowywania powinno się uwzględnić przede wszystkim stan zdrowia skazanego i względy bezpieczeństwa jego oraz jednostki penitencjarnej, system terapeutyczny, odbywanej przez niego kary, czynności procesowe toczące się w jego sprawie, zatrudnienie, naukę i dopiero w dalszej kolejności pozostałe przesłanki. Nie należy dokonywać zmiany grupy

²⁰ P. Jarczewski, K. Jędrzejak, M. Kuświk, K. Setla, *Konwojowanie...*, dz. cyt., s. 13.

czy podgrupy klasyfikacyjnej przetransportowanym skazanym do aresztu śledczego bądź przebywającym w nim, chyba, że nastąpiły inne, niezwiązane z powodem przetransportowania, uzasadniające to okoliczności²¹.

Czynnikiem mającym wpływ na minimalizację zagrożeń podczas konwojowania jest stosunek funkcjonariuszy do zasad bezpieczeństwa podczas jego realizacji. Zasady te są ściśle ustalone i powinny być przestrzegane, aby zmniejszyć prawdopodobieństwo wystąpienia niebezpieczeństwa. Zalicza się do nich: ściśle przestrzeganie ustaleń, które zostały zawarte wcześniej w dokumentacji, wzmożenie obserwacji najbliższego otoczenia oraz zachowanie się osadzonego; ustawienie pojazdu konwojowanego w taki sposób, aby droga dojścia do wyznaczonego miejsca była jak najkrótsza i aby możliwe było obserwowanie terenu oraz ochrona pojazdu, sprawdzenie drogi dojścia do miejsca docelowego, sprawdzenie pomieszczenia w którym osadzony ma przebywać, sprawdzenie otwartych pomieszczeń znajdujących się na korytarzu, ustalenie (przy ew. wizycie medycznej) z lekarzem sposobu ochrony osadzonego, zachowanie szczególnej ostrożności podczas otwierania drzwi pojazdu i doprowadzania, odpowiednie rozstawienie konwojentów, stała obserwacja osadzonego podczas trwania czynności medycznych, utrzymywanie łączności z jednostką macierzystą.

Wyżej wymienione zasady to podstawowe czynności, które powinny być zachowywane przez funkcjonariusza Służby Więziennej, by realizowane konwojowanie było wykonane w sposób zapewniający bezpieczeństwo wszystkim uczestnikom konwoju. Kolejnym elementem, który ma znaczenie w kontekście bezpieczeństwa konwoju jest stosunek funkcjonariuszy do danych obowiązków. W zależności od pełnionego stanowiska ich zakres jest różny. Dowódca konwoju bierze największą odpowiedzialność za właściwe przeprowadzenie transportu. Jego decyzje mają duży wpływ na bezpieczeństwo podczas konwojowania i mogą bezpośrednio przyczynić się do wystąpienia lub ograniczenia zagrożeń. Przed przystąpieniem do konwoju musi on: sprawdzić stan zabezpieczeń techniczno-ochronnych danego pojazdu konwojowego, sprawdzić tożsamość osadzonego a także jego rozmieszczenie w pojeździe konwojowym, przekazać osadzonego, jego dokumenty i depozyt we wskazanym wcześniej zakładzie, ostrzec osadzonego o możliwości użycia broni palnej lub środków przymusu bezpośredniego, prowadzić książkę przebiegu służby w wypadku konwojowania, które realizowane jest na innej podstawie niż polecenie dyrektora; podejmować oraz organizować działania ochronne w przypadku zaistnienia sytuacji zagrażającej bezpieczeństwu konwoju, podejmować decyzje o użyciu sygnałów dźwiękowych i świetlnych. Tak samo duże znaczenie

²¹ Zarządzenie nr 38/23 w sprawie transportowania skazanych z dnia 31 maja 2023 r. (Dz.U. z 2022 r., poz. 2470 oraz z 2023 r. poz. 240, 347 i 641).

podczas konwojowania ma sposób wykonania swoich obowiązków przez samych konwojentów. Do obowiązków konwojenta należy: przeprowadzenie kontroli samego osadzonego, jak i jego bagażu, obserwacja zachowania osadzonego; nie-dopuszczanie do kontaktów osadzonych z osobami postronnymi, pozostawianie w stałej gotowości do ewentualnego przeciwdziałania powstałym zagrożeniom, niezezwalanie osadzonemu na zmianę wyznaczonych miejsc w pojeździe konwojowym oraz podejmowanie niezbędnych działań ochronnych. Kierowca konwoju, który wchodzi w jego skład i podlega służbowo dowódcy konwoju, a który nie jest liczony do jego składu ma obowiązki wynikające z powierzenia wykonywania czynności służbowych na tym stanowisku. Jest to między innymi: przygotowanie pod względem technicznym pojazdu przeznaczonego do transportu; niezatrzymywanie bez uzasadnienia pojazdu w trakcie konwojowania, wykonywanie zadań z zakresu ochrony podczas postoju, wykonywanie poleceń dowódcy konwoju. W konwoju może również uczestniczyć funkcjonariusz lub pracownik służby zdrowia. Jego zadania są skoncentrowane na prawidłowym przebiegu czynności medycznych a także na obserwacji i podejmowaniu właściwych zadań w przypadku wystąpienia zagrożeń związanych ściśle ze sprawami medycznymi (np. pogorszenie stanu zdrowia osoby konwojowanej).

Ustawodawca w sposób sprecyzowany określił katalog kto i co może podlegać czynnościom związanym z konwojowaniem. Stosowanie się do tego katalogu jest niezbędne w przeprowadzaniu transportu. Zakres ten został określony po to by względnie zwiększyć bezpieczeństwo jednostek organizacyjnych Służby Więziennej (w tym osadzonych, samych funkcjonariuszy czy osób postronnych). Istnieje grupa osadzonych, których nie powinno się transportować lub w maksymalnym stopniu ograniczyć czynności konwojowe realizowane wobec tych osób. Przesłanką do ograniczenia możliwości konwojowania danej osoby jest ryzyko wystąpienia zagrożenia zarówno dla osób wykonujących czynności konwojowe, osób postronnych, jednostki penitencjarnej czy jej samej. Dotyczy to między innymi osób, którym udzielane będą świadczenia zdrowotne, a których przerwanie, zaprzestanie lub odroczenie może skutkować negatywnymi skutkami dla ich zdrowia; zastosowano wobec nich sankcje w innej sprawie; organ prowadzący lub nadzorujący ich postępowanie karne bądź sąd, który prowadzi postępowanie cywilne, wystąpił z wnioskiem o pozostawienie ich w określonej jednostce. Odpowiednie dostosowanie sposobu transportowania skazanych do zaistniałych potrzeb pozwala na bezpieczne wykonanie transportu. Jest to kluczowy element, który jest organizowany na dwa sposoby; bezpośredni jak i pośredni i realizowany jest poprzez użycie pojazdów konwojowych. Ważnym jest, aby pamiętać, że transport nie powinien trwać dłużej niż 3 dni, w przypadku zaistnienia takiej sytuacji przyjmujący transport ma obowiązek zawiadomić o tym właściwego dyrektora okręgowego Służby

Więziennej, natomiast jeśli transport przybył spoza danego okręgu – Dyrektora BIS. Podejmuje on działania, które mają zapobiec powstaniu podobnym nieprawidłowościom. Jeśli podczas transportowania bezpośredniego zaistnieje potrzeba pobytu skazanych w danej jednostce penitencjarnej, która usytuowana jest przy trasie przejazdu i jest ona związana z przerwą w tym transportowaniu lub innymi istotnymi powodami to może on odbywać się etapowo. Natomiast jeśli zaistnieje sytuacja, w której nie jest możliwe bez zwłoki przemieszczenie do innego pojazdu konwojowego skazanych transportowanych etapowo akceptuje się możliwość oczekiwania ich na dalsze przemieszczanie, przy czym nie może ono być dłuższe niż dwie doby. Jeśli zaistnieją okoliczności określone w 6 ust. 3 roz. ministra sp, z 29/2015 jednostki penitencjarne mają obowiązek udzielić dowódcy konwoju pomocy, która jest niezbędna w realizacji tego transportu. Powyżej opisane zasady dotyczą również transportu przeprowadzanego przez organ doprowadzający.

Ważnym elementem związanym z zapewnieniem bezpieczeństwa podczas konwojowania jest nie udzielać osobom nieupoważnionym jakiegokolwiek informacji o konwojowaniu, oraz nie wykonywać czynności innych, aniżeli te, które wynikają z realizacji konwojowania.

Powyżej opisane zasady, czynności czy powinności z pewnością ułatwiają wykonanie trudnego i złożonego zadania, jakim jest konwojowanie i przekładają się na zwiększenie bezpieczeństwa podczas wykonywania tych czynności. Ponadto profilaktyka ta daje szansę na ograniczenie osadzonemu możliwości zachwiania porządkiem oraz bezpieczeństwem w jednostkach organizacyjnych Służby Więziennej oraz poza nimi. Są one niezbędne, by czynności związane z konwojowaniem przebiegały w sposób bezpieczny i zgodny z obowiązującym porządkiem prawnym.

Podsumowanie

Konwojowanie stanowi wielkie wyzwanie dla funkcjonariuszy Służby Więziennej. Podczas realizacji zadań transportowych istnieje wiele zagrożeń mających wpływ na bezpieczeństwo społeczeństwa, jak i samych pracowników Służby Więziennej. Zredukowanie prawdopodobieństwa wystąpienia niebezpieczeństw jest możliwe wtedy, gdy funkcjonariusze wywiązują się ze swoich obowiązków w sposób rzetelny oraz stosują się do ściśle określonych zadań. Warto podkreślić, że szczegóły mają znaczenie na całokształt przeprowadzonego konwojowania, dlatego też niezbędnym jest odpowiednie przeszkolenie osób organizujących konwój. Dzięki temu, pomimo występujących trudności, funkcjonariusze Służby Więziennej są w stanie zapewnić ogólne bezpieczeństwo.

Bibliografia

- Bąk T., Ciekanowski Z., *Teorie Bezpieczeństwa*, Wyd. PWSTE, Jarosław 2012.
- Czupryński A., Wiśniewski B., Zboina J., *Bezpieczeństwo Teoria-badania-praktyka*, Wyd. CNBOP-PIB, Warszawa 2016.
- Ficoń K., *Bezpieczeństwo narodowe i jego typologie*, Wyd. BEL Studio, Warszawa 2020.
- Gromadzki W., *Konwojowanie osadzonych*, Wyd. COSSW, Kalisz 1993.
- Jarczewski P., Jędrzejak K., Kuświk M., Setla K., *Konwojowanie w służbie więziennej*, Wyd. COSSW, Kalisz 2006.
- Kuć M., *Rola służb penitencjarnych w polityce kryminalnej*, [w:] *Autorytet i godność służb penitencjarnych a skuteczność metod resocjalizacji*, (red.) J. Świtek, M. Kuć, I. Niewiadomska, Wyd. KUL, Lublin 2004.
- Kwieciński J., Waligóra B., *Zatrudnienie w strategii readaptacji społecznej skazanych – na przykładzie Zakładu Karnego we Wronkach*, [w:] B. Skafrniak, *Pomoc postpenitencjarna w kontekście działań resocjalizacyjnych*, Wyd. Impuls, Kraków 2007.
- Poklek R., *Służba więzienna w systemie bezpieczeństwa państwa*, „Securitologia” 2013, nr 1(17).
- Stańdo-Kawecka B., *Prawne podstawy resocjalizacji*, Wyd. Zakamycze, Kraków 2000.
- Szczepiński A., *Pojęcie bezpieczeństwa i jego typologia – próba systematyzacji*, „Zeszyty Naukowe Collegium Witelona” 2023, nr 48(3).
- Szkudlarek I., Szkudlarek K., *Bezpieczeństwo przewozu towarów niebezpiecznych – przepisy wewnętrzne na przykładzie Polskich Kolei Państwowych Polskich Linii Kolejowych S.A.*, „Studia Kaliskie – Studia Calisiensia” 2024, t. 12, nr 1/2024.
- Śmiałek K., *Zarządzanie kryzysowe wobec wyzwań i zagrożeń dla bezpieczeństwa wewnętrznego państwa*, Wyd. WAT, Warszawa 2020.
- Zarządzenie nr. 29/2015 w sprawie transportowania skazanych z dnia 1 czerwca 2015 r. (Dz.U. 2014 r., poz. 44323 z późn. zm.).
- Zięba J., *Treść i zakres pojęcia bezpieczeństwo Polski*, Wyd. WNSiH, Poznań 2003.

Alternatywny system wykonywania kary pozbawienia wolności

Anna PŁOMIŃSKA¹

Akademia Wymiaru Sprawiedliwości

ORCID: 0009-0009-6683-0625

Streszczenie. Prawo karne przewiduje wiele sposobów odbywania kary, które są zróżnicowane w zależności od popełnionego czynu, uprzedniej karalności a także zachowania w trakcie odbywania kary pozbawienia wolności. Składa się na to wiele czynników takich jak systemy, rodzaje czy typy zakładów karnych. Szczególną uwagę skupić można właśnie na systemie dozoru elektronicznego, który jako alternatywa odbywania kary pozbawienia wolności cechuje się dobrem osadzonych oraz ich rodzin, dzięki czemu więzi między nimi są zachowane. W artykule przybliżone są podstawy teoretyczne, w których zawarte zostały: definicja, środki kontroli, metody i sposoby przeprowadzania dozoru elektronicznego, a także opis procesu zezwalającego na możliwość odbycia kary w systemie dozoru elektronicznego. Uwzględnione zostały również korzyści i konsekwencje jakie mogą powstać dla osoby odbywającej karę w tym systemie. Celem pracy jest przede wszystkim analiza funkcjonowania systemu dozoru elektronicznego z uwzględnieniem procesu resocjalizacji skazanych.

Słowa kluczowe: system penitencjarny, system dozoru elektronicznego, kara pozbawienia wolności, osadzony, zakład karny

Wstęp

Polski system penitencjarny poddawany jest ciągłym modernizacjom na potrzeby zapewnienia przede wszystkim bezpieczeństwa publicznego oraz bezpieczeństwa funkcjonariuszy Służby Więziennej, a także osób pozbawionych wolności. W związku z tym 24 stycznia 2024 roku ustanowiony i wdrożony został „Program modernizacji Służby Więziennej w latach 2022-2025”, który jest

¹ Ppor. mgr Anna Płomińska – oficer Służby Więziennej, absolwentka studiów magisterskich na kierunku penitencjarystyka w Akademii Wymiaru Sprawiedliwości.

realizowany przez Dyrektora Generalnego Służby Więziennej². Co więcej system penitencjarny opiera się w szczególności na humanitarnym traktowaniu osób pozbawionych wolności, na indywidualizacji i dostosowywaniu różnorodnych programów resocjalizacyjnych, czy readaptacyjnych, mających na celu zredukowanie lub wyeliminowanie deficytów psychologicznych wśród osadzonych.

Warto zwrócić uwagę na klasyfikację osadzonych, która odgrywa w systemie penitencjarnym kluczową rolę, gdyż jej głównym celem jest stworzenie dla osadzonego bezpieczeństwa, odpowiednich warunków i doboru metod resocjalizacyjnych, dzięki którym zmniejsza się proces wzajemnej demoralizacji. Osadzonych klasyfikuje się mając na względzie w szczególności:

wiek, płeć, uprzednie odbywanie kary pozbawienia wolności, umyślność lub nieumyślność czynu, czas pozostałej do odbycia kary pozbawienia wolności, stan zdrowia fizycznego i psychicznego, w tym stopień uzależnienia od substancji psychoaktywnej, stopień demoralizacji i zagrożenia społecznego, rodzaj popełnionego przestępstwa, stosunek skazanego do popełnionego przestępstwa³.

Pozwala to funkcjonariuszom Służby Więziennej prawidłowo delegować osadzonego do rodzaju i typu zakładu karnego, a także umieścić w celi mieszkalnej z innymi osobami pozbawionymi wolności, które wzajemnie nie będą negatywnie na siebie oddziaływać. System penitencjarny przewiduje także inny rodzaj odbywania kary, jakim jest system dozoru elektronicznego, który pozwala na wykonanie wyroku w miejscu zamieszkania. Jest to nowy innowacyjny sposób mający na celu monitorowanie skazanych za przestępstwa o niskim wymiarze, którzy w stopniu lekkim są odchyleni od normy, a pobyt w zakładzie karnym mogłby to zmienić. Wymienić tutaj można wiele korzyści jak chociażby najważniejsze – fizyczny kontakt z rodziną, jak i ze społeczeństwem.

Geneza powstania systemu dozoru elektronicznego

Za twórcę powstania elektronicznego monitoringu uznaje się amerykańskiego psychologa Ralpha Schwitzgebela, który zapoczątkował go w roku 1967. Natomiast w praktyce system zastosowano w 1983 r. w stanie Nowy Meksyk – były to pierwsze programy alternatywnego wymiaru kary realizowane w latach 80, w 21 stanach, w Stanach Zjednoczonych Ameryki⁴. Szczególnym założeniem owego

² Dz.U.2024.86, tj. „Program modernizacji Służby Więziennej w latach 2022-2025”, rozdz. 2, art. 7-9.

³ Dz.U.2024.0.706 tj. – Ustawa z dnia 6 czerwca 1997 r. – KKW, art. 82 §1 i 2.

⁴ D. Sielicki, *Elektroniczne monitorowanie przestępców – nowoczesna alternatywa pozbawienia wolności*, „Przegląd Więziennictwa Polskiego” 2005, nr 47-48, s. 15.

system była alternatywa dla kary pozbawienia wolności, czyli znalezienie środka bardziej efektywniejszego od probacji, tzw. *intermediate penalties*⁵.

W Polsce system dozoru elektronicznego swoją historię legislacyjną rozpoczął w 2007 r.⁶, ustawą z dnia 7 września 2007 r. o wykonywaniu kary pozbawienia wolności po za zakładem karnym w systemie dozoru elektronicznego (dalej: UWKPW)⁷, którą reguluje ustawa z dnia 6 czerwca 1997 r. Kodeks karny wykonawczy (dalej: KKW)⁸. Jednak zastosowanie systemu nastąpiło dopiero w 2009 roku i w dodatku obejmując tylko część Polski. W późniejszym czasie poszerzono zakres terytorialny na obszar całego państwa, a sam proces zakończył się w 2012 roku⁹. Trzy lata później, w 2015 roku doszło do rewolucyjnych zmian – dokładnie 20 lutego ustanowiono nowelizację, z której wynikało, że system dozoru został całkowicie usunięty z wykonywania kary pozbawienia wolności, a stał się elementem kary ograniczenia wolności. Niespełna rok później, 11 marca 2016 r. nastąpiło odwrócenie tej reformy, gdzie dozór elektroniczny jest formą wykonywania kary pozbawienia wolności. Zmiany te weszły w życie w dniu 15 kwietnia tego samego roku¹⁰. Wszystkie definicje, objaśnienia i zasady związane z kwalifikowaniem, metodami przeprowadzania, a także zakończeniem wykonywania kary w systemie dozoru elektronicznego oraz środki techniczne wykorzystywane do tego systemu zostały zmodernizowane i umieszczone w Kodeksie karnym wykonawczym, w dodatkowym rozdziale VIIa zatytułowanym *System dozoru elektronicznego*¹¹.

Charakterystyka systemu dozoru elektronicznego

System dozoru elektronicznego (SDE), to forma monitorowania osób skazanych, która ma na celu zapewnienie bezpieczeństwa społeczeństwa oraz wspieranie resocjalizacji osadzonych. Dzięki technologii, osoby odbywające karę pozbawienia wolności na warunkach dozoru elektronicznego mogą wrócić do swoich

⁵ B. Stańdo-Kawecka, *Dozór elektroniczny w systemie sankcji karnych w wybranych krajach europejskich*, „Państwo i Prawo” 2012, nr 5, s. 31.

⁶ P. Kuzior, *System dozoru elektronicznego jako alternatywa dla kary pozbawienia wolności*, „Systemy Wspomagania w Inżynierii Produkcji” 2017, t. 6, z. 5, s. 90-101.

⁷ Ustawą z dnia 7 września 2007 r. o wykonywaniu kary pozbawienia wolności po za zakładem karnym w systemie dozoru elektronicznego, Dz.U. 2007 nr 191 poz. 1366 (UWKPW).

⁸ Ustawa z dnia 6 czerwca 1997 r. Kodeks karny wykonawczy, Dz.U. 2023 poz. 127 (KKW).

⁹ K. Mamak, *Funkcjonowanie dozoru elektronicznego w świetle badań aktowych*, „Czasopismo Prawa Karnego i Nauk Penalnych” 2014, nr 2, s. 140-143.

¹⁰ Ustawa o zmianie ustawy – Kodeks karny oraz ustawy – Kodeks karny wykonawczy, Dz.U. 2016, poz. 42.

¹¹ Ustawa o zmianie ustawy kodeks karny oraz niektórych innych ustaw, Dz.U. 2015, poz. 396.

rodzin i aktywnie uczestniczyć w życiu społecznym, zachowując jednocześnie kontrolę nad ich zachowaniem. Nadzór merytoryczny i techniczny nad funkcjonowaniem SDE sprawuje Służba Więzienna, a konkretnie Biuro Dozoru Elektronicznego Centralnego Zarządu Służby Więziennej (BDE CZSW),

które realizuje obsługę centrali monitorowania. Jest także podmiot dozoru, odpowiedzialny za patrole terenowe, które m.in. sprawdzają warunki techniczne w przyszłym miejscu odbywania kary (zasięg nadajników telefonii komórkowej, zasilanie w energię elektryczną i warunki lokalowo-sanitarne), instalują oraz deinstalują w nim urządzenia i kontrolują ich działanie¹².

Według definicji ustawodawcy:

dozór elektroniczny polega na kontroli zachowania skazanego przy użyciu środków technicznych¹³, a system dozoru elektronicznego jest to ogół metod postępowania i środków technicznych służących do wykonywania dozoru elektronicznego¹⁴.

System karnoprawny przewiduje kilka możliwości dozoru tj. *dozór stacjonarny, dozór mobilny, dozór zbliżeniowy*¹⁵. Są one odpowiednio dostosowywane do rodzaju popełnionego przestępstwa. Właściwe wykonywanie kary pozbawienia wolności w systemie dozoru elektronicznego (SDE) opiera się na monitorowaniu skazanych za pomocą zaawansowanych środków technicznych. System ten ma na celu nie tylko kontrolę, ale również wspieranie resocjalizacji osób odbywających karę. Możliwe formy systemu dozoru elektronicznego obejmują:

- Środki zapobiegawcze: Elektroniczna kontrola miejsca pobytu, która może być stosowana w toku postępowania karnego, zapewniając bezpieczeństwo jego poprawnego przebiegu. Działa to jako forma zabezpieczenia, eliminując ryzyko ucieczki czy powrotu do przestępczych działań.
- Środki karne: Zastosowane w przypadku orzeczenia zakazu zbliżania się do określonych osób lub wyznaczonych miejsc. Tego typu kontrola pomaga chronić ofiary przestępstw oraz zapobiega dalszym incydentom.
- Alternatywne rozwiązania: SDE umożliwia odbywanie kary pozbawienia wolności w warunkach innych, niż osadzenie w jednostce penitencjarnej, co przyczynia się do redukcji przełudnienia w więzieniach oraz pozwala na łatwiejszą reintegrację skazanych w społeczeństwie.

¹² Obrączka, obroża, elektroniczne kajdanki, <https://www.ebos.pl/arttykul/obraczka-obroza-elektroniczne-kajdanki-elektroniczny-dozor-skazanych.html> [dostęp: 01.07.2024 r.].

¹³ KKW, art. 43b §1.

¹⁴ KKW, art. 43b §2.

¹⁵ KKW, art. 43b §3.

Aparatura monitorująca, odpowiadająca za funkcjonowanie osoby objętej systemem dozoru elektronicznego składa się z urządzeń elektronicznych, systemów oraz instalacji zawierające podzespoły elektryczne lub elektroniczne czyli tzw. środki techniczne. W tym systemie aparaturę monitorującą stanowią kolejno:

- **Centrala monitorowania:** Jest to centrum komputerowe wyposażone w zaawansowane narzędzia do przetwarzania danych osobowych zgodnie z Ustawą o ochronie danych osobowych¹⁶. Służy do rejestrowania, gromadzenia, przechowywania, zabezpieczania oraz przekazywania informacji o przestrzeganiu przez skazanych obowiązków, takich jak pozostawanie w określonym miejscu i czasie nałożonym przez sąd.
- **Nadajnik:** Kluczowy element systemu, który skazany musi nieprzerwanie nosić. Jest to urządzenie radiowe, które generuje sygnał identyfikujący lokalizację skazanej osoby. Nadajnik jest montowany na lewej nodze i przypomina bransoletę, zaprojektowaną tak, aby nie można jej było zdjąć bez uszkodzenia. Oprócz wbudowanego nadajnika GPS, urządzenie jest również wodoodporne, co zwiększa jego funkcjonalność w codziennym życiu. Nadajnik posiada unikalny numer identyfikacyjny oraz kod QR, co ułatwia jego monitorowanie. Sam montaż polega na zmierzeniu obwodu lewej nogi w miejscu nad kostką oraz założeniu nadajnika by nie przylegał bezpośrednio do ciała. Ma to na celu w szczególności uniemożliwić demontaż urządzenia, a także zapewnić wygodę w codziennym funkcjonowaniu.



Ryc. 1. Nadajnik

Źródło: Oprac. własne.

¹⁶ Dz.U.2019.1781, Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

- Elektroniczne urządzenie rejestrujące: Odbiera sygnały z nadajnika i przesyła je do centrali monitorowania. Dzięki temu możliwe jest bieżące śledzenie lokalizacji skazanych i reagowanie na ewentualne naruszenia warunków dozorowych¹⁷.

Są dostępne także stacjonarne urządzenia monitorujące ze słuchawką oraz przyciskami:

- przycisk alarmowy (łączy z nr 112 – jednolity numer alarmowy służący do powiadamiania odpowiednich służb w wyniku zagrożenia),
- przycisk łączący z centralą monitorowania (czerwony i zielony przycisk).



Ryc. 2. Stacjonarne urządzenie monitorujące

Źródło: Oprac. własne

Istnieje możliwość dowolnego oprogramowania urządzenia zgodnie z wymaganiami odpowiedniego podmiotu. Z myślą o najwyższym poziomie bezpieczeństwa zastosowano bardzo silne szyfrowanie AES-256. Dotyczy to zarówno komunikacji między nadajnikiem skazanego, a stacjonarnym urządzeniem monitorującym, jak i komunikacji między stacjonarnym urządzeniem monitorującym, a Centrum Monitorowania¹⁸.

Instalowane są zazwyczaj w miejscu stałego pobytu skazanego lub w innym miejscu wskazanym przez sąd penitencjarny. Na urządzenie monitorujące dzwo-

¹⁷ D. Sarzała, *Resocjalizacyjny wymiar dozoru elektronicznego jako nieizolacyjnego modelu wykonywania kary pozbawienia wolności*, „Lubelski Rocznik Pedagogiczny” 2016, nr 2, s. 165.

¹⁸ K. Gucwa-Porębska, *Funkcjonowanie społeczne osadzonych w systemie dozoru elektronicznego uwarunkowania rodzinne i środowiskowe*, Wyd. „Difin”, Warszawa 2020, s. 37.

nią funkcjonariusze dozoru w celu wyjaśnienia jakichś nieprawidłowości, a także sprawdzeniu łączności.

Montowane są także urządzenia radiowe z modulem GPS, mające za zadanie rejestrowanie sygnałów wysyłanych przez pozostający w zasięgu nadajnik. Uzyskane informacje dotyczą przestrzegania obowiązku pozostawania skazanego w miejscu stałego pobytu lub w innym wskazanym miejscu i w wyznaczonym czasie. Powiązane są także z obowiązkiem powstrzymania się skazanego od przebywania w określonych miejscach lub zakazu zbliżania się do określonej osoby. Wyposażone urządzenia w interfejs pozwalają na przekazywanie takich informacji do centrali monitorowania w celu identyfikacji aktualnego miejsca pobytu skazanego¹⁹. Dokonując kontroli przez podmiot dozoru lub pracowników owego podmiotu, skazany ma obowiązek udostępniania pomieszczeń, w których znajduje się zamontowane środki techniczne oraz w których przebywa, w celu kontroli tych urządzeń, naprawy bądź wymiany. Skazany ma również obowiązek

udzielać prezesowi sądu lub upoważnionemu sędziemu, sądowemu kuratorowi zawodowemu, podmiotowi dozoru i podmiotowi prowadzącemu centralę monitorowania wyjaśnień dotyczących przebiegu odbywania kary i wykonywania nałożonych obowiązków oraz stawiać się na wezwania sędziego i kuratora²⁰.

Sposoby ubiegania się o wykonywanie kary w SDE

Obowiązujący od 2023 roku znowelizowany Kodeks Karny Wykonawczy precyzuje możliwości udzielenia zezwolenia na odbycie kary pozbawienia wolności w systemie dozoru elektronicznego. Z przepisów wynika, że Sąd penitencjarny w postępowaniu wykonawczym lub komisja penitencjarna funkcjonująca w zakładzie, w którym przebywa skazany dokonuje decyzji o możliwości wykonywania kary pozbawienia wolności w *systemie dozoru elektronicznego*²¹. Jednak sąd orzekający w sprawie nie ma możliwości uwzględnienia owego systemu w wyroku skazującym, ale zastosowany przez sąd wymiar kary pozbawienia wolności może być przesłanką do określenia wykonania kary w SDE²². Podstawowym warunkiem jest, aby kara pozbawienia wolności nie przekraczała jednego roku i sześciu miesięcy pozbawienia wolności albo wobec skazanego orzeczono karę pozbawienia

¹⁹ Tamże.

²⁰ KKW, art. 43n §1 pkt 4.

²¹ KKW, art. 43e.

²² A. Gerecka-Żołyńska, P. Karlik, M. Kusak, P. Wiliński, M. Zamroczyńska, [w:] *Prawo karne wykonawcze*, red. A. Gerecka-Żołyńska, Wyd. Wolters Kluwer, Warszawa 2021, s. 194-195.

wolności w wymiarze niższym niż trzy lata, a do odbycia w zakładzie karnym została mu część tej kary w wymiarze nie wyższym niż sześć miesięcy, dotyczy to kar orzeczonych w wyroku skazującym.

Zgodnie z art. 43lc Kodeksu karnego wykonawczego tj.

W sprawach o udzielenie skazanemu zezwolenia na odbycie kary pozbawienia wolności w systemie dozoru elektronicznego sąd penitencjarny orzeka na wniosek skazanego lub na wniosek jego obrońcy, prokuratora, sądowego kuratora zawodowego lub dyrektora zakładu karnego²³.

Wniosek o odbywanie kary pozbawienia wolności w systemie dozoru elektronicznego, wraz z uzasadnieniem i wszelkimi zgodami, składa się na piśmie. Ważnym elementem jest zasadność wniosku, ponieważ Kodeks karny wykonawczy określa warunki, które skazany musi spełnić, aby otrzymać takie zezwolenie. Zgodnie z treścią artykułów w KKW w rozdziale VIIa, oddział 2a tj. *Warunki i tryb orzekania o udzieleniu skazanemu zezwolenia na odbycie kary pozbawienia wolności w systemie dozoru elektronicznego*²⁴, osoba ubiegająca się posiada orzeczenie na wykonanie kary pozbawienia wolności nieprzekraczającej jednego roku i sześciu miesięcy, o ile nie zachodzą warunki przewidziane w art. 64 Kodeksu karnego tj. *recydywa szczególna podstawowa i wielokrotna*²⁵. Ponadto, kara ta musi być wystarczająca do osiągnięcia celów kary, skazany musi posiadać stałe miejsce zamieszkania, a pełnoletnie osoby mieszkające z nim muszą wyrazić pisemną, dobrowolną zgodę na dozór. Zgoda ta, zgodnie z art. 43h §3 Kodeksu karnego wykonawczego, obejmuje również umożliwienie podmiotowi dozorujsystemu prowadzenia czynności kontrolnych. Ważne są także warunki techniczne, takie jak dostępność nadajników i rejestratorów, które nie mogą utrudniać odbywania kary w tym systemie.²⁶

Ustawodawca przewidział również sytuację, w której osoby mieszkające ze skazanym nie wyraziły zgody na odbywanie kary przez niego w systemie dozoru elektronicznego. Wówczas zgodnie z art. 43la §4 KKW sąd może mimo to udzielić zezwolenia, jeśli odbywanie kary w tym systemie nie powoduje nadmiernych trudności dla tych osób i tylko w niewielkim stopniu narusza ich prywatność. Osoba, która nie wyraziła zgody, może złożyć zażalenie na postanowienie sądu. Po złożeniu przez skazanego wniosku o odbywanie kary poza zakładem karnym, sąd penitencjarny przeprowadza posiedzenie w zakładzie, w którym przebywa ska-

²³ KKW, art. 43lc.

²⁴ KKW, art. 43la-43ln.

²⁵ KK, art. 64 §2.

²⁶ KKW, art. 43h §1-5.

zany. Sąd uzyskuje informacje od przedstawiciela administracji zakładu karnego co do celowości tego rozwiązania oraz od podmiotu dozoru – w zakresie dostępności warunków technicznych. Sąd przeprowadza także rozmowę z osadzonym, jego obrońcą lub kuratorem sądowym, aby zgromadzić wszelkie istotne informacje potrzebne do rozpatrzenia wniosku, w tym dotyczące osobistych warunków skazanego oraz jego stosunku do odbywania kary w systemie dozoru elektronicznego. Jeśli prokurator sprzeciwi się odbywaniu kary w tym systemie, decyzja sądu staje się prawomocna po jej uprawomocnieniu. W przypadku braku przeciwwskazań, sąd kontynuuje dalsze czynności. Na końcu sąd informuje o miejscu, czasie, rodzaju instalacji urządzeń technicznych oraz sposobie wykonywania obowiązków. Ustalany jest termin i sposób, w jaki skazany ma zgłosić się do instalacji rejestratora stacjonarnego, przenośnego lub nadajnika.

Skazany, który jeszcze nie rozpoczął odbywania kary pozbawienia wolności w zakładzie karnym, może uzyskać zgodę na odbywanie jej w systemie dozoru elektronicznego (SDE), o ile stopień jego demoralizacji, względy bezpieczeństwa oraz inne okoliczności nie uzasadniają umieszczenia go w zakładzie karnym. Wykonywanie kary pozbawienia wolności w systemie dozoru elektronicznego ma w szczególności na celu *pozostawienie na wolności tych skazanych, dla których rygory związane z odbywaniem kary w tym systemie będą wystarczające*²⁷. Sąd penitencjarny, oceniając możliwość zastosowania tego systemu, bierze pod uwagę kryteria klasyfikacji osadzonego, analizując zachowanie skazanego zarówno podczas procesu, jak i po wydaniu wyroku, jego sytuację rodzinną i majątkową, tryb życia, właściwości i warunki osobiste, a także wiek i wcześniejszą karalność.

Sąd penitencjarny może zezwolić skazanemu na odbywanie kary pozbawienia wolności w systemie dozoru elektronicznego, niezależnie od tego, czy skazano go na jedną czy więcej kar, które nie podlegają łączeniu. Jeśli jednak wydano wyrok łączny, o zezwoleniu decyduje suma orzeczonych kar, ale musi ona wynosić maksymalnie rok i sześć miesięcy pozbawienia wolności. Natomiast w przypadku kiedy sąd podejmie decyzję o negatywnym rozpatrzeniu wniosku, skazany ma możliwość złożenia ponownego pisma, jednak musi przedstawić nowe okoliczności lub dowody, które nie były wcześniej brane pod uwagę.

Skazany odbywający karę pozbawienia wolności w systemie dozoru elektronicznego (SDE) może ubiegać się o warunkowe przedterminowe zwolnienie, jeśli jego postawa, warunki osobiste, okoliczności popełnienia przestępstwa oraz zachowanie po jego dokonaniu i podczas odbywania kary dają podstawy do przypuszczenia, że po zwolnieniu nie popełni kolejnego przestępstwa. Decyzja

²⁷ M. Zamroczyńska, [w:] *Prawo karne wykonawcze*, red. A. Gerecka-Żołyńska, Wyd. Wolters Kluwer, Warszawa 2021, s. 195.

o przedterminowym zwolnieniu opiera się na pozytywnej prognozie sądowo-kryminologicznej, która uwzględnia życie sprawcy przed i po popełnieniu przestępstwa. Zwolnienie to nie jest możliwe dla osób odbywających karę zastępczą za przestępstwo lub przestępstwo skarbowe – dotyczy jedynie skazanych na orzeczoną karę pozbawienia wolności. Decyzję o warunkowym przedterminowym zwolnieniu skazanego odbywającego karę w systemie dozoru elektronicznego podejmuje sąd penitencjarny podczas posiedzenia, w którym mogą uczestniczyć skazany, jego obrońca oraz inne osoby uprawnione do złożenia wniosku, jeśli taki wniosek złożyły. W przypadku odmowy przedterminowego zwolnienia, sąd może wydać nakaz zatrzymania i doprowadzenia skazanego do zakładu karnego²⁸.

Z możliwości odbycia kary pozbawienia wolności w systemie dozoru elektronicznego nie może skorzystać osoba, która została skazana za udział w zorganizowanej grupie przestępczej, uczyniła sobie z przestępstwa stałe źródło dochodu, działała w warunkach multirecydywy, orzeczono jej areszt za wykroczenie lub zastępczy areszt za wykroczenie²⁹.

Obowiązki skazanego wykonującego karę w SDE

Kurator sądowy informuje skazanego o wszystkich obowiązkach w rozmowie przeprowadzanej po uruchomieniu środków technicznych, niezbędnych do odbywania kary w SDE. Wszystkie obowiązki i prawa skazanego związane z dozorem elektronicznym zapisane są w kodeksie karnym wykonawczym w artykułach 43m oraz 43n. Zgodnie z nimi, skazany ma obowiązek stawić się w wyznaczonym terminie do podmiotu dozoruującego, w celu zamontowania urządzeń technicznych i elektronicznych. W przypadku niezgłoszenia się do podmiotu dozoruującego, podmiot ten zawiadamia o uchyleniu się od montażu urządzenia kuratora sądowego oraz sąd lub komisję penitencjarną³⁰, co skutkuje anulowaniem odbywania kary w systemie dozoru elektronicznego oraz natychmiastowym zatrzymaniem i doprowadzeniem skazanego do zakładu karnego.

Skazany odbywający karę pozbawienia wolności w systemie dozoru elektronicznego ma obowiązek przestrzegania katalogu obowiązków, które są nakładane obligatoryjnie lub fakultatywnie przez sąd penitencjarny. Jednym z najważniejszych obowiązków skazanego jest dbanie o powierzone mu środki techniczne – ochrona ich przed zniszczeniem, utratą lub uszkodzeniem w sposób uniemoż-

²⁸ KKW, art. 43zaa §1.

²⁹ <https://slmadwokaci.pl/prawo-karne/dozor-elektroniczny> [dostęp: 1.10.2024 r.].

³⁰ KKW, art. 43m §3.

liwiający ponowne użycie oraz stałe zasilania powierzonych urządzeń energią elektryczną.

Nadajnik jest tak skonstruowany, że nie ogranicza czynności życiowych i zawodowych skazanego: nie wykrywają go bramki w sklepach, jest bezpieczny dla kobiet w ciąży, można z nim nurkować i pływać. Trzeba go zdejmować do przeprowadzenia niektórych badań lekarskich (rezonans magnetyczny, tomografia, RTG). Jeśli to możliwe, należy wcześniej zgłosić termin badania i uwzględnić to w systemie komunikacyjno-monitorującym, czyli aplikacji centrali monitorowania służącej do kontroli SDE³¹.

W Kodeksie karnym uwzględnione zostały obowiązki co do wykonywania różnych form systemu dozoru elektronicznego. Jednym z nich jest dozór stacjonarny, w którym skazany ma obowiązek pozostawać w wyznaczonym przez sąd miejscu i czasie. Organ ten ustala przedziały czasowe, w których skazany może opuszczać miejsce stałego pobytu na okres nieprzekraczający 12 godzin dziennie, np. w celu pracy zarobkowej, praktyk religijnych, edukacji, utrzymywania więzi rodzinnych, korzystania z opieki medycznej oraz wykonywania niezbędnych zakupów³². Osoba skazana ma obowiązek odbierać połączenia przychodzące, a także udzielać wyjaśnień innym osobom upoważnionym na ich żądanie za pomocą zamontowanego rejestratora stacjonarnego oraz zezwalania na wejście kuratorowi sądowemu zawodowemu do mieszkania lub na nieruchomości, gdzie został umieszczony rejestrator stacjonarny. Kolejnymi sposobami, w których skazany ma możliwość wykonywania kary jest dozór mobilny lub zbliżeniowy, gdzie ma obowiązek nieprzerwanie nosić rejestrator przenośny, odbierać z niego połączenia przychodzące, a także udzielać za pomocą niego wyjaśnień osobą upoważnionym.

W trakcie odbywania kary pozbawienia wolności w systemie dozoru elektronicznego (SDE) mogą wystąpić nagle zdarzenia, które wymagają natychmiastowej interwencji organów wykonawczych. Zgodnie z artykułem 43r KKW, mówiącym o możliwym przypadku niecierpiącym zwłoki, w którym istnieje szansa zagrożenia życia lub zdrowia ludzkiego, sądowy kurator może wyrazić zgodę na odinstalowanie rejestratora stacjonarnego lub usunięcie nadajnika. Sędzia upoważniony w terminie 7 dni od uzyskania zgody od kuratora może nakazać ponowne zainstalowanie rejestratora lub nadajnika, albo występuje do Sądu o przerwę w wykonaniu kary. Ponowne zamontowanie urządzeń następuje po ustaniu przyczyn, które spowodowały ich usunięcie, na wniosek kuratora sądowego. Przerwę w odbywaniu kary sąd może odwołać, jeśli skazany nie wykorzystuje jej zgodnie

³¹ Tamże.

³² KKW, art. 43na.

z przeznaczeniem lub rażąco narusza przepisy porządkowe. W przypadku postanowienia dotyczącego przerwy lub jej odwołania, skazany ma prawo złożyć zażalenie.

Wady i zalety alternatywnego systemu dozoru elektronicznego

Ze względu na genezę powstania systemu dozoru elektronicznego, a także szereg wad systemów więziennych, już w latach 60. rozpoczęto poszukiwania alternatywnych form i resocjalizacyjnych działań opartych na skazanych. Miało to na celu w szczególności rozwiązanie i zapobieganie problemom, z jakimi się wówczas zmagano. Wyróżnić można następujące:

- *problemy związane z personelem więziennym,*
- *trudności związane z negatywnym wpływem społecznym ze strony zdemoralizowanych osób skazanych,*
- *problemy wynikające z panujących warunków fizycznych więzienia,*
- *problemy wynikające ze struktury organizacyjnej więzienia*³³.

W Polsce zanotowano, że od wielu lat utrzymuje się dość wysoki wskaźnik osób pozbawionych wolności przebywających w zakładach karnych³⁴, co prowadzi do narastających problemów godzących w bezpieczeństwo państwa. Spośród nich wyróżnić można: brak walorów resocjalizacyjnych czy wysokie koszty utrzymania. W związku z tym system dozoru elektronicznego, jako środek nie izolacyjny, stwarza możliwość efektywniejszej realizacji celów polityki karnej³⁵. Wyróżnić można wiele zalet, jakie płyną z elektronicznego dozoru. Jedną z kluczowych jest możliwość odbywania kary w warunkach domowych, gdzie proces stygmatyzacji więźniów w takiej sytuacji jest istotnie zmniejszony, w porównaniu do osób, które przebywają w zakładach karnych. Skazany odbywając karę w swoim środowisku społecznym może kontynuować pracę zawodową, edukację oraz podtrzymywać relacje rodzinne. Zwiększa to szanse na reintegrację społeczną, co wiąże się ze sprzyjaniem procesowi resocjalizacji. System ten jest znacznie bardziej elastyczny,

³³ Z. Nowacki, *Zastosowanie penitencjarne systemu dozoru elektronicznego w ocenie skazanych*, „Humanistyczne Zeszyty Naukowe – Prawa Człowieka” 2017, nr 1, s. 147-164.

³⁴ I. Zgoliński, *Dozór elektroniczny jako instrument polityki karnej. Wybrane uwagi na kanwie nowelizacji kodeksu karnego i kodeksu karnego wykonawczego*, „Studia Prawnicze KUL” 2015, nr 4 (64), s. 89-102.

³⁵ M. Adamczyk, *System dozoru elektronicznego w świetle zmian i nowelizacji*, „Horyzonty Bezpieczeństwa”, 2016, nr 2 (1), s. 49-60.

niż tradycyjna forma kary pozbawienia wolności, jednocześnie zapewnia wysoki poziom bezpieczeństwa społecznego. Monitorowanie skazanych odbywających karę poza więzieniem pozwala minimalizować ryzyko ucieczek, złamania zasad i powrotu do przestępstw, co zwiększa zaufanie do tego rozwiązania jako skutecznej alternatywy dla izolacji.

Warto zwrócić uwagę na przeludnienie więzień, które od lat stanowi poważny problem niosący za sobą szereg negatywnych skutków zarówno dla skazanych, jak i całego systemu penitencjarnego. W tym kontekście SDE odgrywa ważną rolę, umożliwiając skuteczne zmniejszenie liczby osadzonych przebywających w zakładach karnych. To rozwiązanie stwarza przestrzeń w więzieniach dla osób, które muszą tam przebywać z uwagi na poważny charakter popełnionych przestępstw, jednocześnie pozwalając na stosowanie kary proporcjonalnej do mniej poważnych wykroczeń. Odciążenie więzień daje państwu możliwość skupienia się na poprawie warunków bytowych i organizacyjnych w zakładach karnych, co ostatecznie przynosi korzyści zarówno więźniom, jak i całemu społeczeństwu. Patrząc pod względem finansowym koszty utrzymanie skazanego w SDE jest znacznie tańsze niż jego pobyt w więzieniu. Według statystyk

miesięcznie wykonywanie kary z bransoletą kosztuje obecnie 818 zł, za kratami 4 tys. 175 zł.³⁶ Mimo że system dozoru elektronicznego stanowi nowoczesne i efektywne narzędzie resocjalizacyjne to wyróżnić można wady, jakimi będzie konieczność przestrzegania przez danego członka rodziny określonego planu dnia, godziny policyjnej, czy nawet całkowitego domowego aresztu – co wiązać się może z pewną dolegliwością dla członków rodziny³⁷. Ponadto system ten nie jest rozwiązaniem dostępnym dla wszystkich skazanych. Jego zastosowanie ograniczone jest przepisami prawa i określonymi kryteriami, które muszą zostać spełnione, aby osoba skazana mogła korzystać z tej formy odbywania kary. SDE przeznaczony jest głównie dla skazanych za przestępstwa o mniejszej szkodliwości społecznej, np. za drobne przestępstwa przeciwko mieniu, drobne przestępstwa gospodarcze, czy przestępstwa wynikające z zaniedbań. Skazani za przestępstwa o charakterze przemocy, przestępstwa seksualne czy osoby wielokrotnie skazywane, w większości przypadków, nie kwalifikują się do korzystania z dozoru elektronicznego. Dodatkowo określone są pewne warunki jak np. samodyscyplina i współpraca ze strony skazanego. Jeśli skazany nie jest chętny do przestrzegania zasad, może próbować manipulować systemem lub szukać sposobów na jego obejście, co znacznie osłabia efektywność dozoru elektronicznego.

³⁶ <https://samorząd.infor.pl/sektor/zadania/bezpieczenstwo/5649743,system-dozoru-elektronicznego-2023-r-sde.html> [dostęp: 4.10.2024 r.].

³⁷ K. Dyl, G. Janicki, *Dozór elektroniczny*, „Zeszyty Prawnicze UKSW” 2005, nr 52, s. 203.

Nadzór nad skazanymi oparty jest w szczególności na technologii GPS i połączeniach sieciowych, które wymagają stabilnego zasięgu sieci, a w miejscach o ograniczonym dostępie do infrastruktury telekomunikacyjnej skuteczność systemu może być znacznie zmniejszona. Problemy z zasięgiem GPS mogą prowadzić do chwilowej utraty kontroli nad skazanym, a w skrajnych przypadkach uniemożliwić monitorowanie jego zachowania. Dodatkowo awarie techniczne, przerwy w dostawie energii czy problemy z serwisem urządzeń mogą również wpłynąć na funkcjonowanie systemu. Choć tego typu problemy są coraz rzadsze, nadal istnieje zależność od stabilnych warunków technologicznych.

Podsumowanie

W dobie rozwoju technologii, stwierdzić można, że system dozoru elektronicznego to znaczące ulepszenie dla społeczeństwa przestępczego. Istotną kwestią jest tutaj wzrost liczby przestępców, co stanowi przeludnienie w zakładach karnych, tak więc system elektroniczny jest wspaniałym rozwiązaniem, które ma na celu zapobiegania temu zjawisku. Jak wspomniano wyżej system ten skupia się w szczególności na elektronicznym monitoringu i nadzorze nad osobą wykonującą wyrok przy pomocy nadajnika umieszczonego na nodze oraz innych środków technicznych. Stanowi to ułatwienie dla więziennictwa, gdyż skazany poprzez samokontrolę skupia się na prawidłowym wykonaniu wyroku i zaprzestaniu popełnienia ponownego przestępstwa. Natomiast funkcjonariusze pracujący w zakładach karnych czy aresztach śledczych, bazując na czynnościach profilaktycznych, działaniach resocjalizacyjnych, a także zapewnianiu bezpieczeństwa i porządku starają się wzbudzić w skazanym wolę współpracy w ukształtowaniu prawidłowej postawy społecznej, co w środowisku zdemoralizowanym jest znacznie utrudnione. Już sam pobyt za murami więzienia ma charakter przymusu, niż dobrowolnego pobytu, ciągle dostosowywanie się do poleceń funkcjonariuszy, wszelkie obowiązki jak i ograniczenia ciężące na osadzonych mają negatywny wpływ na psychikę człowieka. Konsekwencje tych działań uwidaczniają się w szczególności kiedy dochodzi do zjawiska recydywy, wtedy można stwierdzić, że proces resocjalizacji okazał się nieskuteczny. Wymiar sprawiedliwości stosuje wobec osób objętych systemem dozoru elektronicznego pewien stopień zaufania, dzięki któremu wykonywanie kary odbywa się w warunkach wolnościowych, co daje socjalizację wtórną. Podkreślić tutaj należy, że skazany aktywnie uczestniczy w życiu społecznym, pracuje lub kontynuuje naukę, a przede wszystkim zachowuje ciągłość w utrzymywaniu kontaktu z rodziną. Warto zwrócić uwagę, że w elektronicznym systemie nie każdy skazany ma możliwość odbywać swój wyrok, co w pewnym

stopniu zapobiega rozwojowi przestępczości. Rodzaj popełnionego przestępstwa a także wyrok stanowią główną przesłankę do zezwolenia na wykonywanie kary w systemie dozoru elektronicznego. Tak więc większą szansę na odbycie kary będzie miał osadzony, skazany pierwszy raz np. za kradzież, niż osoba skazana kilkukrotnie za to samo przestępstwo lub za gwałt, przy założeniu, że rodzina osadzonego wyrazi zgodę oraz warunki mieszkaniowe będą spełniały normy do zamontowania urządzeń nadzorujących.

Kontrowersję może budzić przypadek, w którym osoba wykonująca karę za pomocą systemu dozoru elektronicznego dopuści się popełnienia ponownie przestępstwa. Wtedy procedura wyraźnie stanowi, że taka osoba powraca na teren zakładu karnego, co w konsekwencji skutkuje przerwaniem procesu socjalizacji. Aby temu zapobiec ważnym elementem jest podejmowanie nieustannej kontroli, a także analizy w celu ulepszania bieżących aspektów technicznych i systemowych. Wzmocnienie i wzrost efektywności funkcjonowania dozoru elektronicznego może skutkować bezpieczeństwem społeczeństwa, gdyż to właśnie za murami będą osadzeni ci, którzy stanowią zagrożenie.

Bibliografia

- Adamczyk M., *System dozoru elektronicznego w świetle zmian i nowelizacji*, „Horyzonty Bezpieczeństwa” 2016, nr 2 (1).
- Dyl K., Janicki G., *Dozór elektroniczny*, „Zeszyty Prawnicze UKSW” 2005, nr 52.
- Gerecka-Żołyńska, P. Karlik, M. Kusak, P. Wiliński, M. Zamroczyńska, [w:] *Prawo karne wykonawcze*, red. A. Gerecka-Żołyńska, Warszawa 2021.
- Gucwa-Porębska K., *Funkcjonowanie społeczne osadzonych w systemie dozoru elektronicznego uwarunkowania rodzinne i środowiskowe*, Wyd. „Difin”, Warszawa 2020.
- Kuzior P., *System dozoru elektronicznego jako alternatywa dla kary pozbawienia wolności*, „Systemy Wspomagania w Inżynierii Produkcji” 2017, t. 6, z. 5.
- Mamak K., *Funkcjonowanie dozoru elektronicznego w świetle badań aktowych*, „Czasopismo Prawa Karnego i Nauk Penalnych” 2014, nr 2.
- Nowacki Z., *Zastosowanie penitencjarne systemu dozoru elektronicznego w ocenie skazanych*, „Humanistyczne Zeszyty Naukowe – Prawa Człowieka” 2017, nr 1.
- Sarzała D., *Resocjalizacyjny wymiar dozoru elektronicznego jako nieizolacyjnego modelu wykonywania kary pozbawienia wolności*, „Lubelski Rocznik Pedagogiczny” 2016, nr 2.
- Sielicki D., *Elektroniczne monitorowanie przestępców – nowoczesna alternatywa pozbawienia wolności*, „Przegląd Więziennictwa Polskiego” 2005, nr 47-48.
- Stańdo-Kawecka B., *Dozór elektroniczny w systemie sankcji karnych w wybranych krajach europejskich*, „Państwo i Prawo” 2012, nr 5.
- Zamroczyńska M., [w:] *Prawo karne wykonawcze*, red. A. Gerecka-Żołyńska, Warszawa 2021.

Zgoliński I., *Dozór elektroniczny jako instrument polityki karnej. Wybrane uwagi na kanwie nowelizacji kodeksu karnego i kodeksu karnego wykonawczego*, „Studia Prawnicze KUL” 2015, nr 4 (64).

Akty prawne

Ustawa z dnia 6 czerwca 1997 r. – *Kodeks karny wykonawczy* Dz.U.2024.0.706.

Ustawa z dnia 6 czerwca 1997 r. – *Kodeks karny* (Dz.U. 1997 nr 88 poz. 553).

Ustawą z dnia 7 września 2007 r. o wykonywaniu kary pozbawienia wolności po za zakładem karnym w systemie dozoru elektronicznego, (Dz.U. 2007 nr 191 poz. 1366).

Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny wykonawczy*, Dz.U. 2023 poz. 127 (KKW).

Program modernizacji Służby Więziennej w latach 2022-2025 (Dz.U.2024.86).

Ustawa o zmianie ustawy – *Kodeks karny oraz ustawy – Kodeks karny wykonawczy*, Dz.U. 2016, poz. 42.

Ustawa o zmianie ustawy *kodeks karny oraz niektórych innych ustaw*, Dz.U. 2015, poz. 396.

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych Dz.U.2019.1781.

Strony internetowe

<https://samorząd.infor.pl/sektor/zadania/bezpieczenstwo/5649743,system-dozoru-elektronicznego-2023-r-sde.html> [dostęp: 04.10.2024 r.]

<https://slmadwokaci.pl/prawo-karne/dozor-elektroniczny/> [dostęp: 01.10.2024 r.]

<https://www.ebos.pl/arttykul/obraczka-obroza-elektroniczne-kajdanki-elektroniczny-dozor-skazanych.html> / [dostęp 01.07.2024 r.]

Multidyscyplinarna rola psów służbowych w kontekście działań antyterrorystycznych w wybranych służbach mundurowych

Kornelia BREJDAK¹

Akademia Wymiaru Sprawiedliwości

ORCID: 0009-0009-4091-8952

Streszczenie. Psy służbowe odgrywają kluczową rolę w operacjach antyterrorystycznych prowadzonych przez Policję, Straż Graniczną, Wojsko oraz Służbę Więzienną. Ich niezwykle umiejętności i szerokie zastosowanie sprawiają, że stanowią istotny element globalnych strategii bezpieczeństwa. Celem artykułu jest ukazanie jak istotnym elementem funkcjonowania wybranych służb mundurowych są psy i ich zastosowanie w kontekście przeciwdziałania terroryzmowi. Autorka analizuje wieloaspektową rolę psów służbowych w kontekście działań antyterrorystycznych, omawiając różnorodne aspekty ich pracy, szkolenia oraz skuteczności w różnych działaniach antyterrorystycznych. Porusza kwestie prewencji i zapobiegania, podkreślając, że psy służbowe pełnią ważną rolę prewencyjną, przyczyniając się do zwiększenia bezpieczeństwa publicznego. Metodologia badań obejmuje analizę źródeł, metodę indukcji i dedukcji oraz przegląd artykułów naukowych dotyczących badanej tematyki.

Słowa kluczowe: bezpieczeństwo, służby mundurowe, psy, terroryzm

Wstęp

W obecnych czasach rośnie znaczenie działań antyterrorystycznych, co ma bezpośredni związek z coraz większym globalnym zagrożeniem terroryzmem². Poza

¹ Mł. chor. Kornelia Brejda – absolwentka studiów I stopnia na kierunku penitencjarystyka. Obecnie studentka II stopnia w Akademii Wymiaru Sprawiedliwości. Funkcjonariuszka Służby Więziennej w stopniu młodszego chorążego. Aktywna członkini Koła Naukowego Bezpieczeństwa i Resocjalizacji AWS. Swoje zainteresowania badawcze opiera przede wszystkim na tematyce szeroko rozumianego bezpieczeństwa, służb mundurowych oraz przeciwdziałania terroryzmowi.

² T. Dongen, *Terrorist Threat Assessment 2019-2021*, International Centre for Counter-Terrorism, Hague 2020, s. 3-7.

tym powiększająca się liczba stref konfliktu na całym świecie zapewnia transnarodowym organizacjom terrorystycznym wiele frontów działania. Powstają coraz lepiej skoordynowane komórki terrorystyczne powiększające swoje możliwości atakowania społeczeństwa w nieprzewidywalny sposób³. Z tego powodu konieczne jest przeciwdziałanie tego typu zagrożeniom. Kluczową rolę pełnią tu służby mundurowe powołane w kontekście działań antyterrorystycznych. Wynika to również z tego, iż zagrożenie ze strony terrorystów na całym świecie jest bezprecedensowe, co pokazały przykłady ostatnich lat. Co więcej, obecne organizacje terrorystyczne, dzięki swoim wyrafinowanym modelom działania i finansowania, mają coraz większe możliwości ataków na ludność cywilną i infrastrukturę krytyczną⁴. Wszystko sprawia, że działania antyterrorystyczne są jednym z podstawowych elementów zapewniania bezpieczeństwa państwa i obywateli.

W kontekście wskazanego zagrożenia nie można pominąć roli psów służbowych jako kluczowego elementu działań zarówno operacyjnych, jak i prewencyjnych. Psy w działaniach antyterrorystycznych zapewniają nieocenioną pomoc w walce z terroryzmem, co wynika z ich zdolności do rozpoznawania każdej potencjalnie niebezpiecznej substancji posiadającej charakterystyczny zapach. Psy służbowe w wielu miejscach globu stanowią wyszkoloną i wyspecjalizowaną jednostkę wspierającą ludzi w prowadzeniu operacji antyterrorystycznych. Zwierzęta takie są starannie selekcjonowane i przechodzą rygorystyczne programy szkoleniowe, co pozwala na doskonalenie ich umiejętności wykrywania zagrożeń. Również przez to więź z ich przewodnikami, co pozwala osiągnąć optymalne wyniki w ramach takiej współpracy. Specjalistyczne szkolenia pozwalają na ukierunkowanie psiego instynktu na zadania związane z identyfikacją szerokiej gamy zagrożeń. Psy pracują z wyjątkową dokładnością i skutecznością, co daje wiele zalet, z czego najważniejszą jest poprawa skuteczności służb mundurowych. Z racji znaczenia, jak również aktualności tematu, za cel artykułu wybrano analizę multidyscyplinarnej roli psów służbowych w działaniach antyterrorystycznych różnych służb mundurowych.

Trudno jest negować znaczenie psów służbowych w działaniach antyterrorystycznych. Zwierzęta są wykorzystywane w takich operacjach, gdyż posiadają wyjątkowe możliwości węchowe⁵. Są one szkolone w wykrywaniu szerokiego wa-

³ K. Karolczak, *Finansowanie terroryzmu – zarys problematyki*, „Terroryzm – studia, analizy, prewencja” 2022, nr 2(2), s. 129.

⁴ Tamże, s. 130.

⁵ T. Jezierski, *Zmysł węchu psów i jego praktyczne wykorzystanie*, „Prace i Materiały Zootechniczne. Monografie i Rozprawy” 2008, nr 20, s. 12.

chlarza substancji niebezpiecznych i nielegalnych, do czego zalicza się materiały wybuchowe, narkotyki czy broń palną⁶. Z tego względu docenia się ich wszechstronność w operacjach antyterrorystycznych, którą trudno uzyskać przez jakiegokolwiek urządzenie. Psy są wykorzystywane w takich celach, ponieważ posiadają zdolność adaptacji, a także cechuje je wysoka mobilność. Jednostki psów mogą być stosowane do tropienia i wielu innych działań w zróżnicowanych środowiskach. Przez rygorystyczne programy szkoleniowe rośnie również siła więzi łącząca zwierzęta ze swoimi przewodnikami, czego efektem jest wyjątkowa skuteczność w wykonywaniu zadań poprzez pracę zespołową.

Istnieje wiele obszarów zastosowania psów w działaniach antyterrorystycznych, co przekłada się na multidyscyplinarne podejście w ich szkoleniu oraz wykorzystywaniu. Zastosowania psów są mnogie, do czego należy zaliczyć przede wszystkim kontrolę bezpieczeństwa w celu wykrycia materiałów wybuchowych. Odbyna się to nie tylko na lotniskach, ale również we wszelkich budynkach użyteczności publicznej, gdzie bezpieczeństwo jest kluczowe. Ich zadaniem bywa także zabezpieczanie krytycznej infrastruktury, jak również budynków rządowych⁷. Poza tym psy pełnią rolę w wykrywaniu przemytu, do czego zaliczyć należy narkotyki oraz inne substancje. Można je dostrzec podczas imprez masowych, gdzie odpowiadają za bezpieczeństwo uczestników. Są wykorzystywane w trakcie patrolowania granicy, będąc nieocenione ponadto w operacjach poszukiwawczych. W wielu miejscach zapewniają wsparcie dla służb mundurowych, gdyż potrafią działać w różnych warunkach środowiskowych. Warto dokonać przedstawienia roli psów służbowych w odmiennych formacjach, co wskaże na zastosowanie, specyfikę szkolenia oraz przykłady konkretnych operacji.

Rola psów służbowych w Policji

Psy są wykorzystywane przez jednostki policyjne we wszystkich krajach świata, co ma związek z przedstawionymi już cechami tych zwierząt. Ich doskonale rozwinięty zmysł węchu jest wykorzystywany szczególnie w tropieniu oraz patrolowaniu. Poza tym psy znajdują zastosowanie w operacjach antyterrorystycznych, gdzie są odpowiedzialne za wykrywanie materiałów wybuchowych, jak również biorą udział w pościgach za terrorystami⁸.

⁶ P. Toczyński, *Wykorzystanie psów w działaniach zarządzania kryzysowego*, „Studia Bezpieczeństwa Narodowego” 2022, z. 26, s. 77-78.

⁷ Tamże, s. 79.

⁸ M. Gąsiorowski, *Use of Police Dogs in the Polish Police in the Opinion of Dog Handlers*, „Internal Security” 2019, vol. 11(1), s. 161-162.

Owczarek niemiecki to rasa, która jest najpopularniejsza, ale w służbie spotyka się również labradory, dobermany oraz rottweilery. Polska Policja stosuje takie zwierzęta w działaniach antyterrorystycznych, do czego zalicza się przede wszystkim tropienie, ale również wyszukiwania materiałów wybuchowych⁹. Jednak zwykle psy towarzyszą funkcjonariuszom w działaniach operacyjno-śledczych, gdzie biorą udział w poszukiwaniu narkotyków, zwłok ludzkich czy identyfikowaniu śladów zapachowych ludzi. Policja wraz z innymi służbami bierze udział w działaniach z zakresu ratownictwa, gdzie psy również pokazują swoje zalety. Zwierzęta te mogą być także używane w charakterze środków przymusu bezpośredniego. W kontekście działań antyterrorystycznych psy są angażowane do zapewniania bezpieczeństwa w obiektach chronionych, jak również do udaremnienia ucieczki i zatrzymania podejrzanych o próby jego naruszenia¹⁰.

Specyfika szkolenia psów policyjnych odnosi się do konkretnych wymagań, które muszą być spełnione przez takie zwierzęta. Psy trafiają do służby w wieku około jednego roku do maksymalnie dwóch lat, a ich dobór ma miejsce w oparciu o cechy fizyczne i behawioralne. Zwierzęta muszą być odporne, czujne, ale także nie lękliwe. Sprawdzany jest także instynkt aportowania, jaki ma znaczenie dla jakości tropienia. Z racji konieczności obrony przewodnika muszą także wykazywać pewien poziom agresji. Gdy spełniają te cechy, a także gdy weterynarz stwierdzi dobry stan zdrowia, trafiają one do Zakładu Kynologii Policyjnej w Sułkowicach. W tym miejscu szkoli się policyjne zwierzęta, w czym bierze udział przewodnik każdego z nich. Ma miejsce kontrola weterynaryjna, jak także ta prowadzona przez instruktorów, jacy weryfikują posiadane cechy. Pies przez to może być kierowany do danej specjalizacji, gdzie przez pół roku będzie poddawany szkoleniu. Warto zauważyć, że tylko część zajęć odbywa się we wspomnianym zakładzie, gdyż zwierzę musi umieć zachowywać się w naturalnych warunkach służby. Dlatego też psy i ich przewodnicy szkolą się także poza terenem jednostki. Pozwala to na adaptację do wielu elementów otoczenia, jak ruch uliczny, duże zagęszczenie ludzi czy praca w nocy. W procesie szkolenia stale ma miejsce weryfikacja umiejętności. Przez to można upewnić się, że względem psów policyjnych podejmowane są skutecznie działania. Po ukończeniu szkolenia zwierzęta otrzymują ważny przez rok atest¹¹. Co rok ma miejsce egzamin przed komisją, który pozwala go przedłużyć na kolejny rok, co gwarantuje, że pies nadaje się do służby i spełnia swoje zadanie. Z przykładów konkretnych operacji, w których psy odegrały kluczową rolę można

⁹ U. Charytonik, *Psy policyjne*, „Mój Pies” 2000, nr 9, s. 15-17.

¹⁰ J. Kuźniewicz, *Psy pracujące w służbach mundurowych*, Usługi Poligraficzne Bogdan Kokot, Nowa Ruda 2016, s. 51.

¹¹ A. Przybylik, *Psy w służbie Policji*, „Kwartalnik Policyjny” 2016, nr 3, s. 2-3.

zaliczyć dwa niedawne zdarzenia z 2024 roku¹². Pies z legnickiej komendy, dzięki swoim umiejętnościom tropiącym, pomógł w odnalezieniu zaginionej kobiety. Innym przykładem z tego roku jest sukces dzierzoniowskich policjantów, jakim było zabezpieczenie kilkuset porcji amfetaminy, wskazanych przez psa prowadzonego przez przewodnika.

Rola psów służbowych w Straży Granicznej

Rola psów służbowych w Straży Granicznej jest równie znacząca, co w uprzednio opisanej formacji mundurowej. Straż wykorzystuje psy do wykrywania nielegalnego przemytu broni, materiałów wybuchowych i substancji niebezpiecznych¹³. Poza tym mają one znaczenie w ochronie granic, dlatego też towarzyszą funkcjonariuszom w ich patrolach. Psy biorą udział w pościgach i zatrzymaniach osób nielegalnie przekraczających granice. Z racji tego, iż Straż Graniczna pełni istotną rolę w zabezpieczaniu granic państwa, wykorzystanie psów ma tu bardzo duży potencjał. Psy ze Straży Granicznej najczęściej odznaczają się nieocenioną pomocą w wykrywaniu narkotyków czy wyrobów tytoniowych. Ich doskonały węch jest niezastąpiony w takich zadaniach, co pozwala znacząco poprawić skuteczność działania służby. W 2024 roku w Straży Granicznej służbę pełniło ponad dwieście pięćdziesiąt czworonogów posiadających różnorodne specjalności¹⁴. Takie psy służbowe przeznaczone są głównie do wyszukiwania nielegalnych substancji, jak narkotyki, broń palna oraz materiały wybuchowe. Poza tym są stosowane w działaniach patrolowo-obronnych, jak również tropiąco-patrolowych¹⁵. W polskiej Straży Granicznej najpowszechniejsze są owczarki niemieckie i belgijskie. Ich służba ma duże znaczenie szczególnie na wschodniej granicy kraju, jaka stanowi poza tym wschodnią granicę Unii Europejskiej¹⁶.

Za szkolenie i specjalizację psów w tej formacji mundurowej odpowiada Ośrodek Szkoleń Specjalistycznych Straży Granicznej w Lubaniu. W nim ma miejsce

¹² Ponad tysiąc czworonożnych funkcjonariuszy wspiera pracę służb MSWiA, <https://www.gov.pl/web/mswia/ponad-tysiac-czworonożnych-funkcjonariuszy-wspiera-prace-sluzb-mswia> [dostęp: 23.09.2024 r.].

¹³ A. Szen, *Psy w służbie Straży Granicznej*, [w:] *Straż Graniczna RP w systemie ochrony granicy państwowej*, M. Laskowski (red.), Akademia Sztuki Wojennej, Warszawa 2020, s. 166-167.

¹⁴ *Psy służbowe w Straży Granicznej*, <https://www.strazgraniczna.pl/pl/aktualnosci/10329,Psy-sluzbowe-w-Strazy-Granicznej-DzienPsa.html> [dostęp: 23.09.2024 r.].

¹⁵ Rozdział 14, Ustawy z dnia 12 października 1990 r. o Straży Granicznej (Dz.U.2024.915).

¹⁶ I. Szkudlarek, *Polityka zagraniczna Białorusi w aspekcie bezpieczeństwa granic RP* [w:] L. Elak (red. nauk.), *Ochrona granicy państwowej. Wybrane aspekty*, Akademia Sztuki Wojennej, Warszawa 2017, s. 42-54.

kontrola zwierząt przez pracowników z Zakładu Kynologii, w skład których wchodzi lekarze weterynarii, instruktorzy oraz wykładowcy. Pierwszym krokiem jest ocena stanu zdrowia zwierząt, jak także ich cech oraz predyspozycji psychicznych i fizycznych. Psy trafiają na szkolenia w wieku około jednego roku do maksymalnie dwóch lat. Funkcjonariusze Straży Granicznej biorą czynny udział w zakupie psów, gdyż później pełnią oni rolę ich przewodników. Zatem możliwy jest samodzielny wybór zwierzęcia, co ma duże znaczenie dla szybkiego nawiązania więzi między nim a człowiekiem. Co więcej, pies taki będzie przyszłym partnerem na służbie, co ma również znaczenie emocjonalne dla funkcjonariusza. Szkolenie ma za zadanie wypracować u psa umiejętności mające związek z konkretnymi specjalizacjami. Dlatego pies z przewodnikiem uczony jest poszukiwania określonych substancji i przedmiotów, jak również właściwej reakcji na odkryty trop. W trakcie półrocznego szkolenia w lubańskim ośrodku pies wraz ze swoim przewodnikiem przygotowuje się do służby w Straży Granicznej. Ma ono również za zadanie poprawić komunikację pomiędzy człowiekiem a psem, z czego wynikać będzie lepsza więź, wzrośnie także wzajemne zaufanie. Szkolenie polega poza tym na tresurze, tak, by pies był całkowicie posłuszny. Ma to duże znaczenie dla bezpieczeństwa, ale także dla wydajności stosowania psów w Straży Granicznej. Zwierzę uczy się zasad zachowania, a jego przewodnik zasad wykorzystania psa w służbie. Poprzez ćwiczenia terenowe może mieć miejsce symulowanie warunków podczas patrolu granicznego. Co więcej, poznane podstawy weterynarii pomagają lepiej dbać przewodnikom o ich psy. Ma to znaczenie nie tylko w kontekście pierwszej pomocy, ale także odczytywania zachowania zwierzęcia i właściwej reakcji. Do przykładów udanych operacji antyterrorystycznych z udziałem psów na granicach kraju należy zaliczyć między innymi udaremnienie przewozu przez granicę broni palnej oraz amunicji, co miało miejsce na początku 2024 roku. Z kolei w 2023 roku psy służbowe Straży Granicznej przyczyniły się do zabezpieczenia ponad stu kilogramów narkotyków, będących przedmiotem przemytu przez granice Polski¹⁷.

Rola psów służbowych w Wojsku Polskim

W Wojsku Polskim psy również znajdują zastosowanie, gdyż ponad sto zwierząt obecnych jest w wojskach lądowych, wojskach obrony terytorialnej oraz wojskach specjalnych. Co więcej, pełnią one służbę również w Żandarmerii Wojsko-

¹⁷ *Ponad tysiąc czworonożnych funkcjonariuszy wspiera pracę służb MSWiA*, <https://www.gov.pl/web/mswia/ponad-tysiac-czworonoznich-funkcjonariuszy-wspiera-prace-sluzb-mswia> [dostęp: 23.09.2024 r.].

wej, wspierając żołnierzy w zadaniach z zakresu ochrony porządku publicznego na terenach i obiektach jednostek wojskowych. Wiele psów uczestniczy w operacjach militarnych, gdzie ma miejsce rozminowywanie czy też wykrywanie wrogów w trudno dostępnych terenach. Wszędzie, gdzie znaczenie ma węch psa, wojsko korzysta z wysoce rozwiniętych zmysłów tychże zwierząt. W Wojsku Polskim czworonogi szkolone są do wykrywania materiałów wybuchowych, ale także do poszukiwania ludzi, co ma duże znaczenie w przypadku osób zaginionych w trakcie walki. Ich tradycyjną rolą jest stróżowanie i patrolowanie. W tej formacji mundurowej zwierzęta szkoli się w Wojskowym Ośrodku Farmacji i Techniki Medycznej w Celestynowie. Młode psy trafiają tu na kilkumiesięczne szkolenia, ale uprzednio muszą przejść wymagające testy, by mogły być na nie zakwalifikowane¹⁸. Wszystkie psy przechodzą ocenę szkoleniową, aby upewnić się, że mają odpowiedni temperament i bystrość. Stosowanie nagród przyspiesza szkolenie i koncentruje się na krytycznych elementach, dzięki czemu psy dokładnie wiedzą, za co są nagradzane.

Szkolenie psów opiera się na pozytywnej nagrodzie lub informacji zwrotnej. Obejmuje ono wykorzystanie naturalnych instynktów psów, szczególnie aby nauczyć je wykrywania zapachów¹⁹. Ma to kluczowe znaczenie wśród psów, których specjalizacją jest wykrywanie min. Dzięki temu zwierzęta w wojsku są w stanie wspierać żołnierzy w oczyszczaniu terenu, wyznaczaniu granic pól minowych i przeszukiwaniu części lądu, do którego nie można dotrzeć za pomocą mechanicznych urządzeń oczyszczających. Z racji tego, że Wojsko Polskie ma obowiązek chronić państwo i obywateli przed zagrożeniami ze strony terroryzmu, jego specjalne jednostki z psami pełnią istotną rolę w działaniach antyterrorystycznych²⁰. Należy zaliczyć do tego przede wszystkim wykrywanie materiałów wybuchowych, gdzie psi węch jest nieoceniony w eliminowaniu takich zagrożeń w obrębie infrastruktury krytycznej oraz ważnych strategicznie obiektów. Poza tym psy są szkolone do prowadzenia rekonesansu przed podjęciem działań bojowych. Zwierzęta wyposażone w kamerę potrafią zapewnić cenne informacje dla dowodzących, zwiększając bezpieczeństwo działań dla żołnierzy. Przykładem operacji wojskowych z udziałem psów była interwencja Wojska Polskiego w Iraku (a dokładnie Jednostki Wojskowej Komandosów), gdzie były niezawodne w wykrywaniu materiałów

¹⁸ Instrukcja o gospodarce psami służbowymi w siłach zbrojnych RP, Załącznik do decyzji Nr 623/MON Ministra Obrony Narodowej z dnia 27 grudnia 2007 r. (Syg. Zdr. Nr 243/2007 r.).

¹⁹ D. Lefebvre et al., *The quality of the relation between handler and military dogs influences efficiency and welfare of dogs*, „Appl. Anim. Behav. Sci.” 2007, vol. 104 (1-2), s. 49-50.

²⁰ Zob. I. Szkudlarek, *Kobiety Obronność Bezpieczeństwo. Aspiracje oficerów-kobiet a doskonalenie zawodowe żołnierzy*, Wyd. Naukowe Kontekst, Poznań 2025, wyd. II, s. 70.

wybuchowych²¹. Zwierzęta brały udział w desancie ze śmigłowców, a także wykonywały skoki spadochronowe z przewodnikami.

Rola psów służbowych w Służbie Więziennej

Rola psów służbowych w Służbie Więziennej jest również znacząca, gdyż wykorzystywane są one do szukania nielegalnych substancji, jak także ochrony zakładów karnych i aresztów śledczych. W polskiej Służbie Więziennej jest nieco ponad sto psów o różnych specjalnościach, w tym patrolowo-obronnych²². Formacja ta polega na zwierzętach w szukaniu narkotyków i substancji niedozwolonych, gdzie najczęściej spotyka się rasy jak owczarek niemiecki lub foksterier. Wśród psów patrolowo-obronnych powszechna jest także rasa rottweiler. Wykorzystanie psów do monitorowania i zapobiegania aktom terrorystycznym w zakładach penitencjarnych jest mniej powszechne, ale zawsze, gdy pies wyczuje podejrzany przedmiot, mają miejsce wymagane kontrole. Szkolenie psów do zadań w więzieniach jest zbliżone do pozostałych służb, jeśli chodzi o wymagania wiekowe. Są to zatem psy w wieku od jednego roku do dwóch lat. Muszą być w pełni zdrowe oraz posiadać dobrą kondycję i wymagane cechy. Kwalifikacja zwierząt odbywa się w Dziale Szkolenia Przewodników i Tresury Psów Służbowych z Zakładu Karnego w Czarinem²³. Lekarz weterynarii bada wzrok i słuch czworonoga, a także jego reakcje na pewne silne bodźce, jak na przykład wystrzał z broni palnej. W czasie dwunastu tygodni szkolenia psa patrolowo-obronnego poznaje on specyfikę warunków służby, a jego przewodnik stara się nawiązać z nim silną więź. Szkolenie obejmuje pokonywanie torów przeszkód, jak również pościgi za zbiegami²⁴. Wykształca się wtedy współpraca, a zwierzę doskonali się w obronie i ataku. Szkolenie specjalistyczne psów jest wydłużone, ponieważ zwierzęta te muszą potrafić rozpoznawać zapachy narkotyków i substancji zabronionych. Jest to kluczowe w trakcie częstego kontrolowania paczek trafiających do więzień. Po ukończeniu całości szkoleń psy kierowane są do służby w zakładach karnych i aresztach śledczych. Przykłady działań prewencyjnych w zakładach karnych z udziałem psów to przede wszystkim wykrywanie wszelkiego typu kontrabandy, jaką zwierzę jest w stanie wyczuć. Poza tym są one bardzo przydatne w kontroli paczek wysyłanych do osadzonych.

²¹ *Komandosi szkolą psy bojowe w Iraku*, <https://polska-zbrojna.pl/home/articleshow/4136?t=Komandosi-szkola-psy-bojowe-w-Iraku> [data dostępu: 23.09.2024 r.].

²² *Psy w służbie*, <https://www.sw.gov.pl/galeria/psy-w-sluzbie> [data dostępu: 23.09.2024 r.].

²³ Tamże.

²⁴ K. Lubryczyński, *Tresura psów służbowych*, Centrum Szkolenia Policji, Legionowo 2016, s. 32.

Przegląd i refleksja

Przedstawione przykłady roli psów służbowych w kontekście działań antyterrorystycznych w wybranych służbach mundurowych przesądzą o jej multidyscyplinarności. Zwierzęta te pełnią liczne funkcje o uniwersalnym charakterze w każdej z nich, ale różni je nieco specyfika obowiązków. Dlatego też proces szkolenia psów służbowych musi brać pod uwagę potrzeby danej służby, również w obliczu specyfiki zadań. Porównanie różnych podejść szkoleniowych pozwala stwierdzić, że bazują one na pozytywnym wzmocnieniu. Tak określa się wszelkie działanie powodujące, że dana reakcja czy też zachowanie będzie miało większą szansę pojawić się w przyszłości częściej, niż obecnie²⁵. Zatem osoby szkolące psy służbowe nagradzają zwierzę zawsze wtedy, gdy wykonuje odpowiednio dane zadanie. Ma to na celu nauczyć, że takie zachowanie jest pożądane, czego skutkiem jest nagroda, w formie pochwały, smakołyku lub zabawki²⁶. Jest to element łączący wszystkie służby, jeśli chodzi o szkolenie psów. Różnice pojawiają się jednak, gdy weźmie się pod uwagę wymagania każdej z nich. Podczas, gdy psy policyjne szkolone są często do wykrywania narkotyków, to te wojskowe mogą mieć za zadanie branie udziału w działaniach rekonesansu. Podobnie psy na służbie w Straży Granicznej będą szkolone głównie dla celów obronnych i tropiących, gdzie te z Służby Więziennej służą wsparciem w poszukiwaniu kontrabandy. W kontekście działań antyterrorystycznych ma miejsce współpraca między służbami w kontekście szkolenia. Wymieniane są doświadczenia wśród polskich służb, co pozwala lepiej prowadzić działania szkolące dla zwierząt.

Także same metody szkolenia uległy zmianie w ostatnich latach. Odchodzi się od metod awersyjnych, jakie oznaczają szkolenie tradycyjne z użyciem kar. Można mówić, że takie podejście to zwykła tresura, jaka ma wzbudzać lęk u psa²⁷. Poleganie na źródle strachu jest jednak nieskuteczne, gdyż jego brak sprawi, że zwierzę nie zachowa się we właściwy sposób. Dlatego też trening awersyjny jest nieefektywny, chociaż może pozornie przynosić bardzo szybki efekt. Metody tradycyjne w ramach szkolenia psów służbowych polegały na nieaktualnej teorii dominacji²⁸.

²⁵ S. Yin et al., *Efficacy of a Remote-Controlled, Positive-Reinforcement, Dog-Training System for Modifying Problem Behaviors Exhibited When People Arrive at the Door*, "Applied Animal Behaviour Science" 2008, vol. 113(1), s. 123-124.

²⁶ I. Rozempolska-Rucińska, *Trening psa z użyciem wzmocnień środowiskowych i socjalnych*, „Animal Expert” 2017, nr 1, s. 35.

²⁷ E. Hiby, *Dog training methods: their use, effectiveness and interaction with behaviour and welfare*, "Anim. Welf." 2004, vol. 13, s. 65.

²⁸ M. Patan, *Znaczenie eksperymentów badających procesy poznawcze dla współcześnie stosowanych technik modyfikacji zachowania psów domowych*, [w:] *Środowisko przyrodnicze jako obszar badań*, Bogucki Wyd. Naukowe, Poznań 2023, s. 76.

W jej ramach przyjmuje się, że ma miejsce hierarchiczne ułożenie struktury stada. Nie jest to prawdą, gdyż pies reagując agresywnie względem swojego pana nie stara się odwrócić hierarchii, a raczej eksponuje swoje niezadowolenie. Dlatego szkolenie psów służbowych, ale również cywilnych, bazuje coraz powszechniej na skutecznej metodzie pozytywnego wzmocnienia. Szkolenie tego typu, potwierdzone przez wiele badań, daje wysokie tempo nauki i trwałość przyswajanej wiedzy²⁹. Bazuje ono na prostym mechanizmie, gdzie zwierzę wykonuje polecenie w zamian za nagrodę. Jej otrzymanie zwiększa szansę, że zachowanie się powtórzy. Zatem pies w prosty dla niego sposób jest informowany co ma robić, gdyż skutek będzie dla niego przyjemny. W ramach tej metody stosuje się również wygaszenie negatywne, a zatem zabranie ewentualnej nagrody. Choć może to na pierwszy rzut oka przypominać szkolenie awersyjne, to rolę kary pełni tylko brak nagrody. Zatem usuwa się poniekąd źródło strachu, jakie nie jest skuteczną formą uczenia czworonoga. Warto zauważyć, że dzięki takiemu pozytywnemu wzmocnieniu wykształca się lepsza więź między psem i przewodnikiem, co ma duże znaczenie w wykonywaniu działań wielu służb, także w kontekście bezpieczeństwa.

Szkolenia psów do operacji antyterrorystycznych w zależności od rodzaju służb pozwalają na wykazywanie wysokiej skuteczności. Pierwszym i stosunkowo tradycyjnym zadaniem było od lat wyszukiwanie zapachów materiałów wybuchowych, co pozwalało na zapobieżenie ich użyciu. Stale zwierzęta te są w stanie wykryć takie substancje, podobnie jak amunicję i broń palną, co daje służbom dużą przewagę w działaniach antyterrorystycznych. Jednak dziś na znaczeniu zyskuje również działalność patrolowo-tropiąca, jaka pozwala na odnajdywanie osób podejrzanych o terroryzm³⁰. Psy są szkolone w tropieniu śladów, co poprawia skuteczność działań operacyjnych wielu rodzajów służb. Przyszłość roli psów w działaniach antyterrorystycznych z pewnością będzie obfitowała w konieczność dostosowania się programów szkoleniowych do nowych wyzwań. Zawsze jednak psy służbowe będą musiały wykazywać się ponadprzeciętnymi cechami, jak również sprostać mnogim wymaganiom fizycznym i behawioralnym.

Podsumowanie

Podsumowując przedstawione w artykule zagadnienia, należy podkreślić rolę psów służbowych w działaniach antyterrorystycznych. Spełniają one poza tym

²⁹ S. Lindsay, *Handbook of Applied Dog Behavior and Training*, Iowa State University Press, Ames 2000, s. 201-202.

³⁰ P. Toczyński, *Wykorzystanie psów w działaniach...*, dz. cyt., s. 81.

liczne zadania w ramach pozostałych, równie ważnych obowiązków każdej z wymienionych służb. Ich rola jest bez wątpienia multidyscyplinarna, gdyż wykorzystywane są one do wykrywania materiałów wybuchowych, wyszukiwania nielegalnych substancji, tropienia oraz patrolowania. Pełnią również funkcje obronne, co ma miejsce nie tylko w Straży Granicznej i Policji, ale również w Służbie Więziennej. Obecnie rośnie znaczenie rozwoju oraz doskonalenia metod szkolenia i współpracy między służbami³¹. Metody coraz powszechniej czerpią z pozytywnego wzmocnienia, co nie tylko oszczędza często wątpliwych etycznie kar, ale również wykształca lepszą więź między psem i przewodnikiem³². Przede wszystkim jednak skutecznie utrwala przekazywane w trakcie szkolenia umiejętności u czworonoga. Należy podkreślić znaczenie współpracy między służbami mundurowymi oraz znaczenie badań naukowych w tym obszarze. Pierwsze doprowadzi do poprawy w sferze działania antyterrorystycznego, z kolei drugie może dać cenne wnioski dla dalszego usprawniania procesu szkolenia.

Bibliografia

- Charytonik U., *Psy policyjne*, „Mój Pies” 2000, nr 9.
- Dongen T., *Terrorist Threat Assessment 2019-2021*, International Centre for Counter-Terrorism, Hague 2020.
- Gąsiorowski M., *Use of Police Dogs in the Polish Police in the Opinion of Dog Handlers*, „Internal Security” 2019, vol. 11(1).
- Hiby E., *Dog training methods: their use, effectiveness and interaction with behaviour and welfare*, „Anim. Welf.” 2004, vol. 13.
- Instrukcja o gospodarce psami służbowymi w siłach zbrojnych RP, Załącznik do decyzji Nr 623/MON Ministra Obrony Narodowej z dnia 27 grudnia 2007 r., Syg. Zdr. Nr 243/2007 r.
- Jezierski T., *Zmysł węchu psów i jego praktyczne wykorzystanie*, „Prace i Materiały Zootechniczne. Monografie i Rozprawy” 2008, nr 20.
- Karolczak K., *Finansowanie terroryzmu – zarys problematyki*, „Terroryzm – studia, analizy, prewencja” 2022, nr 2(2).
- Komandosi szkolą psy bojowe w Iraku*, <https://polska-zbrojna.pl/home/articleshow/41136?t=Komandosi-szkola-psy-bojowe-w-Iraku> [dostęp: 23.09.2024r.].
- Kuźniewicz J., *Psy pracujące w służbach mundurowych*, Usługi Poligraficzne Bogdan Kokot, Nowa Ruda 2016.
- Lefebvre D. et al., *The quality of the relation between handler and military dogs influences efficiency and welfare of dogs*, „Appl. Anim. Behav. Sci.” 2007, vol. 104 (1-2).

³¹ I. Szkudlarek, *Kobiety Obronność Bezpieczeństwo...*, dz. cyt., s. 116.

³² S. Yin et al., *Efficacy of a Remote-Controlled...*, dz. cyt., s. 126.

- Lindsay S., *Handbook of Applied Dog Behavior and Training*, Iowa State University Press, Ames 2000.
- Lubryczyński K., *Tresura psów służbowych*, Centrum Szkolenia Policji, Legionowo 2016.
- Patan M., *Znaczenie eksperymentów badających procesy poznawcze dla współcześnie stosowanych technik modyfikacji zachowania psów domowych*, [w:] *Środowisko przyrodnicze jako obszar badań*, Bogucki Wyd. Naukowe Poznań 2023.
- Ponad tysiąc czworonożnych funkcjonariuszy wspiera pracę służb MSWiA, <https://www.gov.pl/web/mswia/ponad-tysiac-czworonoznych-funkcjonariuszy-wspiera-prace-sluzb-mswia> [dostęp: 23.09.2024 r.].
- Przybylik A., *Psy w służbie Policji*, „Kwartalnik Policyjny” 2016, nr 3.
- Psy służbowe w Straży Granicznej*, <https://www.strazgraniczna.pl/pl/aktualno/sci/10329,Psy-sluzbowe-w-Strazy-Granicznej-DzienPsa.html> [dostęp: 23.09.2024 r.].
- Psy w służbie*, <https://www.sw.gov.pl/galeria/psy-w-sluzbie> [dostęp: 23.09.2024 r.].
- Rozempolska-Rucińska I., *Trening psa z użyciem wzmocnień środowiskowych i socjalnych*, „Animal Expert” 2017, nr 1.
- Szen A., *Psy w służbie Straży Granicznej*, [w:] *Straż Graniczna RP w systemie ochrony granicy państwowej*, M. Laskowski (red.), Akademia Sztuki Wojennej, Warszawa 2020.
- Szkudlarek I., *Polityka zagraniczna Białorusi w aspekcie bezpieczeństwa granic RP* [w:] Elak L. (red. nauk.), *Ochrona granicy państwowej. Wybrane aspekty*, Akademia Sztuki Wojennej, Warszawa 2017.
- Szkudlarek I., *Kobiety Obronność Bezpieczeństwo. Aspiracje oficerów-kobiet a doskonalenie zawodowe żołnierzy*, Wyd. Naukowe Kontekst, Poznań 2025, wyd. II.
- Toczyński P., *Wykorzystanie psów w działaniach zarządzania kryzysowego*, „Studia Bezpieczeństwa Narodowego” 2022, z. 26.
- Ustawa z dnia 12 października 1990 r. o Straży Granicznej, Dz.U. 2024.915 t.j.
- Yin S. et al., *Efficacy of a Remote-Controlled, Positive-Reinforcement, Dog-Training System for Modifying Problem Behaviors Exhibited When People Arrive at the Door*, „Applied Animal Behaviour Science” 2008, vol. 113(1).

Zasadność stosowania środków przymusu bezpośredniego przez funkcjonariuszy Służby Więziennej podczas konwojowania osób pozbawionych wolności

Tomasz STRYŻ¹

Akademia Wymiaru Sprawiedliwości

ORCID: 0009-0000-1364-070X

Streszczenie. Celem niniejszego artykułu jest próba wskazania słuszności w aspekcie stosowania dostępnych środków przymusu bezpośredniego przez uprawnionych czyli funkcjonariuszy Służby Więziennej podczas realizacji czynności służbowych związanych z konwojowaniem osób pozbawionych wolności. Autor niniejszego opracowania zastosował metodę opisową powiązaną z przedstawieniem w formie dopełnienia wyników przeprowadzonych badań.

Słowa kluczowe: Służba Więzienna, środki przymusu bezpośredniego, konwojowanie

Wstęp

W obliczu następujących zmian w wymiarze szerokiego spektrum środowisk, w którym funkcjonują ludzie, celem nadrzędnym wedle wszelkich hierarchii jest dbałość i zapewnienie odpowiedniego poziomu bezpieczeństwa. Jest ono niezbędne do realizacji niemalże każdego zamierzonego działania czy też przedsięwzięcia, bowiem gwarantuje stabilność a zarazem ciągłość pewnych procesów składających się na określony „produkt końcowy”. Zapewnienie bezpieczeństwa jest rolą w pewnej części każdego człowieka, jednak nadrzędną rolę o szerokim

¹ Ppor. mgr Tomasz Strzyż – oficer Służby Więziennej, absolwent studiów magisterskich na kierunku penitencjarystyka w Akademii Wymiaru Sprawiedliwości.

i kompleksowym wymiarze pełnią rozmaite służby, inspekcje i stráže wpisane ściśle w struktury systemu bezpieczeństwa wewnętrznego, którego zasadniczym celem jest zaspokajanie potrzeb państwa i obywateli w wymiarze porządku i bezpieczeństwa. Jednym z kluczowych podmiotów, odgrywającym znaczącą rolę w tym systemie jest Służba Więzienna, która wedle ustawowych obowiązków chroni społeczeństwo przed sprawcami przestępstw, izolując powyższe osoby i tym samym wykonując tymczasowe aresztowanie bądź kary pozbawienia wolności.

W toku prowadzonych działań i oddziaływań, funkcjonariusze Służby Więziennej pracują na terenie wyznaczonych jednostek organizacyjnych, które są usystematyzowane wg określonych zasad. Warto jednak zaznaczyć, iż służba funkcjonariuszy odbywa się również poza murami jednostek penitencjarnych, wtedy owe czynności noszą miano konwojowania bądź doprowadzania. Prowadząc określone procedurami zadania na rzecz zapewnienia bezpieczeństwa, funkcjonariusze wspomnianej formacji mają do dyspozycji wachlarz uprawnień oraz środków, które stymulują w sposób klarowny zamierzone działania przy jednoczesnym utrzymaniu odpowiedniego i wymaganego poziomu bezpieczeństwa.

Niniejszy artykuł poruszy w sposób kompleksowy kwestię środków przymusu bezpośredniego które są zadysponowane funkcjonariuszom Służby Więziennej do prowadzenia czynności służbowych w codziennym toku służby konwojowej. Ukazany zostanie katalog dostępnych środków wraz z krótką charakterystyką, która przybliży czytelnikom spektrum możliwości ich skutecznego i dozwolonego użycia bądź wykorzystania. Niezbędnym elementem stanie się również przedstawienie wykazu możliwych zagrożeń dla konwojowania, zaznaczający rolę i konieczność doposażenia funkcjonariuszy w omawiane środki przymusu bezpośredniego. Dopełnieniem rozważań autora będzie zamieszczenie wyników przeprowadzonych badań użytych przy okazji innej pracy naukowej, które ściśle są związane ze wskazanym tematem artykułu. Scalenie przedstawionych składników wedle zamierzeń ma dać odpowiedź na pytanie czy jest zasadnym stosowanie środków przymusu bezpośredniego podczas konwojowania osób pozbawionych wolności. Zgromadzona teoria na wskazane powyżej elementy i uzupełnienie jej skrupulatnymi badaniami w tym zakresie, w zamyśle autora powinna wskazać zależność a zarazem niezbędność w aspekcie obecności wspomnianych środków podczas realizacji charakteryzowanych czynności.

Służba Więzienna jako jeden z gwarantów w wymiarze bezpieczeństwa wewnętrznego – zakres podejmowanych działań i uprawnień

Nadrzędnym zadaniem, czy też celem dążenia każdej z formacji mundurowych jest należyta służba na rzecz społeczeństwa, która wyraża się poprzez pry-

zmat podejmowanych działań. W ujęciu bezpieczeństwa wewnętrznego, którego jednym z ogniw jest Służba Więzienna, celem jest zapewnienie równowagi i porządku wewnątrz państwa². Wspomniane przedsięwzięcia mają niejednokrotnie swoje umiejscowienie w wyznaczonych aktach prawnych, które zarówno regulują działalność podległych służb, jak i nadają im zgodne z przeznaczeniem i charakterystyką pracy uprawnienia. Poddana w tym opracowaniu refleksji umundurowana a zarazem apolityczna formacja mundurowa, jaką jest Służba Więzienna, na podstawie nałożonych na nią ustawowych obowiązków, ma również do dyspozycji szereg dostępnych uprawnień i możliwości³. Spoglądając z uwagą na zestawienie wyznaczonych zadań stojących przed funkcjonariuszami Służby Więziennej, pewnym jest, że podejmowanie tak zróżnicowanych i obarczonych odpowiedzialnością czynności wymaga określonych do wykorzystania uprawnień i środków. Na mocy ustawowych zapisów, Służba Więzienna w celu wypełniania nałożonych zadań, jest zdolna do użycia lub wykorzystania środków przymusu bezpośredniego⁴. Ustawodawca sprecyzował tryb postępowania i szeroki zakres zasad oraz przypadków postępowania ze wspomnianymi środkami, charakteryzując je w sposób szczegółowy w odrębnym akcie prawnym⁵.

Spektrum działań podejmowanych przez Służbę Więzienną obejmuje pracę penitencjarną z osobami pozbawionymi wolności, poddany określonej rozmieszczeniu i klasyfikacji m.in. wg typu i rodzaju zakładu karnego a także systemu odbywania kary⁶ oraz osobnych, bardziej zindywidualizowanych kryteriów klasyfikacyjnych⁷. Prowadzone oddziaływania penitencjarne wobec osadzonych cechują się różnorodnością, dynamiką i nieprzewidywalnością. Wielokrotnie są dokonywane zmiany w osadzeniu skazanych co wiąże się nade często ze zmianą jednostki z racji występujących zaleceń. Reasumując, czynności służbowe funkcjonariuszy są podejmowane zarówno w obrębie zakładu karnego czy aresztu śledczego, jak również poza nim w przypadku opisanym powyżej. Wspomniane działania noszą miano konwojowania czyli przetransportowania osób pozbawionych wolności na określonych zasadach do docelowego miejsca pobytu. Podana powyżej definicja jednego z większych przedsięwzięć podejmowanych w sposób ciągły, zaznacza klarownie, że podczas charakteryzowanych czynności, jest dopuszczalne użycie lub wykorzystanie środków przymusu bezpośredniego. To

² J. Gryz, *Zarys teorii bezpieczeństwa państwa*, AON, Warszawa 2016, s. 142.

³ Art.1 ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej, Dz.U. z 2020 r., poz. 848.

⁴ Art.19 pkt 1 ustawy z dnia 9 kwietnia 2010 r. o Służbie Więziennej, Dz.U. z 2020 r., poz. 848.

⁵ Autor ma w tym miejscu na myśli ustawę z dnia 24 maja 2013 r. o środkach przymusu i bezpośredniego i broni palnej (Dz.U. z 2020, poz. 848).

⁶ Art. 69, 70, 81 ustawy z dnia 6 czerwca 1997 r. Kodeks karny wykonawczy (Dz.U.2024.706).

⁷ Art. 82 §2 ustawy z dnia 6 czerwca 1997 r. Kodeks karny wykonawczy (Dz.U.2024.706).

utwierdza w przekonaniu, iż przytaczana jedna z „gałęzi” działalności Służby Więziennej pozwala na wykonywanie powierzonych zadań w sposób kompleksowy przy zastosowaniu wymaganych środków, które mają wpływ na poziom bezpieczeństwa.

Środki przymusu bezpośredniego w ujęciu proceduralnym – katalog, pojęcia, przypadki i zasady stosowania

Określone działania podejmowane przez podmioty oparte są zarówno na wyznaczonych normach i przepisach, ale również na skorelowaniu ww. elementów z dostępnym zapleczem sprzętu i infrastruktury. Biorąc pod uwagę znaczenie bezpieczeństwa w codziennych działaniach funkcjonariuszy Służby Więziennej, nie sposób pominąć aspektu obecności środków przymusu bezpośredniego jako jednego z atrybutów i narzędzi służących wykonywaniu w sposób rzetelny wydanych poleceń. Aby móc w pełni znać zaplecze wspomnianych „atrybutów” należy przedstawić dostępny ich katalog. Do zbioru środków przymusu bezpośredniego przeznaczonych do stosowania dla funkcjonariuszy zaliczamy:

- 1) *siłę fizyczną w postaci technik:*
 - a) *transportowych,*
 - b) *obrony,*
 - c) *ataku,*
 - d) *obezwładnienia;*
- 2) *kajdanki:*
 - a) *zakładane na ręce,*
 - b) *zakładane na nogi,*
 - c) *zespólone;*
- 3) *pas obezwładniający;*
- 4) *kask zabezpieczający;*
- 5) *pałkę służbową;*
- 6) *wodne środki obezwładniające;*
- 7) *psa służbowego;*
- 8) *pociski niepenetracyjne;*
- 9) *chemiczne środki obezwładniające w postaci:*
 - a) *ręcznych miotaczy substancji obezwładniających,*
 - b) *granatów łzawiących,*
 - c) *innych urządzeń przeznaczonych do miotania środków obezwładniających;*

- 10) *przedmioty przeznaczone do obezwładniania osób za pomocą energii elektrycznej;*
- 11) *celę zabezpieczającą⁸.*

Spoglądając na powyżej przedstawione elementy służące wzmocnieniu i utrzymywaniu poczucia bezpieczeństwa funkcjonariuszy, spostrzec można, iż występuje w nich pewna gradacja i zróżnicowanie, która ma swój zauważalny cel. Z pewnością rodzaj sytuacji, z jaką spotyka się uprawniony podczas konwojowania, kształtuje u niego konieczność jej oceny i zarazem zestawienia z opcjami zastosowania określonego środka. Wspomniane powyżej sytuacje to nic innego jak przypadki zastosowania omawianych „nośników bezpieczeństwa”; poniżej w tabeli są wyszczególnione sklasyfikowane przypadki użycia bądź wykorzystania środków przymusu bezpośredniego.

Tabela 1. Zestawienie przypadków sytuacji, które stwarzają możliwość użycia lub wykorzystania środków przymusu bezpośredniego

wyegzekwowanie wymaganego prawem zachowania zgodnie z wydanym przez uprawnionego poleceniem
odparcie bezpośredniego, bezprawnego zamachu na życie, zdrowie lub wolność uprawnionego lub innej osoby
przeciwdziałanie czynnościom zmierzającym bezpośrednio do zamachu na życie, zdrowie lub wolność uprawnionego lub innej osoby
przeciwdziałanie naruszeniu porządku lub bezpieczeństwa publicznego
przeciwdziałanie bezpośredniemu zamachowi na ochraniane przez uprawnionego obszary, obiekty lub urządzenia
ochrona porządku lub bezpieczeństwa na obszarach lub w obiektach chronionych przez uprawnionego
przeciwdziałanie niszczeniu mienia
zapewnienie bezpieczeństwa konwoju lub doprowadzenia
zatrzymanie osoby, udaremnienia jej ucieczki lub pościgu za tą osobą
pokonanie biernego oporu
pokonanie czynnego oporu
przeciwdziałanie czynnościom zmierzającym do autoagresji

Źródło: Z. Gospodarowicz, T. Zajac, *Uprawnienia funkcjonariuszy Służby Więziennej w zakresie użycia i wykorzystania środków przymusu bezpośredniego i broni palnej*, Warszawa 2013, s.11.

⁸ Art.12 ust. 1 ustawy z dnia 24 maja 2013 r. o środkach przymusu i bezpośredniego i broni palnej (Dz.U. z 2020 r., poz. 848).

Katalog przypadków zastosowania charakteryzowanych środków jest znaczący, toteż poziom wykształcenia i wymaganych kompetencji u funkcjonariuszy sprowadza się do jego ciągłego doskonalenia i wysuwa konieczność zachowania zdrowego rozsądku oraz czujności. W zapisach ustawy w sposób uwydatniony zostały nakreślone dwa kluczowe pojęcia dotyczące stosowania środków przymusu bezpośredniego: ich użycia oraz wykorzystania. Funkcjonariusze uprawnieni do posługiwania się środkami przymusu bezpośredniego stosują je w sytuacjach, w których jest to niezbędne zarówno w stosunku do człowieka, stwarzającego swoim zachowaniem okoliczności do ich zastosowania, jak również w stosunku do innych podmiotów bądź obiektów. Zastosowanie wybranego środka przymusu bezpośredniego wobec osoby jest określane mianem użycia środka przymusu bezpośredniego. W przypadku wykorzystania środka przymusu bezpośredniego to nic innego jak posłużenie się nim w stosunku do zwierzęcia oraz celem zatrzymania, zablokowania lub pozbawienia ruchu pojazdu bądź pokonania napotkanej przeszkody⁹.

Poza uprawnieniami i dostępnym katalogiem środków, które budzą w funkcjonariuszach uczucie pewności, ustawodawca określił szczegółowe zasady i tryb ich użycia, które są zgodne z obowiązującymi, pozostałymi przepisami prawa. Jedną z pierwszych zasad prezentuje, iż środki przymusu bezpośredniego stosuje się w sposób należyty do zrealizowania celów ich użycia lub wykorzystania, mając na uwadze proporcje względem stopnia zagrożenia, dobierając środek o możliwie jak najmniejszej dolegliwości wobec osób pozbawionych wolności¹⁰. Omawiany zapis zaznacza wyraźnie, iż nie jest pożądana obojętność w sferze doboru środka a także swobodnego i „nazbyt skutecznego” jego użycia. Kolejną zasadę stosowania środków przymusu bezpośredniego prezentuje w swojej publikacji M. Jurgilewicz, twierdząc, iż środków przymusu bezpośredniego należy stosować w sposób stwarzający możliwie najmniejsze szkody, a jeśli obrany cel został osiągnięty, funkcjonariusz ma obowiązek odstąpić dalszego stosowania środków¹¹. Treść i znaczenie tej zasady cechuje się słusznością i racjonalnością w aspekcie jej zastosowania, jak również ma ona po części związek z innymi zasadami wykonywania kary pozbawienia wolności, takimi jak poszanowanie godności ludzkiej a przede wszystkim humanitaryzmu¹².

⁹ Art. 4 ust. 9 ustawy z dnia 24 maja 2013 r. o środkach przymusu i bezpośredniego i broni palnej (Dz.U. z 2020, poz. 848).

¹⁰ Art. 6 ust. 1 ustawy z dnia 24 maja 2013 r. o środkach przymusu i bezpośredniego i broni palnej (Dz.U. z 2020 r., poz. 848).

¹¹ M. Jurgilewicz, *Środki przymusu bezpośredniego i broń palna. Użycie lub wykorzystanie w ochronie bezpieczeństwa wewnętrznego*, Wyd. Editions Spotkania, Warszawa 2015, s. 35.

¹² Art. 4 §1 ustawy z dnia 6 czerwca 1997 r. *Kodeks karny wykonawczy* (Dz.U.2024.706).

Mimo, iż zachowując wszelkie środki ostrożności oraz zalecenia co do sposobu postępowania w przypadkach zagrożenia bezpieczeństwa, dana sytuacja może eskalować. Ten wariant został również przewidziany przez ustawodawcę i nie został pozostawiony bez adekwatnego rozwiązania. Ustawodawca w takim wypadku przewidział rozwiązanie bowiem uprawniony, gdy poziom zagrożenia wzrósł, zaistniały określone i konkretne okoliczności, może użyć bądź wykorzystać jednorazowo więcej niż jeden środek przymusu bezpośredniego. Decyzja o doborze kilku środków musi być odpowiednio uzasadniona poprzez pryzmat zaistniałej sytuacji oraz okoliczności, które staną się podstawą do użycia lub wykorzystania określonych środków przymusu bezpośredniego. Podsumowując przedstawione treści warto zaznaczyć, że niejednokrotnie sytuacja zagrożenia bezpieczeństwa jest dynamiczna i nieprzewidywalna, jednakże funkcjonariusz winien stosować się do kluczowych zasad wpisanych w jego etos. Praktyki zaczerpnięte z przebiegających działań, wiedza szerokiego grona praktyków oraz zastosowanie porządku prawnego w codziennej działalności Służby Więziennej dają wyraz wielkiego profesjonalizmu i odwagi w kwestii stosowania środków przymusu bezpośredniego. Ponadto warto podkreślić że rozwiązania prawne określone w ramach stosowania środków przymusu bezpośredniego przez Służbę Więzienną, stanowią jej bogate zaplecze.

Konwojowanie jako stały element pracy funkcjonariuszy Służby Więziennej – pojęcia, typologia, procedury i podmioty

Postrzegając całość działalności omawianej formacji mundurowej, zauważyć można zróżnicowaną specyfikę pracy zależną od działu służby, specyfiki i liczebności podległej grupy osób pozbawionych wolności oraz terenu prowadzonych działań. Biorąc pod uwagę specyfikę pracy w formacji zajmującej się ochroną społeczeństwa przed sprawcami przestępstw, występują w niej zagrożenia o zróżnicowanej typologii i charakterystyce. Literatura wskazuje na dwa główne typy zagrożeń zachodzących w jednostce penitencjarnej: zewnętrzne i wewnętrzne¹³. Zwracając uwagę na konwojowanie, jest to wyjątkowa część działalności obarczona w opinii autora wieloma czynnikami mogących stworzyć lub zainicjować zagrożenie. Na wstępie jednak stosownym jest wyjaśnienie owego terminu w sposób fachowy, podając interpretację wieloletniego

¹³ E. Pływaczewski, J. Pomiankiewicz, *Więziennictwo jako element systemu bezpieczeństwa państwa*, [w:] T. Bulenda, A. Rzepliński (red.), *Modernizowanie więziennictwa. V Kongres Penitencjarny*, Warszawa 2015.

praktyka więziennego, obecnego znamienitego wykładowcy z dziedziny bezpieczeństwa:

Konwojowanie osób należy rozumieć jako przemieszczanie osób pobranych z zakładu karnego i aresztu śledczego oraz zespół czynności realizowanych w związku z tym przemieszczaniem przez uprawnionego do używania lub wykorzystywania środków przymusu bezpośredniego lub broni palnej¹⁴.

Powyższe sprecyzowanie daje obraz mnogości czynników, które sprowadzają się do wytężonej pracy i przywiązania uwagi na wszelkiego rodzaju kwestie bezpieczeństwa podczas tych działań. Jak wszelkie elementy i całość naszego otoczenia są w pewien sposób uporządkowane, również konwojowanie posiada swój indywidualny podział, którego obecność nakreśla zauważalną specyfikę prowadzonych czynności w każdym z ich rodzajów. Konwojowanie dzieli się na:

- planowane – organizowane jest w celu umożliwienia przeprowadzenia badań lekarskich, możliwych prześwietleń bądź również zaplanowanych wizyt lekarskich, do tego rodzaju konwojowania kwalifikuje się także transport osadzonych pomiędzy zakładami oraz aresztami śledczymi Służby Więziennej¹⁵,
- doraźne – realizowane w wypadku konieczności udzielenia pomocy lekarskiej w przypadku nagłych sytuacji np. samouszkodzenia lub ataku choroby osadzonego¹⁶.

Uwagę i należyte omówienie treści jest konieczne także w przypadku procedur utworzenia konwoju. Ich wyznaczenie jest uzgadniane przez kilka podmiotów personelu więziennego, które na podstawie analizy informacji z Centralnej Bazy Danych Osób Pozbawionych Wolności, generują w oparciu o nią wykaz transportowy. Jest on jednym z kluczowych dokumentów, dającym podstawę do rozpoczęcia konwojowania osób pozbawionych wolności. Kolejnym krokiem jest wyznaczenie składu konwoju, czyli dobór funkcjonariuszy, którzy wezmą udział w tym przedsięwzięciu. Zasadniczym warunkiem wyznaczania składu konwoju

¹⁴ R. Nowacki, *Konwojowanie i doprowadzenie osób. Doświadczenia podmiotów bezpieczeństwa*, Międzynarodowa Konferencja Naukowa, Kalisz, 13 października 2022 r., definicja konwoju osób, zgodna z ustawą o środkach przymusu bezpośredniego i broni palnej, dostosowana do zadań i uprawnień Służby Więziennej.

¹⁵ M. Cierpiół, G. Kasprzykowski, M. Kryń, *Konwojowanie i zapewnienie bezpieczeństwa konwoju w Służbie Więziennej*, COSSW, Kule 2020, s. 5.

¹⁶ P. Jarczewski, K. Jędrzejak, M. Kuświk, K. Setla, *Konwojowanie w Służbie Więziennej*, Kalisz 2006, s. 19.

jest aspekt kompetencji i poziomu wykształcenia, który korzystnie wpływa na zwiększenie poczucia bezpieczeństwa funkcjonariuszy, jak również wzrost profesjonalizmu i skuteczności w bezpiecznym przebiegu konwojowania. Praktyka więzienna pokazuje, że konwojowanie realizują przeważnie funkcjonariusze działu ochrony, jednakże nie ma przeszkód i przeciwskażeń, aby uzupełniali go funkcjonariusze innych działów. Warunkiem koniecznym jest posiadanie wymaganych umiejętności i predyspozycji do realizacji wyznaczonego zadania. W celu zapewnienia bezpieczeństwa realizowanego konwoju, skład osobowy musi być zróżnicowany ilościowo bowiem podczas konwojowania jednego bądź grupy do dziesięciu tymczasowo aresztowanych lub osadzonych, którzy odbywają karę w zakładzie karnym typu zamkniętego, skład konwoju liczy co najmniej 2 funkcjonariuszy¹⁷. W przypadku skazanych zakwalifikowanych do odbywania kary w zakładzie karnym typu półotwartego i otwartego, przy skazanym o tych cechach lub grupie liczącej maksymalnie 3 osadzonych, zasadnym zdaje się wyznaczyć jednego funkcjonariusza bez konieczności posiadania uzbrojenia i innego wyposażenia.

Przyglądając się pracy konwojentów, z założenia możemy sądzić, że ich głównym celem jest w bezpieczny sposób przetransportowanie wyznaczonych do konwoju osadzonych do wskazanego decyzją odpowiednich organów miejsca. Doprecyzowując wspomniane cele by posiadać całokształt wiedzy w tym zakresie, celem konwojowania pozostaje:

- zapewnienie bezpieczeństwa osadzonego,
- niedopuszczenie do uciezek osób pozbawionych wolności w trakcie przejazdu lub przemieszczania oraz pobytu poza terenem jednostki,
- zabezpieczenie broni palnej oraz pozostałych przedmiotów chronionych przez przepisy prawa i wyeliminowanie sytuacji zawładnięcia przez osoby nieupoważnione¹⁸.

Przechodząc do sfery podmiotów biorących udział w tym przedsięwzięciu jakim jest konwojowanie, scharakteryzowania wymaga funkcjonariusz biorący czynny udział w przetransportowywaniu osób pozbawionych wolności. Wedle zapisów rozporządzenia, osobę konwojenta interpretuje się jako funkcjonariusza bądź pracownika wykonującego czynności związane z konwojowaniem¹⁹. By móc przypisać cechy oraz stopień zaangażowania oraz poznać dokładniej specyfikę pracy na tym stanowisku, właściwym jest przedstawienie zakresu obowiązków charakteryzowanego podmiotu, zawartych w tabeli 2.

¹⁷ M. Cierpiol, G. Kasprzykowski, M. Kryń, *Konwojowanie i zapewnienie...*, dz. cyt., s. 9.

¹⁸ M. Cierpiol, G. Kasprzykowski, M. Kryń, *Konwojowanie i zapewnienie...*, dz. cyt., s. 10.

¹⁹ Rozporządzenie Ministra Sprawiedliwości z dnia 17 X 2016 r. w sprawie sposobów ochrony jednostek organizacyjnych Służby Więziennej, §2 pkt 12, (Dz.U. z 2016., poz. 1804).

Tabela 2. Zadania konwojenta

obserwacja zachowania osadzonych poddanych konwojowaniu
niedopuszczanie do kontaktów osadzonego z osobami postronnymi
pozostawanie w stałej gotowości do przeciwdziałania zagrożeniom bezpieczeństwa realizowanego konwojowania
utrzymywanie broni palnej i środków przymusu bezpośredniego w stałej gotowości do użycia oraz wykorzystania
niezezwalanie osadzonemu na zmianę wyznaczonego miejsca w pojeździe konwojowym oraz przekazywania przedmiotów pomiędzy osadzonymi konwojowanymi

Źródło: Zarządzenie nr 69/23 DGSW z dnia 31 X 2023 r. w sprawie sposobów ochrony, konwojowania oraz zadań ochronnych funkcjonariuszy i pracowników Służby Więziennej.

Funkcjonariuszem bardziej zaangażowanym i odpowiedzialnym za przebieg konwoju i procedury jego organizacji jest dowódca konwoju. Jego udział polega głównie na kierowaniu zespołem ludzi odpowiedzialnych za realizację w sposób bezpieczny i zgodny z obowiązującymi przepisami czynności związanych z konwojowaniem. Katalog przyporządkowanych temu stanowisku obowiązków jest ukazany w poniższej tabeli 3.

Tabela 3. Zadania dowódcy konwoju

sprawdzenie tożsamości osadzonych oraz rozmieszczenie ich w pojeździe konwojowym
sprawdzenie stanu zabezpieczeń techniczno-ochronnych pojazdu konwojowego oraz czy w przedziale dla konwojowanych osadzonych nie znajdują się przedmioty niedozwolone lub substancje
pouczenie osadzonych w jakich sytuacjach – w związku z konwojowaniem, dozwolone jest użycie broni palnej lub środków przymusu bezpośredniego
dokonanie podziału zadań pomiędzy funkcjonariuszy składu konwoju
podejmowanie decyzji o użyciu sygnałów świetlnych i dźwiękowych pojazdu konwojowego
informowanie dowódcy zmiany, dostępnymi środkami łączności, o każdorazowej zmianie ustalonej trasy konwoju;
organizowanie kontroli pobieżnej konwojowanego osadzonego

prorowadzenie książki przebiegu służby konwojowej
podczas realizacji transportowania osadzonych pomiędzy jednostkami organizacyjnymi – pobranie osadzonych z jednostki organizacyjnej i przekazanie ich do właściwej jednostki organizacyjnej, wraz z ich dokumentacją i depozytami

Źródło: Zarządzenie nr 69/23 DGSW z dnia 31 X 2023 r. w sprawie sposobów ochrony, konwojowania oraz zadań ochronnych funkcjonariuszy i pracowników Służby Więziennej.

Reasumując, spektrum działania funkcjonariuszy wyznaczonych w skład konwoju opiera się na szerokiej gamie obowiązków, których celem głównym jest zapewnienie bezpieczeństwa zarówno sobie, osobom pozbawionym wolności, jak również osobom postronnym. Nie wymaga dodatkowego potwierdzenia fakt, iż odpowiedzialność funkcjonariuszy oraz poziom wyszkolenia zostaje wystawiona każdorazowo na najwyższą próbę, mogącą stanowić ogromne zagrożenie.

Środki przymusu bezpośredniego i ich korelacja z konwojowaniem – zasadność ich stosowania w oparciu o wyniki badań

Nieodłącznym elementem w codziennej służbie na terenie jednostek penitencjarnych staje się dbałość o poziom bezpieczeństwa. Dzieje się to przy udziale odpowiednio licznego personelu więziennego, dostępnej infrastruktury wyposażonej w szereg zabezpieczeń techniczno – ochronnych ale również indywidualnego wyposażenia każdego funkcjonariusza w środki przymusu bezpośredniego i ochrony osobistej. Sprawdzając swoje rozważania do osób wyznaczonych do konwoju, ich wyposażenie we wspomniane środki jest warunkiem koniecznym ponieważ liczebność funkcjonariuszy jest ograniczona, zachowanie osób konwojowanych podczas pobytu poza jednostką penitencjarną również może ulec zmianie. Dlatego ku ograniczeniu ryzyka wystąpienia zagrożeń o nieokreślonej charakterystyce i liczbie, funkcjonariuszom realizującym konwojowanie wydaje się następujący asortyment środków ukazanych poniżej w tabeli 4.

Tabela 4. Wyposażenie funkcjonariuszy wyznaczonych do konwojowania

umundurowanie specjalne
hełm kuloodporny oraz rękawice taktyczne
broń palną krótką lub długą albo dwie jednostki broni jednocześnie i amunicję
kamizelkę kuloodporną

chemiczny środek obezwładniający
łączność radiową i bezprzewodową (komórkową) oraz pakiet medyczny
kajdanki (jednorazowe i szcękowe zakładane na ręce lub na nogi oraz zespolone zakładanych na ręce i nogi)
inne środki przymusu bezpośredniego w zależności od sytuacji

Źródło: M. Cierpiół, G. Kasprzykowski, M. Kryń, *Konwojowanie i zapewnienie bezpieczeństwa konwoju w Służbie Więziennej*, COSSW, Kule 2020, s. 9.

Jeśli jest znany poziom wykształcenia funkcjonariuszy oraz ich wyposażenie na wypadek jakichkolwiek zagrożeń, zasadnym winno być usystematyzowanie ich charakterystyki oraz spisu konkretyzując owe zapisy w oparciu o konwojowanie. Dostępna literatura podaje, że wszelkie zagrożenia lub sytuacje mogące naruszyć poziom bezpieczeństwa w jednostkach penitencjarnych mają miano zdarzeń, które definiuje się następująco:

Zdarzeniem mogącym wystąpić w Służbie Więziennej jest zagrożenie lub naruszenie bezpieczeństwa jednostki organizacyjnej Służby Więziennej lub konwojowania, zagrożenie dla zdrowia lub życia osoby pozbawionej wolności, funkcjonariusza Służby Więziennej lub pracownika Służby Więziennej, a także naruszenie prawa przez wymienionych, ścigane z urzędu²⁰.

W kwestii katalogu wspomnianych zdarzeń, występuje znaczące „urozmaicenie”, które od zaangażowanych wtenczas funkcjonariuszy wymaga odpowiedniej wiedzy, umiejętności oraz dużej odporności na stres²¹. Skonkretyzowaną listę dotyczącą wyłącznie zdarzeń podczas konwoju prezentuje skrypt wydany przez jeden z ośrodków szkolenia Służby Więziennej, w którym zdarzeniami z jakimi może zetknąć się konwój mogą być:

Tabela 5. Wykaz zdarzeń mogących mieć miejsce podczas konwoju w Służbie Więziennej

ucieczka konwojowanego
napad na konwój

²⁰ Zarządzenie nr 100/22 DGSW z dnia 29 XII 2022 r. w sprawie ustalenia sposobu i trybu informowania o zdarzeniach, które wystąpiły w Służbie Więziennej oraz ustalenia sposobu i trybu przeprowadzenia czynności sprawdzających dotyczących tych zdarzeń, oraz sposobu ich dokumentowania.

²¹ J. Gierszewski, I. Osmólska, *Bezpieczeństwo personalne i strukturalne w trakcie zmian kulturowych*, Wyd. Difin, Warszawa 2021.

bunt osób konwojowanych
choroba konwojowanego
choroba konwojentów
wypadek drogowy/katastrofa drogowa
awaria pojazdu i jego unieruchomienie
utknięcie w korku samochodowym
zasłabnięcie konwojowanego
autoagresja konwojowanego
śmierć osadzonego w trakcie konwoju

Źródło: Cierpiol M., Kasprzykowski G., Kryń M., *Konwojowanie i zapewnienie bezpieczeństwa konwoju w Służbie Więziennej*, COSSW Kule, Kule 2020, s. 31-32.

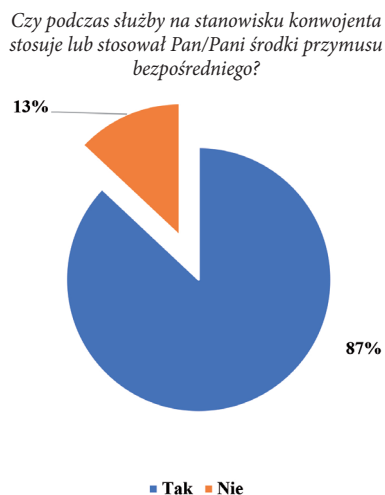
Postrzegając i poddając podsumowaniu zasadne kwestie dotyczące się tematyki konwojowania i powiązania z tym środków przymusu bezpośredniego, zamysł autora sprowadził się do umieszczenia poniżej wybranych wyników prowadzonych badań. Celem dokonanych na potrzeby pracy licencjackiej badań, której temat brzmi: *Środki przymusu bezpośredniego stosowane w czasie konwojowania osób pozbawionych wolności w ocenie funkcjonariuszy Zakładu Karnego nr 1 we Wrocławiu*, było zbadanie opinii funkcjonariuszy Służby Więziennej, biorących udział w konwojach osób pozbawionych wolności na temat środków przymusu bezpośredniego stosowanych podczas realizacji tych działań. Do przeprowadzenia badań została wyznaczona grupa 50 funkcjonariuszy, głównie działu ochrony jednostki z okręgu opolskiego – Zakład Karny nr 1 we Wrocławiu – wobec której został przeprowadzony kwestionariusz ankiety. Umieszczone poniżej pytania wraz z otrzymanymi wynikami w rozumieniu autora mają potwierdzić słuszność tezy o zasadności stosowania wspomnianych środków podczas transportowania osadzonych. W jednym z pierwszych pytań, autor na potwierdzenie jakości prowadzonych badań zbadął udział ankietowanych w konwojach osób pozbawionych wolności.

Spoglądając na graficzne przedstawienie wyników badań na jedno z kluczowych pytań dotyczących poruszanej tematyki należy stwierdzić, że wiarygodność osób poddanych badaniu będzie zadowalająca, bowiem każdy z nich częściej bądź rzadziej brał udział w konwojowaniu.



Ryc. 1. Udział ankietowanych w konwojach osadzonych

Źródło: na podstawie badań własnych



Ryc. 2. Użycie przez respondentów środków przymusu bezpośredniego podczas konwojowania

Źródło: na podstawie badań własnych

Kolejne w odczuciu autora trafne ujęcie pytania dotyczy swą treścią istoty zastosowania środków przymusu bezpośredniego podczas prowadzonych czynności konwojowych. Wynika z nich jednoznacznie, że 87% ankietowanych podczas pełnienia służby na stanowisku konwojenta w ramach konwojowania stosowała środki przymusu bezpośredniego. To utwierdza już częściowo w przekonaniu, że omawiane środki nie są tylko wymieniane jako atut i narzędzie w codziennej pracy, ale stają się elementem usprawniającym pracę i dającym poczucie pewności podczas sytuacji koniecznych.

W następnej kolejności zasadnym i istotnym winno być zaprezentowanie wyników, które ukazałyby częstotliwość stosowania charakteryzowanych środków podczas konwojowania. Wyniki prezentuje tabela 6.

Wyniki badań wskazują w tym przypadku, że stosowanie środków przymusu należy do rzadkości wedle 85% badanych, a tylko 12% stosuje je w sposób regularny i częsty. Powyższe dane dają sygnał, że znikoma częstotliwość stosowania wspomnianych środków może świadczyć o wysokim poziomie wyszkolenia funkcjonariuszy w zakresie przeciwdziałania zagrożeniom, które mają na uwadze odpowiednią pracę z osadzonymi w oparciu o oddziaływania penitencjarne oraz czynności profilaktyczne. Jest to także wedle autora powód do zadowolenia, bowiem udaje się w takim razie „załatwić” wszelkie sprawy i problemy bez konieczności wdrażania dostępnych środków przymusu.

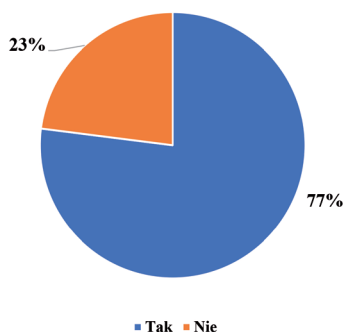
Tabela 6. Częstotliwość stosowania przez respondentów środków przymusu bezpośredniego podczas konwojowania

Proszę określić z jaką częstotliwością stosuje Pan/Pani środki przymusu bezpośredniego podczas realizowanych konwojów osadzonych	Ilość osób	Procent w stosunku do grupy badawczej
Rzadko	22	85%
Często	1	3%
Bardzo często	3	12%

Źródło: na podstawie badań własnych.

Przechodząc do kolejnej z części zamieszczonych badań, możemy zapoznać się z opinią badanych na temat kompletności dostępnego katalogu środków przymusu bezpośredniego. Wedle badanych, 77% uważa obecny katalog za wystarczający do podejmowania konwojowania.

Czy Pana/Pani zdaniem katalog środków przymusu bezpośredniego, w jakie wyposaża się funkcjonariuszy realizujących konwoje osadzonych jest wystarczający?



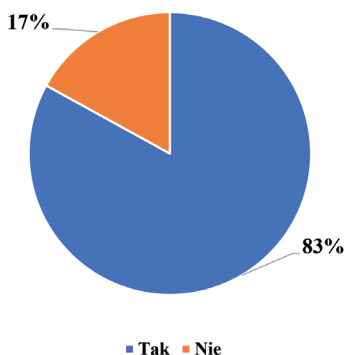
Ryc. 3. Opinia respondentów w kwestii kompletności katalogu środków przymusu bezpośredniego podczas konwojowania

Źródło: na podstawie badań własnych.

Powyższe pytanie pokazuje również, że 23% badanych wskazuje brak kompletności, jednakże podczas prowadzonych badań nie zostały podane i zaproponowane jakiegokolwiek propozycje nowych środków przymusu bezpośredniego, które wedle badanych powinny znaleźć się w dostępnym katalogu. Poniżej

zamieszczone wyniki badań miały za zadanie zweryfikować słuszność stosowania środków przymusu bezpośredniego podczas konwojowania osób pozbawionych wolności. Sformułowane pytanie i uzyskane rezultaty przedstawiły potwierdzenie rozważań autora tejże pracy i tym samym ukazały opinię a zarazem świadomość osób ankietowanych. Wedle podanych odpowiedzi, grupa 83% badanych jest zwolennikiem konieczności stosowania charakteryzowanych środków podczas dokonywania konwoju, pozostałe 17% badanych nie wskazało takiej potrzeby. Wyniki w formie graficznej prezentuje poniższej przedstawiona rycina.

Czy uważa Pan/Pani, że stosowanie dostępnych środków przymusu bezpośredniego podczas realizowanych konwojów osadzonych jest konieczne?



Ryc. 4. Opinia respondentów w kwestii konieczności stosowania dostępnych środków przymusu bezpośredniego podczas konwojowania

Źródło: na podstawie badań własnych.

Powyższe wyniki sprowadzają się także do refleksji i wniosków w kierunku konieczności dołożenia wzmożonej uwagi i organizacji kompleksowych szkoleń o tematyce środków przymusu bezpośredniego, będących jednym z narzędzi do zapewnienia bezpieczeństwa.

Jedno z ostatnich pytań, potwierdzających słuszność obecności wspomnianych środków podczas prowadzonego konwoju dotyczyło wpływu stosowania środków przymusu bezpośredniego podczas konwojowania osadzonych. Wyniki prezentuje tabela 7.

Rezultaty zadanego pytania wskazują jednoznacznie, iż omawiane środki przymusu bezpośredniego mają w głównej mierze wpływ na bezpieczeństwo funkcjonariuszy (80% ankietowanych). Jest to wartość, która jest ceniona w formacji, gdzie jest ono na każdym kroku poddane próbie lub zagrożeniu. Powyżej ukazane badania z uwzględnieniem uzyskanych wyników w sposób czytelny zaznaczają

Tabela 7. Opinia respondentów odnośnie wpływu stosowanych środków przymusu bezpośredniego podczas konwojowania

Jakie według Pana/Pani wpływ ma stosowanie środków przymusu bezpośredniego podczas realizowanych konwojów osadzonych?	Ilość osób	Procent w stosunku do grupy badawczej
Wpływa na bezpieczeństwo funkcjonariuszy	24	80%
Poprawia komfort, profesjonalizm i wydajność pracy	3	10%
Wpływa na bezpieczeństwo osób postronnych / społeczeństwa	3	10%
Wszystkie warianty odpowiedzi	13	43%

Źródło: na podstawie badań własnych.

fundamentalną rolę środków przymusu bezpośredniego podczas realizowanych konwojów. Stanowią one wg autora wartościowe uzupełnienie przedstawionej powyżej teorii dotyczącej redagowanej tematyki. Ich wymiar jest wielowymiarowy bowiem po pierwsze są wspomnianym dopełnieniem omawianego materiału; z drugiej stanowią spojrzenie osób z „środowiska penitencjarnego” które na podstawie przeżytych sytuacji oraz zgromadzonego doświadczenia, podzieliły się swoimi spostrzeżeniami dając dość wiarygodne spojrzenie na realia pracy penitencjarnej.

Podsumowanie

Niniejsze rozważania nad problematyką zasadności stosowania środków przymusu podczas konwojowania osób pozbawionych wolności w opinii autora stanowią komplementarne zaplecze zgromadzonej i wyrafinowanej teorii na wskazane aspekty, poparte dowodami w postaci przedstawionych wyników badań stanowiących jego dorobek naukowy. Przybliżenie kwestii prawno-proceduralnych stosowania środków przymusu bezpośredniego, przedstawienie związanych z nimi pojęć, niezbędnych katalogów oraz informacji, nakreśliło rozmiar znaczenia i rolę omawianych składników w codziennym podejmowaniu przez funkcjonariuszy czynności służbowych. Zbliżone postępowanie z tematyką konwojowania osób pozbawionych wolności pozwoliło na ocenę charakterystyki tejże dziedziny pracy więzienników oraz pozwoliło skorelować poprzednie zagadnienia z obecnymi.

Wspomnianym dopełnieniem stały się przeprowadzone na potrzeby pracy dyplomowej badania w formie kwestionariusza ankiety, które jednoznacznie swoimi wynikami dały sygnał o zasadności a wręcz konieczności stosowania środków przymusu podczas konwojowania osób pozbawionych wolności. W domyśle autora, powyższe rozważania pochyliły się w sposób znaczący nad problematyką bezpieczeństwa penitencjarnego, poruszając swoją analizą jedną z dziedzin działalności SW oraz spektrum zasobów odnoszących się do charakteryzowanych środków będących na jej wyposażeniu.

Bibliografia

- Cierpiol M., Kasprzykowski G., Kryń M., *Konwojowanie i zapewnienie bezpieczeństwa konwoju w Służbie Więziennej*, COSSW Kule, Kule 2020.
- Gierszewski J., Osmólska I., *Bezpieczeństwo personalne i strukturalne w trakcie zmian kulturowych*, Wyd. Difin, Warszawa 2021.
- Gospodarowicz Z., Zajac T., *Uprawnienia funkcjonariuszy Służby Więziennej w zakresie użycia lub wykorzystania środków przymusu bezpośredniego i broni palnej*, Biuro Ochrony i Spraw Obronnych CZSW, Warszawa 2013.
- Gryz J., *Zarys teorii bezpieczeństwa państwa*, AON, Warszawa 2016.
- Jarczewski P., Jędrzejak K., Kuświk M., Setla K., *Konwojowanie w służbie więziennej*, COSSW Kalisz, Kalisz 2006.
- Jurgilewicz M., *Środki przymusu bezpośredniego i broń palna. Użycie lub wykorzystanie w ochronie bezpieczeństwa wewnętrznego*, Wyd. Editions Spotkania, Warszawa 2015.
- Pływaczewski E., Pomiankiewicz J., *Więziennictwo jako element systemu bezpieczeństwa państwa*, [w:] T. Bulenda, A. Rzepliński (red.), *Modernizowanie więziennictwa. V Kongres Penitencjarny*, Warszawa 2015.
- Ustawa z dnia 9.04.2010 r. o Służbie Więziennej.
- Ustawa z dnia 24 V 2013 r. o środkach przymusu i bezpośredniego i broni palnej.
- Ustawy z dnia 6 czerwca 1997 r. *Kodeks karny wykonawczy*.
- Rozporządzenie Ministra Sprawiedliwości z dnia 17 października 2016 r. w sprawie sposobów ochrony jednostek organizacyjnych Służby Więziennej.
- Zarządzenie nr 69/23 DGSW z dnia 31 X 2023 r. w sprawie sposobów ochrony, konwojowania oraz zadań ochronnych funkcjonariuszy i pracowników Służby Więziennej.
- Zarządzenie nr 100/22 DGSW z dnia 29 XII 2022 r. w sprawie ustalenia sposobu i trybu informowania o zdarzeniach, które wystąpiły w Służbie Więziennej oraz ustalenia sposobu i trybu przeprowadzenia czynności sprawdzających dotyczących tych zdarzeń, oraz sposobu ich dokumentowania.

Podsumowanie

Zintegrowane w publikacji perspektywy – od kwestii ochrony informacji niejawnych i cyberbezpieczeństwa, przez rolę służb porządkowych, aż po holistyczne ujęcie systemów penitencjarnych – wskazują na nieuchronną konieczność porzucenia fragmentarycznego postrzegania zagrożeń. Autorzy i redaktorzy niniejszej publikacji stoją na stanowisku, że największym wyzwaniem nadchodzących lat pozostanie wypracowanie i utrzymanie optymalnej równowagi między imperatywem skuteczności a poszanowaniem wolności jednostki. W dobie zagrożeń hybrydowych i „czarnych łabędzi” to nie tylko rygorystyczne procedury, ale przede wszystkim świadomość społeczna, profesjonalizm kadr i etyka działania stanowić będą o odporności państwa.

Część pierwsza monografii dowiodła, że transformacja cyfrowa i rozwój nowych technologii niesie ze sobą zarówno potężne narzędzia dla organów ścigania, jak i bezprecedensowe zagrożenia. Analiza problematyki ochrony informacji niejawnych oraz cyberprzestrzeni wskazała na pilną potrzebę aktualizacji ram legislacyjnych, które muszą nadążać za dynamiką przestępczości zorganizowanej w czasach rozwoju technologicznego. Postulowana w pracy profesjonalizacja kadr oraz uszczelnienie systemów ochrony danych są niezbędne, by państwo mogło skutecznie przeciwdziałać nowym formom agresji hybrydowej.

Druga część publikacji rzuciła nowe światło na system penitencjarny jako kluczowy, choć często marginalizowany w debacie publicznej, element systemu bezpieczeństwa wewnętrznego. Badania potwierdziły hipotezę, że po opuszczeniu zakładu karnego przez sprawcę, to właśnie od jakości oddziaływań resocjalizacyjnych i zapewnienia standardów bytowych w trakcie izolacji, zależy bezpieczeństwo społeczne. Wykazano, że profesjonalizm funkcjonariuszy, wsparty nowoczesnymi

procedurami, jest gwarantem ochrony zarówno osób osadzonych, jak i personelu oraz całego społeczeństwa.

Mamy nadzieję, że zaprezentowane w monografii rozważania staną się impulsem do dalszych, pogłębionych studiów nad bezpieczeństwem, a sformułowane postulaty znajdą odzwierciedlenie w przyszłych rozwiązaniach systemowych, służąc budowie stabilnego i bezpiecznego jutra w erze globalnej niepewności.

dr Adrian Pachciarz

ppor. mgr Daniel Nowakowski

Streszczenie

Monografia naukowa pod tytułem „Wymiar bezpieczeństwa w XXI wieku: Integracja perspektyw w kontekście współczesnych zagrożeń” ma na celu stworzenie zbioru artykułów, w których Autorzy podjęli się badań nad różnymi aspektami bezpieczeństwa w kontekście wyzwań współczesnego świata. Interdyscyplinarne podejście do problematyki doprowadziło Badaczy do interesujących wniosków.

Przedmiotowa monografia naukowa podejmuje problematykę wymiaru bezpieczeństwa w XXI wieku w kontekście współczesnych zagrożeń. Głównym celem publikacji jest konsolidacja perspektyw oraz badania nad różnymi aspektami bezpieczeństwa poprzez interdyscyplinarne podejście, czerpiące z dorobku prawa, socjologii, kryminologii i nauk o zarządzaniu. Analiza opiera się na założeniu, że istotę bezpieczeństwa stanowi proces nieliniowy i dynamiczny, stale negocjujący granice ryzyka.

W części pierwszej, poświęconej nowym obliczom bezpieczeństwa publicznego w erze globalizacji, analizie poddano strategię neutralizacji globalnych i transgranicznych wyzwań. Zakres badawczy obejmuje problematykę ochrony informacji niejawnych na gruncie prawa krajowego, uwarunkowania prawne monitoringu przestrzeni publicznej oraz rolę służb porządkowych. Szczególny nacisk położono na bezpieczeństwo w cyberprzestrzeni, analizując nowoczesne technologie i strategie w zwalczaniu przestępczości zorganizowanej oraz cyberprzestępczości. Wykazano na pilną potrzebę aktualizacji ram legislacyjnych, które muszą nadążać za dynamiką transformacji cyfrowej.

Druga część publikacji analizuje bezpieczeństwo penitencjarne w ujęciu holistycznym. Badania koncentrują się na warunkach życia osadzonych, prawie do

praktykowania wiary oraz wpływie praktyk religijnych na resocjalizację. Poddano analizie kwestie operacyjne i systemowe: alternatywny system wykonywania kary pozbawienia wolności, zagrożenia wynikające z konwojowania osadzonych, zasadność stosowania środków przymusu bezpośredniego oraz rolę psów służbowych w działaniach antyterrorystycznych.

Wyniki badań potwierdzają, że w dobie zagrożeń hybrydowych i „czarnych łabędzi” o odporności państwa stanowić będą: świadomość społeczna, profesjonalizm kadr oraz etyka działania. Kluczowym wyzwaniem pozostaje wypracowanie i utrzymanie optymalnej równowagi między imperatywem skuteczności a poszanowaniem wolności jednostki.

Słowa kluczowe

bezpieczeństwo, zagrożenia hybrydowe, resocjalizacja, prawa człowieka, penitencjarystyka

Summary

The academic monograph entitled 'The dimension of security in the 21st century: Integrating perspectives in the context of contemporary threats' aims to create a collection of articles in which the authors undertake research on various aspects of security in the context of the challenges of the modern world. An interdisciplinary approach to the issue has led the researchers to interesting conclusions.

This scientific monograph addresses the issue of security in the 21st century in the context of contemporary threats. The main objective of the publication is to consolidate perspectives and research on various aspects of security through an interdisciplinary approach, drawing on the achievements of law, sociology, criminology and management sciences. The analysis is based on the assumption that the essence of security is a non-linear and dynamic process, constantly negotiating the boundaries of risk.

In the first part, devoted to the new face of public security in the era of globalisation, the strategy of neutralising global and cross-border challenges is analysed. The scope of the research covers the protection of classified information under national law, the legal conditions for monitoring public space and the role of law enforcement agencies. Particular emphasis is placed on cybersecurity, analysing modern technologies and strategies for combating organised crime and cybercrime. The urgent need to update the legislative framework, which must keep pace with the dynamics of digital transformation, has been demonstrated.

The second part of the publication analyses penitentiary security from a holistic perspective. The research focuses on the living conditions of inmates, the right to practise their faith and the impact of religious practices on

rehabilitation. Operational and systemic issues were analysed: alternative systems of imprisonment, threats arising from the transport of prisoners, the legitimacy of the use of direct coercive measures, and the role of service dogs in counter-terrorism operations.

The results of the research confirm that in the era of hybrid threats and 'black swans', the resilience of the state will be determined by public awareness, the professionalism of its personnel and ethical conduct. The key challenge remains to develop and maintain an optimal balance between the imperative of effectiveness and respect for individual freedoms.

Keywords

security, hybrid threats, rehabilitation, human rights, penology



WYDAWNICTWO NAUKOWE

Wydawnictwo Naukowe Kontekst. Poznań 2026. Wydanie I.

Papier offsetowy 80 g/m², 13 a.w.

Oddano do składu: 5 I 2026. Podpisano do druku: 6 II 2026

Printed in Poland

ADRIAN PACHCIARZ

Doktor nauk prawnych. Adiunkt w Instytucie Nauk Prawnych w Akademii Wymiaru Sprawiedliwości. Kierownik Katedry Prawa Penitencjarnego i Praw Człowieka. Pełnomocnik ds. ochrony praw człowieka. Opiekun Koła Naukowego Praw Człowieka AWS. Absolwent studiów prawniczych. Następnie rozpoczął studia doktoranckie w Katedrze Praw Człowieka na Wydziale Prawa i Administracji Uniwersytetu Mikołaja Kopernika w Toruniu, które zakończył obroną rozprawy doktorskiej. Zainteresowania badawcze: ochrona praw człowieka.

DANIEL NOWAKOWSKI

Oficer Służby Więziennej. Doktorant Uniwersytetu Kaliskiego, gdzie przygotowuje dysertację doktorską pt. „Dezinformacja jako narzędzie wpływu na środowisko bezpieczeństwa”. Autor publikacji naukowych oraz prelegent na kilkudziesięciu konferencjach o zasięgu ogólnopolskim i międzynarodowym. Zainteresowania badawcze koncentrują się wokół problematyki szeroko rozumianego bezpieczeństwa państwa, w szczególności bezpieczeństwa informacyjnego, a także wojskowości oraz stosunków międzynarodowych.

Praca wieloautorska pt. „Wymiar bezpieczeństwa w XXI wieku: integracja perspektyw w kontekście współczesnych zagrożeń” pod redakcją naukową dr. Adriana Pachciarza oraz ppor. mgr. Daniela Nowakowskiego stanowi dzieło poruszające istotne zagadnienia w sposób interdyscyplinarny, zarówno na gruncie krajowym jak i międzynarodowym, w szczególności w naukach społecznych i humanistycznych z elementami nauk prawnych. Monografia akcentuje swój ciężar szczególnie w dyscyplinie nauk o bezpieczeństwie, uwzględniając niezwykle aktualne aspekty z zakresu cyberbezpieczeństwa, bezpieczeństwa wewnętrznego czy też interdyscyplinarnej dziedziny jaką jest niewątpliwie penitencjarystyka. Opracowanie stanowi cenne źródło wiedzy zarówno dla funkcjonariuszy, jak i wszystkich zainteresowanych tematyką współczesnego bezpieczeństwa.

Z recenzji wydawniczej
por. dr inż. Iwony Szkudlarek



Kontekst
Wydawnictwo

WYDAWNICTWO NAUKOWE

www.wkn.com.pl