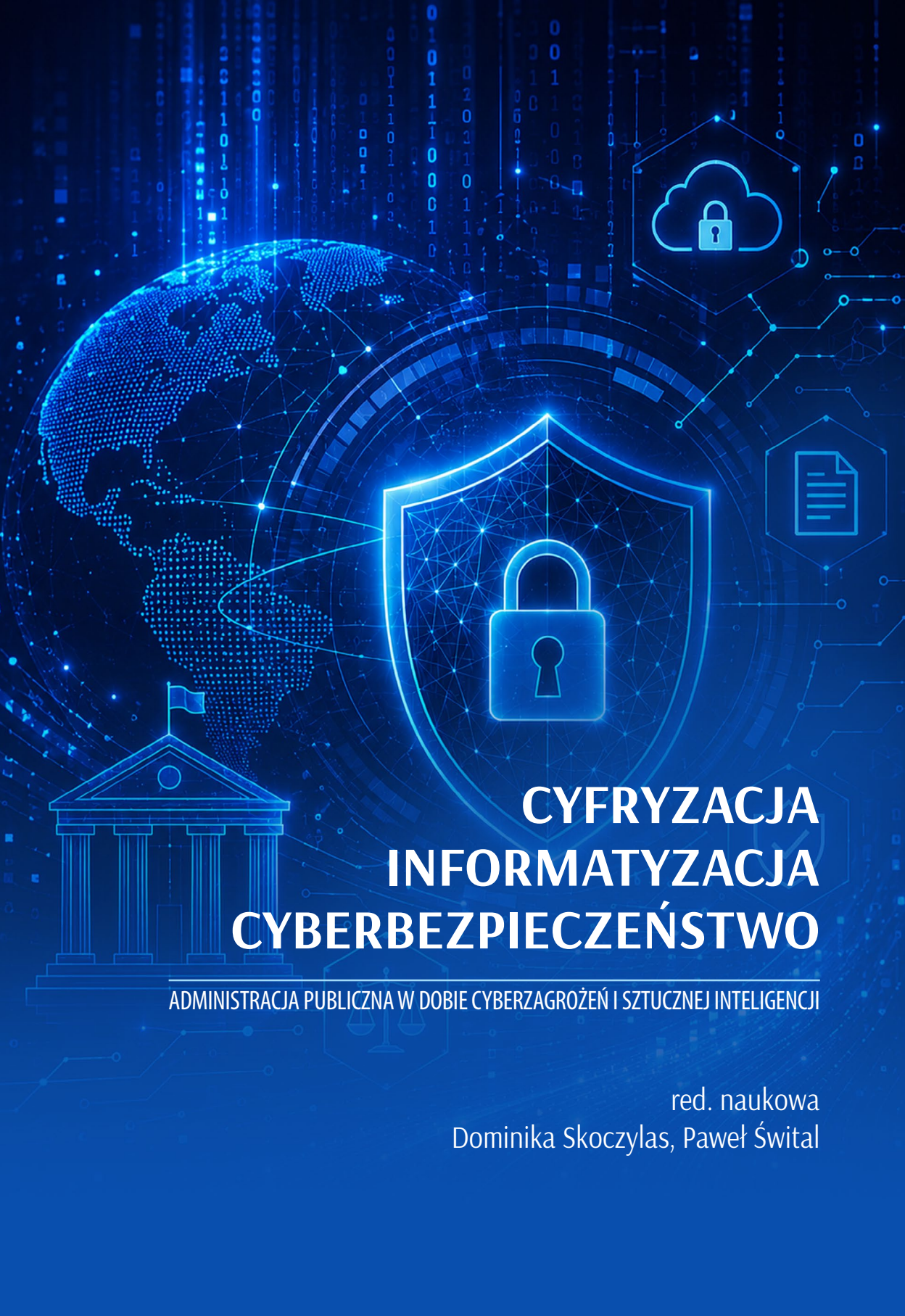


CYFRYZACJA INFORMATYZACJA CYBERBEZPIECZEŃSTWO

ADMINISTRACJA PUBLICZNA W DOBIE CYBERZAGROŻEŃ I SZTUCZNEJ INTELIGENCJI

red. naukowa
Dominika Skoczylas, Paweł Świtał

Recenzja naukowa

ks. dr hab. Sławomir Fundowicz
(Katolicki Uniwersytet Lubelski Jana Pawła II w Lublinie)

Opracowanie graficzne: Sieć Badawcza Łukasiewicz – Instytut Technologii Eksploatacji w Radomiu

ISBN 978-83-7789-827-7

Współpraca wydawnicza: Łukasiewicz – Instytut Technologii Eksploatacji

Radom-Szczecin 2026

Projekt okładki i opracowanie wydawnicze: Anna Skrok

Łukasiewicz
Instytut Technologii Eksploatacji

Wydawnictwo Naukowe
ul. K. Pułaskiego 6/10, 26-600 Radom, tel. (48) 364-42-41
e-mail: instytut@itee.radom.pl http://www.itee.radom.pl

Spis treści

Wprowadzenie

Informatyzacji administracji publicznej towarzyszy szereg wyzwań natury organizacyjno-prawnej i technologicznej. Do kluczowych z nich należą zapewnienie cyberbezpieczeństwa realizowanych przez administrację zadań publicznych, ochrona danych osobowych użytkowników technologii informacyjno-komunikacyjnych oraz zastosowanie sztucznej inteligencji w kontekście algorytmizacji usług publicznych. Problemy istniejące na polu cyberbezpieczeństwa i cyberzagrożeń determinują konieczność przeglądu i wdrożenia w krajowych i unijnych strategii dotyczących zapewnienia bezpiecznego środowiska cyberprzestrzeni. Przedmiotowa problematyka stała przedmiotem zainteresowania prawników, administratywistów i przedstawicieli doktryny.

W dniu 27 czerwca 2024 r. w wersji hybrydowej odbyła się II Ogólnopolska konferencja naukowa „Cyfryzacja – informatyzacja – cyberbezpieczeństwo. Administracja publiczna w dobie cyberzagrożeń i sztucznej inteligencji". Konferencja została zorganizowana przez Wydział Prawa i Administracji Uniwersytetu Szczecińskiego oraz Wydział Prawa i Administracji Uniwersytetu Radomskiego im. Kazimierza Pułaskiego. Celem konferencji była wymiana poglądów środowiska naukowego na temat aktualnych problemów w zakresie wdrożenia technologii informacyjno-komunikacyjnych w sektorze publicznym. Diagnozie poddano takie wyzwania cyfryzacji, jak ochrona przed cyberzagrożeniami czy zastosowanie sztucznej inteligencji w administracji publicznej. Konferencja stanowiła pole do dyskusji na temat prawnych i technologicznych uwarunkowań informatyzacji administracji publicznej oraz wpływu nowych technologii na rozwój społeczno-gospodarczy. Dokonano analizy trzech kluczowych zagadnień tj. sposobów zapewnienia cyberbezpieczeństwa administracji publicznej, przeciwdziałania cyberzagrożeniom oraz wykorzystania systemów sztucznej inteligencji w sektorze publicznym.

Mając na uwadze doniosłość problematyki cyfryzacji i informatyzacji administracji publicznej, w tym konieczność zintensyfikowania działań z zakresu cyberbezpieczeństwa oraz znaczenie sztucznej inteligencji w obszarze algorytmizacji usług świadczonych przez administrację publiczną, redaktorzy niniejszej monografii zaprosili wybitnych naukowców do stworzenia wspólnego opracowania pt. „Cyfryzacja – informatyzacja – cyberbezpieczeństwo. Administracja publiczna w dobie cyberzagrożeń i sztucznej inteligencji". Monografia stanowi przegląd aktualnych

perspektyw, szans i wyzwań w obszarze cyfryzacji administracji publicznej, ze szczególnym uwzględnieniem aspektów cyberbezpieczeństwa i algorytmizacji e-usług publicznych. Monografia zawiera 8 rozdziałów, w których poruszone zostały następujące zagadnienia: *Prawne uwarunkowania stosowania systemu sztucznej inteligencji w procesie kształcenia na uczelni* (Maciej Błażewski); *Cyberzagrożenia, cyberryzyka oraz jakość publicznych danych w zakresie turystyki w Polsce – rozważania administracyjnoprawne* (Dominik Borek, Katarzyna Podhorodecka, Piotr Dobrzyński); *Rola i zadania gminy w systemie zarządzania kryzysowego i cyberbezpieczeństwa* (Dominika Cendrowicz); *E-demokracja w czasie zagrożeń wewnętrznych i zewnętrznych* (Aleksandra Puczko); *Administracyjno-prawne warunki kreowania cyberbezpieczeństwa w samorządzie województwa – wybrane zagadnienia* (Paweł Romaniuk); *Podniesienie poziomu e-usług i wzmocnienie cyberbezpieczeństwa w jednostkach samorządu terytorialnego* (Dominika Skoczylas, Kamil Czaplicki); *Czy korzystanie ze sztucznej inteligencji godzi w prawa twórców? Uwagi na tle działalności organów administracji publicznej* (Marcin Stępień); *Obraźliwa infografika jako przedmiot postępowania dyscyplinarnego - ocena odpowiedzialności dyscyplinarnej studenta uczelni mundurowej za naruszenie etosu służby i dobrego imienia wykładowcy* (Paweł Świtał, Damian Witczak).

Pragniemy podziękować Autorom rozdziałów zawartych w przedmiotowej monografii za trud włożony w ich przygotowanie.

Głównym celem monografii jest podjęcie debaty na temat kompleksowego wdrożenia strategii i zasad cyberbezpieczeństwa, przy jednoczesnej popularyzacji sztucznej inteligencji i algorytmizacji usług publicznych. Zadanie jest o tyle trudne, o ile zarówno administracja publiczna, jak i jej użytkownicy napotykają na coraz bardziej różnorodne i wyrafinowane cyberzagrożenia, takie jak *phishing*, czy dezinformacja. Książka skierowana jest do osób zajmujących się informatyzacją, cyfryzacją, cyberbezpieczeństwem, algorytymizacją usług publicznych oraz wszystkich zainteresowanych przedmiotową tematyką. Zapraszamy do lektury monografii „Cyfryzacja – informatyzacja – cyberbezpieczeństwo. Administracja publiczna w dobie cyberzagrożeń i sztucznej inteligencji".

dr Dominika Skoczylas

dr Paweł Świtał

Radom-Szczecin, 2026

dr hab. Maciej Błażewski
Uniwersytet Wrocławski
adres e-mail: maciej.blazewski@uwr.edu.pl
ORCID: 0000-0003-2812-8199

Prawne uwarunkowania stosowania systemu sztucznej inteligencji w procesie kształcenia na uczelni

Legal aspects the use of systems of artificial intelligence in the education process at a universities

Streszczenie

Sztuczna inteligencja jest narzędziem, które potencjalnie może ułatwić świadczenie usług kształcenia w toku studiów na uczelniach funkcjonujących w ramach systemu szkolnictwa wyższego i nauki. System sztucznej inteligencji może służyć augmentacji (rozszerzeniu) wykonywanych działań nauczyciela akademickiego, jeżeli jest używany komplementarnie względem jego działań. System ten może także zautomatyzować usługi kształcenia. Zgodnie z polskim prawem, system sztucznej inteligencji może być używany jednie komplementarnie względem działań nauczyciela akademickiego. Wymagania dotyczące świadczenia usług kształcenia na uczelniach pośrednio odnoszą się do ich wykonywania przez człowieka. Zapewnieniu spełnienia tych wymagań służą środki nadzoru nad działalnością uczelni.

Wprowadzenie

System sztucznej inteligencji jest narzędziem, które może zostać zastosowane m. in. w sferze świadczenia usług kształcenia w toku studiów na uczelniach funkcjonujących w ramach systemu szkolnictwa wyższego i nauki[1]. Stosowanie systemu sztucznej inteligencji w tej sferze może mieć znaczący wpływ zarówno na jakość usług kształcenia świadczonych w toku studiów na uczelni, jak również na sposób realizacji tych usług. Wpływ ten, w zależności od metody użycia systemu sztucznej inteligencji może mieć pozytywny lub negatywny charakter. Pozytywny jak i negatywny wpływ może dotyczyć jakości lub efektywności świadczenia usług kształcenia. Standardy jakości oraz efektywności usług kształcenia w toku studiów na uczelniach są określane w postaci wymagań ogólnych wyinterpretowanych z przepisów ustawy Prawo o szkolnictwie wyższym i nauce[2]. Wymagania te mają

[1] Szerzej pojęcie sztucznej inteligencji przedstawia A. Zalewska-Bochenko, *Sztuczna inteligencja w procesie edukacji*, „Optimum. Economic Studies" 2024, nr 2(116), s. 196-199.

[2] Ustawa z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t. j. Dz. U. z 2024 r., poz. 1571 ze zm.),

charakter uniwersalny, a zatem nie odnoszą się one bezpośrednio do użycia systemu sztucznej inteligencji. Były one bowiem ustanowione w okresie przed wprowadzeniem do powszechnego obrotu systemów sztucznej inteligencji. Jednak są one właściwe także dla usług kształcenia wykonywanych z użyciem tego rodzaju systemu. Zgodność świadczenia usług kształcenia z tymi wymaganiami jest istotna ze względu na potrzebę realizacji interesu publicznego, który w tym zakresie obejmuje m. in. potrzebę rozwoju stosunków społeczno-gospodarczych w Polsce.

Stosowanie systemu sztucznej inteligencji w dydaktyce można analizować z perspektywy zakresu działań wykonywanych przez system sztucznej inteligencji. Z tej perspektywy możliwe są wówczas dwie sytuacje: 1. system sztucznej inteligencji jest stosowany komplementarnie względem działań nauczyciela akademickiego; 2. system sztucznej inteligencji wykonuje całość działań dydaktycznych.

Celem opracowania jest określenie, która z tych sytuacji jest możliwa w świetle obowiązującego prawa. Przedmiotem rozdziału są aktualne regulacje obowiązujące w polskim porządku prawnym. W opracowaniu przyjmuję tezę, że w obecnie obowiązującym porządku prawnym możliwa jest jedynie pierwsza sytuacja obejmująca stosowanie systemu sztucznej inteligencji komplementarnie względem działań nauczyciela akademickiego.

Pojęcie sztucznej inteligencji

„Sztuczna inteligencja" jest narzędziem technicznym, o autonomicznym lub interaktywnym charakterze. Jest ona narzędziem wykonującym zadania w oparciu o proces uczenia się i uwzględnienia nowych okoliczności w związku z rozwiązaniem problemu[3]. W opracowaniu przyjęto pojęcie „systemu sztucznej inteligencji" oznaczającej konkretne narzędzie technologiczne wykorzystywane w związku ze świadczeniem usług kształcenia.

System sztucznej inteligencji, jako narzędzie techniczne, służy wykonywaniu określonych działań mających na celu bezpośrednie lub pośrednie zaspokojenie potrzeb człowieka, który jest odbiorcą tych działań. System sztucznej inteligencji może służyć augmentacji (rozszerzeniu) wykonywanych działań, względem pracy człowieka będącego wykonawcą działania, lub automatyzacji działań, czyli samodzielnemu ich wykonywania bez udziału człowieka. W przypadku augmentacji działań człowieka (wykonawcy działań), system sztucznej inteligencji może być używany komplementarnie względem tych działań, a czynności realizowane przez system służą optymalizacji tej pracy. W sytuacji automatyzacji działań, są

dalej: u.p.s.w.n.

[3] T. Zalewski, *Definicja sztucznej inteligencji*, [w:] *Prawo sztucznej inteligencji*, L. Lai, M. Świerczyński (red.), Warszawa 2020, Legalis.

one w całości realizowane przez system sztucznej inteligencji, z pominięciem czynności realizowanych przez człowieka (wykonawcy działania)[4].

Zaznaczenia wymaga, że system sztucznej inteligencji samodzielnie wykonujący działanie może wymagać np. prac serwisowych wykonywanych przez człowieka (serwisanta). Prace te są jednak zewnętrzne względem działań realizowanych przez system sztucznej inteligencji.

Łańcuch wartości procesu kształcenia z użyciem systemu sztucznej inteligencji

Stosowanie systemu sztucznej inteligencji w sferze usług kształcenia w toku studiów na uczelniach wiąże się z wydłużeniem łańcucha wartości tych usług w analizowanej sferze. Łańcuchem wartości jest sekwencja działań nakierowanych na stworzenie tych usług[5]. Stosowanie systemu sztucznej inteligencji wydłuża ten łańcuch wartości m. in. o działania obejmujące produkcję tego systemu. Mając na uwadze aktualne gospodarcze uwarunkowania Polski, produkcja systemu sztucznej inteligencji, jako działanie będące częścią łańcucha wartości usług kształcenia, ma miejsce w sektorze prywatnym, na który administracja publiczna ma ograniczony wpływ.

Ze względu na przedmiot tego opracowania, należy wyróżnić trzy rodzaje modeli sytuacji odnoszących się do długości łańcucha wartości usług kształcenia. Przedstawione modele mają uproszczony charakter.

Pierwszy model sytuacji obejmuje usługi kształcenia wykonywane przez nauczyciela akademickiego bez użycia systemu sztucznej inteligencji (model A). Ten model łańcucha wartości obejmuje m. in. działania związane z zapewnieniem infrastruktury dydaktycznej, z dystrybucją usług kształcenia, z obsługą administracyjną oraz z pracą nauczyciela akademickiego.

---

[4] Szeroko problematykę augmentacji i automatyzacji działań, w związku z użyciem sztucznej inteligencji przedstawiają Y-W. Lei, R. Kim, *Automation and Augmentation: Artificial Intelligence*, "Robots, and Work, Annual Review of Sociology"2024, vol. 50, s. 252. Szerzej problematykę augmentacji, czyli rozszerzenia działań człowieka o działania sztucznej inteligencji przedstawiają: M. H. Jarrahihttps, C. Lutzhttps, G. Newlands, *Artificial intelligence, human intelligence and hybrid intelligence based on mutual augmentation*, "Big Data & Society" 2022, vol. 9, issue 2, s. 2-4.

[5] Koncepcja „łańcucha wartości" jest właściwa dla nauki ekonomii. Koncepcja ta jest zastosowana w tym opracowaniu, ponieważ umożliwia porównanie poszczególnych modeli sytuacji świadczenia usług kształcenia. Szerzej pojęcie „łańcucha wartości" zostało określone w literaturze właściwej dla nauki ekonomii. Zob. więcej: R. Matwiejczuk, *Przesłanki tworzenia wartości w łańcuchu wartości*, „Przegląd Organizacji" 2010, nr 5, s. 17; J. Borowski, Łańcuch wartości jako nowa teoria zarządzania strategicznego, „Optimum. Studia Ekonomiczne" 2013, nr 2(62), s. 12-14; T. Rojek, *Koncepcja łańcucha wartości w zarządzaniu przedsiębiorstwem*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Finanse, Rynki Finansowe, Ubezpieczenia" 2014, nr 66, s. 814-815. Zob. też: B. Kos, *Znaczenie łańcuchów dostaw we współczesnej gospodarce*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Problemy Zarządzania, Finansów i Marketingu" 2013, nr 29, s. 75-76.

Drugi model sytuacji obejmuje usługi kształcenia wykonywane przez nauczyciela akademickiego z komplementarnym użyciem systemu sztucznej inteligencji (model B). W tym modelu, w łańcuchu wartości mieszczą się m. in. działania związane z zapewnieniem infrastruktury dydaktycznej, z dystrybucją usług kształcenia, z obsługą administracyjną, z produkcją i dystrybucją systemu sztucznej inteligencji oraz z pracą nauczyciela akademickiego przy komplementarnym użyciu systemu sztucznej inteligencji.

W trzecim modelu sytuacji usługi kształcenia wykonywane są z użyciem systemu sztucznej inteligencji z pomięciem nauczyciela akademickiego (model C). W tym przypadku model łańcucha wartości obejmuje m. in. działania związane z zapewnieniem infrastruktury dydaktycznej, z dystrybucją usług kształcenia, z obsługą administracyjną, z produkcją i dystrybucją systemu sztucznej inteligencji oraz z użyciem systemu sztucznej inteligencji.

W świetle przedstawionych modeli sytuacji, przy założeniu o produkcji systemów sztucznej inteligencji w sektorze prywatnym (poza uczelniami oraz organami administracji publicznej), stosowanie tych systemów w usługach kształcenia skutkuje, w przypadku modelu B, rozszerzeniem łańcucha wartości o działania wykonywane przez przedsiębiorców albo, w przypadku modelu C, rozszerzenie łańcucha wartości o działania realizowane przez przedsiębiorców, przy jednoczesnym wyłączeniu działań związanych z pracą nauczyciela akademickiego. Zaznaczenia wymaga, że przedsiębiorcy zajmujący się produkcją i dystrybucją systemów sztucznej inteligencji, a ewentualnie także użyciem tych systemów, nie są częścią systemu szkolnictwa wyższego, a w rezultacie nie podlegają nadzorowi ministra nauki i szkolnictwa wyższego. Nadzór nad jakością i efektywnością usług kształtowania w toku studiów na uczelniach ma jedynie pośredni charakter, ponieważ jego przedmiotem może być działalność uczelni, które świadczą te usługi kształcenia przy użyciu systemu sztucznej inteligencji.

Wymagania dotyczące świadczenia usług kształcenia na uczelniach z użyciem systemów sztucznej inteligencji

Wymagania dotyczące świadczenia usług kształcenia w toku studiów na uczelniach odnoszą się m. in. do jakości oraz efektywności tych usług. Jakość usług kształcenia jest jednym z celów działalności uczelni[6]. Kształcenie powinno odbywać się jednocześnie z poszanowaniem standardów międzynarodowych, zasad etycznych i dobrych praktyk[7]. Efektywność usług kształcenia odnosi się do rezultatów działań me-

[6] W świetle art. 2 u.p.s.w.n., misją systemu szkolnictwa wyższego i nauki jest m. in. prowadzenie najwyższej jakości kształcenia.

[7] Zgodnie z art. 3 ust. 2 u.p.s.w.n., system szkolnictwa wyższego i nauki funkcjonuje z poszanowaniem standardów międzynarodowych, zasad etycznych i dobrych praktyk m.in. w zakresie kształcenia.

rytorycznych oraz wychowawczych. Działania merytoryczne odnoszą się do jasnego przekazywania wiedzy. Działania wychowawcze są związane m.in. z kształtowaniem postaw obywatelskich oraz zachęcania do aktywnego uczestnictwa w rozwoju społecznym[8]. Przedmiotem działań wychowawczych powinno być kształtowanie u studentów poczucia odpowiedzialności za państwo polskie i tradycję narodową, jak również umacnianie u nich zasad demokracji i poszanowanie praw człowieka[9].

Wymagania te są związane z koniecznością aktywnego udziału nauczyciela akademickiego. Dla przedstawienia tego związku jest konieczna prezentacja wyników analizy zapewnienia jakości i efektywności wykonania tych usług kształcenia, która odnosi się do dwóch sytuacji: 1. realizacji tych usług przez nauczyciela akademickiego przy użyciu komplementarnych systemów sztucznej inteligencji (właściwej dla modelu B); 2. realizacji tych usług w całości przez system sztucznej inteligencji (w sposób właściwy dla modelu C).

W przypadku sytuacji realizacji usług kształcenia przez nauczyciela akademickiego przy użyciu komplementarnego systemu sztucznej inteligencji, jakość tych usług jest rezultatem synergii działań nauczyciela akademickiego oraz tego systemu. Ma wówczas miejsce augmentacja (rozszerzenie) działań nauczyciela akademickiego o działania systemu sztucznej inteligencji. Nauczyciel akademicki może transponować aktualne wyniki badań do programu studiów, ze względu na indywidulane zaznajomienie z tymi wynikami, jak również przy pomocy komplementarnego systemu sztucznej inteligencji ułatwiającego dotarcie do tych wyników. Efekty tych usług odnoszą się do wykonywanych działań merytorycznych oraz wychowawczych. Działania merytoryczne mogą być wówczas dwutorowe. Z jednej strony nauczyciel akademicki samodzielnie przekazuje wiedzę studentowi lub grupie studentów. Z drugiej strony, nauczyciel akademicki może zapewnić spersonalizowane przekazywanie studentowi wiedzy przy użyciu systemu sztucznej inteligencji. Jednocześnie nauczyciel akademicki zachowuje możliwość realizacji działań wychowawczych względem studentów[10].

---

[8] W świetle art. 2 u.p.s.w.n., misją systemu szkolnictwa wyższego i nauki jest prowadzenie m. in. kształtowania postaw obywatelskich, a także uczestnictwo w rozwoju społecznym. Zob. szerzej: H. Izdebski, *Komentarz do art. 2*, [w:] *Prawo o szkolnictwie wyższym i nauce. Komentarz,* wyd. III, H. Izdebski, J. M. Zieliński (red.), Warszawa 2023, LEX/el., teza 6-7; J. Woźnicki, *Komentarz do art. 2*, [w:] *Prawo o szkolnictwie wyższym i nauce. Komentarz*, J. Woźnicki (red.), Warszawa 2019, LEX/el., teza 2.

[9] Zgodnie z art. 11 ust. 1 pkt. 7 u.p.s.w.n., podstawowymi zadaniami uczelni są m.in. wychowywanie studentów w poczuciu odpowiedzialności za państwo polskie, tradycję narodową, umacnianie zasad demokracji i poszanowanie praw człowieka. Zob. więcej: J. Woźnicki, *Komentarz do art. 11*, [w:] *Prawo o szkolnictwie wyższym i nauce. Komentarz*, J. Woźnicki (red.), Warszawa 2019, LEX/el., teza 4.

[10] Jak podkreślają L. Jurczuk oraz P. Tadejko, narzędzia sztucznej inteligencji są aktualnie używane w procesie dydaktycznym jako uzupełnienie tradycyjnych metod nauczania. L. Jurczuk, P. Tadejko, *Wykorzystywanie narzędzi sztucznej inteligencji w rozwiązywaniu zadań akademickich. Ocena wpływu narzędzi AI na sposób nauki studentów*, „Akademia Zarządzania" 2025, nr 9(3), s. 707, 715. Jak podkreśla A. Zalewska-Bochenko, sztuczna inteligencja umożliwia dostosowanie metody nauczania do indywidualnych potrzeb, a w rezultacie ułatwia

W sytuacji realizacji usług kształcenia w całości przez system sztucznej inteligencji, co oznacza ich automatyzację, jakość tych usług jest zależna głównie od producenta tego systemu. Uczenia nie ma wówczas bezpośredniego wpływu na jakość tych usług, a jedynie może wybrać system sztucznej inteligencji oferowany przez jego producenta. Efekty tych usług mogą odnosić się jedynie do działań merytorycznych, które obejmują spersonalizowane przekazywanie studentowi wiedzy. System sztucznej inteligencji nie może wykonywać działań wychowawczych, ponieważ one odnoszą się do kształtowania studenta w relacji z innymi członkami wspólnoty akademickiej, jakimi są m. in. inni studenci oraz pracownicy uczelni.

W świetle przedstawionej analizy, usługi kształcenia na uczelni przy użyciu systemu sztucznej inteligencji umożliwiają zapewnienie spersonalizowanego przekazywania studentowi wiedzy. Jedynie użycie komplementarnych systemów sztucznej inteligencji umożliwia jednoczesne zachowanie odpowiedniej jakości usług kształcenia oraz spełnienie wymogu wykonania działań wychowawczych. Usługi kształcenia świadczone w całości przy w użyciu systemu sztucznej inteligencji są pozbawione tych aspektów.

Środki nadzoru pośrednio odnoszące się do użycia systemów sztucznej inteligencji w związku ze świadczeniem usług kształcenia na uczelni

Spełnienie wymagań dotyczących świadczenia usług kształcenia w toku studiów na uczelni jest nadzorowane przez ministra właściwego do spraw szkolnictwa wyższego i nauki. Środki nadzoru podejmowane przez ten organ mogą mieć charakter prewencyjny lub bieżący. Zaznaczenia wymaga, że przedmiotem tego nadzoru jest działalność uczelni, a nie używanie systemów sztucznej inteligencji. Jednakże, ze względu na fakt, że używanie systemów sztucznej inteligencji jest elementem działalności uczelni, środek nadzoru może pośrednio odnosić się do modelu użycia tego systemu.

Przepisy prawa regulujące te środki nadzoru determinują zatem konieczność stosowania przez uczelnię modelu A (wykonywanie usług kształcenia przez nauczyciela akademickiego bez użycia systemu sztucznej inteligencji) lub modelu B (wykonywanie usług kształcenia przez nauczyciela akademickiego z komplementarnym użyciem systemu sztucznej inteligencji), przy jednoczesnym wykluczeniu modelu C (realizacji usług kształcenia z użyciem systemu sztucznej inteligencji z pomięciem nauczyciela akademickiego). Wykonywanie usług kształcenia w toku studiów na uczelni wymaga bowiem aktywnego działania nauczyciela akademickiego. Podstawą tego stanu są przesłanki stosowania przez ministra właściwego do spraw szkolnictwa wyższego i nauki środków nadzoru prewencyjnego oraz nadzoru bieżącego względem działalności uczelni.

szybsze przyswajanie wiedzy i umiejętności. A. Zalewska-Bochenko, *Sztuczna inteligencja*..., op.cit., s. 207.

Środkiem nadzoru prewencyjnego jest pozwolenie na utworzenie studiów na określonym kierunku, poziomie i profilu. Minister właściwy do spraw szkolnictwa wyższego i nauki wydaje te pozwolenie na wniosek uczelni, gdy spełnia ona m. in. wymagania dotyczące prowadzenia studiów[11]. W świetle tych wymagań, w ramach prowadzonych studiów, usługi kształcenia mogą być wykonywane jedynie przez nauczycieli akademickich lub inne osoby prowadzące zajęcia[12].

Środkiem nadzoru bieżącego jest decyzja w sprawie cofnięcia pozwolenia na utworzenie studiów na określonym kierunku, poziomie i profilu. Minister właściwy do spraw szkolnictwa wyższego i nauki wydaje tę decyzję m. in., gdy Polska Komisja Akredytacyjna wydała negatywną ocenę jakości kształcenia[13]. Polska Komisja Akredytacyjna przeprowadza ewaluację jakości kształcenia na studiach, która jest dokonywana m. in. w formie oceny programowej[14]. Organ ten przeprowadza ocenę programową z uwzględnieniem m. in. kadry dydaktycznej[15].

Przepisy ustawy prawo o szkolnictwie wyższym i nauce wymagają zatem, aby świadczenie usług kształcenia, które stanowi element nadzorowanej działalności uczelni, było wykonywane w całości lub w części przez człowieka.

---

11 Atr. 54 w zw. z art. 81 u.p.s.w.n. Zob. więcej J. M. Zieliński, *Komentarz do art. 54*, [w:], *Prawo o szkolnictwie wyższym i nauce. Komentarz*, wyd. III, H. Izdebski, J. M. Zieliński (red.) Warszawa 2023, LEX/el., teza 2.

12 Zgodnie w przepisami rozporządzenia Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie studiów (t. j. Dz. U. z 2023 r., poz. 2787 ze zm.), dalej: r.s.s., nauczyciele akademicy oraz inne osoby prowadzące zajęcia, są konieczne do prowadzenia zajęć z ich bezpośrednim udziałem lub zajęć prowadzonych z wykorzystaniem metod i technik kształcenia na odległość. W świetle § 9 ust 1 pkt. 6 lit. a r.s.s., wniosek o pozwolenie na utworzenie studiów zawiera m. in. wykaz nauczycieli akademickich oraz innych osób, proponowanych do prowadzenia zajęć. W myśl wykładni językowej § 3 ust. 1 pkt. 6 r.s.s., nauczyciel akademicki lub inna osoba prowadząca zajęcia, prowadzą zajęcia z ich bezpośrednim udziałem. W świetle wykładni językowej § 12 ust. 1 pkt. 1 dalej r.s.s., zajęcia prowadzone z wykorzystaniem metod i technik kształcenia na odległość są prowadzone przez nauczycieli akademickich lub inne osoby prowadzącej zajęcia.

13 W świetle art. 56 ust. 1 pkt. 1 u.p.s.w.n., minister właściwy do spraw szkolnictwa wyższego i nauki może cofnąć pozwolenie na utworzenie studiów na określonym kierunku, poziomie i profilu, jeżeli na tych studiach Polska Komisja Akredytacyjna, dalej PKA, wydała negatywną ocenę jakości kształcenia. Jak podkreśla M. Dokowicz, jedną z przesłanek cofnięcia pozwolenia na utworzenie studiów jest negatywna ocena jakości kształcenia dokonana przez PKA. Jego zdaniem, w praktyce PKA może wydać negatywną ocenę jakości kształcenia jedynie w ramach dokonywanej cyklicznie oceny programowej, o której mowa w art. 241 ust. 2 u. p.s.w.n. M. Dokowicz, *Komentarz do art. 56*, [w:] *Prawo o szkolnictwie wyższym i nauce. Komentarz*, J. Woźnicki (red.), Warszawa 2019, LEX/el., teza 4.

14 W myśl art. 241 ust. 1 u.p.s.w.n., jakość kształcenia na studiach podlega ewaluacji przeprowadzanej przez PKA. Zgodnie z art. 241 ust. 2 u.p.s.w.n., ewaluacji dokonuje się w formie oceny programowej lub oceny kompleksowej. W świetle art. 258 ust. 1 pkt. 3 u.p.s.w.n., zadaniem PKA jest m. in. przeprowadzanie oceny programowej.

15 Zgodnie z art. 242 ust. 2 pkt. 2 u.p.s.w.n., przeprowadzając ocenę programową, bierze się pod uwagę w szczególności kadrę dydaktyczną i naukową. Jak podkreśla H. Izdebski, kryteria oceny programowej odnoszącą się m. in. do poziomu kompetencji i doświadczenia kadry prowadzącej kształcenie. H. Izdebski, *Komentarz do art. 242*, [w:] *Prawo o szkolnictwie wyższym i nauce. Komentarz*, wyd. III, H. Izdebski, J. M. Zieliński (red.), Warszawa 2023, LEX/el., teza 4.

Zakończenie

Przepisy prawa regulujące działalność uczelni w ramach systemu szkolnictwa wyższego i nauki, dopuszczają możliwość stosowania systemu sztucznej inteligencji w związku ze świadczeniem usług kształcenia w toku studiów na uczelni, jedynie gdy sposób świadczenia tych usług uwzględnia aktywne działanie nauczyciela akademickiego z komplementarnym użyciem tego systemu. Regulacje te obejmują wymagania dotyczące świadczenia usług kształcenia na uczelniach z użyciem systemów sztucznej inteligencji oraz środków nadzoru pośrednio odnoszących się do użycia tych systemów w ramach usług kształcenia.

Dopuszczenie przez prawodawcę w wymaganiach dotyczących świadczenia usług kształcenia jedynie modelu komparatywnego użycia systemu sztucznej inteligencji może być korzystne dla jakości i efektywności tych usług. W przypadku tego modelu możliwe jest bowiem osiągnięcie synergii możliwości nauczyciela akademickiego oraz systemu sztucznej inteligencji. Ma wówczas miejsce augmentacja (rozszerzenie) działań nauczyciela akademickiego.

Zapewnienie możliwości wdrożenia jedynie modelu komparatywnego użycia systemu sztucznej inteligencji jednocześnie ułatwia skuteczne sprawowanie nadzoru nad tymi usługami. Świadczenie tych usług stanowi bowiem węzłowy zbiór działań w obrębie działalność uczelni, a tym samym wykonywanie ich przez nauczyciela akademickiego z użyciem systemu sztucznej inteligencji, ułatwia ich nadzorowanie przez ministra właściwego do spraw szkolnictwa wyższego i nauki.

Bibliografia:

Akty prawne

1) Ustawa z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (t. j. Dz. U. z 2024 r., poz. 1571 ze zm.).
2) Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie studiów (t. j. Dz. U. z 2023 r., poz. 2787 ze zm.).

Literatura

1) Borowski J., Łańcuch wartości jako nowa teoria zarządzania strategicznego, „Optimum. Studia Ekonomiczne" 2013, nr 2(62).
2) Izdebski H., Zieliński J. M. (red.), *Prawo o szkolnictwie wyższym i nauce. Komentarz,* wyd. III, Warszawa 2023, LEX/el.
3) Jarrahihttps M. H., Lutzhttps C., Newlands G., *Artificial intelligence, human intelligence and hybrid intelligence based on mutual augmentation,* "Big Data & Society" 2022, vol 9, issue 2.
4) Jurczuk L., Tadejko P., *Wykorzystywanie narzędzi sztucznej inteligencji*

w rozwiązywaniu zadań akademickich. Ocena wpływu narzędzi AI na sposób nauki studentów, „Akademia Zarządzania" 2025, nr 9(3).
5) Kos B., *Znaczenie łańcuchów dostaw we współczesnej gospodarce*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Problemy Zarządzania, Finansów i Marketingu" 2013, nr 29.
6) Lai L., Świerczyński M. (red.), *Prawo sztucznej inteligencji*, Warszawa 2020, Legalis.
7) Lei Y-W., Kim R., *Automation and Augmentation: Artificial Intelligence*, "Robots, and Work, Annual Review of Sociology" 2024, vol. 50.
8) Matwiejczuk R., *Przesłanki tworzenia wartości w łańcuchu wartości*, „Przegląd Organizacji" 2010, nr 5.
9) Rojek T., *Koncepcja łańcucha wartości w zarządzaniu przedsiębiorstwem*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego. Finanse, Rynki Finansowe, Ubezpieczenia" 2014, nr 66.
10) Woźnicki J. (red.), *Prawo o szkolnictwie wyższym i nauce. Komentarz*, Warszawa 2019, LEX/el.
11) Zalewska-Bochenko A., *Sztuczna inteligencja w procesie edukacji*, „Optimum. Economic Studies" 2024, nr 2(116).

dr Dominik Borek
Szkoła Główna Handlowa w Warszawie
adres e-mail: dpborek@wp.pl
ORCID: 0000-0002-4359-9426

dr hab. Katarzyna Podhorodecka, prof. ucz.
Uniwersytet Warszawski
adres e-mail: katarzyna.podhrodecka@uw.edu.pl
ORCID: 0000-0003-3075-7453

mgr inż. Piotr Dobrzyński
Ministerstwo Sportu i Turystyki
Departament Turystyki
adres e-mail: piotr.dobrzynski@msit.gov.pl

Cyberzagrożenia, cyberryzyka oraz jakość publicznych danych w zakresie turystyki w Polsce – rozważania administracyjnoprawne

Cyberthreats, cyberrisks, and the quality of public data in the field of tourism in Poland – administrative and legal considerations

Streszczenie

Celem rozdziału jest przedstawienie wszystkich dostępnych źródeł publicznej informacji z zakresu turystyki w Polsce oraz wskazanie zagrożeń związanych z wiarygodnością oraz cyberbezpieczeństwem informacji zawartych w bazach danych i rejestrach. W artykule wskazano również zagrożenia związane z jakością i dostępnością danych oraz luki informacyjne dla obszaru związanego z badaniami w turystyce. W rozdziale opisano także pionierski projekt z zakresu wykorzystania sztucznej inteligencji do prognozowania danych z zakresu ruchu turystycznego w Polsce. W opracowaniu wykorzystano adekwatne źródła danych i metody badawcze właściwe dla prawa administracyjnego. Rozdział prezentuje stan prawny właściwy na dzień 10.09.2025 r. oraz prywatne stanowisko autorów i nie może być postrzegany jako stanowisko jakiegokolwiek podmiotu, jednostki czy instytucji.

Wprowadzenie

Do podejmowania decyzji przez administrację rządową i samorządową, a także przez przedsiębiorców, niezbędne są badania oraz dane i informacje z rynku

turystycznego, w tym w obszarze *compliance*[16]. Badania służą monitorowaniu i prognozowaniu stanu sektora turystycznego w Polsce i są potrzebne do oceny sektora oraz do tworzenia polityki turystycznej.

Najważniejszym źródłem danych ilościowych z zakresu turystyki w Polsce jest rządowy Program Badań Statystycznych Statystyki Publicznej[17]. Ministerstwo Sportu i Turystyki jest współrealizatorem dwóch badań cyklicznych. Bardzo istotne są w tym względzie zmieniające się potrzeby turystów w zakresie usług turystycznych, a dla administracji publicznej ważne jest również to że prowadzona polityka, powinna być dostosowana do potrzeb przedsiębiorców[18]. Wymaga to zbierania i udostępniania danych, którą posiadają odpowiednią jakość. Z badań statystycznych korzystają przedsiębiorcy turystyczni, a także wiele uczelni wyższych, które kształcą na kierunkach związanych z turystyką.

Poza badaniami, które są zapisane w rządowym Programie Badań Statystycznych Statystyki Publicznej, Ministerstwo Sportu i Turystyki realizuje corocznie inne niezbędne tematy badawcze, które służą do zabezpieczenia danych. Dane te są potrzebne do obliczania wskaźników ekonomicznych, są także wykorzystywane do monitoringu budżetu zadaniowego oraz do oceny stanu i możliwości rozwoju gospodarki turystycznej, a także do ceny zjawisk na rynku gospodarki turystycznej[19].

Badania statystyczne i obowiązek ich realizowania związany jest z koniecznością pozyskania informacji na temat stanu sektora turystycznego, aby móc określić politykę w tym sektorze (np. analiza zasadności wprowadzenia opłaty turystycznej). Istotne jest także przygotowywanie rządowych programów rozwoju turystyki, w tym strategii rozwoju turystyki oraz promocji turystyki. Wyniki badań służą do konstrukcji mierników i wskaźników wykorzystywanych w latach ubiegłych np. do oceny stanu realizacji dokumentów strategicznych sektora turystyki. Mierniki i wskaźniki nie tylko dostarczają informacji do oceny realizacji zadań wynikających z dokumentów strategicznych oraz budżetu zadaniowego, a także zaspokajają potrzeby informacyjne wynikające z członkostwa Polski w Unii Europejskiej, polegające na przekazywaniu danych do EUROSTAT-u (zobowiązanie Rozporządzenia Parlamentu Europejskiego

[16] D. Borek, *The decision of the European Commission State Aid SA. 101979 (2022/N) - a word of commentary, opinion and conclusions,* „Zeszyty Naukowe Wyższej Szkoły Gospodarki - Turystyka i Rekreacja" 2021, nr 16, s. 11-19; B. Makowicz, *Compliance w Przedsiębiorstwie,* Warszawa 2011, s. 5-212.

[17] Rozporządzenie Rady Ministrów z dnia 24 września 2024 r. w sprawie programu badań statystycznych statystyki publicznej na rok 2025 (Dz. U. poz. 1653).

[18] D. Borek, *Przedsiębiorca w ustawie o imprezach turystycznych i powiązanych usługach turystycznych – koncepcja przedmiotowego charakteru regulacji,* „Internetowy Kwartalnik Antymonopolowy i Regulacyjny UW" 2018, nr 4(7), s. 22-34.

[19] D. Borek, K. Świtaj, H. Zawistowska, *O zgodności z prawem UE regulacji art. 15k ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw* [w:] *Prawo – narzędzie sprawiedliwości czy władzy*, I. Barwicka-Tylek, P. Dziewałtowski-Gintowt, K. Zyzik, L. Łyżwa (red.), Kraków 2020, s. 11-17.

i Rady (UE) nr 692/2011 z dnia 6 lipca 2011 r. w sprawie europejskiej statystyki w dziedzinie turystyki i uchylające dyrektywę Rady 95/57/WE). Dane pochodzące z badań służą do realizacji zobowiązań Polski na rzecz organizacji międzynarodowych. Dane są przekazywane głównie do UN Tourism (dawniej UNWTO) i OECD (*Organisation for Economic Co-operation and Development* - Organizacja Współpracy Gospodarczej i Rozwoju), w tym w szczególności dostarczanie danych na temat zagranicznej turystyki przyjazdowej do Polski. Dodatkowo badania są wsparciem dla jednostek samorządu terytorialnego przy tworzeniu dokumentów strategicznych, w tym kierunków rozwoju regionów, a także programów promocji. Wyniki badań wspierają przedsiębiorców przy decyzjach inwestycyjnych w zakresie turystyki.

Problematyka badań statystycznych w turystyce była poruszana przez T. Studzieniecki i A. Wołoszyk. Autorzy wskazali, iż zasadne jest zsynchronizowanie statystyki publicznej ze statystyką transgraniczną[20]. Natomiast A. Zajadacz zwróciła uwagę, iż metodologia polskich badań granicznych musiała ulec zmianie po wejściu Polski do strefy Schengen. Z tego względu w sprawozdawczości statystycznej używa się zaleceń, które zostały zawarte w Kodeksie granicznym Schengen[21].

Bazy danych i rejestry w turystyce

System Rejestrów Publicznych w Turystyce jest dostępny w Internecie i został stworzony dla osób, które chcą skorzystać z usług przedsiębiorców turystycznych (www.turystyka.gov.pl). Dzięki rejestrowi obywatele mają możliwość zweryfikowania czy podmiot działa legalnie co oznacza, że posiada wpis do rejestrów prowadzonych przez Urzędy Marszałkowskie. Jest to niewątpliwie jeden z elementów tzw. *big data* w turystyce[22].

Centralny Wykaz Obiektów Hotelarskich (CWOH)

Centralny Wykaz Obiektów Hotelarskich prowadzony jest na podstawie ustawy. o usługach hotelarskich oraz usługach pilotów wycieczek i przewodników turystycznych[23]. Marszałkowie województw są zobowiązani do przekazywania informacji w formie elektronicznej dotyczącej skategoryzowanych w województwie obiektów hotelarskich. Te informacje są publikowane w Centralnym Wykazie Obiektów Hotelarskich.

---

20 T. Studzieniecki, A. Wołoszyk, *Statystyka publiczna jako narzędzie badawcze turystyki na obszarach transgranicznych w Polsce*, „Folia Turirstica" 2016, nr 38, s. 81-111.

21 A. Zajadacz, *Ruch turystyczny w ujęciu statystycznym*, [w:] *Uwarunkowania i plany rozwoju turystyki, Zasoby Antropogeniczne. Krajobraz. Ruch turystyczny*, t. II, Z. Młynarczyk., A. Zajadacz (red), Poznań 2008, s. 211-244.

22 K. Racka., *Big Data – znaczenie, zastosowania i rozwiązania technologiczne*, „Zeszyty Naukowe PWSZ w Płocku Nauki Ekonomiczne" 2016, t. XXIII, s. 11-323.

23 Ustawa z dnia 29 sierpnia 1997 r. o usługach hotelarskich oraz usługach pilotów wycieczek i przewodników turystycznych (tj. Dz. U. z 2023 r. poz. 1944).

Centralny Wykaz Organizatorów Szkoleń dla Kandydatów na Przewodników Górskich

Zgodnie z art. 24 ustawy o usługach hotelarskich oraz usługach pilotów wycieczek i przewodników turystycznych, wykonywanie działalności w zakresie szkolenia dla kandydatów na przewodników górskich wymaga uzyskania wpisu do rejestru organizatorów szkoleń dla kandydatów na przewodników górskich, prowadzonego przez marszałka województwa. Wpisu do rejestru organizatorów szkoleń marszałek województwa dokonuje się na wniosek organizatora szkolenia. Na podstawie informacji o dokonanych wpisach do rejestru organizatorów szkoleń przekazywanych w postaci elektronicznej przez marszałków województw, na stronie internetowej ministra właściwego do spraw turystyki zamieszcza się Centralny Wykaz Organizatorów Szkoleń dla Kandydatów na Przewodników Górskich.

Centralny Wykaz Przewodników Górskich

Zgodnie z art. 28 ustawy o usługach hotelarskich oraz usługach pilotów wycieczek i przewodników turystycznych, ewidencje uprawnień przewodników górskich prowadzą marszałkowie województw. Nadanie uprawnień przewodnika górskiego dokumentuje się przez wydanie legitymacji i identyfikatora przewodnika górskiego. W trakcie wykonywania zadań przewodnik górski jest obowiązany do posiadania przy sobie legitymacji przewodnika górskiego oraz do okazywania jej na żądanie osoby upoważnionej do wykonywania kontroli. Na podstawie danych o nadanych uprawnieniach przewodnika górskiego przekazywanych w postaci elektronicznej przez marszałków województw na stronie internetowej ministra właściwego do spraw turystyki są udostępniane dane liczbowe dotyczące uprawnień nadanych przez poszczególnych marszałków województw. Dane te są jawne. Informacje o nadanych uprawnieniach przewodnika górskiego wpisywane i przekazywane w postaci elektronicznej przez marszałków województw ministrowi właściwemu do spraw turystyki są udostępniane przez ministra właściwego do spraw turystyki w postaci elektronicznej wszystkim marszałkom.

Centralna Ewidencja Organizatorów Turystyki i Przedsiębiorców Ułatwiających Nabywanie Powiązanych Usług Turystycznych

Od 1 lipca 2018 r. zasady funkcjonowania Turystycznego Funduszu Gwarancyjnego oraz warunki oferowania, sprzedaży i realizacji imprez turystycznych oraz powiązanych usług turystycznych określa ustawa z dnia 24 listopada 2017 roku o imprezach turystycznych i powiązanych usługach turystycznych[24] oraz akty

[24] Dz.U. z 2022 r. poz. 511 ze zm.

wykonawcze do tej ustawy[25]. Organem właściwym do prowadzenia rejestru organizatorów turystyki i przedsiębiorców ułatwiających nabywanie powiązanych usług turystycznych jest marszałek województwa właściwy ze względu na siedzibę przedsiębiorcy turystycznego lub adres zamieszkania przedsiębiorcy turystycznego będącego osobą fizyczną. Na podstawie informacji o dokonanych wpisach do rejestru przekazywanych w postaci elektronicznej przez marszałków województw minister właściwy do spraw turystyki na stronie internetowej obsługującego go urzędu udostępnia Ewidencję, którą prowadzi Ubezpieczeniowy Fundusz Gwarancyjny. Dzięki ewidencji obywatele mogą sprawdzić czy biuro podróży, z którym chcą podpisać umowę działa legalnie, na jaki obszar ma wykupione zabezpieczenie finansowe, jakiej wartości jest to zabezpieczenie finansowe oraz do kiedy organizator turystyki lub pośrednik posiada gwarancje. Ponadto na stronach ewidencji prowadzone są podstawowe statystyki dotyczące liczby organizatorów turystyki w podziale na typ oraz województwo, w którym zostało zarejestrowane.

Portale informacyjne

Dwoma głównymi portali informacyjnymi z zakresu turystyki są: portal Turystyka PLUS (turystyka.stat.gov.pl) prowadzony przez Główny Urząd Statystyczny oraz portal turystyka.gov.pl – w części poświęconej badaniom i komunikatom z badań, tam też udostępnia się Centralną Ewidencję Organizatorów Turystyki i Przedsiębiorców Ułatwiających Nabywanie Powiązanych Usług Turystycznych, dostępną na stronie ewidencja.ufg.pl.

Na portalach informacyjnych dostępne są dane pochodzące z badań statystycznych Statystyki Publicznej – badanie turystycznej bazy noclegowej – realizowane przez GUS oraz dwa badania z zakresu turystyki[26]. Pierwszym z nich jest badanie podróży nierezydentów do Polski. Jest to badanie, które daje informacje o charakterystyce pobytu przyjeżdżających do Polski (nierezydentów) według głównego celu przyjazdu, długości pobytu, formy organizacyjnej, rodzaju bazy noclegowej wykorzystywanej w Polsce, odwiedzanych województw i środka transportu wykorzystywanego podczas pobytu w Polsce. W wyniku badania opisana jest także charakterystyka przyjeżdżających z zagranicy według kraju stałego zamieszkania, płci i wieku, a także określany jest poziom wydatków[27] przyjeżdżających z zagranicy w Polsce według rodzaju kategorii z podziałem m.in. na zakwaterowanie, wyżywienie oraz zakupy. Określana jest również charakterystyka celów podróży, a także kraju stałego zamieszkania oraz szacowane są w wydatki[28] w związku z podróżą

[25] Rozporządzenie Ministra Sportu i Turystyki z dnia 1 marca 2018 r. w sprawie Centralnej Ewidencji Organizatorów Turystyki i Przedsiębiorców Ułatwiających Nabywanie Powiązanych Usług Turystycznych.

[26] A. Żurawicz A., *Działalność Rady Statystyki w I półroczu 2014 r.*„Wiadomości Statystyczne" 2014, nr 59, s. 56-63

[27] R. Kubiak, *Prawo dewizowe*, Warszawa 2004, s. 20-102.

[28] P. Sitek, *Ustrojowe wyzwania Polski przed przystąpieniem do unii walutowej w kontekście niezależności Narodowego Banku Polskiego*, „Przegląd Prawa Konstytucyjnego" 2023, nr 6, s. 213-228.

poniesione w kraju stałego zamieszkania. Opisana jest również charakterystyka wyjazdów odwiedzających jednodniowych przyjeżdzających do Polski mając na uwadze główny cel przyjazdu wraz z charakterystyką odwiedzających jednodniowych przybywających do Polski według kraju stałego zamieszkania.

Drugie badanie dotyczące uczestnictwa mieszkańców Polski w podróżach jest badaniem ankietowym na ogólnopolskiej reprezentatywnej próbie osób w wieku 15 i więcej lat. Badania będą realizowane cztery razy w roku na próbie o założonej minimalnej wielkości 4 tysięcy osób. Badanie dotyczy krajowych i zagranicznych turystycznych wyjazdów Polaków w ciągu kwartału poprzedzającego badanie. Przedmiotem analizy są wyjazdy krajowe i zagraniczne w zakresie: celów i form organizacyjnych wyjazdów, rodzaju wykorzystanych środków transportu i bazy noclegowej, czasu trwania wyjazdu, odwiedzanych województw (w przypadku wyjazdów krajowych) i krajów (w przypadku wyjazdów zagranicznych), poniesionych wydatków[29], cech społeczno-demograficznych badanych. Badania realizowane za pomocą ankiety w celu stałego monitorowania krajowych i zagranicznych wyjazdów mieszkańców Polski roku. Te dwa badania są finansowane przez Ministerstwo Sportu i Turystyki oraz Narodowy Bank Polski.

Bezpieczeństwo rejestrów w turystyce

Zasady i standardy zabezpieczenia rejestrów państwowych obejmują określone wymogi technologiczne i organizacyjne, które mają na celu zapewnienie bezpieczeństwa, integralności oraz poufności danych przechowywanych w tych rejestrach[30]. W Polsce szczegóły tych zasad zawarte są w dokumentach Ministerstwa Cyfryzacji, regulacjach prawnych takich jak Krajowe Ramy Interoperacyjności oraz normach branżowych.

Standardy technologiczne Systemu Rejestrów:

- obejmują protokoły wymiany danych, struktury tych danych oraz zasady integracji z podmiotami zewnętrznymi;
- bezpieczeństwo realizowane jest poprzez mechanizmy uwierzytelnienia, identyfikacji użytkownika, autoryzacji, audytu oraz nadawania odpowiednich uprawnień;
- system zapewnia poufność, integralność i dostępność danych, w tym szyfrowanie komunikacji i kontrolę dostępu;
- architektura systemu składa się z warstwy prezentacji danych (GUI), logiki biznesowej i warstwy danych.

[29] D. Borek., M. Bugajska, S. Raniszewski., *Innovative trends in health tourism – medical, legal and organizational aspects,* "Scientific Papers of Silesian University of Technology Organization and Management Series" 2023, no 172, s. 25-40.

[30] M. Kachniewska, *Tourism value added creation through a user-centric context-aware digital system,* " "Economic Problems of Tourism" 2014, nr 4 (28), s. 103-118; M. Kachniewska, *Big Data Analysis as the tool for predictive intelligence and experience personalization in tourism,* "Przedsiębiorczość i Zarządzanie" 2019, t. 20, z. 2, cz. 2, s. 35-54.

Do głównych zasad zabezpieczania rejestrów należą:

- nadawanie ról i uprawnień użytkownikom;
- audytowanie działań w systemie celem wykrywania i zapobiegania nieautoryzowanym działaniom;
- szyfrowanie transmisji danych zapewniające poufność;
- zapewnienie integralności i dostępności danych przez odpowiednie mechanizmy technologiczne w tym redundancje i backup. Zapewnienie integralności i dostępności danych w rejestrach państwowych jest realizowane za pomocą zaawansowanych mechanizmów technologicznych i organizacyjnych.

Mechanizmy zapewnienia integralności danych

Integralność danych chroniona jest przez stosowanie certyfikatów, które umożliwiają weryfikację autentyczności i nienaruszalności informacji. Systemy rejestrów wykorzystują mechanizmy kontroli dostępu, uwierzytelniania użytkowników oraz audytu wszystkich działań, co pozwala wykrywać i zapobiegać nieautoryzowanym zmianom. Dane przesyłane i przechowywane są z użyciem protokołów zabezpieczających takie jak TLS, które chronią przed manipulacją danych w trakcie transmisji.

Mechanizmy zapewnienia dostępności danych

Zapewnienie dostępności realizowane jest przez architektury systemów redundancji oraz mechanizmy wysokiej dostępności, które umożliwiają ciągłość działania rejestrów nawet w przypadku awarii. System objęty jest ochroną *Security Operations Center* (SOC) stosowane są procedury monitorowania systemów, zarządzania awariami oraz plany awaryjne (*disaster recovery*), które minimalizują ryzyko utraty dostępu do danych. Dane w rejestrach są udostępniane w sposób efektywny, poprzez usługi sieciowe, które spełniają standardy interoperacyjności i dostępności zgodnie z wymogami prawnymi i technicznymi. Specjaliści monitorują i doskonalą procedury oraz narzędzia, aby zapewnić ciągłość funkcjonowania i szybkie reagowanie na incydenty zagrażające dostępności danych. Normy i standardy dotyczące rejestrów państwowych w Polsce są określane przede wszystkim w dokumentach Ministerstwa Cyfryzacji i dotyczą zarówno aspektów technologicznych, jak i organizacyjnych funkcjonowania Systemu Rejestrów w Turystyce. Obejmują m.in. interoperacyjność, poufność, integralność, dostępność, stabilność, poprawność i kompletność danych. Nakładają obowiązek monitoringu jakości danych i systemu oraz prowadzenia archiwizacji danych i mechanizmów przywracania stanu po awarii.

Te normy i standardy zapewniają spójne, bezpieczne i efektywne funkcjonowanie rejestrów. Standardy ISO regulujące aspekty związane z systemami informatycznymi to przede wszystkim rodzina norm z serii ISO/IEC 27000, które dotyczą zarządzania bezpieczeństwem informacji (ISMS).

Kluczowe standardy ISO dla systemów informatycznych:

- ISO/IEC 27001 – to podstawowa i najbardziej znana norma dotycząca systemu zarządzania bezpieczeństwem informacji. Określa wymagania dotyczące ustanawiania, wdrażania, utrzymywania i ciągłego doskonalenia systemu, który pozwala chronić poufność, integralność i dostępność informacji w organizacji. Wdrożenie tej normy pomaga minimalizować ryzyko utraty danych i innych incydentów bezpieczeństwa;
- ISO/IEC 27002 – norma zawiera szczegółowe praktyczne wytyczne i najlepsze praktyki związane z bezpieczeństwem informacji, które wspierają wdrażanie wymagań ISO/IEC 27001;
- ISO/IEC 27005 – dotyczy zarządzania ryzykiem w obszarze bezpieczeństwa informacji, opisując metody i procesy oceny oraz minimalizacji ryzyka;
- ISO/IEC 27701 – rozszerzenie ISO 27001, które skupia się na systemie zarządzania ochroną prywatności informacji (*Privacy Information Management System*);
- ISO/IEC 27017 i ISO/IEC 27018 – wytyczne i standardy dotyczące bezpieczeństwa informacji w środowiskach chmurowych oraz ochrony danych osobowych przetwarzanych w chmurze;
- ISO/IEC 22301 – norma dotycząca zarządzania ciągłością działania, zapewniająca mechanizmy utrzymania dostępności krytycznych systemów informatycznych podczas zakłóceń.

Normy te stanowią globalne ramy, które pomagają organizacjom chronić dane, zarządzać ryzykiem i zapewnić zgodność z regulacjami prawnymi oraz najlepszymi praktykami branżowymi w obszarze bezpieczeństwa systemów informatycznych[31].

Główne działania *Security Operations Center* (SOC) w zakresie ochrony rejestrów w turystyce to ciągłe monitorowanie, wykrywanie, analiza oraz reagowanie na zagrożenia bezpieczeństwa w infrastrukturze IT organizacji. SOC działa 24/7/365 i łączy ludzi, procesy oraz technologie, aby chronić systemy przed cyberatakami. Do kluczowych funkcji należą:

- ciągły monitoring sieci, systemów, aplikacji i urządzeń końcowych przy pomocy narzędzi takich jak SIEM, EDR i IDS/IPS;
- wykrywanie i analiza incydentów bezpieczeństwa w czasie rzeczywistym w celu szybkiego określenia ich charakteru, skali i wpływu na organizację;
- reakcja na incydenty cyberbezpieczeństwa, co obejmuje neutralizację zagrożeń i minimalizację skutków ataków;
- zarządzanie ryzykiem i wdrażanie działań prewencyjnych mających na celu zwiększenie odporności na przyszłe ataki;
- testowanie i wzmacnianie zabezpieczeń IT oraz integracja danych z zewnętrznych źródeł informacji o zagrożeniach (*threat intelligence*).

[31] M. Kachniewska M., *Tourism value added creation...*, op. cit., s. 103-118.

SOC pełni rolę centralnego centrum dowodzenia bezpieczeństwem cyfrowym firmy, zapewniając skuteczną ochronę i szybką reakcję na incydenty, co znacznie skraca czas wykrycia i ogranicza potencjalne szkody.

Funkcjonalności systemu

Udostępniono szereg e-usług A2A, A2C, A2B w celu ułatwienia składania wniosków i komunikacji z systemem, ponadto system wyposażono w API w celu umożliwienia zasilania zewnętrznych systemów w informacje zgromadzone w rejestrach.

API chronione jest przez dedykowany firewall aplikacyjny (WAF). Mając na uwadze jeden z głównych celów projektu, jakim jest udostępnienie materiałów informacji z rejestrów w turystyce w sieci możliwie szerokiemu gronu odbiorców i poprzez to realizację zapisów Dyrektywy Reuse (podstawowym założeniem dyrektywy jest udoskonalenie instytucji ponownego wykorzystywania informacji sektora publicznego z naciskiem na jej praktyczną technologiczną realizację) niezwykle ważne jest umiejętne serwowanie dokumentów w sieci z wykorzystaniem wszystkich dostępnych obecnie narzędzi.

Rejestr korzysta z semantycznego modelu udostępniania metadanych o obiektach hotelarskich z wykorzystanie RDF i *linkeddata*, oraz udostępnienie danych na zasadach usług przestrzennych zgodnych z standardami INSPIRE (wms).

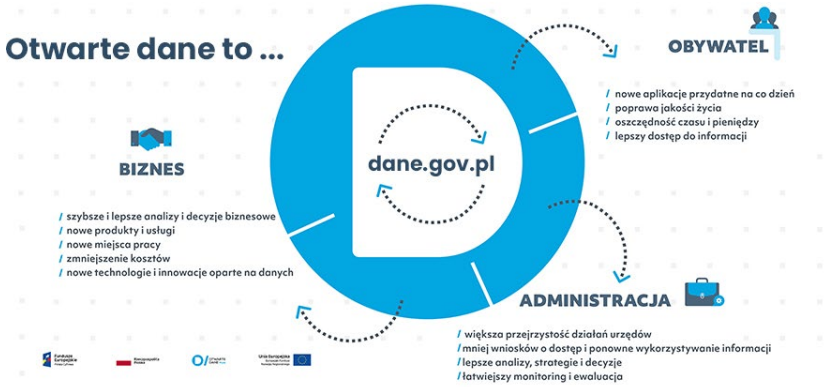
Rejestr korzysta z :

1) URI (*Uniform Resource Identifier*) jako jednego ze sposobów odróżnienia wybranych zasobów rejestrów;
2) protokołu HTTP do uzyskiwania informacji o zgromadzonych zasobach;
3) udostępnia informacje o zasobach identyfikowanych przez URI za pomocą standardów RDF - język RDF (*Resource Description Format*) /XML. Powyższa konwencja daje RDF zdolność do zdefiniowania obiektu poprzez wskazanie go w sieci;
4) wykorzystuje możliwości powiązania z innymi obiektami z innych baz i systemów z a pomocą URI, aby zapewnić możliwość eksploracji i wiązania informacji pomiędzy różnymi zbiorami informacji.

Mając na uwadze powyższy model prezentowanie przez system danych i dojścia do dokumentów online w ustrukturyzowanej formie opisanych metadanymi możliwymi do przetwarzania maszynowo z wykorzystaniem standardów RDF i SPARQL oraz linkami wychodzącymi do innych danych pozwala stwierdzić, że system będzie można skwalifikować na poziomie 5 gwiazdek w hierarchii modelu 5 Star Open Data model.

Publikacja zbioru danych na witrynie Dane publiczne - https://danepubliczne.gov.pl/, w formie usługi API i eksportu danych do formatu CSV.

Ryc. 1. Portal danych



Źródło: www.dane.gov.pl/pl.(dostęp: 29.09.2025 r.).

Zaawansowane narzędzia i algorytmy sztucznej inteligencji w oparciu o dane publiczne wspomagające wzrost gospodarczy w obszarze turystyki - grant badawczy na badania

W chwili obecnej Ministerstwo Sportu i Turystyki jest w trakcie realizacji konkursu razem z Narodowym Centrum Badań i Rozwoju w ramach INFOSTRATEG VIII (konkurs na projekty zamawiane przez Ministerstwo Sportu i Turystyki). Proces wyłaniana wykonawcy został ogłoszony. Program INFOSTRATEG został przygotowany, by wspierać rozwój polskiego potencjału sztucznej inteligencji poprzez opracowanie rozwiązań wykorzystujących sztuczną inteligencję. Sektor turystyczny chce wykorzystać to narzędzie do szacowania ruchu turystycznego oraz jego prognozowania. Do konkursu mogą przystąpić jednostki naukowe wyłącznie zarejestrowane i prowadzące działalność na terytorium Polski, a także przedsiębiorstwa – samodzielnie lub konsorcja, które mogą składać się z maksimum 3 podmiotów. Mogą być to również same jednostki naukowe albo same przedsiębiorstwa.

Konkurs został ogłoszony w sierpniu 2025 r., rozpoczęcie naboru nastąpiło we wrześniu 2025 r., koniec został zaplanowany na grudzień 2025 r., a rozstrzygnięcie maksymalnie w terminie do czerwca 2026 r.[32]

Celem realizacji projektu dotyczącego zaawansowanych narzędzi i algorytmów sztucznej inteligencji w oparciu o dane publiczne wspomagające wzrost gospodarczy w obszarze turystyki będzie opracowanie rozwiązania informatycznego, które będzie wspomagać monitorowanie ruchu turystycznego. Może to w przyszłości przyczynić się do stymulowania ruchu turystycznego w Polsce.

[32] www.gov.pl/web/ncbr/viii-konkurs-infostrateg-na-projekty-zamawiane (dostęp: 08.09.2025 r.).

Zakłada się, że system będzie wykorzystywać mechanizmy przetwarzania danych w czasie rzeczywistym, a także algorytmy sztucznej inteligencji. Ma to służyć powiązaniu danych z różnych źródeł, a także przyczynić się do prognozowania ruchu turystycznego. Dane będą pochodzić z odpowiednio dostoswanego rejestru obiektów hotelarskich, a także z systemów rezerwacyjnych, danych z sieci komórkowych oraz innych systemów administracji publicznej (dane z lotnisk, dane dot. ruchu na autostradach), a co najważniejsze system będzie korzystać z zanonimizowanych danych transakcji kartami płatniczymi. Istotność wykorzystywania danych z alternatywnych źródeł była wskazywana przez M. Kachniewską (2019).

Zakończenie

Turystka dysponuje bogatymi źródłami informacji statystycznej oraz informacji administracyjnej dostępnej dla obywateli. Na uwagę zasługuje możliwości sprawdzenia obiektów hotelarskich czy działają legalnie oraz ich kategorii i lokalizacji jak również możliwość sprawdzenia organizatorów i pośredników turystycznych wraz z informacją o wysokości zabezpieczenia finansowego na rzecz klientów. Dodatkowo branża turystyczna ma dostęp do statystyk dotyczących ruchu turystycznego, obłożenia hoteli oraz prognoz ruchu turystycznego. Planowane jest poszerzenie możliwości prognozowania danych oraz skrócenia okresu przetwarzania danych z zakresu ruchu turystycznego do momentu ich publikacji. Bardzo istotnym elementem utrzymania portali internetowych prezentujących dane i informacje z zakresu turystyki jest ich bezpieczeństwo[33]. Ataki cybernetyczne na struktury rządowe są coraz bardziej powszechne. Zapewnienie ciągłości ich funkcjonowania oraz jakości przetwarzania danych stanowi w dzisiejszych czasach priorytet. Istotne jest także upowszechnianie informacji dotyczących dostępności danych oraz ich atrakcyjne formy wizualnej (automatycznie generujące się mapy oraz wykresy).

Bibliografia:

Akty prawne

1) Ustawa z dnia 29 sierpnia 1997 r. o usługach hotelarskich oraz usługach pilotów wycieczek i przewodników turystycznych (t.j. Dz. U. z 2023 r. poz. 1944).
2) Ustawa z dnia 24 listopada 2017 roku o imprezach turystycznych i powiązanych usługach turystycznych (Dz.U. z 2022 r. poz. 511 ze zm.).
3) Rozporządzenie Ministra Sportu i Turystyki z dnia 1 marca 2018 r. w sprawie Centralnej Ewidencji Organizatorów Turystyki i Przedsiębiorców Ułatwiających Nabywanie Powiązanych Usług Turystycznych. (Dz.U. 2018 poz. 518).

[33] M. Kachniewska, *Internetowe platformy upowszechniania wiedzy jako narzędzie poprawy konkurencyjności przedsiębiorstw i regionów turystycznych*, [w:] *Zarządzanie wiedzą a efektywność gospodarki turystycznej*, M. Morawski (red), Wrocław 2012, s. 13-34.

4) Rozporządzenie Rady Ministrów z dnia 24 września 2024 r. w sprawie programu badań statystycznych statystyki publicznej na rok 2025 (Dz. U. poz. 1653).
5) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 692/2011 z dnia 6 lipca 2011 r. w sprawie europejskiej statystyki w dziedzinie turystyki i uchylające dyrektywę Rady 95/57/WE.

Literatura

1) Borek D., P*rzedsiębiorca w ustawie o imprezach turystycznych i powiązanych usługach turystycznych – koncepcja przedmiotowego charakteru regulacji*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny UW" 2018, nr 4(7).
2) Borek D., *The decision of the European Commission State Aid SA. 101979 (2022/N) - a word of commentary, opinion and conclusions*, „Zeszyty Naukowe Wyższej Szkoły Gospodarki - Turystyka i Rekreacja" 2021, nr 16.
3) Borek D., Bugajska M., Raniszewski S., *Innovative trends in health tourism – medical, legal and organizational aspects*, "Scientific papers of Silesian University of Technology Organization and Management Series" 2023, no 172.
4) Borek D., Świtaj K., Zawistowska H., *O zgodności z prawem UE regulacji art. 15k ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19*, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw, [w:] *Prawo – narzędzie sprawiedliwości czy władzy*, I. Barwicka-Tylek, P. Dziewałtowski-Gintowt, K. Zyzik, L. Łyżwa (red.), Kraków 2020.
5) Kachniewska M, *Big Data Analysis as the tool for predictive intelligence and experience personalization in tourism*, „Przedsiębiorczość i Zarządzanie" 2019, t. 20, z. 2, cz. 2.
6) Kachniewska M., *Internetowe platformy upowszechniania wiedzy jako narzędzie poprawy konkurencyjności przedsiębiorstw i regionów turystycznych*, [w:] *Zarządzanie wiedzą a efektywność gospodarki turystycznej*, M. Morawski (red.), Wrocław 2012.
7) Kachniewska M., *Tourism value added creation through a user-centric context-aware digital system,* "Economic Problems of Tourism" 2014, nr 4 (28).
8) Kubiak R., *Prawo dewizowe*, Warszawa 2004.
9) Makowicz B., *Compliance w Przedsiębiorstwie*, Warszawa 2011.
10) Racka K., *Big Data – znaczenie, zastosowania i rozwiązania technologiczne,* „Zeszyty Naukowe PWSZ w Płocku Nauki Ekonomiczne" 2016, t. XXIII.
11) Sitek P., *Ustrojowe wyzwania Polski przed przystąpieniem do unii walutowej w kontekście niezależności Narodowego Banku Polskiego*, „Przegląd Prawa Konstytucyjnego" 2023, nr 6.
12) Studzieniecki T., Wołoszyk A., *Statystyka publiczna jako narzędzie badawcze turystyki na obszarach transgranicznych w Polsce*, „Folia Turirstica" 2016, nr 38.

13) Zajadacz A., *Ruch turystyczny w ujęciu statystycznym*, [w:] *Uwarunkowania i plany rozwoju turystyki. Zasoby Antropogeniczne. Krajobraz. Ruch turystyczny*, t. II, Z. Młynarczyk, A. Zajadacz, Poznań 2008.
14) Żurawicz A., *Działalność Rady Statystyki w I półroczu 2014 r.*, „Wiadomości Statystyczne" 2014, nr 59.

Inne źródła

1) www.dane.gov.pl/pl (dostęp: 29.09.2025 r.).
2) www.ewidencja.ufg.pl/ewidencja/obywatel/wyszukiwanie (dostęp: 29.09.2025 r.).
3) www.gov.pl/web/ncbr/viii-konkurs-infostrateg-na-projekty-zamawiane (dostęp: 08.09.2025 r.).
4) www.turystyka.gov.pl (dostęp: 08.09.2025 r.).
5) www.turystyka.stat.gov.pl (dostęp: 08.09.2025 r.).

dr hab. Dominika Cendrowicz, prof. UWr
Uniwersytet Wrocławski
adres e-mail: dominika.cendrowicz@uwr.edu.pl
ORCID: 0000-0002-2358-7188

Rola i zadania gminy w systemie zarządzania kryzysowego i cyberbezpieczeństwa

The role and tasks of the municipality in crisis management and cybersecurity system

Streszczenie

Celem publikacji jest analiza zadań gminy w zakresie zarządzania kryzysowego i cyberbezpieczeństwa, ocena rozwiązań prawnych regulujących te obszary oraz przedstawienie propozycji de lege ferenda. Rozdział podejmuje próbę wykazania, że skuteczność działań podejmowanych przez gminę w zakresie ochrony bezpieczeństwa publicznego wymaga łączenia tradycyjnych podejść z nowoczesnymi narzędziami, zapewniającymi odporność na zagrożenia pojawiające się w cyberprzestrzeni.

Wstęp

Bez względu na epokę, w której funkcjonowała administracja publiczna, oraz niezależnie od ustroju państwa, do kluczowych jej zadań należało i nadal należy zapewnienie bezpieczeństwa, utrzymanie ładu społecznego i gospodarczego oraz ochrona przed zagrożeniami zewnętrznymi[34]. Bezpieczeństwo stanowi jedną z najważniejszych wartości zarówno dla jednostek, jak i dla administracji oraz państwa, a także jest podstawowym warunkiem rozwoju cywilizacyjnego i aktywności społecznej. Współcześnie jednak zakres i charakter zagrożeń uległy znacznemu poszerzeniu, co wynika zarówno z postępu technologicznego, jak i procesów globalizacyjnych[35].

Oprócz tradycyjnych zagrożeń, takich jak katastrofy naturalne, awarie techniczne czy skażenia środowiska, coraz większe znaczenie zyskują zagrożenia o charakterze cybernetycznym. Współczesne cyberataki mogą paraliżować funkcjonowanie usług publicznych, zakłócać pracę systemów infrastruktury krytycznej, prowadzić

[34] A. Błaś, *Zadania administracji publicznej* [w:] *Nauka administracji*, J. Boć (red.), Wrocław 2013, s. 131.

[35] B. Stefaniuk, *Bezpieczeństwo a zarządzanie kryzysowe* [w] *Oblicza i wyzwania obronności w XXI wieku*, A. Polak, A. Smarzewska, P. Borek (red.), Biała Podlaska 2015, s. 158.

do utraty danych wrażliwych, a także wywoływać dezinformację na dużą skalę. Z tego względu cyberbezpieczeństwo stało się istotnym elementem bezpieczeństwa państwa i pozostaje ściśle powiązane z problematyką zarządzania kryzysowego. Cyberprzestrzeń stanowi nową domenę aktywności, w której zagrożenia są niewidzialne, trudne do wykrycia i mają dynamiczny charakter, co wymaga od administracji publicznej nie tylko dostosowania metod działania, lecz również rozwijania struktur odpowiedzialnych za szybkie i skuteczne reagowanie[36].

Pojęcie zarządzania kryzysowego i cyberbezpieczeństwa – analiza i relacje między pojęciami

Zagadnienia związane z zarządzaniem kryzysowym są uregulowane w ustawie o zarządzaniu kryzysowym[37]. Zarządzanie kryzysowe obejmuje opracowywanie planów i programów określających strategie zapobiegania kryzysom, reagowania na nie, minimalizowania skutków oraz odbudowy kluczowej infrastruktury i zasobów krytycznych[38]. Działania te mają charakter prewencyjny, organizacyjny i regulacyjny, a ich zakres powinien być dostosowany do rozwoju sytuacji wynikającej z zagrożeń[39]. Definicja legalna zarządzania kryzysowego zawarta jest w art. 2 u.z.k. i brzmi następująco: „Zarządzanie kryzysowe to działalność organów administracji publicznej będąca elementem kierowania bezpieczeństwem narodowym, która polega na zapobieganiu sytuacjom kryzysowym, przygotowaniu do przejmowania nad nimi kontroli w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia sytuacji kryzysowych, usuwaniu ich skutków oraz odtwarzaniu zasobów i infrastruktury krytycznej."

Z powyższym pojęciem wiąże się pojęcie sytuacji kryzysowej, które zgodnie z definicją zawartą w art. 3 ust. 1 u.z.k. oznacza sytuację „wpływającą negatywnie na poziom bezpieczeństwa ludzi, mienia w znacznych rozmiarach lub środowiska, wywołującą znaczne ograniczenia w działaniu właściwych organów administracji publicznej ze względu na nieadekwatność posiadanych sił i środków". Sytuacja kryzysowa może nie tylko poprzedzać nadejście kryzysu, ale może również wystąpić po jego zakończeniu, podczas gdy sam kryzys jest jednym z elementów sytuacji kryzysowej[40].

---

36 A. Brzostek, *Cyberbezpieczeństwo w administracji publicznej - aspekty prawne*, „Zeszyty Prawnicze" 2023, nr 3, s. 4-5 .

37 Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz. U. z 2023 r. poz. 122 z późn. zm.), dalej: u.z.k.

38 Wyrok Wojewódzkiego Sądu Administracyjnego w Gdańsku z dnia 28 listopada 2012 r., sygn. akt I SA/Gd 1171/12, LEX nr 1247413.

39 K. Płonka-Bielenin, *Inkorporacja prawa w zakresie zarządzania kryzysowego w samorządzie terytorialnym – wnioski i postulaty*, „Samorząd Terytorialny" 2021, nr 3, s. 56.

40 M. Wilińska, *Zarządzanie kryzysowe w systemie bezpieczeństwa państwa*, „Obronność. Zeszyty Naukowe" 2015, nr 3(15), s. 129.

Zarządzanie kryzysowe pełni funkcję uzupełniającą wobec konstytucyjnych mechanizmów dotyczących stanów nadzwyczajnych[41]. Do problematyki stanów nadzwyczajnych nawiązuje Konstytucja Rzeczypospolitej Polskiej[42], zgodnie z którą w sytuacjach szczególnych zagrożeń, jeżeli zwykłe środki konstytucyjne są niewystarczające, może zostać wprowadzony odpowiedni stan nadzwyczajny, tj. stan wojenny, stan wyjątkowy lub stan klęski żywiołowej (art. 228 ust. 1 Konstytucji RP). Zarządzania kryzysowego nie należy jednak utożsamiać ze stanami nadzwyczajnymi, ponieważ stosuje się je w sytuacjach, gdy zagrożenie nie wymaga wprowadzenia stanu nadzwyczajnego, a dostępne środki pozwalają na zapewnienie bezpieczeństwa[43].

Jednocześnie w kontekście współczesnych wyzwań bezpieczeństwa państwa szczególnego znaczenia nabiera pojęcie cyberbezpieczeństwa, które obecnie stanowi jedno z kluczowych obszarów ochrony interesu publicznego. Podstawowym aktem prawnym regulującym funkcjonowanie krajowego systemu cyberbezpieczeństwa jest ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[44]. Ustawa ta stanowi implementację pierwszej unijnej dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych, tzw. dyrektywy NIS z 2016 r.[45] Z kolei wejście w życie nowej dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 powoduje konieczność dostosowania krajowych regulacji do szerszych, bardziej szczegółowych i zaostrzonych wymogów unijnych[46].

Należy podkreślić, że zgodnie z art. 2 pkt 4 u.k.s.c. cyberbezpieczeństwo jest rozumiane jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych oraz usług świadczonych przez te systemy.

Z cyberbezpieczeństwem ściśle wiąże się pojęcie zagrożenia cyberbezpieczeństwa, które oznacza potencjalną przyczynę wystąpienia incydentu wpływającego

41 K. Kostur, *Zarządzanie kryzysowe w gminie - wybrane zagadnienia*, „Roczniki Administracji i Prawa" 2020, nr 2, s. 157.

42 Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78 poz. 483 z późn. zm.), dalej: Konstytucja RP.

43 B. Opaliński, *Rozdzielenie kompetencji władzy wykonawczej między Prezydenta RP oraz Radę Ministrów na tle Konstytucji Rzeczypospolitej Polskiej z 1997 roku*, Warszawa 2012, LEX/el.

44 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077 z późn. zm.), dalej: u.k.s.c. W kontekście administracji publicznej należy jednak pamiętać także o ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2025 r. poz. 1703 z późn. zm.).

45 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 (Dz. U. UE. L. z 2016 r. Nr 194, str. 1).

46 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, str. 80 z późn. zm.), dalej: dyrektywa NIS 2.

negatywnie na funkcjonowanie systemów informacyjnych[47]. Pojęcie incydentu zgodnie z art. 4 pkt 5 u.k.s.c. oznacza zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo. Z kolei w rozumieniu art. 6 pkt 2 dyrektywy NIS 2 oznacza ono „zdarzenie naruszające dostępność, autentyczność, integralność lub poufność przechowywanych, przekazywanych lub przetwarzanych danych lub usług oferowanych przez sieci i systemy informatyczne lub dostępnych za ich pośrednictwem". W u.k.s.c. wymieniono następujące rodzaje incydentów: incydent krytyczny (art. 4 pkt 6 u.k.s.c.), incydent poważny (art. 4 pkt 7 u.k.s.c.), incydent istotny (art. 4 pkt 8 u.k.s.c.) oraz incydent w podmiocie publicznym (art. 4 pkt 9 u.k.s.c.). Od pojęcia incydentu należy odróżniać pojęcie ryzyka, które zgodnie z art. 4 pkt 12 u.k.s.c. oznacza kombinację prawdopodobieństwa wystąpienia zdarzenia niepożądanego i jego konsekwencji.

W kontekście analizy powyższych pojęć warto zauważyć, że w sytuacji, gdy incydent cyberbezpieczeństwa powoduje dezorganizację usług publicznych, zakłócenia w dostępie do zasobów lub naruszenie integralności infrastruktury, może dojść do powstania sytuacji kryzysowej w rozumieniu zarządzania kryzysowego. W takich przypadkach uruchamiane mogą być procedury właściwe dla zarządzania kryzysowego[48].

Gmina w systemie organów i podmiotów odpowiedzialnych za realizację zadań w zakresie zarządzania kryzysowego i cyberbezpieczeństwa

System zarządzania kryzysowego w Polsce został skonstruowany tak, aby w obliczu konkretnego zagrożenia pierwsze działania podejmowały służby funkcjonujące na szczeblu właściwym do jego eliminacji[49]. Podmiotem sprawującym zarządzanie kryzysowe na terenie kraju jest Rada Ministrów, a w przypadkach niecierpiących zwłoki jest to minister właściwy do spraw wewnętrznych. Decyzje podjęte przez ministra podlegają rozpatrzeniu na najbliższym posiedzeniu Rady Ministrów (art. 7 ust. 1-3 u.z.k.). Przy Radzie Ministrów działa organ opiniodawczo-doradczy, jakim jest Rządowy Zespół Zarządzania Kryzysowego. Co istotne, w jego skład wchodzi Pełnomocnik Rządu ds. Cyberbezpieczeństwa. Na szczeblu centralnym tworzy się Rządowe Centrum Bezpieczeństwa, które jest państwową jednostką budżetową podległą Prezesowi Rady Ministrów (art. 10 ust. 1 u.z.k.).

Z kolei na terenie województwa organem właściwym w zakresie zarządzania kryzysowego jest wojewoda (art. 14 ust. 1 u.z.k.). Organem pomocniczym wojewody w zapewnieniu wykonywania zadań z tego obszaru jest wojewódzki zespół zarządzania

[47] Zob. art. 2 pkt 4 i 5 u.k.s.c.

[48] M. Karpiuk, *Crisis management vs. cyber threats*, „Sicurezza, Terrorismo e Societa" 2022, nr 2, s. 122.

[49] *Współpraca z jednostkami publicznymi* [w:] *Księga dobrych praktyk w zakresie zarządzania ciągłością działania*,. R. Kaszubski, D. Romańczuk (red.), Warszawa 2011, s. 150.

kryzysowego, powoływany przez wojewodę, który określa jego skład, organizację, siedzibę oraz tryb pracy (art. 14 ust. 7 u.z.k.). Wojewoda realizuje zadania z zakresu zarządzania kryzysowego we współpracy z innymi organami administracji publicznej (art. 14 ust. 1 i 5 u.z.k.). W województwach tworzy się wojewódzkie centra zarządzania kryzysowego, których obsługę zapewniają komórki organizacyjne, właściwe w sprawach zarządzania kryzysowego, wyodrębnione w urzędach wojewódzkich (art. 14 ust. 6 u.z.k.).

W systemie zarządzania kryzysowego uczestniczą również jednostki samorządu terytorialnego (dalej: JST). Zadania samorządu województwa polegają na udziale zarządu województwa w realizacji działań z tego obszaru, w tym w planowaniu cywilnym, w zakresie wynikającym z jego kompetencji (art. 15 u.z.k.). Na obszarze powiatu organem właściwym w sprawach zarządzania kryzysowego jest starosta, który nałożone na niego zadania wykonuje przy pomocy powiatowej administracji zespolonej i jednostek organizacyjnych powiatu (art. 17 ust. 1 i 3 u.z.k.). W powiatach funkcjonują powiatowe zespoły zarządzania kryzysowego, a także tworzy się powiatowe centra zarządzania kryzysowego. W miejscowościach będących jednocześnie siedzibami powiatów i miast na prawach powiatu, na podstawie porozumienia zawartego między tymi JST, może być tworzone wspólne centrum zarządzania kryzysowego obejmujące zasięgiem działania obszar obu jednostek samorządu terytorialnego (art. 18 ust. 4 u.z.k.)[50]. Z kolei w gminie w myśl zasady jednoosobowego kierownictwa zarządzanie kryzysowe realizowane jest przez wójta (burmistrza, prezydenta miasta)[51], a jego organem pomocniczym w zapewnieniu wykonywania omawianej kategorii zadań jest gminny zespół zarządzania kryzysowego (art. 19 ust. 4 u.z.k.). W gminie może ponadto zostać utworzone gminne centrum zarządzania kryzysowego (GCZK).

Struktura zarządzania kryzysowego w Polsce obejmuje zatem różne podmioty administracji publicznej działające na szczeblu centralnym, wojewódzkim, powiatowym i gminnym. Ich współdziałanie pozwala na skoordynowane zapobieganie zagrożeniom, reagowanie w sytuacjach kryzysowych oraz ograniczanie skutków tych zdarzeń, zapewniając spójność działań w całym kraju.

Równolegle do systemu zarządzania kryzysowego funkcjonuje krajowy system cyberbezpieczeństwa, którego ramy organizacyjne oraz zadania i obowiązki podmiotów wchodzących w jego skład określa u.k.s.c. Kluczową rolę w zakresie cyberbezpieczeństwa pełni minister właściwy do spraw informatyzacji, którego zadania zostały określone w rozdziale u.k.s.c. Rozdział 10 ustawy został poświęcony zadaniom ministra do spraw obrony narodowej, co podkreśla znaczenie

[50] A. Mituś, *Zarządzanie kryzysowe w Polsce – reguły, mechanizmy, efektywność* [w:] *Przywództwo w administracji publicznej. Perspektywa zarządzania kryzysowego*, K. Baran, S. Mazur (red.), Warszawa 2022, s. 74.

[51] M. Żmigrodzki, *Zarządzanie kryzysowe w państwie*, Warszawa 2012, s. 105.

cyberbezpieczeństwa także w wymiarze obronnym. Zgodnie z art. 4 u.k.s.c. krajowy system cyberbezpieczeństwa obejmuje aż 20 różnych podmiotów[52]. Są to: 1) operatorzy usług kluczowych; 2) dostawcy usług cyfrowych; 3) CSIRT MON[53]; 4) CSIRT NASK[54]; 5) CSIRT GOV[55]; 6) sektorowe zespoły cyberbezpieczeństwa; 7) jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1–6, 8, 9, 11 i 12 ustawy z 27.08.2009 r. o finansach publicznych[56]; 8) instytuty badawcze; 9) Narodowy Bank Polski; 10) Bank Gospodarstwa Krajowego; 11) Urząd Dozoru Technicznego; 12) Polska Agencja Żeglugi Powietrznej; 13) Polskie Centrum Akredytacji; 14) Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej; 15) spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy z 20.12.1996 r. o gospodarce komunalnej[57]; 16) podmioty świadczące usługi z zakresu cyberbezpieczeństwa; 17) organy właściwe do spraw cyberbezpieczeństwa; 18) Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa; 19) Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa; 20) Kolegium do Spraw Cyberbezpieczeństwa.

Włączenie tak szerokiego katalogu podmiotów publicznych do systemu cyberbezpieczeństwa wynikało z potrzeby zbudowania kompleksowego, wielowymiarowego modelu zapewnienia cyberbezpieczeństwa państwa, a nie jedynie z obowiązku implementacji dyrektywy NIS[58]. Jeżeli chodzi o miejsce gminy w systemie tych podmiotów, należy podkreślić, że w pojęciu określonym w art. 4 pkt 7 u.k.s.c. mieszczą się JST i ich związki, związki metropolitalne, jednostki budżetowe oraz zakłady budżetowe. Obejmuje to zatem również gminy i ich jednostki organizacyjne. Jako podmioty realizujące zadania publiczne zależne od systemów informacyjnych są one zobowiązane do wypełniania obowiązków określonych w ustawie o krajowym systemie cyberbezpieczeństwa, w szczególności tych wynikających z rozdziału 5 u.k.s.c. Aby dany podmiot podlegał przepisom u.k.s.c., powinien on spełniać nie tylko kryterium przynależności do systemu, ale także kryterium w postaci wykonywania zadań publicznych zależnych od systemu informacyjnego[59]. Pojęcie systemu

52 G. Szpor [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, K. Czaplicki, A. Gryszczyńska (red.), Warszawa 2019, art. 4, Lex/el.

53 Jest to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej.

54 Jest to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy.

55 Jest to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego.

56 Ustawa z dnia 27 sierpnia2009 r. o finansach publicznych (t.j. Dz. U. z 2025 r. poz. 1483).

57 Ustawa z dnia 20 grudnia1996 r. o gospodarce komunalnej (t.j. Dz. U. z 2021 r. poz. 679).

58 K. Czaplicki [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, A. Gryszczyńska, G. Szpor (red.), Warszawa 2019, art. 21, Lex/el.

59 *Ibidem.*

informacyjnego należy rozumieć zgodnie z art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne. Należy uznać, że praktycznie wszystkie JST realizują zadania zależne od tego rodzaju systemów[60].

Omawiając powyższe kwestie, warto wskazać, że rozwój cyfryzacji życia publicznego oraz narastająca skala cyberzagrożeń sprawiają, że aktywność legislacyjna w tej dziedzinie obejmuje zarówno poziom krajowy, jak i unijny, w szczególności w zakresie ochrony infrastruktury krytycznej i systemów istotnych dla bezpieczeństwa państwa[61]. Należy zatem odnotować, że już prawodawca unijny w art. 9 ust. 1 dyrektywy NIS 2 zobowiązał państwa członkowskie do wyznaczenia lub ustanowienia co najmniej jednego organu odpowiedzialnego za zarządzanie incydentami i zarządzanie kryzysowe w cyberbezpieczeństwie na dużą skalę. Obowiązkiem państw członkowskich jest zapewnienie spójności z istniejącymi ogólnymi krajowymi ramami zarządzania kryzysowego[62].

Zadania gminy w zakresie zarządzania kryzysowego i cyberbezpieczeństwa

W zakresie zadań gminy związanych z zarządzaniem kryzysowym należy wskazać, że zgodnie z art. 166 ust. 1 Konstytucji RP jednostki samorządu terytorialnego realizują zadania publiczne służące zaspokajaniu potrzeb wspólnoty lokalnej jako zadania własne. Artykuł 7 ust. 1 ustawy o samorządzie gminnym[63] stanowi, że zaspokajanie zbiorowych potrzeb wspólnoty należy do zadań własnych gminy, a zgodnie z art. 6 ust. 1 u.s.g. obejmują one wszystkie sprawy publiczne o znaczeniu lokalnym, które nie zostały zastrzeżone dla innych podmiotów. Zadania gminy nie mają jednolitego charakteru prawnego i dzielą się na zadania własne obligatoryjne i fakultatywne oraz zlecone gminie z zakresu administracji rządowej lub powierzane w drodze porozumień[64]. Szczególnie istotne jest, że zgodnie z art. 7 ust. 1 pkt 14 u.s.g. do zadań własnych gminy należy zapewnienie porządku publicznego i bezpieczeństwa obywateli, co obejmuje również działania z zakresu ochrony przeciwpożarowej i przeciwpowodziowej[65]. W odniesieniu do zarządzania kryzysowego podstawę prawną stanowi u.z.k., a w odniesieniu do cyberbezpieczeństwa jest to u.k.s.c.

Organem administracji publicznej właściwym w zakresie zarządzania kryzysowego w gminie jest wójt[66]. Do jego zadań należy kierowanie monitorowaniem, plano-

60 W.Z. Dziomdziora, *Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik*, Warszawa 2021, Lex/el.

61 D. Skoczylas, *Wzmocnienie zdolności Unii Europejskiej w zakresie cyberbezpieczeństwa – cybersolidarność w kontekście cyberzagrożeń*, „Europejski Przegląd Sądowy" 2024, nr 12, s. 42-43.

62 Zob. art. 9 ust. 1 dyrektywy NIS 2.

63 Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2025 r. poz. 1153), dalej: u.s.g.

64 P. Dobosz [w:] *Ustawa o samorządzie gminnym*, P. Chmielnicki (red.), Warszawa 2022, art. 7, LEX/el.

65 *Ibidem.*

66 Zob. art. 19 ust. 1 u.z.k.

waniem, reagowaniem i usuwaniem skutków zagrożeń; realizacja zadań z zakresu planowania cywilnego, w tym zaleceń do gminnego planu zarządzania kryzysowego; jak również opracowywanie i przedkładanie staroście do zatwierdzenia gminnego planu zarządzania kryzysowego. Ponadto wójt odpowiada za organizację i prowadzenie szkoleń, ćwiczeń i treningów z zakresu zarządzania kryzysowego; realizację przedsięwzięć wynikających z planu operacyjnego funkcjonowania gmin i gmin o statusie miasta; czy zapobieganie, przeciwdziałanie i usuwanie skutków zdarzeń o charakterze terrorystycznym. Do jego zadań należy również współdziałanie z Szefem Agencji Bezpieczeństwa Wewnętrznego w zakresie przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym oraz organizowanie i realizacja zadań ochrony infrastruktury krytycznej[67]. Wskazane zadania wójt realizuje przy wsparciu komórki organizacyjnej urzędu gminy odpowiedzialnej za zarządzanie kryzysowe. Organem pomocniczym wójta w zakresie realizacji zadań z obszaru zarządzania kryzysowego jest natomiast gminny zespół zarządzania kryzysowego[68]. Skład zespołu nie jest ograniczony przez ustawodawcę, a decyzję o liczbie jego członków podejmuje wójt, który powinien kształtować strukturę zespołu, biorąc pod uwagę lokalne uwarunkowania i dążąc do efektywnego działania[69]. Stosownie do art. 20 ust. 1 u.z.k., do zadań wójta należy również zapewnienie realizacji na terenie gminy całodobowego alarmowania członków zespołu zarządzania kryzysowego i dyżurów w sytuacjach kryzysowych. Wójt powinien współdziałać z centrami zarządzania kryzysowego administracji publicznej oraz sprawować nadzór nad systemami wykrywania, alarmowania i wczesnego ostrzegania ludności. Do jego zadań należy też współpraca z podmiotami prowadzącymi monitoring środowiska oraz realizacja zadań związanych z podwyższaniem gotowości obronnej państwa. W tym celu wójt może tworzyć gminne (miejskie) centra zarządzania kryzysowego. Z uwagi na to, że decyzja o ich utworzeniu leży w dyspozycji wójta, powoduje to, że w praktyce tego rodzaju centrum może nie funkcjonować w każdej gminie[70]

Zgodnie z art. 40 ust. 1 u.s.g., gminie przysługuje prawo stanowienia aktów prawa miejscowego obowiązujących na obszarze gminy. Z kolei stosownie do art. 40 ust. 3 u.s.g., w zakresie nieuregulowanym w odrębnych ustawach lub innych powszechnie obowiązujących przepisach, rada gminy może wydawać przepisy porządkowe, jeżeli jest to niezbędne dla ochrony życia lub zdrowia obywateli oraz dla zapewnienia porządku, spokoju i bezpieczeństwa publicznego. W orzecznictwie

67 Zob. art. 19 ust. 3-7 u.z.k.

68 Zob. art. 20 ust. 1-2 u.z.k.

69 M. Karpiuk, *Zarządzanie kryzysowe na poziomie gminnym* [w:] *Prawo zarządzania kryzysowego. Zarys systemu*, M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop (red.), Olsztyn 2016, s. 95.

70 Najwyższa Izba Kontroli, *Informacja o wynikach kontroli w zakresie ochrony ludności w ramach zarządzania kryzysowego i obrony cywilnej,* Warszawa 2018, s. 36, https://www.nik.gov.pl/plik/id,18895,vp,21498.pdf (dostęp: 05.10.2025 r.).

wskazuje się, że przepis art. 40 ust. 3 u.s.g., określający kompetencje rady gminy w zakresie wydawania przepisów porządkowych, wyraźnie wskazuje że takie przepisy mogą być wprowadzone jedynie wtedy, gdy jest to niezbędne dla ochrony wartości (dóbr) wymienionych w tym przepisie. Normy zawarte w art. 40 ust. 3 u.s.g. nie podlegają wykładni rozszerzającej, ponieważ przepisy porządkowe mogą być wydawane wyłącznie w wyjątkowych, ściśle określonych sytuacjach[71]. Warto przy tym wskazać, że zgodnie z art. 40 ust. 4 u.s.g., przepisy porządkowe mogą przewidywać za ich naruszanie karę grzywny wymierzaną w trybie i na zasadach określonych w ustawie – Kodeks postępowania w sprawach o wykroczenia[72].

Jednym z instrumentów zarządzania kryzysowego w gminie jest gminny plan zarządzania kryzysowego (art. 5 ust. 1 u.z.k.)[73]. W skład planów zarządzania kryzysowego wchodzą: plan główny, zespół przedsięwzięć na wypadek sytuacji kryzysowych oraz załączniki funkcjonalne planu głównego. Plan główny powinien obejmować charakterystykę zagrożeń oraz ocenę ryzyka ich wystąpienia, w tym dla infrastruktury krytycznej, mapy ryzyka i mapy zagrożeń; zadania i obowiązki uczestników zarządzania kryzysowego w formie siatki bezpieczeństwa; zestawienie sił i środków planowanych do wykorzystania w sytuacjach kryzysowych; a także zadania wynikające z planów działań krótkoterminowych, o których mowa w art. 92 ustawy – Prawo ochrony środowiska[74]. Zgodnie z art. 5 ust. 3 u.z.k., plany zarządzania kryzysowego podlegają systematycznej aktualizacji, a cykl planowania nie może przekraczać dwóch lat. Cykl planowania realizują właściwe organy administracji publicznej oraz podmioty przewidziane do realizacji przedsięwzięć określonych w planie zarządzania kryzysowego, w zakresie ich dotyczącym (art. 5 ust. 4 u.z.k.). Plany zarządzania kryzysowego uzgadnia się z kierownikami jednostek organizacyjnych, w zakresie ich dotyczącym, planowanych do wykorzystania przy realizacji przedsięwzięć określonych w planie (art. 5 ust. 6 u.z.k.).

Trybunał Konstytucyjny w wyroku z dnia 3 lipca 2016 r. stwierdził, że planowanie działań w ramach poszczególnych szczebli administracji publicznej nie może odbywać się w sposób autonomiczny. Plany zarządzania kryzysowego powinny być ze sobą spójne pod względem celów działania. W związku z tym u.z.k. przewiduje mechanizm planowania oparty na dokumentach wyjściowych: raportach (art. 5a ust. 5 u.z.k.), wytycznych do wojewódzkich planów zarządzania kryzysowego wydawanych w drodze zarządzenia przez ministra właściwego do spraw wewnętrznych

[71] Wyrok Naczelnego Sądu Administracyjnego z dnia 13 lutego 2018 r., sygn.. akt II OSK 994/16, ONSAiWSA 2019, nr 5, poz. 79.

[72] Zob T. Góra, *Zarządzanie kryzysowe na szczeblu gminnym – wybrane zagadnienia*, „Prawo i „Bezpieczeństwo" 2023, nr 1, s. 36.

[73] Poza gminnymi planami zarządzania kryzysowego tworzy się także Krajowy Plan Zarządzania Kryzysowego oraz plany wojewódzkie i powiatowe.

[74] Ustawa z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska (t.j. Dz. U. z 2025 r. poz. 647 z późn. zm.).

(art. 14 ust. 3 u.z.k.), zaleceniach wojewody dla starostów dotyczących powiatowych planów zarządzania kryzysowego (art. 14 ust. 2 pkt 2 lit. a u.z.k.) oraz zaleceniach starosty dla organów gminy w zakresie gminnych planów zarządzania kryzysowego (art. 17 ust. 2 pkt 2 lit. c u.z.k.). Dzięki tym dokumentom wyjściowym organy zarządzania kryzysowego mogą wpływać na treść planów sporządzanych na niższym szczeblu, co zapewnia spójność poszczególnych planów oraz ujednolica cele działań i zasoby służące ich realizacji[75].

Odnosząc się natomiast do zadań gminy w zakresie cyberbezpieczeństwa, należy podkreślić, że dyrektywa NIS 2 nakłada na państwa członkowskie obowiązek zapewnienia zdolności, zasobów i procedur umożliwiających reagowanie na sytuacje kryzysowe w cyberprzestrzeni. W Polsce obowiązki te realizowane są na podstawie u.k.s.c. oraz u.z.k., które obejmują także JST[76]. W świetle przepisów u.k.s.c. gminy, jako jednostki samorządu terytorialnego realizujące zadania publiczne zależne od systemów informacyjnych, podlegają obowiązkom określonym w rozdziale 5 u.k.s.c.[77] Przede wszystkim gminy mają obowiązek wyznaczyć osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa (art. 21 u.k.s.c). Wyznaczenie osoby kontaktowej nie jest jednak jedynym obowiązkiem gminy, ponieważ do jej obowiązków należy też zapewnienie zarządzaniem incydentami w swoich systemach teleinformatycznych, ich zgłaszanie w terminie nie dłuższym niż 24 godziny od wykrycia, oraz współpraca z właściwym CSIRT GOV, CSIRT NASK lub CSIRT MON w procesie obsługi incydentów oraz incydentów krytycznych (art. 22 u.k.s.c.). Obsługa incydentu obejmuje czynności umożliwiające wykrywanie, rejestrowanie, analizowanie, klasyfikowanie, priorytetyzację, podejmowanie działań naprawczych i ograniczenie skutków incydentu (art. 2 pkt 10 u.k.s.c.)[78]. Minimalny zakres danych, jakie gmina powinna uwzględnić w zgłoszeniu incydentu w podmiocie publicznym, określa art. 23 u.k.s.c. Informacje te można podzielić na trzy grupy. Pierwsza grupa obejmuje dane identyfikacyjne podmiotu, w którym doszło do incydentu, dane kontaktowe inspektora ochrony danych oraz osoby uprawnionej do udzielania wyjaśnień. Druga grupa dotyczy samego incydentu, m.in. przyczyny jego zaistnienia, czy opis wpływu incydentu na realizowane zadanie publiczne. Trzecia grupa obejmuje informacje o działaniach zapobiegawczych i o podjętych działaniach naprawczych. Zgodnie z art. 23 ust. 2 u.k.s.c. podmiot publiczny przekazuje informacje znane mu w chwili dokonywania zgłoszenia, które następnie uzupełnia w trakcie obsługi incydentu w podmiocie

[75] W. Skomra, *Zarządzanie kryzysowe - praktyczny przewodnik po nowelizacji ustawy*, Warszawa 2010, s. 78-80. Zob. szerzej: Wyrok Trybunału Konstytucyjnego z dnia 3 lipca 2012 r., sygn.. akt K 22/09, OTK-A 2012, nr 7, poz. 74.

[76] M. Czuryk, *Zarządzanie kryzysowe w obszarze cyberbezpieczeństwa*, „Ius et Securitas" 2025, nr 1, s. 8.

[77] K. Wąsowski [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz (red.), Warszawa 2019, art. 24, Legalis.

[78] W. Z. Dziomdziora, *Cyberbezpieczeństwo w samorządzie...* op.cit.

publicznym. Warto zaznaczyć, że katalog informacji przesyłanych w zgłoszeniu nie jest katalogiem zamkniętym[79]. W razie uznania gminy za operatora usługi kluczowej stosuje się względem niej również przepisy rozdziału 3 u.k.s.c. (art. 25 u.k.s.c.).

Porównując zadania gminy w zakresie zarządzania kryzysowego z obowiązkami wynikającymi z u.k.s.c., należy wskazać, że zarządzanie kryzysowe koncentruje się przede wszystkim na zagrożeniach o charakterze fizycznym, naturalnym lub technicznym i wymaga działań organizacyjnych, logistycznych oraz opracowania planów reagowania. Natomiast zadania z zakresu cyberbezpieczeństwa skupiają się na ochronie systemów informacyjnych oraz reagowaniu na incydenty w sferze cyfrowej. Mimo tych odmienności, oba obszary łączy wspólny cel, jakim zapewnienie bezpieczeństwa mieszkańców i ciągłości działania gminy.

Wnioski

Bezpieczeństwo stanowi jeden z fundamentów demokratycznego państwa prawnego[80]. Już z art. 5 Konstytucji RP wynika, że państwo jest zobowiązane do ochrony swojej niepodległości i nienaruszalności terytorium, co z kolei determinuje realizację zadań związanych z zapewnieniem praw i wolności obywatelskich, bezpieczeństwa oraz ochroną dziedzictwa narodowego i środowiska naturalnego[81]. Mimo że system zarządzania kryzysowego w Polsce opiera się na administracji rządowej, to realny ciężar działań spoczywa w dużej mierze na jednostkach samorządu terytorialnego, zwłaszcza gminach. To na ich terenie najczęściej ujawniają się skutki zagrożeń, zarówno naturalnych, jak i technicznych czy społecznych, czego przykładem była powódź z września 2024 r.[82]. Z tego względu zasadne jest wzmacnianie roli gmin w strukturze bezpieczeństwa państwa oraz zapewnienie im zasobów umożliwiających szybką i skuteczną reakcję[83].

Z przeprowadzonej analizy wynika, że gmina, jako podstawowa JST, odgrywa kluczową rolę w zarządzaniu kryzysowym. To właśnie na poziomie lokalnym zagrożenia są najszybciej dostrzegalne, a ich skutki najbardziej dotkliwe dla mieszkańców. Gmina, dzięki znajomości lokalnych uwarunkowań geograficznych, społecznych, infrastrukturalnych i informacyjnych, posiada największe możliwości podejmowania skutecznych działań zapobiegawczych, organizacyjnych oraz reagowania na sytuacje kryzysowe. Należy jednak zauważyć, że zwłaszcza mniejsze gminy borykają się

[79] K. Czaplicki [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, A. Gryszczyńska, G. Szpor (red.), Warszawa 2019, art. 23, Lex/el.

[80] D. Skoczylas, *Krajowy system cyberbezpieczeństwa*, Warszawa 2023, Legalis.

[81] W. Skrzydło [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2013, art. 5, LEX/el.

[82] A. Mituś, *Zarządzanie kryzysowe w Polsce...*, op. cit., s. 74.

[83] J. Bubiło, *Rola administracji publicznej w systemie zarządzania kryzysowego w polskim porządku prawnym - wybrane aspekty praktyczne* [w:] *Dziesięć lat reformy ustrojowej administracji publicznej w Polsce*, J. Parchomiuk, B. Ulijasz, E. Kruk (red.), Warszawa 2009, s. 760-761

z ograniczonymi zasobami finansowymi, kadrowymi i organizacyjnymi. W gminach wiejskich często jedyną jednostką mogącą profesjonalnie wspierać działania kryzysowe jest Ochotnicza Straż Pożarna[84]. W związku z tym konieczne są nie tylko regulacje prawne określające sposób reagowania administracji publicznej w sytuacjach kryzysowych, ale także zapewnienie ich finansowania ze środków publicznych[85].

Jednocześnie gminy są coraz bardziej narażone na różnego rodzaju cyberzagrożenia, które mogą zakłócić pracę administracji, sparaliżować usługi publiczne, narazić mieszkańców na utratę danych lub wpłynąć na bezpieczeństwo infrastruktury krytycznej. Należy wobec tego podkreślić, że cały sektor administracji publicznej został zaliczony do kategorii podmiotów kluczowych w rozumieniu krajowego systemu cyberbezpieczeństwa.

Mając to na uwadze, należy podkreślić, że współczesne pojmowanie bezpieczeństwa, jako dobra publicznego, ma charakter dynamiczny i ewoluuje wraz z rozwojem technologii oraz pojawianiem się nowych, złożonych zagrożeń[86]. Jednym z nich są cyberzagrożenia, które coraz częściej stanowią pierwotną przyczynę sytuacji kryzysowych. Atak na systemy teleinformatyczne gminy może prowadzić do zakłócenia usług publicznych, przerwania dostaw energii, utraty danych, a w konsekwencji poważnych zagrożeń dla życia, zdrowia lub porządku publicznego. Dlatego integracja zarządzania kryzysowego z systemem cyberbezpieczeństwa staje się koniecznością, a nie wyborem. Oba systemy łączy wspólny cel, jakim jest zapewnienie ciągłości działania instytucji publicznych oraz ochrona mieszkańców. Wymaga to wspólnych procedur, koordynacji, szybkiej wymiany informacji oraz uwzględnienia cyberzagrożeń na każdym etapie planowania kryzysowego. Równie istotne pozostaje budowanie świadomości społecznej oraz wzmacnianie odporności lokalnych wspólnot. Dopiero zintegrowane, wielopoziomowe podejście pozwoli sprostać współczesnym, hybrydowym zagrożeniom i zapewnić bezpieczeństwo mieszkańcom w rzeczywistości, w której granica między światem realnym a cyfrowym coraz bardziej się zaciera.

Bibliografia:

Akty prawne

1) Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. Nr 78 poz. 483 z późn. zm.).
2) Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2025 r. poz. 1153).

[84] A. Pakuła, *Rola terenowej administracji publicznej w zapobieganiu sytuacjom kryzysowym*, „Przegląd Prawa i Administracji" 2016, t. 106, s. 134.

[85] T. Góra, *Zarządzanie kryzysowe...*, op. cit., s. 35-36.

[86] F. Mroczko, *Zarządzanie kryzysowe w sytuacjach niemilitarnych. Zakres problemów regionów Dolnego Śląska*, Wałbrzych 2017, s. 17.

3) Ustawa z dnia 20.grudnia 1996 r. o gospodarce komunalnej (t.j. Dz. U. z 2021 r. poz. 679).
4) Ustawa z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska (t.j. Dz. U. z 2025 r. poz. 647 z późn. zm.).
5) Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2024 r. poz. 1557 z późn. zm.).
6) Ustawa z dnia 26 kwietnia2007 r. o zarządzaniu kryzysowym (t.j. Dz. U. z 2023 r. poz. 122 z późn. zm.).
7) Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz. U. z 2025 r. poz. 1483).
8) Ustawa z dnia 5 lipca2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077 z późn. zm.).
9) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. U. UE. L. z 2016 r. Nr 194, str. 1).
10) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia2022 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, str. 80 z późn. zm.).

Literatura

1) Błaś A., *Zadania administracji publicznej* [w:] *Nauka administracji*, J. Boć (red.), Wrocław 2013.
2) Brzostek A., *Cyberbezpieczeństwo w administracji publicznej - aspekty prawne*, „Zeszyty Prawnicze" 2023, nr 3.
3) Bubiło J., *Rola administracji publicznej w systemie zarządzania kryzysowego w polskim porządku prawnym - wybrane aspekty praktyczne* [w:] *Dziesięć lat reformy ustrojowej administracji publicznej w Polsce*, J. Parchomiuk, B. Ulijasz, E. Kruk (red.), Warszawa 2009.
4) Czaplicki K. [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, A. Gryszczyńska, G. Szpor (red.), Warszawa 2019, art. 21, art. 23, Lex/el.
5) Czuryk M., Zarządzanie kryzysowe w obszarze cyberbezpieczeństwa, „Ius et Securitas" 2025, nr 1.
6) Dobosz P. [w:] *Ustawa o samorządzie gminnym*, P. Chmielnicki (red.), Warszawa 2022, art. 7, LEX/el.
7) Dziomdziora W.Z., *Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik*, Warszawa 2021, Lex/el.
8) Góra T., *Zarządzanie kryzysowe na szczeblu gminnym – wybrane zagadnienia*, „Prawo i „Bezpieczeństwo" 2023, nr 1.

9) Karpiuk M., *Crisis management vs. cyber threats*, „Sicurezza, Terrorismo e Societa" 2022, nr 2.
10) Karpiuk M., *Zarządzanie kryzysowe na poziomie gminnym* [w:] *Prawo zarządzania kryzysowego. Zarys systemu*, M. Czuryk, K. Dunaj, M. Karpiuk, K. Prokop (red.), Olsztyn 2016.
11) Kostur K., *Zarządzanie kryzysowe w gminie - wybrane zagadnienia*, „Roczniki Administracji i Prawa" 2020, nr 2.
12) Mituś A., *Zarządzanie kryzysowe w Polsce – reguły, mechanizmy, efektywność* [w:] *Przywództwo w administracji publicznej. Perspektywa zarządzania kryzysowego*, K. Baran, S. Mazur (red.), Warszawa 2022.
13) Mroczko F., *Zarządzanie kryzysowe w sytuacjach niemilitarnych. Zakres problemów regionów Dolnego Śląska*, Wałbrzych 2017.
14) Opaliński B., *Rozdzielenie kompetencji władzy wykonawczej między Prezydenta RP oraz Radę Ministrów na tle Konstytucji Rzeczypospolitej Polskiej z 1997 roku*, Warszawa 2012, LEX/el.
15) Pakuła A., *Rola terenowej administracji publicznej w zapobieganiu sytuacjom kryzysowym*, „Przegląd Prawa i Administracji" 2016, t. 106.
16) Płonka-Bielenin K., *Inkorporacja prawa w zakresie zarządzania kryzysowego w samorządzie terytorialnym – wnioski i postulaty*, „Samorząd Terytorialny" 2021, nr 3.
17) Skoczylas D., *Krajowy system cyberbezpieczeństwa*, Warszawa 2023, Legalis.
18) Skoczylas D., *Wzmocnienie zdolności Unii Europejskiej w zakresie cyberbezpieczeństwa – cybersolidarność w kontekście cyberzagrożeń*, „Europejski Przegląd Sądowy" 2024, nr 12.
19) Skomra W., *Zarządzanie kryzysowe - praktyczny przewodnik po nowelizacji ustawy*, Warszawa 2010.
20) Skrzydło W. [w:] *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2013, art. 5, LEX/el.
21) Stefaniuk B., *Bezpieczeństwo a zarządzanie kryzysowe* [w] *Oblicza i wyzwania obronności w XXI wieku*, A. Polak, A. Smarzewska, P. Borek (red.), Biała Podlaska 2015.
22) Szpor G. [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, K. Czaplicki, A. Gryszczyńska (red.), Warszawa 2019, art. 4, Lex/el.
23) Wąsowski K. [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz (red.), Warszawa 2019, art. 24, Legalis.
24) Wilińska M., *Zarządzanie kryzysowe w systemie bezpieczeństwa państwa*, „Obronność. Zeszyty Naukowe" 2015, nr 3(15).
25) *Współpraca z jednostkami publicznymi* [w:] *Księga dobrych praktyk w zakresie zarządzania ciągłością działania*, R. Kaszubski, D. Romańczuk (red.), Warszawa 2011.
26) Żmigrodzki M., *Zarządzanie kryzysowe w państwie*, Warszawa 2012.

Orzecznictwo

1) Wyrok Trybunału Konstytucyjnego z dnia 3 lipca 2012 r., sygn. akt K 22/09, OTK-A 2012, nr 7, poz. 74.
2) Wyrok Naczelnego Sądu Administracyjnego z dnia 13 lutego 2018 r., sygn. akt II OSK 994/16, ONSAiWSA 2019, nr 5, poz. 79.
3) Wyrok Wojewódzkiego Sądu Administracyjnego w Gdańsku z dnia 28 listopada 2012 r., sygn. akt I SA/Gd 1171/12, LEX nr 1247413.

Inne źródła

1) Najwyższa Izba Kontroli, *Informacja o wynikach kontroli w zakresie ochrony ludności w ramach zarządzania kryzysowego i obrony cywilnej,* Warszawa 2018, https://www.nik.gov.pl/plik/id,18895,vp,21498.pdf (dostęp: 05.10.2025 r.).

dr Aleksandra Puczko
Uniwersytet Jagielloński
adres e-mail: a.puczko@uj.edu.pl
ORCID: 0000–0002–9929–0196

„Demokracja przychodzi w wielu kształtach i rozmiarach"
(J. Keane, *The Life and Death of Democracy*, Londyn 2009)

E-demokracja w czasie zagrożeń wewnętrznych i zewnętrznych

E-democracy in times of internal and external dangers

Streszczenie

E-demokracja to zjawisko charakterystyczne dla współczesności, wskazujące, że cyfryzacja życia nie jest jedynie elementem sfery komercyjnej, ale dotyczy również realizacji praw politycznych. Przy pomocy narzędzi cyfrowych umożliwia ona rozwijanie społeczeństwa obywatelskiego przez zbliżanie obywateli do organów władzy państwowej, spraw państwa i procesów decyzyjnych. Na szybkość rozwoju e-demokracji i jej popularność wpływ mają różnorodne elementy, w tym zagrożenia. W niniejszym opracowaniu sklasyfikowano je jako zewnętrzne tj. pochodzące z zewnątrz państwa (jak m. in. cyberataki, dezinformacja, uzależnienie od zewnętrznych technologii) i wewnętrzne, będące skutkiem dysfunkcji problemów wewnętrznych w państwie (jak m. in. wykluczenie cyfrowe, brak transparentności algorytmów i przede wszystkim regulacji zapewniających bezpieczeństwo korzystania z narzędzi e-demokratycznych). Ich zidentyfikowanie umożliwiło wywiedzenie też postulatów *de lege ferenda* obejmujących zarówno prawne (zwiększenie spójności i zakresu regulacji prawnych chroniących użytkowników e-demokracji), jak i faktyczne (jak edukacja, rozwijanie umiejętności cyfrowych) postulaty, które nie tyle mają charakter następczy, co w szczególności wskazują działania prewencyjne umożliwiające rozwijanie e-demokracji i zwiększają jej atrakcyjność.

Wstęp

Rozwój nowych technologii, a wraz z nimi społeczeństwa informacyjnego oznacza nie tylko zmiany w sferze komercyjnej i w prostych sprawach życia codziennego[87].

[87] T. Parys, *ICT i ich wpływ na życie człowieka i społeczeństwa – wybrane problemy*, „Studia i Materiały Wydziału Zarządzania UW" 2024, nr 1, s. 101.

Rewolucja technologiczna, która głęboko odmieniła życie codziennie wpłynęła również na funkcjonowanie państwa, a także zmianę relacji pomiędzy organami władzy publicznej a jednostkami spoza ich struktur. Cyfryzacja skróciła dystans pomiędzy jednostkami administrującymi a administrowanymi tworząc administrację bardziej dostępną i otwartą na interesanta. W ten sposób zbliżyła bardziej ten model do biznesowego, przez to działania administracji nie tylko te podejmowane przy pomocy narzędzi cyfrowych zaczęły być nazywane usługami, a działania administracji zaczęły być realizowane w myśl kryteriów jakości, satysfakcji i efektywności.

W tym kierunku rozwijają się w szczególności wszelkie rodzaje administracyjnych serwisów cyfrowych (np. e-budownictwo, ePUAP, czy e-doręczenia) i poszerzany jest katalog usług w ramach administracji publicznej, które świadczone są dla administrowanych w sposób cyfrowy. W konsekwencji, kontakt z państwem przez organy administracji publicznej staje się w szczególności wygodny i bezpośredni, nieograniczony też godzinami pracy urzędu i koniecznością dotarcia do nich.

Wskazane wyżej przykłady cyfryzacji nie wyczerpują jednak wszystkich możliwości. Technologia umożliwia bowiem jednostkom nie tylko kontakt z administracją publiczną w ramach realizowania przez nie administracyjnoprawnych praw i obowiązków, ale w szczególności też uczestniczenie w wykonywaniu władzy. W tym wypadku skrócenie dystansu między władzą a obywatelami ułatwia im kontakt z organami władzy i otwiera nowe możliwości współuczestniczenia przez nich w decydowaniu o istotnych kwestiach w państwie zarówno przez samo zasięganie informacji, konsultacje, jak i partycypację w procesach decyzyjnych w cyfrowy sposób. . Terminem nadanym takim rozwiązaniom jest e-demokracja, której koncepcja kształtowana jest na szczeblu międzynarodowym, europejskim i krajowym już od dłuższego czasu, zmieniając i wzmacniając demokratyzację życia politycznego i społecznego.

Możliwość jednak takiego otwarcia procesu decydowania o sprawach państwa jest też źródłem szeregu zagrożeń, które wpływają na spowolnienie rozwoju e-demokracji, czy jej zaniku. Z uwagi na doniosłą rolę e-demokracji w modyfikacji dotychczasowego sposobu rządzenia i administrowania państwem jest ona podatna na zagrożenia zarówno o charakterze wewnętrznym (pochodzącym zarówno od samych obywateli, jak i samych władz państwowych), jak i zewnętrznym (np. cyberataki, globalna dezinformacja). Zagrożenia dla e-demokracji (w szczególności z uwagi na wymogi jakie stawia ona państwu i jego organom) skutkować mogą sabotowaniem przez samo państwo rozwoju tego typu form, co nie pozwoli na zwiększenie kontroli obywatelskiej nad jego działaniami. Jednocześnie też otwierają nowe możliwości zewnętrznej ingerencji w sprawy państwa. W każdym z wyróżnionych wypadków mogą one skutkować w szczególności osłabieniem zaufania

państwa i jednostek do tego typu form współuczestnictwa ludzi w sprawach państwa, a w konsekwencji udaremnieniem zmian podjętych w tym kierunku.

W niniejszym rozdziale podjęta została próba opisania tych zagrożeń wynikających z rozwoju nowych technologii informatycznych, w sytuacji, gdy obywatele angażują się politycznie za pomocą nowoczesnych technologii, jak znalezienia rozwiązań pozwalających na uchronienie e-demokracji przed ich wpływem. Przy pomocy metody teoretycznej, domagtyczno-opisowej, jak i prawnoporównawczej przeprowadzona analiza dotyczyła obszarów:

- ustalenia znaczenia pojęcia e-demokracji i wytyczenia w oparciu o znaczenie tego pojęcia sfer narażonych na zagrożenia i ich przyczyn;- zbadania samych zagrożeń i ich przejawów, przez ustalenie, jaki mogą mieć charakter, co pozwala wywieść zagrożenia o charakterze wewnętrznym i zewnętrznym;
- wyprowadzenia postulatów *de lege ferenda*.

Pojęcie e-demokracji

Wpływ na rozwój e-demokracji miał w szczególności rozwój technologii, zwłaszcza cyfrowych, które określa się jako ICT- technologie informatyczno-komunikacyjne (ang. *Information and Communication Technologies*), dedykowane przetwarzaniu, gromadzeniu i przesyłaniu informacji w formie elektronicznej[88]. Jak się przyjmuje, e-demokracja polega na zastosowaniu technologii informacyjno-telekomunikacyjnych dla zwiększenia uczestnictwa obywateli w procesach demokratycznych, zarówno w ujęciu ilościowym, jak i w formie realnego wpływu wywieranego przez jednostki na funkcjonowanie instytucji publicznych[89]. Związek e-demokracji z technologią obrazuje szereg pojęć służących jej opisywaniu, jak cyberdemokracja, teledemokracja, wirtualna demokracja, demokracja cyfrowa, elektroniczna demokracja, demokracja internetowa[90]. Mimo, że nazwy te kładą nacisk na różne narzędzia wykorzystywane w realizacji e-demokracji, to słusznie zauważa się, że niezależnie od przyjętej nazwy łączy je założenie, że funkcje nowych technologii, jak m. in. interaktywność, szybszy tryb przekazywania informacji, możliwość komunikacji zwrotnej, mogą pozytywnie oddziaływać na mechanizmy demokratyczne[91].

Ścisły związek z ICT i pozytywny wpływ technologii na demokrację stanowi też podstawę definicyjną e-demokracji. W rezolucji Parlamentu Europejskiego z dnia 16 marca 2017 r. w sprawie e-demokracji w Unii Europejskiej: potencjał i wyzwania

88 Tamże, s. 104.

89 M. Marczewska-Rytko, Idea *demokracji bezpośredniej odokresu antycznego do czasów Internetu i globalizacji,* [w:] M. Marczewska-Rytko, A. K. Piasecki (red.) *Demokracja bezpośrednia. Wymiar globalny i lokalny*, Lublin 2010, s. 25.

90 L. Hennen, I. van Keulen, I. Korthagen, G, Aichholzer, R. Lindner, R. Ø. Nielsen, *European e-democracy in practice* ,Cham 2020, s. 15.

91 Por. T. Białobłocki, J. Moroz, M. Nowina-Konopka, *Społeczeństwo informacyjne: istota, rozwój, wyzwania*, Warszawa 2006.

(2016/2008(INI) w oparciu o przeprowadzone badania nad e-demokracją i e-partycypację, przez e-demokrację rozumie się wsparcie i wzmocnienie demokracji tradycyjnej za pomocą ICT, która może uzupełniać i wzmacniać procesy demokratyczne przez wprowadzenie elementów wzmacniających pozycję obywateli. Dzięki takim rozwiązaniom cyfrowym możliwym do realizacji za pośrednictwem nowych technologii informacyjno-komunikacyjnych, jak e-administracja, e-rządzenie (*e-government*), e-debaty, e-uczestnictwo i e-głosowanie otwarciu i udostępnieniu dla obywateli ulegają procesy demokratyczne[92]. Z tego względu e-demokrację można zdefiniować jako „zastosowanie technologii informacyjno-telekomunikacyjnych dla zwiększenia uczestnictwa obywateli w procesach demokratycznych, zarówno w ujęciu ilościowym, jak i w formie realnego wpływu wywieranego przez jednostki na funkcjonowanie instytucji publicznych."[93].

W tych kontekstach e-demokracja postrzegana być może zarówno jako koncepcja, proces, jak i mechanizm polegający na wzmocnieniu dotychczasowej demokracji przy pomocy rozwiązań cyfrowych. Ustalając znaczenie e-demokracji można, wobec tego w szczególności spróbować ją uchwycić w kontekście:

a) różnic pomiędzy e-demokracją a e-administracją;
b) relacji e-demokracji i społeczeństwa obywatelskiego;
c) wykorzystywanych narzędzi umożliwiających urzeczywistnienie e-demokracji.

Rozpoczynając od różnic pomiędzy e-demokracją a e-administracją, widoczne jest, że chociaż łączą je podobne założenia i cele, to nie są one tożsame[94]. W świetle wcześniej przywołanych definicji, określając relację pomiędzy nimi można zauważyć, że e-administracja zawiera się w e-demokracji, która jest też urzeczywistniana przez rozwiązania z zakresu administracji elektronicznej. E-administrację określa się bowiem jako usługi publiczne świadczone przez administrację przy użyciu ICT (*e-government* oraz *e-governance*), natomiast e-demokracja to już partycypowanie w planowaniu działania państwa i branie udziału w procesach decyzyjnych. Pojęcie to obejmuje nie tylko usługi, ale odnosi się zarówno do samego aparatu administracyjnego, jak i wykorzystywanych przez niego narzędzi, w tym wypadku e-narzędzi. Ogólnie można określić e-administrację jako mechanizm obejmujący elementy podmiotowe i przedmiotowe, który tworzy warunki współpracę pracowników na różnych szczeblach w celu załatwienia indywidualnych spraw interesantów i przez to zaspokajania ich zbiorowych potrzeb obywateli[95].

---

92 e-Demokracja w Unii Europejskiej: potencjał i wyzwania Rezolucja Parlamentu Europejskiego z dnia 16 marca 2017 r. w sprawie e-demokracji w Unii Europejskiej: potencjał i wyzwania (2016/2008(INI)), s. 3, https://www.europarl.europa.eu/doceo/document/TA-8-2017-0095_PL.html (dostęp: 7.12.2025 r.).

93 D. Grodzka, *Edemokracja*, „Infos" 2009, nr 14, s. 1.

94 Tamże.

95 Por. szerzej: D. Fleszer, *Wokół problematyki e-administracji*, „Roczniki Administracji i Prawa" 2014, nr 14, s. 125–136.

Z tego względu, e-demokracja sprzyja zaangażowaniu obywateli w sprawy publiczne, zwiększaniu ich świadomości i odpowiedzialności. Tworzenie modelu społeczeństwa, które za pomocą ICT bierze aktywny udział w procesach demokratycznych powoduje znoszenie możliwych granic takiego zaangażowania a także sprzyja czynnemu uczestnictwu w życiu politycznym[96]. Wykorzystanie nowych technologii w budowaniu demokracji zwiększa liczbę różnorodnych uczestników procesów demokratycznych, w tym obywateli czyniących użytek ze swoich praw w procesach decyzyjnych w formach zarówno demokracji bezpośredniej, jak i we współudziale z organami państwowymi. Ponadto, przy pomocy środków technicznych które w ogólnym rozrachunku nie generują wysokich kosztów ani po stronie organizatorów, ani uczestników, tworzy się wirtualna przestrzeń umożliwiająca wymianę poglądów zarówno pomiędzy jednostkami, jak i pomiędzy nimi i a przedstawicielami władzy. Takie działania umożliwiają zdiagnozowanie możliwych problemów, ich przedyskutowanie i wspólne wypracowanie rozwiązań.

Na szczeblu międzynarodowym przyjmuje się, że są trzy poziomy wykorzystania ICT w celu wzmocnienia zaangażowania obywateli w sprawy publiczne: informowanie, konsultowanie oraz aktywne uczestniczenie w kształtowaniu polityki[97]. W powołanej wcześniej rezolucji PE także zwraca się uwagę na e-uczestnictwo jako kluczowy element charakterystyczny e-demokracji obejmujący trzy formy interakcji między instytucjami unijnymi i rządami z jednej strony a obywatelami z drugiej strony tj.: e-informacje, e-konsultacje i elektroniczne podejmowanie decyzji. Na e-demokrację składają się, wobec tego trzy elementy informacja, konsultacja i partycypacja. Rezolucja PE zachęca państwa członkowskie do dalszego rozwijania takich praktyk na szczeblu krajowym i lokalnym[98]. Ich urzeczywistnienie jest natomiast możliwe przez istniejące i projektowane narzędzia umożliwiające funkcjonowanie e-demokracji.

Rozwijanie społeczeństwa obywatelskiego w ramach e-demokracji obejmuje w szczególności elektroniczne formy partycypacyjne zarówno w fazach konsultacyjnych, jak i decyzyjnych polityki krajowej i lokalnej. W istocie e-demokracja korzysta i opisywana jest też przez szeroki zakres interaktywnych narzędzi komunikacji elektronicznej, które dotyczą w szczególności istniejących i dopiero powstających narzędzi komunikacyjnych pozwalających na udział w sprawowaniu władzy. Może to być znana powszechnie technologia, jak radio, telewizja, ale również internet, narzędzia wykorzystywane w telefonii komórkowej, które

[96] Por. szerzej: J. Lerner, *Making Democracy Fun. How Game Design Can Empower Citizens and Transform Politics*, Londyn 2014.

[97] D. Grodzka, *E-demokracja...*,op.cit., s. 2.

[98] *e-Demokracja w Unii Europejskiej: potencjał i wyzwania Rezolucja Parlamentu Europejskiego z dnia 16 marca 2017 r. w sprawie e-demokracji w Unii Europejskiej: potencjał i wyzwania (2016/2008(INI))*, s. 3.

umożliwiają bezpośrednią partycypację zarówno w zakresie uzyskania informacji, konsultacjach, jak i podejmowaniu decyzji[99].

Przykładami takich rozwiązań są w szczególności: możliwość uczestnictwa w głosowaniach i referendach drogą elektroniczną (*e- voting*)[100], konsultowane online aktów prawnych, a także sporządzanie petycji i zbieranie podpisów, czy też możliwość zgłaszania, za pomocą internetu, lokalnych problemów i kontrolowanie procesu ich rozwiązania (np. projektów budżetu obywatelskiego). Umożliwiają one zaangażowanie we wszystkie te działalnie większej liczby członków danych społeczności. W ten sposób mogą oni wyrażać swoje opinie na udostępnionych przez władzę publiczną stronach internetowych, przez e-mail, a także inne formy komunikacji elektronicznej, w zależności od prawnych skutków generowanych przez dane działanie, jak i przewidzianych prawnych formach i następstwach prawnych takiego wpływu na działania władz.

Istniejące i rozwijane liczne formy e-demokracji nie gwarantują jednak, że będzie ona się rozwijała zawsze w pożądanym kierunku. Równocześnie z szansami, jakie e-demokracja niesie ze sobą powstają nowe zagrożenia, dotychczas nawet nieznane, które spowalniają generowane przez nią zmiany, a w szczególności ograniczają zaufanie do nowych technologii, a przez to do e-demokracji.

Zagrożenia dla e-demokracji

E-demokracja jako element życia społecznego i rzeczywistości kształtowanej rozwiązaniami cyfrowymi, poddana jest zasadniczo takim samym zagrożeniom, jak i inne aktywności realizowane w sferze cyfrowej i rzeczywistości wirtualnej. Z tego względu nie da się też wyraźnie oddzielić od siebie zagrożeń dla e-demokracji od innych wpływających na cyberbezpieczeństwo. Z uwagi na znaczenie e-demokracji dla rozwoju społeczeństwa obywatelskiego, decydowanie przy pomocy jej narzędzi o kierunku rozwoju państwa i prowadzonej przez nie polityki, grożące jej czynniki automatycznie mają wpływ również na te aspekty. Powoduje to, że wszelkiego rodzaju zagrożenia dla e-demokracji i wywołane przez nie skutki wpływają na sposób funkcjonowania państwa, w tym zwłaszcza na zaufanie obywateli do władz publicznych.

Zagrożenia dla e-demokracji ściśle wiążą się z charakterem działań, które składają się na to pojęcie i narzędzia, które umożliwiają jego urzeczywistnienie. W istocie

[99] Public Participation Guide: Electronic Democracy, https://www.epa.gov/international-cooperation/public-participation-guide-electronic-democracy (dostęp: 6.01.2026 r.).

[100] M. Musiał-Karg, *Głosowanie przez Internet Skąd czerpać wzorce i jak wprowadzać innowacje wyborcze?*, Warszawa 2024, s. 2; R. Krimmer, *E-voting as a New Form of Voting*, [w:] *Explorations in eGovernment & eGovernance*, vol.2: *Selected proceedings of the Second International Conference on eGovernment and eGovernance*, A. Balci, C. Can Actan, O. Dalbay (red.), Antalya 2010, s. 148; S. Koczubiej, E-*głosowanie jako element demokracji współczeństwie informacyjnym*, „Problemy Humanistyki" 2003/2004, nr 8/9, s.261-273.

działania organów administracji, które je wykorzystują i beneficjentów e-demokracji mogą być dla niej zarówno korzystne, jak i stanowić zagrożenie. Oddziaływania sprzyjające można scharakteryzować jako działania odgórne tj. podjęte np. przez rząd, władze lokalne oraz działania oddolne tj. inicjatywy podjęte np. przez obywateli, czy organizacje społeczne. Działania mogą mieć charakter procesów jednokierunkowych (*oneway*) tj. np. rozpowszechnianie informacji lub dwukierunkowych (*twoway*) np. konsultacje dotyczące projektów ustaw[101].

W każdym wymienionym ujęciu narażone są one na zagrożenia, które ujemnie wpływają na procesy e-demokratyzacji życia. Istotne jest, że mogą one być zarówno zewnętrzne tj. być skutkiem oddziaływania sił zewnętrznych, międzynarodowych, jak i wewnętrzne, których źródłem są problemy społeczne i instytucjonalne istniejące w danym państwie. Przyjęty w niniejszej analizie podział zagrożeń dla e-demokracji na zewnętrzne i wewnętrzne nie jest rozłączny, ani wyczerpujący. Część z przykładów podanych zagrożeń może mieć równocześnie charakter wewnętrzny, jak zewnętrzny, tak samo też wymienione nie wyczerpują całego katalogu potencjalnych zagrożeń. Zaproponowany podział umożliwia jednak zobrazowanie ryzyk przez pryzmat możliwego ich pochodzenia, a także przeprowadzanie ich dalszej klasyfikacji.

Do zagrożeń zewnętrznych zalicza się przede wszystkim cyberataki. Systemy informatyczne wykorzystywane w e-demokracji mogą stać się celem hakerów, którzy próbują zakłócić przebieg głosowań, zmienić wyniki lub zablokować dostęp do platform obywatelskich. Szczególnie niebezpieczna jest ingerencja obcych państw w procesy demokratyczne, ponieważ podważa suwerenność i zaufanie społeczeństwa do instytucji publicznych. Innym istotnym zagrożeniem jest dezinformacja, szerzona za pomocą mediów społecznościowych, botów i fałszywych kont. Manipulowanie opinią publiczną przez *fake newsy* może prowadzić do podejmowania decyzji wyborczych opartych na nieprawdziwych informacjach.

Zagrożenia wewnętrzne wynikają głównie z problemów społecznych i instytucjonalnych. Jednym z najważniejszych jest wykluczenie cyfrowe, czyli brak dostępu do internetu lub odpowiednich kompetencji cyfrowych. W efekcie część obywateli zostaje pozbawiona realnego wpływu na procesy demokratyczne, co prowadzi do pogłębiania nierówności społecznych. Istotnym problemem jest także obniżenie jakości debaty publicznej. Anonimowość w sieci sprzyja agresji słownej, mowie nienawiści oraz polaryzacji społeczeństwa, a dyskusje często ograniczają się do emocjonalnych i uproszczonych przekazów[102].

[101] D. Grodzka, *Edemokracja...*,op.cit., s. 2.

[102] K. Ferreira-Fernandes, *Internetowa partycypacja obywatelska: wyzwania I zagrożenia dla demokracji w erze cyfrowej*, „Wiedza Obronna" 2024, nr 3, s. 144 i n.

Zagrożeniami zewnętrznymi mogą być w szczególności:

a) cyberataki, skutkujące włamaniami do systemów wyborczych, manipulacją opinią publiczną i nastrojami społecznymi, a przez to też wynikami głosowań, w tym ataki *Distributed Denial of Service* w skrócie DDoS - blokujące dostęp do platform obywatelskich, powodujące przeciążenie serwerów, sieci lub aplikacji dużymi częstotliwościami sztucznego ruchu z tysięcy zainfekowanych urządzeń;
b) dezinformacja i propaganda w postaci *fake newsów* rozpowszechnianych w mediach społecznościowych, działalności farmy trolli i boty wpływających na opinię publiczną, ingerencję obcych państw w procesy demokratyczne;
c) uzależnienie od zagranicznych technologii przez korzystanie z platform należących do globalnych korporacji, wskutek czego państwo i obywatele nie mają brak kontroli nad algorytmami i danymi obywateli;
d) szpiegostwo cyfrowe polegające na wykradaniu danych osobowych, jak i monitorowanie aktywności politycznej obywateli przez podmioty zewnętrzne i wykorzystywanie tych informacji do dalszych celów.

Zagrożenia wewnętrzne to m. in.:

a) wykluczenie cyfrowe oparte o nierówności społeczne, polegające na braku dostępu do internetu, oraz niskie kompetencje cyfrowe (np. u osób starszych);
b) brak rozwijania nowych technologii i narzędzi e-demokracji przez państwo przy jednoczesnych deficytach regulacji prawnych rozwijających wykorzystanie tych narzędzi i zabezpieczających obywateli i ustanawiających zasady odpowiedzialności państwa za naruszenie ich bezpieczeństwa;
c) niska jakość debaty publicznej obfitująca w hejt i mowę nienawiści, spłycona do chwytliwych haseł i gry na emocjach, polaryzacja i bańki informacyjne;
d) ogólny brak zaufania do państwa i wykorzystywanych przez nie systemów, co skutkuje obawami o brak anonimowości i bezpieczeństwo głosowania, manipulacje wynikami głosowań. Przyczyną ograniczonego zaufania jest przede wszystkim brak transparentności wykorzystywanych w e-demokracji algorytmów, służących pozyskiwaniu danych i przeprowadzaniu procesów decyzyjnych. Obawy te związane są też z wykorzystywaniem przez władze informacji o obywatelach, pozyskanych w ten sposób prowadzące do nadmiernej kontroli i inwigilacji obywateli, a także cenzury ich aktywności politycznej.

Postulaty *de lege ferenda*

Analiza zagrożeń związanych z funkcjonowaniem e-demokracji prowadzi do wniosku, iż są one różnorodne i wielowymiarowe, co stawia przed państwami poważne wyzwania dotyczące stanu prawnego. Konieczne jest w szczególności wprowadzenie wielu instrumentów ochronnych, które zapewnią pełną i systemową regulację tego obszaru oraz zapewnią warunki edukacji zarówno na poziomie obywateli, jak i władzy.

Formułując postulaty *de lege ferenda,* w pierwszej kolejności należy postulować **ustanowienie kompleksowych regulacji prawnych dotyczących e-demokracji uwzględniających jej specyfikę, odróżniającą ją od sfery funkcjonowania realizowanych w dotychczasowym kształcie demokracji przedstawicielskiej i bezpośredniej.** Powinny one być spójne z art. 2 Konstytucji RP[103], gdyż z zasady demokratycznego państwa prawnego wynika, aby procedury demokratyczne były jasne, stabilne i oparte na przejrzystych normach prawnych. Obecny sposób regulacji e-demokracji opierający się o fragmentaryczne i szczątkowe uregulowania m. in. w Kodeksie wyborczym[104] oraz ustawach dotyczących informatyzacji administracji publicznej, skutkuje brakiem spójnego systemu, co wpływa na stabilność, pewność i przewidywalność regulacji.

Równolegle z powyższym istnieje konieczność **wprowadzenia jednolitych i obligatoryjnych standardów cyberbezpieczeństwa** dla systemów wykorzystywanych w procesach demokratycznych, co wywodzić można z zasady ochrony dobra wspólnego (art. 1 Konstytucji RP) oraz zasady legalizmu (art. 7 Konstytucji RP). Ochronę w tym zakresie częściowo zapewniają już przepisy ustawy o krajowym systemie cyberbezpieczeństwa oraz unijna dyrektywa NIS2[105], jednak brak jest szczególnych regulacji odnoszących się bezpośrednio do infrastruktury e-demokracji, wskutek czego wpada ona w lukę regulacyjną przez co osłabiona zostaje jej skuteczność.

W tym też kontekście, szczególnego znaczenia nabiera konieczna w demokratycznym państwie prawnym **ochrona praw i wolności jednostki**, w szczególności prawa do prywatności (art. 47 Konstytucji RP) oraz prawa do ochrony danych osobowych (art. 51 Konstytucji RP). W kontekście e-demokracji postulować należy jednoznaczne zagwarantowanie anonimowości głosowania elektronicznego oraz minimalizacji przetwarzania danych dotyczących preferencji politycznych obywateli. Ochronę tę wzmacniają już przepisy RODO (rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679)[106] wprowadzając szczególne zasady ochrony danych wrażliwych oraz ustawy o ochronie danych osobowych, jednak nie odnoszą się one wprost do specyfiki systemów e-głosowania.

---

[103] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1999 r. (Dz. U. z 1997 r. Nr 78, poz. 483 ze zm.), dalej: Konstytucja RP.

[104] Ustawa z dnia 5 stycznia 2011 r. Kodeks wyborczy (Dz. U. z 2025 r. poz. 365 ze zm.).

[105] 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. Urz. UE 2022, L 333/80).

[106] 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 oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), (Dz.Urz.UE.L 2016 Nr 119, str. 1).

W celu rozwoju e-demokracji potrzebne jest też tworzenie precyzyjnych instrumentów prawnych służących przeciwdziałaniu dezinformacji, która może naruszać zasadę suwerenności narodu (art. 4 Konstytucji RP) poprzez wpływanie na procesy wyborcze i opiniotwórcze. Instrumenty te powinny pozostawać w zgodzie z konstytucyjną wolnością wyrażania poglądów (art. 54 Konstytucji RP) oraz zasadą proporcjonalności (art. 31 ust. 3 Konstytucji RP). Częściową ochronę w tym zakresie zapewniają przepisy Kodeksu karnego[107], prawa prasowego, czy ustawy o radiofonii i telewizji oraz unijne rozporządzenie DSA (*Digital Services Act*)[108], jednak brak jest rozwiązań dedykowanych ochronie procesów e-demokratycznych jako takich.

Bardziej technicznym, ale również istotnym wymogiem jest **zapewnienie przejrzystości algorytmów wykorzystywanych w e-demokracji,** co pozostaje w bezpośrednim związku z zasadą jawności życia publicznego (art. 61 Konstytucji RP) oraz zasadą zaufania obywateli do państwa i prawa, wywodzoną z art. 2 Konstytucji RP. Obowiązujące regulacje, takie jak przepisy unijnego aktu o sztucznej inteligencji (*AI Act*)[109], stanowią krok w kierunku zwiększenia transparentności systemów algorytmicznych, jednak nie regulują w sposób kompleksowy algorytmów wykorzystywanych w procesach partycypacji demokratycznej. Stawia to wyzwanie nie tylko regulacjom krajowym, ale i unijnym. Wydaje się bowiem, że w kontekście e-administracji w zakresie zwłaszcza wyborów zasadne jest tworzenie jednolitych reguł na poziomie całej wspólnoty, począwszy też od wyborów do Parlamentu Europejskiej i na poziomie samorządowym.

Kolejnym istotnym postulatem, który bardziej opiera się nie tyle co o regulacje prawne, co o metody działania jest **przeciwdziałanie wykluczeniu cyfrowemu**, które należy rozpatrywać w świetle konstytucyjnej zasady równości wobec prawa (art. 32 Konstytucji RP) oraz zasady powszechności wyborów (art. 96 i 127 Konstytucji RP). Prawo powinno nakładać na organy państwa obowiązek zapewnienia alternatywnych form uczestnictwa w procesach demokratycznych oraz systemowego wsparcia w zakresie edukacji cyfrowej. Obowiązujące regulacje dotyczące dostępności cyfrowej, w szczególności ustawa o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych[110], realizują ten cel jedynie częściowo.

---

107 Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2025 r. poz. 383 ze zm.).

108 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych), (Dz. Urz. UE. L 2022 Nr 277, str. 1)

109 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz. U. UE. L. z 2024 r. poz. 1689).

110 Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2023 r. poz. 1440).

Podsumowanie

E-demokracja stanowi ważny element rozwoju współczesnych systemów demokratycznych, umożliwiając obywatelom łatwiejszy i szybszy udział w decydowaniu o sprawach państwa zarówno przez postulaty, jak i w procesach decyzyjnych. Dzięki wykorzystaniu technologii cyfrowych może ona zwiększać transparentność działań władzy, poprawiać komunikację między państwem a społeczeństwem oraz wzmacniać partycypację obywatelską.

Przeprowadzona wyżej analiza zagrożeń zewnętrznych i wewnętrznych pokazuje, że e-demokracja wiąże się z poważnymi wyzwaniami, które mogą wpływać na spowolnienie jej rozwoju, ale też na rezygnację z narzędzi służących jej realizacji, z uwagi na zbyt duże ryzyko jakie w przypadku braku odpowiednich zabezpieczeń może ona nieść za sobą. Cyberataki, dezinformacja oraz ingerencja podmiotów zewnętrznych mogą prowadzić do manipulacji procesami demokratycznymi i podważenia zaufania obywateli do instytucji państwa. Z kolei zagrożenia wewnętrzne, takie jak wykluczenie cyfrowe, obniżenie jakości debaty publicznej czy nadmierna kontrola ze strony władz, mogą skutkować ograniczeniem równości i wolności obywatelskich.

Wydaje się, że aby e-demokracja mogła skutecznie wspierać demokrację, konieczne jest zapewnienie wysokiego poziomu bezpieczeństwa systemów informatycznych, przejrzystości procedur oraz odpowiednich regulacji prawnych. Równie istotna jest edukacja obywateli w zakresie kompetencji cyfrowych i krytycznego odbioru informacji. Tylko spełnienie tych warunków pozwoli wykorzystać potencjał e-demokracji bez narażania podstawowych wartości demokratycznych.

Bibliografia:

Akty prawne

1) Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1999 r. (Dz. U. z 1997 r. Nr 78, poz. 483 ze zm.).
2) Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2025 r. poz. 383 ze zm.).
3) Ustawa z dnia 5 stycznia 2011 r. Kodeks wyborczy (Dz. U. z 2025 r. poz. 365 ze zm.).
4) Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2023 r. poz. 1440).
5) 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 oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), (Dz.Urz.UE.L 2016 Nr 119, str. 1).

6) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych), (Dz.Urz.UE.L 2022 Nr 277, str. 1)
7) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz. U. UE. L. z 2024 r. poz. 1689).
8) 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. Urz. UE 2022, L 333/80).

Literatura

1) Białobłocki T., Moroz J., Nowina-Konopka M., *Społeczeństwo informacyjne: istota, rozwój, wyzwania*, Warszawa 2006.
2) Ferreira-Fernandes K., *Internetowa partycypacja obywatelska: wyzwania I zagrożenia dla demokracji w erze cyfrowej*, „Wiedza Obronna" 2024, nr 3.
3) Fleszer D., *Wokół problematyki e-administracji*, „Roczniki Administracji i Prawa" 2014, nr 14.
4) Grodzka D., *Edemokracja*, „Infos" 2009, nr 14.
5) Hennen L., van Keulen I., Korthagen I., Aichholzer G., Lindner R., Nielsen R. Ø., *European e-democracy in practice*, Cham 2020.
6) Koczubiej S., *E-głosowanie jako element demokracji w społeczeństwie informacyjnym*, „Problemy Humanistyki" 2003/2004, nr 8/9.
7) Krimmer R., *E-voting as a New Form of Voting,* [w:] *Explorations in eGovernment & eGovernance*, vol. 2: *Selected proceedings of the Second International Conference on eGovernment and eGovernance*, A. Balci. , C. Can Actan , Dalbay O. (red.), Antalya 2010.
8) Lerner J., *Making Democracy Fun. How Game Design Can Empower Citizens and Transform Politics*, Londyn 2014.
9) Marczewska-Rytko M., *Idea demokracji bezpośredniej od okresu antycznego do czasów Internetu i globalizacji* [w:] *Demokracja bezpośrednia. Wymiar globalny i lokalny*, M. Marczewska-Rytko, A.K. Piasecki (red.), Lublin 2010.
10) Musiał-Karg M., *Głosowanie przez Internet Skąd czerpać wzorce i jak wprowadzać innowacje wyborcze?*, Warszawa 2024.
11) Parys, T, *Technologie ICT i ich wpływ na życie człowieka i społeczeństwa – wybrane problemy*, „Studia i Materiały Wydziału Zarządzania UW" 2024, nr 1.

Inne źródła

1) e-Demokracja w Unii Europejskiej: potencjał i wyzwania Rezolucja Parlamentu Europejskiego z dnia 16 marca 2017 r. w sprawie e-demokracji w Unii Europejskiej: potencjał i wyzwania (2016/2008(INI)), s. 3, https://www.europarl.europa.eu/doceo/document/TA-8-2017-0095_PL.html (dostęp: 7.12.2025 r.).
2) Public Participation Guide: Electronic Democracy, https://www.epa.gov/international-cooperation/public-participation-guide-electronic-democracy (dostęp: 6.01.2026 r.).

dr hab. Paweł Romaniuk, prof. UWM
Uniwersytet Warmińsko-Mazurski w Olsztynie
adres e-mail: pawel.romaniuk@uwm.edu.pl
ORCID: 0000-0002-7217-956X

Administracyjno-prawne warunki kreowania cyberbezpieczeństwa w samorządzie województwa (wybrane zagadnienia)

Administrative and legal conditions for creating cybersecurity in regional government (selected issues)

Streszczenie

Przedmiotowe cyberbezpieczeństwo jest zagadnieniem, które staje się ważne nie tylko dla organizacji biznesowych, ale również dla wszystkich podmiotów administracji publicznej. Cyberbezpieczeństwo stanowi współcześnie priorytet każdego państwa w zakresie globalnych zagrożeń, wpływających w różnym zakresie na poziom bezpieczeństwa. Rosnące zagrożenia cybernetyczne stanowią jedne z ważniejszych zagrożeń dla bezpieczeństwa organizacji publicznych. Zatem inwestowanie w rozwiązania, dotyczące gwarancji cyberbezpieczeństwa, stają się kluczowym priorytetem dla administracji publicznej, w tym dla samorządu województwa.

Wprowadzenie

Zamierzeniem Autora, z uwagi na niezwykle szeroki zakres prowadzonych rozważań naukowych, będzie wskazanie wybranych administracyjno-prawnych warunków kształtowania cyberbezpieczeństwa w wybranej jednostce samorządu terytorialnego, jakim jest samorząd województwa. Trzeba przy tym zaznaczyć, że dynamiczny i nieuchronny rozwój technologii informacyjno-komunikacyjnych w systemie państwa i samej administracji publicznej (ang. *Information and Communication Technologies*: ICT), jest działaniem aktywnie wspierającym integrację społeczną, podnoszącym przy tym jakość życia obywateli i budującym nowe i kreatywne narzędzia kontaktów międzyludzkich i instytucjonalnych. Właściwe wykorzystanie narzędzi ICT, zapewnia wprowadzenie wielu udogodnień w zaspokajaniu różnych potrzeb, obserwowanych w wymiarze społecznym, gospodarczym i informacyjnym[111]. W takich okolicznościach, niezwykle ważnym staje się zapewnienia odpowiedniego poziomu cyberbezpieczeństwa, którego głównym zadaniem jest

[111] Por. B. Kasprzyk, *Aspekty funkcjonowania e-administracji dla jakości życia obywateli*, „Nierówności Społeczne a Wzrost Gospodarczy" 2011, nr 23, s. 343-344.

ochrona i przeciwdziałanie różnym zagrożeniom, obejmującym wiele ważnych danych i informacji, które są w posiadaniu administracji publicznej, w tym przypadku - samorządu województwa. W rozdziale wykorzystano metodę opisową. Zastosowano również metodę dogmatyczno-prawną, której głównym zadaniem stała się analiza obowiązujących przepisów prawa oraz przegląd literatury.

Prawne umocowanie kompetencyjne samorządu województwa

Istotną rolę dla statusu prawnego województwa, miało prawne ukształtowanie zasadniczego podziału państwa, dotyczące szeroko rozumianego samorządu terytorialnego. Przyjęcie ustawy o wprowadzeniu zasadniczego trójstopniowego podziału terytorialnego państwa, na nowo zreformowało podział terytorialny państwa[112]. Ustawa ta, w opinii H. Izdebskiego, była drugą częścią zarówno reformy samorządowej oraz reformy centrum państwa[113]. Utworzenie z dniem 1 stycznia 1999 r. nowego porządku terytorialnego, tj. utworzenie gmin, powiatów i województw, nastąpiło po uchwaleniu i wejściu w życie Konstytucji Rzeczypospolitej Polskiej z 1997 r., która przy pewnych drobnych modyfikacjach, obowiązuje do dnia dzisiejszego[114]. W gminach i powiatach występuje wyłącznie władza samorządowa. Natomiast w województwach możemy mówić o swoistym dualizmie władzy, gdzie obok władzy samorządowej, reprezentowanej przez marszałka województwa z szerokim wachlarzem zadań i kompetencji, wpływających bezpośrednio na kształt rozwoju województwa, obecna jest również władza rządowa, reprezentowana przez wojewodę[115].

W ustawie zasadniczej pojawiła się naczelna zasada decentralizacji, która na nowo określiła naczelną zasadę ustroju państwa[116]. Był to ważny etap reformy samorządowej, który ugruntował model decentralizacji, jako kompozycji organizacji władzy publicznej. Rolą tego procesu było przypisanie podmiotom administracyjnym ustawowych oraz wyraźnie zdefiniowanych kompetencji, przekazanych im przez organy państwowe. Odbywać się to może w drodze ustawy, gdzie jednostki samorządu terytorialnego mogą realizować zadania w sposób niezależny, suwerenny, samodzielny, podlegający jedynie nadzorowi weryfikacyjnemu[117].

---

112 Ustawa z dnia 24 lipca 1998 r. o wprowadzeniu zasadniczego trójstopniowego podziału terytorialnego państwa (Dz. U. z 1998 r. Nr 96, poz. 603 ze zm.).

113 H. Izdebski, *Reformy samorządu terytorialnego oraz centrum administracyjnego i gospodarczego rządu po 1989 roku*, [w:] *Administracja państwowa i samorząd w ujęciu historyczno-prawnym. Wybrane zagadnienia*, E. Mareńca, P.B. Zientarski, B. Czwojdrak (red.), Warszawa 2018, s. 171.

114 Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1999 r. (Dz. U. z 1997 r. Nr 78, poz. 483 ze zm.), dalej: Konstytucja RP.

115 Por. Ł. Małota, *Samorząd terytorialny w Polsce od okresu międzywojennego do czasów współczesnych*, Łódź 2020, s. 94.

116 Patrz art. 15 ust. 1 Konstytucji RP.

117 Por. B. Dolnicki, *Samorząd terytorialny*, Warszawa 2019, s. 56-57; D. Dąbek, J. Zimmerman, *Decentralizacja przez samorząd terytorialny w ustawodawstwie i orzecznictwie pokonstytucyjnym*, [w:] *Samorząd terytorialny. Zasady ustrojowe i praktyka*, P. Sarnecki (red.),Warszawa 2005, s. 7-8.

Konstytucja RP, odwołuje się również do kluczowych uregulowań, dotyczących nie tylko wspomnianego ustroju, ale również i zadań jednostek samorządu terytorialnego na wszystkich jej poziomach. Zgodnie z art. 163 Konstytucji RP, samorząd terytorialny wykonuje zadania publiczne nie zastrzeżone przez Konstytucję lub ustawy dla organów innych władz publicznych. Głównym celem twórców reformy terytorialnej, było stworzenie, obok gminy - jako podstawowej jednostki samorządu terytorialnego - samorządowego powiatu i samorządowego województwa. Ustawa zasadnicza zapewniła możliwość tworzenia innych niż gmina jednostek samorządu terytorialnego[118]. Następstwem takich decyzji była reforma centralnych organów administracji publicznej, dokonanej za pomocą przekazania wielu ich zadań na poziom powiatu i województwa[119]. Przy czym Konstytucja RP, jak wskazuje J. Sobczak, otworzyła drogę w drodze ustawy, do stworzenia silnych podstaw dla ustanowienia samorządu terytorialnego szczebla województwa[120].

Samorząd województwa został ustanowiony na podstawie ustawy o samorządzie województwa[121], obok licznych, powiązanych z nim, pakietem przepisów[122]. Przyjęcie tak ważnych regulacji prawnych, było niejako gwarancją implementacji konstytucyjnej zasady decentralizacji władzy publicznej. Należy zaznaczyć, że ustrój województwa w Polsce silnie wkomponowuje się w pojęcie regionu, zwykle traktowanego jako „(...) najwyższa w hierarchii wewnątrzpaństwowej jednostka terytorialna państwa, stanowiąca najczęściej wyodrębniony geograficznie obszar o silnych więzach historycznych, kulturalnych, gospodarczych, społecznych i często etnicznych, w ramach którego prowadzona jest samodzielna polityka gospodarcza, społeczna i kulturalna, zabezpieczająca wspólnotę interesów społeczności określonego terytorium"[123]. Region powinien być zatem wyposażony w możliwość budowy wspólnoty interesów gospodarczych, komponowania reprezentacji organów, pochodzących z wyborów, kształtowania więzi społecznej, opartej na poczuciu wspólnej tożsamości i przynależności regionalnej oraz posiadać zdolność do realizacji zadań publicznych[124].

---

118 Art. 164 ust. 2 Konstytucji RP.

119 Por. H. Izdebski, *Reformy samorządu...*, op.cit., s. 171-179.

120 J. Sobczak, *Status prawny województwa*, „Przegląd Prawa Administracyjnego" 2023, vol. 6 , s. 228.

121 Ustawa z dnia 5 czerwca 1998 r. *o samorządzie województwa* (t.j. Dz. U. z 2025 r. poz. 581), dalej: u.s.w.

122 Do tego zestawu aktów normatywnych można zakwalifikować: ustawę z dnia 24 lipca 1998 r. *o zmianie niektórych ustaw określających kompetencje organów administracji publicznej w związku z reformą ustrojową państwa* (Dz.U. 1998 Nr 106, poz. 668 ze zm.); ustawę z dnia 24 lipca 1998 r. *o wejściu w życie ustawy o samorządzie powiatowym, ustawy o samorządzie województwa oraz ustawy o administracji rządowej w województwie* (Dz.U. 1998 Nr 99, poz. 631 ze zm.); ustawę z dnia 13 października 1998 r. - *Przepisy wprowadzające ustawy reformujące administrację publiczną* (Dz.U. 1998 Nr 133, poz. 872 ze zm.).

123 Patrz: E. Nowacka, *Zagadnienia regionalizacji w Polsce*, [w:] *Funkcjonowanie samorządu terytorialnego - doświadczenia i perspektywy*, S. Dolata (red.), t. 1, Opole 1998, s. 65.

124 Por. M. Kozak, A. Pyszkowski, R. Szewczyk, *Słownik rozwoju regionalnego*, Warszawa 2001, s. 44.

Trzeba również zaznaczyć, że Konstytucja RP w swojej preambule, ustanowiła ponadto niezwykle ważną zasadę pomocniczości, zwaną także zasadą subsydiarności, której zadaniem było wzmocnienie uprawnień obywateli a także ich wspólnot dla wszystkich poziomów samorządowych. Co do zasady, reguła pomocniczości w odniesieniu do organów administracji publicznej, zakłada wdrażanie zadań przez taki szczebel władzy, który jest najbliżej obywatela. W tym przypadku, to gmina, jako podstawowa jednostka samorządu terytorialnego, przejmuje taką rolę. Jednak samorząd województwa, również wykonuje zadania obwarowane realizacją zasady pomocniczości. Przykładem takiego zaangażowania może być np. pomoc finansowa oferowana samorządom potrzebującym takiego wsparcia, co przedkłada się w sposób pośredni na pomoc ich mieszkańcom. Filozofia tego działania zmierza do tego, aby organy administracyjne wyższego szczebla, wspierały i uzupełniały działalność funkcjonowania organów niższych, pod warunkiem, że nie są one w tym zakresie samowystarczalne a także taka pomoc jest prawnie dozwolona. Zasada pomocniczości, odwołująca się do samodzielności jednostek samorządu terytorialnego, akcentuje również ich odpowiedzialność, gdzie państwo nie powinno swoimi działaniami ograniczać społeczne inicjatywy, pozbawiając przy tym możliwość ponoszenia przez nie odpowiedzialności za podejmowane działania[125].

W odniesieniu do ustawy o samorządzie województwa, mieszkańcy województwa tworzą z mocy prawa regionalną wspólnotę samorządową, zaś mówiąc o województwie lub samorządzie województwa, należy przez to rozumieć regionalną wspólnotę samorządową oraz odpowiednie terytorium[126]. Samorząd województwa otrzymał możliwość bycia samodzielnie prawnym i rzeczywistym podmiotem władzy publicznej, do kompetencji którego należy wykonywanie zadań publicznych o charakterze wojewódzkim, niezastrzeżonych ustawami na rzecz organów administracji rządowej[127]. To z kolei przyczyniło się do uzyskania przez samorząd województwa samodzielności w wielu obszarach działalności, w szczególności:

- prawa do posiadania organu stanowiącego i wykonawczego, za pośrednictwem których wykonuje swoje zadania;
- kompetencji do uregulowania poprzez akty prawa miejscowego organu stanowiącego własnej organizacji wewnętrznej;
- posiadania własnego majątku i praw majątkowych;
- wykonywania przypisanych sobie zadań własnych, realizowanych w imieniu własnym i na własną odpowiedzialność;
- stanowienie aktów prawa miejscowego;

[125] Por. I. Sierpowska, *Zasada pomocniczości w pomocy społecznej*, „*Acta Universitatis Wratislaviensis*. Przegląd Prawa i Administracji" 2009, nr 3109 LXXIX, s. 205-206.

[126] Art. 1 ust. 1-2 u.s.w.

[127] Zob. art. 2 ust. 2 u.s.w.

- posiadania samodzielności gospodarki finansowej, wdrażanej na podstawie uchwały budżetowej;
- sądowej ochrony praw i obowiązków województwa[128].

Specyfika zadań samorządu województwa wynika z roli, jaką to województwo wypełnia. Za pomocą organów województwa (zarząd województwa i sejmik województwa), realizowane są zadania, które przybierają charakter zadań regionalnych, o czym literalnie wskazuje art. 16 ust. 1 u.s.w. Przy czym, podobnie jak to ma miejsce w przypadku zarówno gmin oraz powiatów, samorząd województwa, realizuje przyjęty przez Konstrukcję RP[129] główny podział zadań, na zadania własne i zlecone[130].

Warunki gwarancji cyberbezpieczeństwa w samorządzie województwa

Odwołując się do kształtowania cyberbezpieczeństwa w samorządzie województwa, należy ogólnie zauważyć, że zagadnienia dotyczące systemem bezpieczeństwa w szeroko rozumianej administracji publicznej, są uznawane w sposób generalny i traktowane, jako dobro należące do społeczeństwa. Bezpieczeństwo jest stanem, w którym zadaniem każdego państwa jest gotowość do reakcji w zakresie przeciwdziałania zagrożeniom a także likwidacja konsekwencji pojawienia się takich niebezpieczeństw[131]. Aktywność taka pozostaje w ścisłej korelacji z troską o zapewnienie gwarancji bezpieczeństwa przez państwo, ukierunkowane na powszechny dostęp do potrzeb i dóbr powszechnych.

Bezpieczeństwo zatem „(...) ma tak długą historię, jak długa jest historia ludzkości. Człowiek od zawsze miał żywotne i mniej istotne potrzeby i interesy, które zderzały się z potrzebami i interesami innych ludzi, którym to potrzebom i interesom zagrażały także najzwyklejsze fizyczne siły natury (pożary, burze, powodzie, trzęsienia ziemi, epidemie, mrozy i inne tego typu kataklizmy). Oprócz tych czysto zewnętrznych i fizycznych (materialnych) czynników, już od samego początku człowieka trapiły również rozterki i obawy wewnętrzne, świadomościowe, duchowe i psychologiczne"[132]. Inne, również interesujące podejście charakteryzujące bezpieczeń-

[128] Obszary samodzielności samorządu województwa prezentują np.: A. Szewc, *Ustawa o samorządzie województwa. Komentarz*, Warszawa 2008, s. 48-49; P. Jankowski, *Województwo jako region europejski*, Toruń 2013, s. 228-230.

[129] Art. 166 ust. 1-2 Konstytucja RP.

[130] Również w związku z określeniem dochodów jednostek samorządu terytorialnego, Trybunał Konstytucyjny w swoim wyroku dokonuje wyodrębnienia zadań województwa, na zadania własne i zlecone: wyrok Trybunału Konstytucyjnego z dnia 25 lipca 2006 r., sygn. akt K 30/04.

[131] Por. R. Gwardyński, *Racjonalizacja działań Policji na poziomie lokalnym* [w:] *Racjonalizacja zarządzania jednolitymi formacjami umundurowanymi odpowiedzialnymi za bezpieczeństwo wewnętrzne*, t. V, B. Wiśniewski, P. Lubiewski, T. Zwęgliński (red.), Warszawa 2020, s. 120.

[132] Stanowisko takie prezentuje S. Koziej, *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, „Bezpieczeństwo Narodowe" 2011, nr 18, s. 34.

stwo, odwołujące się do definicji i potocznego rozumienia tego pojęcia, przez długi okres było łączone ze stanem zabezpieczenia istnienia czy przetrwania. Jednak i takie stanowisko było kwestionowane, jako zbyt wąskie i nawet odrobinę konserwatywne. W nowym, współczesnym ujęciu - bezpieczeństwo oznacza nie tylko gwarancje nienaruszalnego przetrwania danego podmiotu, ale również swobodę jego naturalnego rozwoju[133]. Bezpieczeństwo staje się zatem stanem zapewnienia tzw. „dóbr uniwersalnych", obecnych obok innych pojęć, jak dobro, prawda, czy sprawiedliwość[134].

W analizie definicyjnej bezpieczeństwa, trafną ocenę prezentuje J. Prońko, według którego próba zdefiniowania bezpieczeństwa konkretnego podmiotu, uzależniona jest od precyzyjnego wyodrębnienia jego głównych wartości, czyli cech, mających kluczowe znaczenie dla jego bytności[135]. Cechy takie przyporządkowane są podmiotom, które realnie istnieją. Taka argumentacja dowodzi, że bezpieczeństwo może być przypisywane jedynie podmiotom faktycznie rzeczywistym. Przy czym byty traktowane jako abstrakcyjne, nie mają zdolności do odczuwania, zatem nie ma możliwości ocenić, czy faktycznie czują się w danej sytuacji bezpieczne czy zagrożone. Taki sposób myślenia, wyznacza zasadniczy zbiór zagrożeń i niebezpieczeństw w stosunku do każdego podmiotu. Mogą to być zatem zagrożenia dla jego egzystencji. Idąc dalej takim tokiem rozumowania, w przypadku człowieka, zagrożeniem jest jego byt, natomiast w stosunku do państwa, zagrożeniem dla jego wszystkich atrybutów jest sytuacja, w której państwo z różnych powodów, przestaje posiadać fundamentalne właściwości państwa. Bezpieczeństwo jest stanem, wymagającym ochrony, gdzie stan ten może być uzależniony od kształtowanych relacji poczucia zagrożenia z poczuciem bezpieczeństwa. Zatem im odczucie zagrożenia jest większe, tym poziom bezpieczeństwa maleje. W takich warunkach, o czym wspomina S. Pieprzny, bezpieczeństwo jest pochodną pojawienia się niebezpieczeństwa (zagrożenia)[136].

Na gruncie gwarancji bezpieczeństwa, rodzi się konieczność zapewnienia cyberbezpieczeństwa w samorządzie województwa, akcentując jej główne atrybuty, która w sposób naturalny i nieunikniony, na wielu płaszczyznach, dynamicznie się rozwija. Zatem coraz więcej działań podejmowanych jest w przestrzeni wirtualnej (cyfrowej), którą wyróżnia swoista kultura zachowań jej użytkowników, budująca

[133] Ocenę taką prezentuje: P. Majer, *W poszukiwaniu uniwersalnej definicji bezpieczeństwa wewnętrznego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 7 (4), s. 11.

[134] Więcej: B. Wiśniewski, J. Kozioł, J. Falecki, *Podejmowanie decyzji w sytuacjach kryzysowych*, Szczytno 2018, s. 14.

[135] J. Prońko, *Bezpieczeństwo państwa. Zarys teorii problemu i zadań administracji publicznej*, Bielsko-Biała 2007, s. 9-10.

[136] Więcej: S. Pieprzny, *Ochrona bezpieczeństwa i porządku publicznego w prawie administracyjnym*, Rzeszów 2007, s. 14.

rosnącą wirtualną społeczność. Należy również dbać o zapewnienie odpowiedniego poziomu kontroli nad obszarem funkcjonujących w instytucjach publicznych sieci teleinformatycznych, które każdego roku agregują coraz więcej danych i informacji, niejednokrotnie informacji prawnie chronionych, które w sytuacji ich nieautoryzowanego udostepnienia, mogłoby narazić takie podmioty na wiele strat, również w wymiarze finansowym. Zagadnienie cyberbezpieczeństwa, co słusznie zauważa K. Chałubińska-Jentkiewicz, „(...) odnosić się może do ściśle określonego obszaru działa związanych z bezpieczeństwem informacji (zawartości sieci), bezpieczeństwem komunikowania (przekazu) oraz bezpieczeństwem samej sieci umożliwiających komunikowanie, jednak nie wyczerpuje wszystkich kwestii związanych z potrzebami ochrony przed niepożądanymi działaniami w cyberprzestrzeni"[137]. Inny z autorów, C. Banasiński uważa, że cyberbezpieczeństwo jest procesem, zapewnianiającym bezpieczne funkcjonowanie w cyberprzestrzeni państwa jako całości, jego wszystkich struktur, osób fizycznych, prawnych a także innych podmiotów oraz zasobów informacyjnych, będących w globalnej cyberprzestrzeni[138]. Cyberbezpieczeństwo traktowane jest również, jako bezpieczeństwo sieci i systemów teleinformatycznych, szczególnie rozumiane, jako odporność systemów teleinformatycznych na działania naruszające w szczególności: dostępność, integralność, autentyczność lub poufność przechowywania, przekazywania, przetwarzania danych lub związanych z nimi usług cyfrowych[139]. Ważnym z punktu widzenia budowy systemu cyberbezpieczeństwa, jest ustawa o krajowym systemie cyberbezpieczeństwa[140]. Należy również przywołać wciąż obowiązującą Strategię Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, gdzie obecnie toczą się prace konsultacyjne nad nową strategią na lata 2025-2029[141].

Zagadnienie cyberbezpieczeństwa nie wyczerpuje wszystkich problemów, związanych z zapewnieniem należytej ochrony przed niepożądanymi działaniami w cyberprzestrzeni. Cyberprzestrzeń również w działaniach samorządu województwa, w ujęciu szerokim, o czym dowodzi T. Iwanek - stanowi globalną

[137] K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo - zagadnienia definicyjne*, „Cybersecurity and Law" 2019, nr 2, s. 13.

[138] C. Banasiński, *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, [w:] *Cyberbezpieczeństwo. Zarys wykładu*, C. Banasiński (red.), Warszawa 2018, s. 31.

[139] A. Brzostek, *Cyberbezpieczeństwo w administracji publicznej – aspekty prawne*, „Zeszyty Prawnicze" 2023, t. 23, nr 3,, s. 97.

[140] Ustawa z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (t.j. Dz. U. z 2024 r. poz. 1077 ze zm.). która określa organizację krajowego systemu cyberbezpieczeństwa, wskazując na zadania i obowiązki podmiotów, wchodzących w skład takiego systemu, charakteryzuje metody sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy a także wyznacza zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

[141] Strategia została przyjęta Uchwałą Nr 125 Rady Ministrów z dnia 22 października 2019 r. *w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024* (M. P. z 2019 r. poz. 1037), gdzie nadrzędnym celem Strategii jest podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorze publicznym, militarnym i prywatnym.

infrastrukturę informacyjną, określającą wzajemne relacje łączące ludzi (np. pracowników administracyjnych) z komputerami i ich praktycznym zastosowaniem. Przestrzeń komunikacyjna jest mechanizmem powiązań internetowych, ułatwiająca użytkownikom sieci tworzenie relacji w czasie rzeczywistym, składająca się z różnych systemów komunikacji elektronicznej. W ramach takiego procesu, przesyłane są dane pochodzące ze źródeł numerycznych oraz domeny informacyjnej, gdzie nośnik informacji stanowi centrum m.in. otwartego komunikowania się za pomocą połączonych ze sobą licznych komputerów i pamięci informatycznych, pracujących na całym świecie[142]. Cyberprzestrzeń wyróżniania jest określonymi cechami technicznymi. Można do nich zaliczyć m.in. otwartą architekturę, której najważniejszym budulcem jest Internet, ageograficzność, jako założenie braku istnienia jakichkolwiek granic fizycznych czy niematerialność, zależna od istniejącej struktury informatycznej[143].

Funkcjonowanie współczesnego Internetu, za pomocą którego samorząd województwa opiera realizację większości swoich zadań, swoboda komunikowania, czy możliwość korzystania z wielu elektronicznych usług (np. obsługa bankowa, dostęp do wielu repozytoriów danych itp.), bazuje na obecności nie tylko coraz bardziej rozbudowanej infrastrukturze informatycznej, ale również na kulturze jego twórców wraz z rosnącą liczbą użytkowników. Powszechność zastosowania, swoista prostota dostępność do danych i łatwość korzystania z urządzeń, zapewniających dostęp do Internetu, staje się wyzwaniem dla osób, budujących odpowiednie systemy zabezpieczeń sieci teleinformatycznych[144]. Należy to mieć na uwadze, gdyż coraz więcej informacji i danych w dobie postępu technologicznego, w sposób naturalny, zostaje przechowywanych w różnych systemach informatycznych.

Uwzględniając powyższe warunki, należy dopełnić wszelkiej staranności, aby w urzędach marszałkowskich, będących aparatem wspomagającym działanie organów województwa, dbać o właściwe środki zabezpieczające posiadane przez nie informacji. Jest to istotne tym bardziej, że w coraz większej liczbie instytucji publicznych, dokonuje się swoista „rewolucja" w zakresie ich funkcjonowania. Tradycyjna (papierowa) forma załatwiania spraw urzędowych, zostaje zastępowana formą elektroniczną, stosując tzw. elektroniczne zarządzanie dokumentami (EZD). Jest to bezpłatny system, którego specyfika, budowa i oferowane funkcje, realizują realne potrzeby polskiej administracji publicznej, w tym samorządu województwa. System ten, stworzony został przez specjalistów NASK[145] oraz ekspertów,

[142] Patrz więcej: T. Iwanek, *Cyberbezpieczeństwo na przykładzie własnych badań empirycznych*, „Bezpieczeństwo Obronność Socjologia" 2024, nr 1 (19), s. 89.

[143] R. Zięba (red.), *Bezpieczeństwo międzynarodowe w XXI wieku*, Warszawa 2018, s. 56-57.

[144] Więcej: T. Goban-Klas, *Cywilizacja medialna*, Warszawa 2005, s. 151-152.

[145] NASK (Naukowa i Akademicka Sieć Komputerowa) jest państwowym instytutem badawczym, zajmującym się cyberbezpieczeństwem.

wdrażających technologie informatyczne (IT), dostarczając funkcje cyfrowe, nowe rozwiązania technologiczne, dopasowane do potrzeb i wymagań stawianych instytucjom publicznym w dobie nie tylko rozwoju technologicznego, ale również w sferze możliwości pojawienia się wielu zagrożeń cyfrowych[146].

Obok przywołanych poglądowo systemów ochrony, trzeba pamiętać również o możliwych zagrożeniach, które mogą pojawić się w samorządzie województwa. Zostanie wymienionych tylko kilka, które są wyzwaniem dla osób, budujących politykę bezpieczeństwa teleinformatycznego urzędów marszałkowskich. Pierwszym zagrożeniem może być *ransomware*, który jest atakiem hakerów, przejmujących kontrolę nad danymi lub siecią, żądając w zamian opłaty za przywrócenie i dostęp do przejętych danych[147]. Kolejnym wyzwaniem dla polityki bezpieczeństwa internetowego samorządu województwa może być zagrożenie związane z *malware*. Jest to złośliwe oprogramowanie (np. wirusy, konie trojańskie i oprogramowanie szpiegowskie), które potrafi w sposób nielegalny, często podstępny, zainfekować za pomocą złośliwego oprogramowania sam komputer a także urządzenia, które są podłączone do komputera (drukarki, rutery, kamery)[148]. Można spotkać jeszcze i inne zagrożenia, na które samorządy województw muszą szczególnie uważać. Mogą to być niebezpieczeństwa, które powiązane są z wykorzystaniem socjotechniki, gdzie urzędnicy mogą być podstępnie zachęcani do otwierania złośliwych dokumentów, dołączanych do wiadomości przesyłanych na służbowe poczty elektroniczne. Ważna przy tym staje się odpowiednia edukacja w tym zakresie a także odpowiedzialność, związana z równoczesnym zachowaniem ostrożności podczas weryfikacji takich załączników. Taka forma przestępczego działania przybiera najczęściej formę *phishingu*. Stosuje się ją za pośrednictwem wiadomości e-mail wraz z załącznikiem, którego otwarcie może spowodować kradzież danych osobowych lub finansowych a także zainfekowanie komputera złośliwym i inwazyjnym oprogramowaniem[149]. Można też spotkać się z działaniami hackerskimi, gdzie zamierzeniem oszustów jest nieautoryzowany

[146] https://www.gov.pl/web/ezd-rp/o-ezd-rp (dostęp: 12.09.2025 r.) - system EZD zapewnia przejrzystość działania instytucji publicznych. Jest to również skuteczne narzędzie kierownictwa do zarządzania jednostką. System EZD gwarantuje niższe koszty funkcjonowania podmiotów administracji publicznej i umożliwia m.in. prowadzenie korespondencji elektronicznej pomiędzy podmiotami publicznymi i klientami, podmiotami publicznymi poprzez integrację z ePUAP-em oraz pracownikami danej jednostki, w ramach komunikacji wewnętrznej.

[147] Według raportu Threat Landscape 2022, przygotowanego przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) - w 2022 r. ataki typu *ransomware* nadal były jednym z głównych cyberzagrożeń, które stają się z każdym rokiem coraz bardziej złożone. Z danych ENISA wynika, że średnia wartość okupu zapłaconego w atakach *ransomware* podwoiła się z 71 000 euro w 2019 r. do 150 000 euro w 2020 r. Szacuje się, że globalne szkody, wywołane przez ataki tego typu, mogą w nieodległej przyszłości osiągnąć wartość blisko 50 mld euro. https://www.europarl.europa.eu/topics/pl/article/20220120STO21428/cyberbezpieczenstwo-glowne-i-nowe-zagrozenia (dostęp: 12.09.2025 r.).

[148] Patrz więcej: Raport ENISA Threat Landscape, European Union Agency for Cybersecurity, 2022, s. 49.

[149] Więcej: Raport ENISA Threat Landscape, European Union Agency for Cybersecurity, 2022, s. 50-69.

dostęp do danych, które są w posiadaniu urzędów. Pojawia się przy tym ryzyko ich ujawnienia, co może narazić jednostkę na wielkie szkody, zarówno finansowe, jak i wizerunkowe[150].

Rolą wszystkich instytucji publicznych, w tym samorządów województw, jest zapewnienia odpowiedniego poziomu koordynacji infrastruktury, określanej miałem infrastruktury krytycznej. Tego rodzaju budowa, powinna być realizowana na wszystkich szczeblach, zaczynając od szczebla centralnego, kończąc na szczeblu regionalnym i lokalnym, przy wzajemnej współpracy i stworzeniu jednorodnego sytemu reakcji na różnego rodzaju zagrożenia w sieci. Administracja publiczna, w szczególności administracja rządowa, powinna również na bieżąco regulować prawnie te rozwiązania, na podstawie których będzie mogła sprawnie monitorować postępy wdrażania systemów ochronnych i współpracować z podmiotami, w tym z urzędami marszałkowskimi, będącymi właścicielami poszczególnych elementów infrastruktury krytycznej[151]. Infrastruktura sieci teleinformatycznej w Polsce wraz z systemami zabezpieczeń, nieustannie jest rozwijana i dostosowana do potrzeb i wymogów technicznych, przy jednoczesnym dostosowaniu jej do specyfiki warunków prawnych. Przy czym samorządy województw, realizują kluczowe zadania, gdyż to one odpowiadając za implementację regionalnych programów operacyjnych, przy ścisłej współpracy z Ministerstwem Funduszy i Polityki Regionalnej, organizują konkursy na projekty, zarządzają nimi i wdrażają przedsięwzięcia, zgodnie z polskimi i unijnymi przepisami prawa a także krajową strategią rozwoju[152], na podstawie której przyjmowane są regionalne strategie rozwoju (poszczególnych województw)[153]. Kreując zatem właściwy poziom zabezpieczeń cyfrowych, inwestując w cyberbezpieczeństwo, samorządy województw muszą pamiętać o odpowiednim poziomie zapewnienia bezpieczeństwa cyfrowego, gdyż to on determinuje bezpieczny rozwój usług publicznych, świadczonych drogą elektroniczną, budując jednocześnie zaufanie do instytucji publicznych[154].

[150] Por. M. Matacz, W. Vodičková, *Zjawisko phishingu w Polsce*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności"2023, t. 9, nr 1, s. 110-120.

[151] Por. S. Woszek, *Cyberbezpieczeństwo państw w XXI wieku na przykładzie Rzeczypospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego"2022, nr 27 (14), s. 212-213.

[152] Krajowa Strategia Rozwoju Regionalnego 2030 rozwija postanowienia Strategii na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.). W strategii tej wskazano nowy model rozwoju regionalnego Polski. Przewidziano w nim rozwój kraju, jako społecznie i terytorialnie zrównoważony, dzięki któremu efektywnie będą rozwijane oraz wykorzystywane miejscowe zasoby i potencjały wszystkich regionów. Strategia jest podstawowym dokumentem strategicznym polityki regionalnej państwa w perspektywie do 2030 r. (Strategia przyjęta uchwałą Nr 102 Rady Ministrów z dnia 17 września 2019 r.).

[153] Przykładem regionalnej strategii jest przyjęta dnia 18 lutego 2020 r. przez Sejmik Województwa Warmińsko-Mazurskiego uchwał Nr XIV/243/20 - „Warmińsko-Mazurskie 2030. Strategia rozwoju społeczno-gospodarczego". Strategia rozwoju społeczno-gospodarczego należy do czwartej generacji dokumentów strategicznych, przygotowywanych na poziomie województw w Polsce. Strategia Warmińsko-Mazurskie 2030, stanowiąca rozwinięcie i modyfikację dotychczasowego podejścia do procesów rozwoju, jest rzeczywistą odpowiedzią na zmieniające się otoczenie województwa.

[154] Por. H. Wyrębek, Z. Ciekanowski, *Administracja publiczna w cyberprzestrzeni*, „Przegląd Policyjny" 2019, t. 136, nr 4, , s. 19.

Zakończenie

Problematyka cyberbezpieczeństwa stanowi obecnie ważny element sprawnie funkcjonującej administracji publicznej. Podejmowane w tekście rozważania naukowe związane z cyberbezpieczeństwem, dotyczą zasad i reguł rozwoju tego segmentu w samorządzie województwa. Jest to o tyle ważne, gdyż rozwijająca się cyfryzacja usług publicznych a wraz z nią zwiększająca się ilość gromadzonych i przetwarzanych danych, wymusza na instytucjach publicznych zastosowanie nowoczesnych instrumentów technologicznych. Pojawiające się jednocześnie zagrożenia cybernetyczne, powodują konieczność wzmacniania odpowiedzialności za działania podejmowane w Internecie, nie tylko wśród urzędników, ale również i obywateli. Wiąże się z tym posiadanie akceptowalnego poziomu wiedzy o potencjalnych zagrożeniach w cyberprzestrzeni, np. poprzez społeczną edukację czy prowadzenie szkoleń dla wszystkich pracowników, bezpośrednio lub pośrednio odpowiedzialnych za zapewnienie odpowiedniego poziomu cyberbezpieczeństwa. Niezbędna staje się również faktyczna zdolność urzędów do budowania odpowiednich mechanizmów chroniących systemy teleinformatyczne przed różnymi zagrożeniami.

Funkcjonowania samorządów województw i nieustanny rozwój całej administracji publicznej, powoduje konieczność inwestycji zarówno w infrastrukturę informatyczną, jak również w budowę świadomości pracowników na temat potencjalnych niebezpieczeństw. Ważne przy tym jest konstruowanie spójnych procedur, których zadaniem jest szybkie reagowanie na pojawiające się incydenty. Stąd każdy z urzędów marszałkowskich musi dbać o wysoki poziom bezpieczeństwa cyfrowego, chroniąc posiadane przez siebie dane i zasoby obywateli, wzmacniając zaufanie społeczne do jednostek samorządów terytorialnych. W perspektywie długookresowej, cyberbezpieczeństwo jest nie tylko kluczowym wyzwaniem technologicznym dla urzędów, ale również i filarem sprawnego i skutecznego sposobu zarządzania sprawami publicznymi.

Bibliografia:

Akty prawne

1) Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1999 r. (Dz. U. z 1997 r. Nr 78, poz. 483 ze zm.).
2) Ustawa z dnia 24 lipca 1998 r. *o wprowadzeniu zasadniczego trójstopniowego podziału terytorialnego państwa* (Dz. U. z 1998 r. Nr 96, poz. 603 ze zm.).
3) Ustawa z dnia 24 lipca 1998 r. *o wejściu w życie ustawy o samorządzie powiatowym, ustawy o samorządzie województwa oraz ustawy o administracji rządowej w województwie* (Dz.U. 1998 Nr 99, poz. 631, ze zm.).
4) Ustawa z dnia 24 lipca 1998 r. *o zmianie niektórych ustaw określających kompetencje organów administracji publicznej w związku z reformą ustrojową państwa* (Dz.U. 1998 Nr 106, poz. 668, ze zm.).

5) Ustawa z dnia 13 października 1998 r. - *Przepisy wprowadzające ustawy reformujące administrację publiczną* (Dz.U. 1998 Nr 133, poz. 872, ze zm.).
6) Ustawa z dnia 5 czerwca 1998 r. *o samorządzie województwa* (t.j. Dz. U. z 2025 r. poz. 581).
7) Ustawa z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (t.j. Dz. U. z 2024 r. poz. 1077 ze zm.).
8) Uchwała Nr 102 Rady Ministrów z dnia 17 września 2019 r. w sprawie przyjęcia Krajowej Strategii Rozwoju Regionalnego 2030.
9) Uchwała Nr 125 Rady Ministrów z dnia 22 października 2019 r. *w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024* (M. P. z 2019 r. poz. 1037).
10) Uchwała Nr XIV/243/20 Sejmiku Województwa Warmińsko-Mazurskiego z dnia 18 lutego 2020 r. - „Warmińsko-Mazurskie 2030. Strategia rozwoju społeczno-gospodarczego".

Literatura

1) Banasiński C., *Podstawowe pojęcia i podstawy prawne bezpieczeństwa w cyberprzestrzeni*, [w:] *Cyberbezpieczeństwo. Zarys wykładu*, C. Banasiński (red.), Warszawa 2018.
2) Brzostek A., *Cyberbezpieczeństwo w administracji publicznej – aspekty prawne*, „Zeszyty Prawnicze" 2023,. t. 23, nr 3.
3) Chałubińska-Jentkiewicz K., *Cyberbezpieczeństwo - zagadnienia definicyjne*, „Cybersecurity and Law" 2019, nr 2.
4) Dąbek D., Zimmerman J., *Decentralizacja przez samorząd terytorialny w ustawodawstwie i orzecznictwie pokonstytucyjnym*, [w:] *Samorząd terytorialny. Zasady ustrojowe i praktyka*, P. Sarnecki (red.), Warszawa 2005.
5) Dolnicki B., *Samorząd terytorialny*, Warszawa 2019.
6) Goban-Klas T., *Cywilizacja medialna*, Warszawa 2005.
7) Gwardyński R., *Racjonalizacja działań Policji na poziomie lokalnym* [w:] *Racjonalizacja zarządzania jednolitymi formacjami umundurowanymi odpowiedzialnymi za bezpieczeństwo wewnętrzne*, t. V, B. Wiśniewski, P. Lubiewski, T. Zwęgliński (red.), Warszawa 2020.
8) Izdebski H., *Reformy samorządu terytorialnego oraz centrum administracyjnego i gospodarczego rządu po 1989 roku*, [w:] *Administracja państwowa i samorząd w ujęciu historyczno-prawnym. Wybrane zagadnienia*, E. Mareńca, P.B. Zientarski, B. Czwojdrak (red.), Warszawa 2018.
9) Iwanek T., *Cyberbezpieczeństwo na przykładzie własnych badań empirycznych*, „Bezpieczeństwo Obronność Socjologia" 2024, nr 1(19).
10) Jankowski P., *Województwo jako region europejski*, Toruń 2013.
11) Kasprzyk B., *Aspekty funkcjonowania e-administracji dla jakości życia obywateli*, „Nierówności Społeczne a Wzrost Gospodarczy" 2011, nr 23.

12) Kozak M., Pyszkowski A., Szewczyk R., *Słownik rozwoju regionalnego*, Warszawa 2001.
13) Koziej S., *Bezpieczeństwo: istota, podstawowe kategorie i historyczna ewolucja*, „Bezpieczeństwo Narodowe" 2011, nr 18.
14) Majer P., *W poszukiwaniu uniwersalnej definicji bezpieczeństwa wewnętrznego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 7 (4).
15) Małota Ł., *Samorząd terytorialny w Polsce od okresu międzywojennego do czasów współczesnych*, Łódź 2020.
16) Matacz M., Vodičková W., *Zjawisko phishingu w Polsce*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności" 2023, t. 9, nr 1.
17) Nowacka E., *Zagadnienia regionalizacji w Polsce*, [w:] *Funkcjonowanie samorządu terytorialnego - doświadczenia i perspektywy*, S. Dolata (red.), t. 1, Opole 1998.
18) Pieprzny S., *Ochrona bezpieczeństwa i porządku publicznego w prawie administracyjnym*, , Rzeszów 2007.
19) Prońko J., *Bezpieczeństwo państwa. Zarys teorii problemu i zadań administracji publicznej*, Bielsko-Biała 2007.
20) Sierpowska I., *Zasada pomocniczości w pomocy społecznej*, „*Acta Universitatis Wratislaviensis*. Przegląd Prawa i Administracji", 2009, nr 3109 LXXIX.
21) Sobczak J., *Status prawny województwa*, „Przegląd Prawa Administracyjnego" 2023, vol.6.
22) Szewc A., *Ustawa o samorządzie województwa. Komentarz*, Warszawa 2008.
23) Wiśniewski B., Kozioł J., Falecki J., *Podejmowanie decyzji w sytuacjach kryzysowych*, Szczytno 2018.
24) Woszek S., *Cyberbezpieczeństwo państw w XXI wieku na przykładzie Rzeczypospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2022, nr 27 (14).
25) Wyrębek H., Ciekanowski Z., *Administracja publiczna w cyberprzestrzeni*, „Przegląd Policyjny" 2019, t.136, nr 4.
26) Zięba R. (red.), *Bezpieczeństwo międzynarodowe w XXI wieku*, Warszawa 2018.

Orzecznictwo

1) Wyrok Trybunału Konstytucyjnego z dnia 25 lipca 2006 r., sygn. akt K 30/04.

Inne źródła

1) Raport ENISA Threat Landscape, European Union Agency for Cybersecurity, 2022.
2) https://www.gov.pl/web/ezd-rp/o-ezd-rp (dostęp: 12.09.2025 r.).
3) https://www.europarl.europa.eu/topics/pl/article/20220120STO21428/cyberbezpieczenstwo-glowne-i-nowe-zagrozenia (dostęp: 12.09. 2025 r.).

dr Dominika Skoczylas
Uniwersytet Szczeciński
adres e-mail: dominika.skoczylas@usz.edu.pl
ORCID: 0000-0003-1231-8078

dr Kamil Czaplicki
Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie
adres e-mail: k.czaplicki@uksw.edu.pl
ORCID: 0000-0002-3777-4339

Podniesienie poziomu e-usług i wzmocnienie cyberbezpieczeństwa w jednostkach samorządu terytorialnego

Improving the level of e-services and strengthening cybersecurity in local government units

Streszczenie

Transformacja cyfrowa przyczyniła się do modernizacji administracji publicznej zarówno na płaszczyźnie organizacyjno-prawnej, jak i usługowej. Jednym z kluczowych elementów jest podniesienie poziomu e-usług, co należy rozumieć przez pryzmat poprawy jakości, dostępności i bezpieczeństwa. Cyfryzacja przyczyniła się do rozwoju e-usług, pozwoliła na zwiększenie efektywności i skuteczności w zakresie rozwiązywania spraw administracyjnych. Nie ulega wątpliwości, że narzędzia teleinformatyczne zapewniają komfort obsługi petenta, co sprzyja budowaniu pozytywnego wizerunku administracji publicznej. Działania na rzecz cyfryzacji usług publicznych są szczególnie widoczne w jednostkach samorządu terytorialnego. Dostosowanie samorządów do współczesnych standardów cyfrowych stanowi jednak niemałe wyzwanie z uwagi na zapewnienie cyberbezpieczeństwa systemów teleinformatycznych, jak i użytkowników cyberprzestrzeni.

Celem rozdziału jest przedstawienie niezbędnych działań, jakie powinny podjąć jednostki samorządu terytorialnego w celu podniesienia poziomu e-usług i wzmocnienia cyberbezpieczeństwa. W rozdziale podniesiono znaczenie technologii informacyjno-komunikacyjnych w kontekście poprawy jakości świadczonych usług i usprawnienia procedur administracyjnych. Analiza tematu, pozwoli odpowiedzieć na następujące pytania: „jakie czynniki wpływają na rozwój e-usług?" oraz „ czy warunkiem *sine qua non* świadczenia e-usług przez jednostki samorządu terytorialnego jest wdrożenie tzw. polityk cyberbezpieczeństwa?". W pierwszej części pracy wskazano cele cyfryzacji administracji publicznej, rodzaje e-usług oraz potencjalne

bariery w ich wdrażaniu w jednostkach samorządu terytorialnego. Druga część zawiera charakterystykę potencjalnych cyberzagrożeń i warunków cyberbezpieczeństwa świadczenia e-usług przez samorządy oraz propozycje działań na rzecz podniesienia poziomu e-usług i wzmocnienia cyberbezpieczeństwa w samorządach.

Determinanty transformacji cyfrowej jednostek samorządu terytorialnego

Transformacja cyfrowa przyczyniła się do zmiany sposobu zarządzania sprawami publicznymi, co w skali makro wpłynęło na rozwój elektronicznej administracji, tzw. e-administracji. Dostosowanie administracji publicznej do nowego modelu opartego na e-komunikacji i e-zarządzaniu wymagało wprowadzenia zmian natury organizacyjno-prawnej, społecznej i technologicznej. Ważnym elementem świadczącym o skuteczności zastosowania środków komunikacji elektronicznej[155] w funkcjonowaniu administracji publicznej jest zapewnienie dostępności e-usług na kilku istotnych poziomach: informacyjnym interakcyjnym, transakcyjnym i integracyjnym. Należy przy tym dodać, że komunikacja elektroniczna sprzyja tworzeniu relacji zarówno o charakterze wewnętrznym (pomiędzy urzędami), jak i tych mających charakter zewnętrzny (pomiędzy urzędami a obywatelami)[156]. Punktem wyjścia dla omawianej w rozdziale materii jest wskazanie podstawowych celów informatyzacji administracji publicznej i cyfryzacji usług. Wydaje się, że pierwszym z nich jest zasygnalizowane powyżej, usprawnienie komunikacji pomiędzy urzędami a obywatelami/przedsiębiorcami oraz wdrożenie transparentnych kanałów komunikacji w wewnętrznych strukturach administracji publicznej. Nie bez znaczenia jest to, że administracja dąży do maksymalnego wykorzystania technologii informacyjno-komunikacyjnych, czego efektem ma być zwiększenie spraw urzędowych rozpatrywanych zdalnie (online). Takie działania czynią zadość nadrzędnemu postulatowi transformacji cyfrowej, czyli konieczności standaryzacji usług świadczonych w ramach e-administracji, tj. usieciowienia urzędów, unowocześnienia infrastruktury i narzędzi cyfrowych oraz digitalizacji dokumentów. Nie sposób nie zgodzić się z Ewą Lecką, która wskazuje, że „strategiczny kierunek informatyzacji usług publicznych jest ściśle powiązany z koncepcją państwa usługowego (...)", „ (...) a tworzone systemy teleinformatyczne mają na celu ułatwianie obywatelom dostępu do informacji publicznej i załatwienia spraw urzędowych."[157]. Transfor-

[155] Zgodnie z art. 2 pkt 5 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2024 r. poz. 1513) środki komunikacji elektronicznej – rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy wykorzystaniu transmisji danych między systemami teleinformatycznymi, a w szczególności pocztę elektroniczną.

[156] P. Romaniuk, *Tradycje i przyszłość administracji publicznej w zakresie rozwoju e-usług*, „Journal of Modern Science" 2020, t. 44, nr 1, s. 276-277.

[157] E. Lecka, *Ewolucja e-usług administracji publicznej w Polsce w kontekście przyspieszenia społecznego*, „Wschodni Rocznik Humanistyczny" 2024, t. XXI, nr 4, s. 41.

macja cyfrowa nie ominęła również jednostek samorządu terytorialnego, co można zauważyć przede wszystkim w kluczowych obszarach, takich jak: dostępność e-usług dla mieszkańców, automatyzacja obiegu spraw w urzędach, cyberbezpieczeństwo infrastruktury teleinformatycznej i przetwarzania danych osobowych w e-rejestrach.

Można wymienić kilka powodów wdrażania e-usług w jednostkach samorządu terytorialnego. Oprócz przyśpieszenia procesów urzędowych (chociażby w zakresie procedury zamówień publicznych czy wymiany danych) na uwagę zasługują związane z tym efektywne zarządzanie informacją (transfer danych) i automatyzacja przekazu. Cyfryzacja usług na poziomie lokalnym ma wpłynąć na transparentność i interoperacyjność e-usług, lepsze administrowanie danymi (standaryzacja procedur w zakresie zarządzania dokumentami i efektywności obiegu spraw), zapewnić elastyczność działania organów administracji publicznej, pozwolić na oszczędność czasu i kosztów zarządzania sprawami publicznymi (zarówno po stronie urzędu, jak i petentów). Należy także odnotować, że e-usługi wpływają na rozwój sprzyjający włączeniu społecznemu i odpowiadający oczekiwaniom osób ze szczególnymi potrzebami (w tym osób z niepełnosprawnościami)[158]. Działania na rzecz inkluzywności odzwierciedlają aktualne wymagania dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych[159]. Zapewnienie dostępności cyfrowej jest kolejnym z zadań jednostek samorządu terytorialnego w obszarze cyfryzacji urzędów. Na płaszczyźnie prawno-technologicznej konieczne są natomiast działania dotyczące wdrożenia polityk cyberbezpieczeństwa. Nie można bowiem zapomnieć, że z uwagi na cyfrowy wymiar wykonywania zadań z zakresu użyteczności publicznej, jednostki samorządu terytorialnego są zobligowane do stworzenia odpowiednich polityk cyberbezpieczeństwa. Katalog środków na rzecz cyberbezpieczeństwa jest dość szeroki i uwzględnia bezpieczeństwo systemów i sieci teleinformatycznych, przetwarzania informacji i danych osobowych oraz wzmacnianie kompetencji cyfrowych użytkowników cyberprzestrzeni[160]. Automatyzację, mobilność, decentralizację, dostępność, przejrzystość i dostępność e-usług, jednostki samorządu terytorialnego osiągną tylko wtedy, gdy będą kierować się zasadami użyteczności publicznej i obowiązującymi przepisami prawa[161].

158 E. Szczygieł, R. Śliwa, J. Stąporek, *Ku cyfryzacji usług publicznych – transformacja cyfrowa Unii Europejskiej*, „Rocznik Administracji Publicznej" 2024, nr 10, s. 280-281.

159 Zob. ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2023 r. poz. 1440).

160 D. Skoczylas, *Determinanty cyfryzacji a instrumenty prawnofinansowe wspierające wzrost poziomu cyberbezpieczeństwa w jednostkach samorządu terytorialnego – analiza projektu „Cyberbezpieczny Samorząd"*, „Studia Politologiczne" 2025, vol. 77, s. 379- 380.

161 M. Kowalczyk, *Nowoczesne technologie wykorzystywane w jednostkach samorządu terytorialnego na przykładzie gminy Zabór w latach 20182022*, „Dyskurs Prawniczy i Administracyjny" 2025, nr 1, s. 77-78.

Rodzaje e-usług w jednostkach samorządu terytorialnego

W dobie intensywnej cyfryzacji administracji publicznej, jednostki samorządu terytorialnego stanęły przed nowymi, niezwykle ważnymi wyzwaniami związanymi z zapewnieniem bezpieczeństwa informacji oraz cyberodporności. Obecne funkcjonowanie urzędów administracji publicznej jak też realizacja wielu usług dla mieszkańców uzależniona jest od technologii, dlatego też władze jednostek samorządu terytorialnego muszą zwracać szczególną uwagę na bezpieczeństwo i zapewnienie ciągłości działania urzędów.

Współcześnie wzrasta rola jednostek samorządu terytorialnego w zapewnianiu mieszkańcom usług publicznych. Od czasu reformy samorządowej z 1999 r. jednostki samorządu terytorialnego jako najbliższy obywatelowi szczebel administracji publicznej przejmują na siebie coraz więcej zadań, stając się kluczowym ogniwem w realizacji usług publicznych i najszybciej odpowiadając na lokalne potrzeby społeczne. Dynamiczny rozwój technologiczny, a także stale postępująca cyfryzacja administracji publicznej sprawia, iż jednostki samorządu terytorialnego, w tym w głównie gminy uczestniczą w cyfrowej transformacji państwa. Zgodnie z danymi statycznymi udostępnionymi przez portal Statista.com w 2020 r. ponad 90 % gospodarstw domowych posiadało dostęp do internetu[162]. Wykorzystanie internetu przez mieszkańców, zauważone było też przez organy administracji publicznej, które to zaczęły udostępniać więcej e-usług publicznych. W 2020 r. aż 98,6% jednostek administracji publicznej udostępniało mieszkańcom usługi przez internet[163]. Jednostki samorządu terytorialnego wykorzystują nowe technologie głównie do kontaktu z mieszkańcami oraz zarządzania własnej działalności. Wykorzystywane są one również do poprawy efektywności działania, usprawnienia funkcjonowania, zwiększenia dostępności usług oraz zwiększenia transparentności działania urzędników. Rozwój e-usług w jednostkach samorządu terytorialnego stanowi jeden z kluczowych elementów procesu informatyzacji administracji publicznej, której celem jest zwiększenie efektywności działań organów władzy publicznej, poprawa dostępności usług publicznych oraz wzmocnienie partycypacji obywatelskiej.

E-usługi w jednostkach samorządu terytorialnego klasyfikowane są według różnych kryteriów, jednakże jednym z najczęściej stosowanych jest tzw. stopień dojrzałości e-usług, który to odzwierciedla zakres interakcji pomiędzy obywatelem a administracją. W kryterium tym, wyróżnia się e-usługi informacyjne, polegające na jednostronnym udostępnianiu informacji publicznej za pośrednictwem stron internetowych, w tym też Biuletynu Informacji Publicznej czy portali gminnych.

[162] https://www.statista.com/statistics/1036205/households-internet-access-poland/ (dostęp: 14.02.2026 r.).

[163] To nie brak finansów największą barierą w cyfryzacji gmin i samorządów. Większy problem to kompetencje cyfrowe urzędników, https://biznes.newseria.pl/news/to-nie-brak-finansow,p140084589 (dostęp: 14.02.2026 r.).

Usługi informacyjne wykorzystywane są do realizacji zasady jawności działania administracji publicznej. Istotną kategorią e-usług są tzw. e-usługi interakcyjne, umożliwiające dwustronny kontakt użytkownika z urzędem, w szczególności pobieranie formularzy (np. wykorzystywane w kampanii wymiany dowodów osobistych z papierowych na polimerowe), składanie zapytań czy też rezerwacja wizyt w urzędach. Komunikacja ta, ma szczególne znaczenie dla usprawnienia obsługi interesantów oraz przygotowania czynności proceduralnych, choć jeszcze bez wywoływania skutków prawnych. Skutki te występują dopiero w kolejnej, najbardziej zaawansowanej formie e-usług tzw. transakcyjnych. Usługi te umożliwiają pełne załatwienie sprawy administracyjnej drogą elektroniczną, w tym złożenie wniosku, prowadzenie korespondencji, wniesienie opłaty oraz otrzymanie rozstrzygnięcia. Najczęściej wykorzystywane są one do spraw meldunkowych, podatkowych, świadczeń społecznych na poziomie lokalnym czy też udostępniania danych z rejestrów publicznych. E-usługi transakcyjne wymagają zarówno identyfikacji stron jak też najwyższego poziomu bezpieczeństwa i integralności danych.

Odrębną, ale bardzo istotną kategorią e-usług są tzw. usługi wewnętrzne, skierowane w całości do pracowników urzędów i obejmujące takie usługi jak m.in elektroniczne zarządzanie dokumentacją czy systemy obiegu spraw. Warto również zauważyć, iż możliwy jest również podział e-usług w jednostkach samorządu terytorialnego z punktu widzenia funkcjonalnego, wyróżniając tym samym usługi o charakterze administracyjnym, finansowym, społecznych oraz partycypacyjnym, związanym m.in. z elektronicznymi konsultacjami społecznymi czy też budżetem obywatelskim[164].

Nowe technologie niosą niestety również zagrożenia, narażając Jednostki samorządu terytorialnego na nowe, coraz bardziej złożone cyberprzestępstwa. W 2024 r. Naukowa Akademicka Sieć Komputerowa NASK odnotowała ponad 60000 tyś zgłoszeń i zarejestrowała 103449 incydentów bezpieczeństwa[165]. Liczba incydentów zakwalifikowanych do sektora administracja publiczna przekroczyła 2300 przypadków, z czego dodatkowe incydenty obejmują takie sektory jak energetyka, oświata, transport, ochrona zdrowia, kultura, wodociągi, gospodarka odpadami, które również w dużej mierze są zarządzane przez organy administracji publicznej[166]. W kontekście wzrastających zagrożeń, budowanie cyberodporności jednostek samorządu terytorialnego jest niezbędnym elementem zapewnienia bezpieczeństwa danych, zaufania społecznego oraz ciągłości działania administracji publicznej.

[164] Szerzej na temat e-usług: K. Wojsyk, L. Grochowski, *e-Usługa*, [w:] *Wielka Encyklopedia Prawa, t. XXII, Prawo informatyczne*, G. Szpor, L. Grochowski (red.), Warszawa 2021, s. 171- 172.

[165] Raport roczny z działalności CERT Polska w 2024 r., https://cert.pl/uploads/docs/Raport_CP_2024.pdf#page=89 (dostęp: 14.02.2026 r.).

[166] Ibidem.

Podmioty administracji publicznej jako podmioty kluczowe. Standardy cyberbezpieczeństwa a dyrektywa NIS2

Wdrażanie zasad e-administracji w jednostkach samorządu terytorialnego nie można identyfikować wyłącznie przez pryzmat potencjalnych korzyści, ale również barier w marko i mikro skali. Zasadne wydaje się być stwierdzenie, że „sukces transformacji cyfrowej zależy od dwóch zasadniczych czynników: poziomu adaptacji cyfrowej oraz potencjału pracowników, którzy muszą nieustannie podnosić swoje kwalifikacje, by nadążyć za nowymi wymaganiami rynkowymi."[167]. Oczywiście, bariery natury psychologiczno-społecznej, polegające na z jednej strony braku zaufania do nowych technologii (preferowanie tradycyjnego modelu załatwiania spraw urzędowych), z drugiej braku kompetencji cyfrowych petentów i pracowników urzędów stanowią wyzwania na polu budowy otwartej, tj. dostępnej cyberprzestrzeni. Nie ulega jednak wątpliwości, że czynnikami ograniczającymi cyfryzację jednostek samorządu terytorialnego są kwestie prawne (np. brak odpowiednich regulacji dotyczących zastosowania nowych technologii na poziomie urzędu) czy technologiczne (niedostosowanie infrastruktury teleinformatycznej, brak sprzętu, oprogramowań, antyinnowacyjność, brak interoperacyjności usług z systemami centralnymi). Powyższe pozostaje w związku z nieprzystosowaniem urzędów pod kątem organizacyjnym (strukturalnym), a także niedostatecznym dofinansowaniem działań na rzecz cyfryzacji. Uznanie na mocy dyrektywy NIS2[168] podmiotów administracji publicznej za podmioty kluczowe powoduje, że samorządy muszą podjąć działania na rzecz podniesienia poziomu e-usług i wzmocnienia cyberbezpieczeństwa.

Na kanwie Konstytucji Rzeczypospolitej Polskiej trudno szukać wytycznych w sprawie cyberbezpieczeństwa. Skądinąd podlega ono konstytucyjnej ochronie prawnej jako szczególny rodzaj bezpieczeństwa[169]. W ślad za Łukaszem Dudarskim należy wskazać, że podstawy cyfryzacji znajdują swój wyraz Konstytucji RP. Autor podkreśla, że „Konstytucja RP gwarantuje obywatelom prawo do uzyskiwania informacji o działalności organów władzy publicznej (art. 61) oraz chroni prywatność i autonomię informacyjną jednostki (art. 51)"[170]. W tym znaczeniu zasady i tryb

[167] K. Wasilewski, *E-administracja w Polsce: determinanty rozwoju i bariery wdrożeniowe*, „Przegląd Prawno-Ekonomiczny" 2025, nr 2, s. 102.

[168] 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 NIS2), (Dz.Urz.UE.L 2022 Nr 333), str. 80.

[169] Art. 5 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483) stanowi, że Rzeczpospolita Polska strzeże niepodległości i nienaruszalności swojego terytorium, zapewnia wolności i prawa człowieka i obywatela oraz bezpieczeństwo obywateli, strzeże dziedzictwa narodowego oraz zapewnia ochronę środowiska, kierując się zasadą zrównoważonego rozwoju, dalej: Konstytucja RP.

[170] Ł. Dudarski, *Cyfryzacja administracji publicznej w Polsce: wyzwania i perspektywy*, „Zeszyty Naukowe Collegium Witelona" 2024, nr 53(4), s. 58.

gromadzenia oraz udostępniania (przetwarzania) danych osobowych oraz prawo obywateli do informacji o działalności organów władzy publicznej mają również wydźwięk cyfrowy. Powyższe implikuje konieczność podjęcia działań na rzecz zapewnienia wysokiego poziomu cyberbezpieczeństwa w jednostkach samorządu terytorialnego.

Niewątpliwie jedną z kluczowych zasad funkcjonowania jednostek samorządu terytorialnego jest zasada subsydiarności (pomocniczości). W kontekście cyfryzacji przejawia się ona przede wszystkim w ułatwieniu dostępu do e-usług na poziomie lokalnym oraz zwiększeniu niezależności (autonomii) samorządów dzięki korzystaniu z narzędzi online np. w przypadku przetwarzaniu danych w chmurze obliczeniowej. Jak zauważa Sławomir Patyra „zespolenie mieszkańców w ramach tej wspólnoty nie ma tylko charakteru terytorialnego, ale wyraża się także w realizacji dobra wspólnego, jakim jest prawidłowy rozwój cywilizacyjny społeczności lokalnej (...)"[171]. Z uwagi na istniejące zagrożenia, właściwie cyberzagrożenia dla prawidłowego rozwoju e-usług w jednostkach samorządu terytorialnego zasadne wydaje się wdrożenie odpowiednich polityk cyberbezpieczeństwa. Zapewnienie odporności lokalnych systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[172] stanowi punkt odniesienia w kwestii wzmocnienia cyberbezpieczeństwa w gminach, powiatach i województwach. Cyberzagrożenia, takie jak *phishing,* złośliwe oprogramowania, np. ransomware i DDoS, *spyware, eksploit* mają często różnorodny charakter i oddziałują zarówno na użytkowników narzędzi cyfrowych (urzędników i petentów), jak i infrastrukturę krytyczną[173]. W efekcie mogą spowodować nie tylko przerwanie ciągłości świadczenia usługi, ale również utratę danych (przekazanie osobom trzecim), straty finansowe czy spadek zaufania petentów do e-administracji. Konieczność zmian w zakresie wzmocnienia cyberbezpieczeństwa na poziomie lokalnym zauważył również ustawodawca unijny. Jak już wskazano w rozdziale w świetle dyrektywy NIS2 podmioty administracji publicznej na szczeblu regionalnym (lokalnym) uznane zostały za tzw. podmioty kluczowe, co wyraża się m.in. przez pryzmat wprowadzenia odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych, w celu zarządzania ryzykiem oraz zapobiegania wpływowi incydentów na odbiorców ich usług lub na inne usługi bądź minimalizowania takiego wpływu. Środkami tymi są m.in. wdrożenie polityki analizy ryzyka i bezpieczeństwa systemów informatycznych, obsługa incydentu, za-

[171] S. Patyra, *Samorząd terytorialny jako czynnik wzmacniający zasadę dobra wspólnego,* „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2018, nr 80(1), s. 232.

[172] Zgodnie z definicją cyberbezpieczeństwa, zob. art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 ze zm.), dalej: u.k.s.c.

[173] D. Skoczylas, *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe*, „Prawo w Działaniu. Sprawy Karne" 2023, nr 53, s. 101-102.

pewnienie bezpieczeństwa łańcucha dostaw czy praktyki cyberhigieny i szkolenia w zakresie cyberbezpieczeństwa (art. 21 dyrektywy NIS2). Dyrektywa NIS2 stanowi impuls do zmian w ustawodawstwie krajowym. Jej pokłosiem ma być nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa. Niemniej jednak w oczekiwaniu na zmiany prawa, jednostki samorządu terytorialnego już dzisiaj muszą wdrażać działania na rzecz podniesienia poziomu e-usług i wzmocnienia cyberbezpieczeństwa na poziomie lokalnym.

Propozycje działań na rzecz podniesienia poziomu e-usług i wzmocnienia cyberbezpieczeństwa w samorządach

Cyberodporność zdefiniować możemy jako zdolność do nieprzerwanego osiągania zamierzonych celów pomimo wystąpienia niekorzystnych zdarzeń związanych z cyberbezpieczeństwem[174]. Cyberodporność jest zatem czymś innym niż cyberbezpieczeństwo, które definiujemy jako odporność systemów informacyjnych na działanie naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy[175]. Definicja cyberodporności dopuszcza wystąpienie cyberataku (incydentu) ale kluczowe jest aby podmiot był przygotowany na incydent i był w stanie go obsłużyć. Przez obsługę incydentu, zgodnie z art. 2 pkt 13 u.k.s.c. rozumiemy zespół działań podejmowanych w celu rozpoznania, analizowania i reagowania na incydent. W ramach reagowania na incydent podejmujemy m.in. identyfikację zagrożenia, analizę techniczną i ocenę wpływu incydentu na organizację, działania naprawczej i przeciwdziałające, zgłoszenie do właściwych organów takich jak CERT lub Urząd Ochrony Danych Osobowych. Reasumując, cyberodporność jednostek samorządu terytorialnego to zdolność do przeciwdziałania cyberzagrożeniom, reagowanie na wystąpienie ataku lub awarii oraz zapewnienie ciągłości działania po wystąpieniu cyberataku[176].

Rola cyberodporności nabrała szczególnego znaczenia w związku z sytuacją geopolityczną po zaatakowaniu przez Rosję Ukrainy w 2022r. Polska jako państwo graniczne stało się celem cyberterroryzmu rosyjskiego. Cyberataki obejmowały takie sektory jak infrastruktura wodna, energetyka, administracja publiczna, sieci pomocowe dla Ukrainy czy nawet systemy wyborcze[177].

---

174 F. Björck, M. Henkel, J. Stirna, J. Zdravkovic, *Cyber Resilience – Fundamentals for a Definition*, [w:] *New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing*, vol. 353, A.Rocha, A. M. Correia., S. Costanzo,, L. P. Reis (red.)), Cham 2015 s. 312.

175 B. Szafrański *Cyberbezpieczeństwo*, [w] *Wielka Encyklopedia Prawa, t. XXII, Prawo Informatyczne*, G. Szpor, L. Grochowski (red.), Warszawa 2021, s. 88.

176 Szerzej na temat definicji cyberodporności M.S. de Araujo, B.A.S. Machado,. F.U. Passos, *Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance*, "Applied Science" 2024, nr 14(5), 2116.

177 https://businessinsider.com.pl/wiadomosci/polska-rosyjskie-cyberataki-na-infrastrukture-krytyczna-co-wiemy/94l8q3g?utm_source=chatgpt.com (dostęp: 15.02.2026 r.).

Cyberodporność jednostek samorządu terytorialnego należy rozpatrywać na wielu poziomach, zarówno w odniesieniu do działań zewnętrznych (skierowanych do innych podmiotów i obywateli) jak i działań wewnętrznych. Od 1 stycznia 2025 r. jednostki samorządu terytorialnego zobowiązane były do wdrożenia e-doręczeń. Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych[178] wprowadziła obowiązek wdrożenia systemu e-doręczeń opartego na usłudze rejestrowanego doręczenia elektronicznego. Proces informatyzacji urzędów administracji publicznej, w tym jednostek samorządu terytorialnego przewiduje pełną informatyzację urzędów już od 1 stycznia 2028 r. kiedy to nastąpi obowiązek stosowania elektronicznego zarządzania dokumentacją. Ideą systemu e-doręczeń jest przeniesienie rozwiązań znanych z listów poleconych do komunikacji elektronicznej i zastosowanie e-doręczeń do realizacji wymiany korespondencji wymagającej przez nadawcę potwierdzenia jej nadania lub odbioru[179]. Organy administracji publicznej, w tym jednostki samorządu terytorialnego w komunikacji wewnętrznej (pomiędzy podmiotami publicznymi) stosować mają tzw. cyfrową domyślność, czyli przesyłać całą dokumentację drogą elektroniczną z wykorzystaniem usługi e-doręczeń. Cyfrowa domyślność realizowana jest zgodnie z deklaracją w sprawie administracji elektronicznej wygłoszoną w Tallinie 6 października 2017 r. w myśl której „Usługi publiczne powinny być dostępne domyślnie cyfrowo, z zapewnieniem przez państwo alternatywnych dróg komunikacji dla obywateli niechcących lub niemogących ich używać w tej postaci"[180].

Wdrożenie e-doręczeń ma doprowadzić do całkowitego (a przynamniej znacznego) ograniczenia papieru w urzędach administracji publicznej i wdrożenia kolejnego poziomu informatyzacji administracji publicznej. Powyższe zapewnić ma możliwości korzystania z jednego, własnego adresu do doręczeń elektronicznych, który będzie mógł być wykorzystany do korespondencji ze wszystkimi pozostałymi podmiotami korzystającymi z usług rejestrowanego doręczenia elektronicznego. E-doręczenia umożliwią również realizację idee odmiejscowienia procesu doręczania korespondencji poprzez umożliwienie wysyłania i odbierania korespondencji z dowolnego miejsca (i czasu).

Ustawodawca przewidział również pozostawienie osobom wykluczonym cyfrowo lub tym, które na wymianę korespondencji w postaci elektronicznej z różnych przyczyn nie są jeszcze gotowe, komfortu korzystania z aktualnie dostępnej przesyłki listowej poprzez tzw. usługę hybrydową, która co warto zauważyć, jednostki samorządu terytorialnego obejmie dopiero 1 stycznia 2029 r. Prawidłowe a co

178 Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (t.j. Dz. U. z 2024 r. poz. 1045 ze zm.).

179 Szerzej na temat e-doręczeń, M. Wilbrandt-Gotowicz, K. Czaplicki, A. Gryszczyńska, M. Świerczyński, K. Świtała, K. Wojsyk, [w:] *Doręczenia elektroniczne. Komentarz, wyd. II*, M. Wilbrandt-Gotowicz, K. Czaplicki, A. Gryszczyńska, M. Świerczyński, K. Świtała, K. Wojsyk (red.),Warszawa 2025.

180 https://www.gov.pl/web/ia/deklaracja-tallinska-w-sprawie-e-administracji (dostęp: 15.02.2026 r.).

najważniejsze bezpieczne wdrożenie systemu e-doręczeń i Elektronicznego Zarządzania Dokumentacją (EZD) musi być sprzężone z zapewnieniem odpowiedniego poziomu cyberodporności.

Niestety systemy klasy EZD były już przedmiotem cyberataków. W 2022 r. doszło do ataku typu *ransomware* na system EZD Mazowieckiego Urzędu Wojewódzkiego, w wyniku którego dokonano zaszyfrowania systemu „Wrota Mazowsza". Pomimo tego, że sam atak nie wpłynął na funkcjonowanie Urzędu Marszałkowskiego Województwa Mazowieckiego to skutki odczuły niektóre jednostki samorządu terytorialnego które korzystały z systemu EZD wdrożonego w ramach realizacji projektu „wrota mazowsza"[181]. Duża część jednostek samorządu terytorialnego w województwie mazowieckim do teraz nie odzyskała danych, utraconych w tym incydencie, rodzi to nie tylko problemy organizacyjne, ale powoduje również niechęć i złe nastawienie urzędników do wdrażania analogicznych rozwiązań.

Stan informatyzacji i cyberbezpieczeństwa jednostek samorządu terytorialnego budził i nadal budzi wiele zastrzeżeń. Najwyższa Izba Kontroli wielokrotnie badała poziom bezpieczeństwa danych i wdrażanie cyberbezpieczeństwa w samorządzie terytorialnym. 17 kwietnia 2025 r. opublikowano wyniki kontroli pt. „Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego"[182]. W ramach powyższej kontroli sprawdzono funkcjonowanie 24 urzędów w tym 17 urzędów gmin i 7 starostw powiatowych. Konkluzje z kontroli są bardzo negatywne. Najwyższe Izba Kontroli stwierdziła 222 nieprawidłowości, co ostatecznie przerodziło się na stwierdzenie iż „zadania w zakresie zapewnienia bezpieczeństwa informacji nie były skutecznie, rzetelnie i prawidłowo wykonywane w większości skontrolowanych urzędów jednostek samorządu terytorialnego, a NIK negatywnie oceniła przygotowanie do zapewnienia ciągłości działania systemów informatycznych w 71 % tych urzędów. Istotne nieprawidłowości ujawniono w 23 z 24 objętych kontrolą jednostek, w tym w przypadku dwóch urzędów sformułowano negatywną ocenę ogólną[183]. Co więcej, działania w zakresie organizacji zapewnienia bezpieczeństwa informacji nie były w pełni skutecznie, należycie i prawidłowo realizowane. Urzędy nie przeprowadzały analiz bezpieczeństwa i nie potrafiły identyfikować posiadanych zasobów, co doprowadzało do braku kontroli nad ich bezpieczeństwem. Ponad 1/3 urzędów nie opracowało lub nie wdrożyło prawidłowo Systemu Zarządzania Bezpieczeństwem Informacji, którego obowiązek wdrożenia zapisano w rozporządzeniu o Krajowych

[181] https://platformacyberbezpieczenstwa.pl/aktualnosci/atak-ransomware-na-wrota-mazowsza/?utm_source=chatgpt.com (dostęp: 15.02.2026 r.).

[182] Raport Najwyższej Izby Kontroli nr ewidencyjny: P/24/004 https://www.nik.gov.pl/kontrole/P/24/004/?utm_source=chatgpt.com (dostęp: 15.02.2026 r.).

[183] Raport Najwyżej Izby Kontroli, pt. Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego s. 8

Ramach Interoperacyjności[184]. Zgodnie z art. 19 ust. 1 KRI Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Dodatkowo w 20% badanych urzędów System Zarządzania Bezpieczeństwem Informacji nie był aktualizowany, co również było złamaniem przepisów rozporządzenia KRI, w tym w szczególności art. 19 ust 2 pkt 1, który nakłada na kierowników podmiotu publicznego zapewnienia warunków umożliwiających aktualizację regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.

Powyższe oznacza, iż przeszło połowa badanych podmiotów nie realizowała obowiązków prawnych nałożonych wprost w przepisach prawa. Warto przypomnieć, iż krajowe ramy interoperacyjności określają wymagania dla systemów teleinformatycznych administracji publicznej, a głównym celem ich ustanowienia było zapewnienie bezpieczeństwa i interoperacyjności systemów używanych w administracji publicznej. W celu zapewnienia bezpieczeństwa systemów KRI nałożyły obowiązek wdrożenia Systemu Zarządzania Bezpieczeństwem Informacji wzorowanego na rozwiązaniach normy ISO PN-ISO/IEC 27001 i będącego zestawem zasad i procedur stosowanych w celu zarządzania bezpieczeństwem informacji w organizacji. Składniki Systemu Zarządzania Bezpieczeństwem Informacji określone są w art. 19 rozporządzenia KRI i obejmują takie elementy jak inwentaryzację posiadanych zasobów, wykonywanie okresowych analiz ryzyka, monitorowanie uprawnień osób zaangażowanych do przetwarzania informacji, zapewnienie szkoleń pracowników , zapewnienie ochrony informacji przed głównymi znanymi ryzykami, a także wprowadzenie procedur bezzwłocznego zgłaszania incydentów naruszających bezpieczeństwo informacji. Ponadto KRI nakładają obowiązek przeprowadzania nie rzadziej niż raz na rok audytu wewnętrznego w zakresie bezpieczeństwa informacji[185].

Fakt iż 53% badanych przez Najwyższą Izbę Kontroli podmiotów nie wdrożyło powyższych wymogów budzić może bardzo duże obawy o bezpieczeństwo informacji przetwarzanych w tych podmiotach. Ponadto w 71% badanych urzędów nie ustanowiono polityk ciągłości działania oraz planów odtworzenia działania systemów informatycznych i informacyjnych. NIK dopatrzył się nieprawidłowości w większości badanych urzędów (83%). Nieprawidłowości te dotyczyły takich obszarów jak:

[184] Rozporządzenie Rady Ministrów z dnia 21 maja 2024 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. poz. 773), dalej: KRI

[185] Szerzej na temat krajowych ram interoperacyjności, A. Gryszczyńska, M. Ganczar, *Rejestry i systemy informacyjne a zadania samorządu terytorialnego (interoperacyjność)* [w:] *System Prawa Samorządu Terytorialnego. Tom III. Samodzielność samorządu terytorialnego – granice i perspektywy*, I. Lipowicz (red.), Warszawa 2023.

zabezpieczenia serwerowni, sporządzania kopii zapasowych, braku w umowach na zakup usług IT lub serwis sprzętu/oprogramowania odpowiednich zapisów w zakresie bezpieczeństwa informacji.

Negatywne wyniki kontroli przeprowadzonej przez Najwyższą Izbę Kontroli, są potwierdzeniem wyników wcześniejszych kontroli. W 2024 r. przeprowadzono badanie wybranych jednostek samorządu terytorialnego na terytorium województwa podlaskiego. W toku kontroli sprawdzono jak zapewniana jest ochrona i prawidłowość przetwarzania danych, w tym danych osobowych gromadzonych w formie elektronicznej na stronach internetowych i w poczcie elektronicznej. Kontrola wykazała olbrzymie zaniedbania związane z ochroną danych osobowych, nieświadomość zagrożeń oraz brak jednoznacznych wytycznych. W rezultacie kontroli wykazano m.in. używanie przez jednostki samorządu terytorialnego prywatnych adresów mailowych do celów służbowych. W skrzynkach e-mailowych wykazano, iż w sposób nieprawidłowy przetwarzano dane osobowe osób fizycznych w tym imiona, nazwiska, adresy, numery PESEL, numery telefonów), dane o ich stanie zdrowia (m.in. wyniki badań lekarskich), dane o korzystaniu ze świadczeń opieki społecznej, dane o zatrudnieniu i wysokości wynagrodzenia oraz dane o sytuacji rodzinnej[186].

Negatywne wnioski płyną również z kontroli przeprowadzonej przez Najwyższą Izbę Kontroli w województwie zachodniopomorskim. W wyniku kontroli nr. I/23/001/LSZ pt. „Zapewnienie bezpieczeństwa teleinformatycznego przez jednostki samorządu terytorialnego województwa zachodniopomorskiego" wykazano wieloletnie zaniedbania dotyczące cyberbezpieczeństwa, brak skutecznych procedur reagowania na zagrożenia, a także wykorzystywanie oprogramowania, zawierającego krytyczne luki bezpieczeństwa. Jak wskazano w wystąpieniu pokontrolnym NIK „samorządy te nie były w stanie zapewnić skutecznej ochrony przed potencjalnymi atakami cyberprzestępców"[187]. W wyniku kontroli wykazano szereg nieprawidłowości, w tym m.in. wskazano iż żaden z kontrolowanych urzędów nie dysponował kompletną dokumentacją bezpieczeństwa przewidywaną zarówno w rozporządzeniu KRI jak i w normie PN-ISO/IEC 27001, połowa skontrolowanych urzędów nie przygotowała procedury odtworzenia utraconych zasobów na wypadek cyberataku. Nie weryfikowano kompletności i prawidłowości tworzenia kopii zapasowych, a w jednym z urzędów kopia zapasowa była tworzona w taki sposób, że w przypadku zawirusowania serwera głównego, zostałaby ona automatycznie zainfekowana. Wykazano również błędy w konfiguracji oprogramowania, co istotnie obniżało poziom bezpieczeństwa. Warto też zauważyć, iż w większości kontrolowanych gmin nie powołano osoby do kontaktu z CSIRT, co stanowiło istotną barierę w zgła-

[186] https://www.nik.gov.pl/aktualnosci/bezpieczenstwo-ochrony-danych-osobowych-w-jst.html (dostęp: 15.02.2026 r.).
[187] https://www.nik.gov.pl/aktualnosci/zachodniopomorskie-gminy-cyberzagrozenia.html (dostęp: 15.02.2026 r.).

szaniu i obsłudze cyber incydentów[188]. W raporcie NIKu podkreślono również brak lub bardzo małą wiedzę pracowników badanych urzędów o cyberzagrożeniach. Większość pracowników (60%) nie potrafiło rozpoznać *phishingu*, 75% nie znało zasad tworzenia silnych haseł oraz nie potrafiło zabezpieczyć urządzeń mobilnych. Ponad 90% pracowników nie potrafiło wskazać procedur reagowania na incydent i nie znało konsekwencji ryzykownych działań online.

Negatywny obraz bezpieczeństwa danych osobowych i cyberbezpieczeństwa w jednostkach samorządu terytorialnego wyłania się również z decyzjach Prezesa Urzędu Ochrony Danych Osobowych. W wyszukiwarce orzeczeń Prezesa Urzędu Ochrony Danych Osobowych można odnaleźć ponad 50 decyzji przeciwko jednostkom samorządu terytorialnego[189]. Prezes Urzędu Ochrony Danych Osobowych (Prezesa UODO) coraz częściej kontroluje i nakłada administracyjne kary finansowe na podmioty publiczne w tym gminy, gdy te wykazują się brakiem adekwatnych zabezpieczeń lub całkowitym lekceważeniem zasad cyberbezpieczeństwa. Przykładem takiej decyzji Prezesa UODO, może być decyzja przeciwko wójtowi Gminy N. z dnia 20 grudnia 2023 r.[190] nakładająca karę pieniężną w wysokości 50 000 zł za niezastosowanie odpowiednich środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych, w szczególności w zakresie wdrożenia zdolności do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania oraz zdolności do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Podobną karę nałożył Prezes Urzędu na Burmistrza Miasta Z. w ramach postępowania prowadzonego w 2022 r. Zgodnie z decyzją o sygnaturze DKN.5131.56.2022 Prezes Urzędu nałożył na Burmistrza karę finansową w wysokości 30 000 zł. za dobór nieskutecznych zabezpieczeń systemu informatycznego wykorzystywanego do przetwarzania danych osobowych oraz braku odpowiedniego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych w systemach informatycznych objętych naruszeniem, w szczególności w zakresie podatności, błędów oraz ich możliwych skutków dla tych systemów oraz podjętych działań minimalizujących ryzyko ich wystąpienia[191]. Decyzje Prezesa Urzędu Ochrony Danych Osobowych wskazują, podobnie jak raporty z kontroli Najwyższej Izby Kontroli, że stan cyberbezpieczeństwa jednostek samorządu terytorialnego jest daleki od doskonałości i wymaga jeszcze wiele pracy po stronie zarówno jednostek samorządu terytorialnego jak i podmiotów odpowiedzialnych za cyberbezpieczeństwo, w tym CSIRT i właściwe ministerstwa.

188 Ibidem.

189 https://orzeczenia.uodo.gov.pl/search (dostęp: 15.02.2026 r.).

190 Decyzja PUODO o sygnaturze DKN.5131.34.2022.

191 https://orzeczenia.uodo.gov.pl/document/urn:ndoc:gov:pl:uodo:2022:dkn_5131_56/content?query= (dostęp: 15.02.2026 r.).

Podsumowanie

Cyberodporność jednostek samorządu terytorialnego powinna być priorytetem władz i kadry zarządzającej podmiotów publicznych, musi być traktowana jako stały, kompleksowy proces zarządzania ryzykiem i bezpieczeństwa informacji. Warunkiem *sine qua non* świadczenia e-usług przez jednostki samorządu terytorialnego jest wdrożenie tzw. polityk cyberbezpieczeństwa, dzięki którym możliwe będzie osiągnięcie celów cyfryzacji administracji publicznej, zapewnienie różnorodnych e-usług oraz ograniczenie potencjalnych barier w ich wdrażaniu w jednostkach samorządu terytorialnego. W ramach polityki cyberbezpieczeństwa samorządy powinny wdrożyć polityki analizy ryzyka i bezpieczeństwa systemów informatycznych, określić standardy obsługi incydentów, zapewnić bezpieczeństwo łańcucha dostaw i położyć nacisk na kwestię cyberhigieny Tym samym cyberodporność powinna być kluczowym elementem zapewnienia ciągłości działania urzędów i świadczenia usług publicznych.

Niestety wyniki kontroli NIK oraz decyzje wydane przez Prezesa Urzędu Ochrony Danych Osobowych wskazują, że wiele samorządów nadal nie spełnia podstawowych standardów bezpieczeństwa, co negatywnie wpływa nie tylko na funkcjonowanie tych urzędów ale również na prawa i obowiązki mieszkańców. Należy mieć nadzieję, że dyrektywa NIS2 a także nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa zwiększy świadomość istotności cyberodporności oraz przyczyni się do poprawy funkcjonowania podmiotów publicznych.

Bibliografia:

Akty prawne

1) Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78, poz. 483).
2) Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2024 r. poz. 1513).
3) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2024 r. poz. 1077 ze zm.).
4) Ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz. U. z 2023 r. poz. 1440).
5) Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (t.j. Dz. U. z 2024 r. poz. 1045 ze zm.).
6) 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. Urz. UE 2022, L 333/80).

7) Rozporządzenie Rady Ministrów z dnia 21 maja 2024 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. poz. 773).

Literatura

1) Araujo M.S. de, Machado B.A.S., Passos F.U., *Resilience in the Context of Cyber Security: A Review of the Fundamental Concepts and Relevance*, "Applied Science" 2024 , nr 14(5), 2116.
2) Björck F., Henkel M., Stirna J., Zdravkovic J., *Cyber Resilience – Fundamentals for a Definition*, [w:] *New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing*, vol. 353, A.Rocha, A. M. Correia., S. Costanzo,, L. P. Reis (red.), Cham 2015.
3) Dudarski Ł., *Cyfryzacja administracji publicznej w Polsce: wyzwania i perspektywy*, „Zeszyty Naukowe Collegium Witelona" 2024, nr 53(4).
4) Gryszczyńska A., Ganczar M., *Rejestry i systemy informacyjne a zadania samorządu terytorialnego (interoperacyjność)* [w:] *System Prawa Samorządu Terytorialnego. Tom III. Samodzielność samorządu terytorialnego – granice i perspektywy*, I. Lipowicz (red.), Warszawa 2023.
5) Kowalczyk M., *Nowoczesne technologie wykorzystywane w jednostkach samorządu terytorialnego na przykładzie gminy Zabór w latach 20182022*, „Dyskurs Prawniczy i Administracyjny" 2025, nr 1.
6) Lecka E., *Ewolucja e-usług administracji publicznej w Polsce w kontekście przyspieszenia społecznego*, „Wschodni Rocznik Humanistyczny" 2024, t. XXI, nr 4.
7) Patyra S., *Samorząd terytorialny jako czynnik wzmacniający zasadę dobra wspólnego*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2018, nr 80(1), s. 231-239.
8) Romaniuk P., *Tradycje i przyszłość administracji publicznej w zakresie rozwoju e-usług*, „Journal of Modern Science" 2020, t. 44, nr 1.
9) Skoczylas D., *Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe*, „Prawo w Działaniu. Sprawy Karne" 2023, nr 53,
10) Skoczylas D., *Determinanty cyfryzacji a instrumenty prawnofinansowe wspierające wzrost poziomu cyberbezpieczeństwa w jednostkach samorządu terytorialnego – analiza projektu „Cyberbezpieczny Samorząd"*, „Studia Politologiczne" 2025, vol. 77.
11) Szafrański B., *Cyberbezpieczeństwo*, [w] *Wielka Encyklopedia Prawa, t. XXII, Prawo Informatyczne,* G. Szpor, L. Grochowski (red.), Warszawa 2021.
12) Szczygieł E., Śliwa R., Stąporek J., *Ku cyfryzacji usług publicznych – transformacja cyfrowa Unii Europejskiej*, „Rocznik Administracji Publicznej" 2024, nr 10.

13) Wasilewski K., *E-administracja w Polsce: determinanty rozwoju i bariery wdrożeniowe*, „Przegląd Prawno-Ekonomiczny" 2025, nr 2.
14) Wilbrandt-Gotowicz M., Czaplicki K., Gryszczyńska A., Świerczyński M., Świtała K., Wojsyk K., [w:] *Doręczenia elektroniczne. Komentarz, wyd. II*, M. Wilbrandt-Gotowicz, K. Czaplicki, A. Gryszczyńska, M. Świerczyński, K. Świtała, K. Wojsyk (red.),Warszawa 2025.
15) Wojsyk K., Grochowski L. , *e-Usługa,* [w:] *Wielka Encyklopedia Prawa, t. XXII, Prawo informatyczne*, G. Szpor, L. Grochowski (red.), Warszawa 2021.

Inne źródła

1) https://businessinsider.com.pl/wiadomosci/polska-rosyjskie-cyberataki-na-infrastrukture-krytyczna-co-wiemy/94l8q3g?utm_source=chatgpt.com (dostęp: 15.02.2026 r.).
2) https://www.gov.pl/web/ia/deklaracja-tallinska-w-sprawie-e-administracji (dostęp: 15.02.2026 r.).
3) https://www.nik.gov.pl/aktualnosci/bezpieczenstwo-ochrony-danych-osobowych-w-jst.html (dostęp: 15.02.2026 r.).
4) https://www.nik.gov.pl/aktualnosci/zachodniopomorskie-gminy-cyberzagrozenia.html (dostęp: 15.02.2026 r.).
5) https://orzeczenia.uodo.gov.pl/document/urn:ndoc:gov:pl:uodo:2022:dkn_5131_56/content?query= (dostęp: 15.02.2026 r.).
6) https://orzeczenia.uodo.gov.pl/search (dostęp: 15.02.2026 r.).
7) https://platformacyberbezpieczenstwa.pl/aktualnosci/atak-ransomware-na-wrota-mazowsza/?utm_source=chatgpt.com (dostęp: 15.02.2026 r.).
8) https://www.statista.com/statistics/1036205/households-internet-access-poland/ (dostęp: 14.02.2026 r.).
9) Raport roczny z działalności CERT Polska w 2024 r., https://cert.pl/uploads/docs/Raport_CP_2024.pdf#page=89 (dostęp: 14.02.2026 r.).
10) Raport Najwyższej Izby Kontroli nr ewidencyjny: P/24/004 https://www.nik.gov.pl/kontrole/P/24/004/?utm_source=chatgpt.com (dostęp: 15.02.2026 r.).
11) To nie brak finansów największą barierą w cyfryzacji gmin i samorządów. Większy problem to kompetencje cyfrowe urzędników, https://biznes.newseria.pl/news/to-nie-brak-finansow,p140084589 (dostęp: 14.02.2026 r.).

dr Marcin Jan Stępień
Uniwersytet Szczeciński
adres e-mail: marcin.stepien@usz.edu.pl
ORCID: 0000-0002-0762-548X

Czy korzystanie ze sztucznej inteligencji godzi w prawa twórców? Uwagi na tle działalności organów administracji publicznej

Does the Use of Artificial Intelligence Infringe the Copyright of Authors? Observations in the Context of Public Administration Activities

Streszczenie

Technologia sztucznej inteligencji wzmacnia aktywność człowieka w wielu obszarach. Nie pozostaje ona bez znaczenia również dla działalności organów administracji publicznej. Materiały oraz dane pozyskiwane lub dostarczane na potrzeby szkolenia systemów sztucznej inteligencji mogą zawierać rezultaty chronione prawami własności intelektualnej. Do rezultatów takich mogą należeć przede wszystkim utwory chronione prawami autorskimi. Organy administracji publicznej, wykorzystujące lub dążące do szerszego użycia technologii generatywnej sztucznej inteligencji w swojej działalności, muszą mieć na uwadze, kiedy takie użycie może ingerować w prawa twórców i innych podmiotów uprawnionych z praw autorskich.

Utwór. Uwagi wprowadzające o definicji przedmiotu praw autorskich

Ustawodawca w art. 1 ust. 1 upapp[192] wprowadza definicję legalną przedmiotu praw autorskich - utworu. Zgodnie z tym przepisem „przedmiotem prawa autorskiego jest każdy przejaw działalności twórczej o indywidualnym charakterze, ustalony w jakiejkolwiek postaci, niezależnie od wartości, przeznaczenia i sposobu wyrażenia (utwór)". Szerokie ujęcie przesłanek ochrony prawnoautorskiej[193] prowadzi do wniosku, iż znaczne spektrum wytworów intelektualnych człowieka może

[192] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2025 r. poz. 24 ze zm.), dalej: upapp.

[193] Za D. Flisakiem, w kontekście brzmienia art. 1 ust. 1 upapp, można stwierdzić, że „zawiera ono dwie przesłanki warunkujące istnienie utworu: po pierwsze, musi być on przejawem działalności twórczej, po drugie – wykazywać indywidualny charakter. Trzecią, konstytutywną przesłanką jest ustalenie utworu w jakiejkolwiek postaci" (D. Flisak, [w:] *Prawo autorskie i prawa pokrewne. Komentarz*, D. Flisak (red.), Warszawa 2015, LEX, s. 23. Przesłanek powyższych ustawodawca nie wyjaśnia, pozostawiając ustalenie ich znaczenie praktyce oraz nauce prawa.

aspirować do ochrony prawnoautorskiej[194]. Uznanie, iż chodzi wyłącznie o wytwory pochodzące od człowieka nie jest przypadkowe. Słusznie bowiem przyjmuje się zarówno w doktrynie, jak i orzecznictwie, iż do działalności twórczej zdolny jest wyłącznie człowiek[195]. Skoro pierwsza z przesłanek ochrony (które powinny być spełnione łącznie) wymaga, aby utwór był rezultatem działalności twórczej, a do działalności twórczej zdolny jest wyłącznie człowiek, to zasadnie należy twierdzić, że twórcą w świetle upapp może być wyłącznie człowiek (osoba fizyczna)[196].

Powyższe zastrzeżenie na początku niniejszych wywodów wydaje się istotne co najmniej z dwóch przyczyn. Pierwsza, polska upapp nie zawiera przepisu, z którego by wynikało, że wyłącznie człowiek – osoba fizyczna może być twórcą. Druga, zgodnie z upapp wytwory wygenerowane przez systemy sztucznej inteligencji nie mogą aspirować do ochrony prawnoautorskiej[197].

Dodać należy, że upapp wyróżnia przy tym szczególne kategorie utworów, objętych ochroną prawa autorskiego. Należą do nich opracowania (art. 2 upapp), zbiory (art. 3 upapp), utwory zbiorowe (art. 11 upapp), utwory połączone (art. 10 upapp) oraz utwory współautorskie (art. 9 upapp). Wynika to z okoliczności, iż ustawodawca pragnie objąć ochroną prawa autorskiego rezultaty najróżniejszych form działalności twórczej człowieka. I tak - tytułem przykładu - może ona polegać na twórczej modyfikacji (opracowaniu), a nawet twórczym doborze, układzie lub zestawieniu materiałów (zbiory), przy czym materiały te same nie muszą podlegać ochronie prawnoautroskiej.

Mając na względzie powyższe, wiele z wytworów działalności intelektualnej człowieka, w tym utworów, może stanowić przedmiot eksploatacji organów administracji publicznej. Niekiedy ich eksploatacja wymagać będzie zezwolenia twórcy.

Jednocześnie ustawodawca wprowadza uregulowania, które wyłączają spod ochrony prawa autorskiego pewne wytwory, które mógłby aspirować do ochrony prawnoautorskiej. Zgodnie z art. 4 upapp spod ochrony prawa autorskiego wyłączone zostały m.in. akty normatywne lub ich urzędowe projekty (pkt. 1) oraz urzędowe dokumenty, materiały, znaki i symbole (pkt. 2). Są to więc wytwory o niebagatelnym znaczeniu dla funkcjonowania organów administracyjnych. Powyższe

194 Zob. uwagi J. Błeszyński, *Prawo autorskie*, Warszawa, 1988, s. 38-39.

195 Zob. m.in.: J. Barta, R. Markiewicz, [w:] *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, M. Czajkowska-Dąbrowska, Z. Ćwiąkalski, K. Felchner, E. Traple, J. Barta, R. Markiewicz (red.), Warszawa 2011, LEX, s. 19; Wyrok Sądu Apelacyjnego w Poznaniu z 20 grudnia 2022 r., sygn. akt I AGa 89/22, LEX nr 3488150; Wyrok Sądu Apelacyjnego w Gdańsku z 30 września 2020 r., sygn. akt V AGa 74/19, LEX nr 3102186.

196 Zob. A. Bar, *Obrazy generowane z wykorzystaniem sztucznej inteligencji. Status prawnoautorski*, Warszawa 2025, s. 152-153.

197 „[P]rzedmioty wygenerowane przez sztuczną inteligencję nie korzystają z ochrony prawa autorskiego. Jest tak dlatego, że nie stworzył ich człowiek" (A. Niewęgłowski, *Prawo autorskie. Komentarz*, Warszawa 2025, LEX, s. 334).

jest celowym rozwiązaniem ustawodawcy, zmierzającym do uwzględnienia interesu społecznego, który w kontekście umożliwienia do dostępu do ww. dóbr, przeważa nad indywidualnym interesem twórcy[198]. Jednocześnie służy skutecznej realizacji działań państwa na płaszczyźnie sfery imperium[199]. Obok ww. włączeń (tzw. ekskluzji) spod ochrony prawa autorskiego, ustawodawca wprowadza regulację dozwolonego użytku utworu (zob. rozdział 3, oddział 3 upapp, zatytułowany „Dozwolony użytek chronionych utworów"). Korzystanie z utworu w granicach dozwolonego użytku nie wymaga zezwolenia twórcy ani – w przeważającej liczbie przypadków – zapłaty stosownego wynagrodzenia na jego rzecz. Na wiele postaci dozwolonego użytku utworu mogą powołać się również organy administracyjne.

Znaczenie dozwolonego użytku utworu w działalności organów administracyjnych

Ustawa wprowadza dwa rodzaje dozwolonego użytku utworu, a mianowicie dozwolony użytek prywatny oraz dozwolony użytek publiczny.

Dozwolony użytek prywatny, zwany również osobistym, który reguluje art. 23 upapp. Został on pomyślany w celu zapewnienia szerokiego dostępu do dóbr kultury i nauki osobom fizycznym[200] „w zakresie własnego użytku osobistego". Użytek osobisty w świetle art. 23 ust. 2 upapp „obejmuje korzystanie z pojedynczych egzemplarzy utworów przez krąg osób pozostających w związku osobistym, w szczególności pokrewieństwa, powinowactwa lub stosunku towarzyskiego". W efekcie, na ten przypadek szerokiego dozwolonego użytku utworu organ administracyjny nie może się powołać w zakresie swojej działalności.

Dozwolony użytek publiczny, obejmuje najróżniejsze postacie dozwolonego użytku utworu. W tym wiele z nich może stanowić podstawę do nieskrepowanego korzystania z utworu przez organu administracyjne w zakresie ich działalności. Tytułem przykładu art. 33^2 upapp stanowi, że wolno korzystać z utworów m.in. na potrzeby postępowania administracyjnego. Artykuł 31 ust. 1 upapp przewiduje możność korzystania z utworu podczas oficjalnych uroczystości organizowanych przez władze publiczne, jeżeli nie łączy się z tym osiąganie pośrednio lub bezpośrednio korzyści majątkowej. Najbardziej rozpowszechnioną postacią dozwolonego użytku publicznego utworu zdaje się być tzw. prawo cytatu, o którym stanowi art. 29 upapp. Przepis ten może odgrywać również ważną rolę w działalności organów administracji, która wymaga eksploatacji utworu. Zgodnie z treścią powyższego

198 „Motywem ustanowienia wyłączeń przewidzianych w art. 4 pr. aut. są względy interesu publicznego, wyrażającego się w dostępie do informacji i możliwości nieskrępowanego prawami autorskimi korzystania z wymienionych w przepisie dóbr" (A. Nowicka, *Komentarz do ustawy o prawie autorskim i prawach pokrewnych*, [w:] *Ustawy autorskie. Komentarze*, t. I, R. Markiewicz (red.), Warszawa 2021, LEX, s. 188).

199 Zob. M.J. Stępień, *Rzeczpospolita Polska w stosunkach prawnoautorskich*, [w:] *Prawo i państwo: księga jubileuszowa 200-lecia Prokuratorii Generalnej Rzeczypospolitej Polskiej*, L. Bosek (red.), Warszawa 2017, s. 584-585.

200 S. Stanisławska-Kloc [w:] *Prawo autorskie...*, op.cit., s. 349.

przepisu wolno przytaczać w utworach stanowiących samoistną całość urywki rozpowszechnionych utworów w zakresie uzasadnionym celami cytatu, takimi jak wyjaśnianie, polemika, analiza krytyczna lub naukowa, nauczanie lub prawami gatunku twórczości. W przypadku rozpowszechnionych utworów plastycznych, utworów fotograficznych lub drobnych utworów można przytaczać je w całości.

Korzystanie z utworów w granicach dozwolonego użytku (zarówno prywatnego, jak i publicznego) w świetle art. 34 upapp wymaga wymienienia imienia i nazwiska twórcy utworu, a także źródła. Przy tym podanie twórcy oraz źródła powinno uwzględniać istniejące możliwości. Dodatkowym wymogiem ustawy jest, aby dozwolony użytek nie naruszał „normalnego korzystania z utworu" ani godził w słuszne interesy twórcy (art. 35 upapp).

Katalog postaci dozwolonego użytku utworu we wrześniu 2025 r. został uzupełniony o dwie nowe postacie odnoszące się do użycia utworów na potrzeby szkolenia systemów sztucznej inteligencji, tj. art. 26^2 i 26^3 upapp[201]. Mają one postać publicznego dozwolonego użytku utworu. Dalszego rozważania wymaga zatem, czy również organy administracyjne w zakresie swojej działalności będą mogły skorzystać z tej postaci dozwolonego użytku utworu.

Technologia sztucznej inteligencji a prawo autorskie – wzmianka

Na gruncie wypowiedzi doktryny różnie ujmuje się pojęcia sztucznej inteligencji[202]. Niemniej jednak można uznać, że systemy sztucznej inteligencji to „systemy komputerowe obejmujące oprogramowania, które dzięki analizie otoczenia i podejmowaniu działań w celu osiągniecia konkretnych celów wykazują inteligentne zachowania"[203]. Definicję legalną pojęcia sztucznej inteligencji wprowadza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r., tzw. akt ws. sztucznej inteligencji[204]. Zgodnie z art. 3 pkt. 1 dla celów powyższego rozporządzenia system sztucznej inteligencji „oznacza system maszynowy, który został zaprojektowany do działania z różnym poziomem autonomii po jego wdrożeniu oraz który może wykazywać zdolność adaptacji po jego wdrożeniu, a także który - na potrzeby wyraźnych lub dorozumianych celów - wnioskuje, jak

[201] Powyższe przepisy zostały dodane do upapp zgodnie z art. 1 pkt 8 ustawy z dnia 26 lipca 2024 r. o zmianie ustawy o prawie autorskim i prawach pokrewnych, ustawy o ochronie baz danych oraz ustawy o zbiorowym zarządzaniu prawami autorskimi i prawami pokrewnymi (Dz. U. poz. 1254).

[202] Zob. szerzej A. Bar, *Obrazy generowane*..., op.cit., s. 45-50.

[203] A. Auleytner, M.J. Stępień, *Dostęp do sztucznej inteligencji – równość i inne aspekty prawne dostępu do systemów sztucznej inteligencji*, „Monitor Prawniczy" 2019, nr 21, s. 69.

[204] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz. U. UE. L. z 2024 r. poz. 1689).

generować na podstawie otrzymanych danych wejściowych wyniki, takie jak predykcje, treści, zalecenia lub decyzje, które mogą wpływać na środowisko fizyczne lub wirtualne". Technologia sztucznej inteligencji odgrywa aktualnie istotną rolę w działalności człowieka, a rola ta najpewniej w najbliższych latach będzie coraz bardziej znacząca. Użycie technologii sztucznej inteligencji obejmuje najróżniejsze obszary aktywności człowieka. W efekcie, wykorzystanie technologii generatywnej sztucznej inteligencji może wpływać na poprawę oraz szybkość działania organów administracji publicznej[205].

Technologia sztucznej inteligencji zakłada procesy uczenia lub trenowania, które mają na celu analizę materiałów, danych dostępnych z otoczenia, czy to pozyskanych przez sztuczną inteligencję czy też dostarczonych jej przez człowieka[206]. Te dane lub materiały mogą zawierać wytwory chronione prawem własności intelektualnej. Jak zauważa A. Niewęgłowski „w ramach eksploracji sztuczna inteligencja napotyka wszelkiego typu dobra niematerialne, które mogą być chronione prawami wyłącznymi. Są wśród nich utwory i przedmioty praw pokrewnych"[207]. W efekcie, w procesie użycia systemów sztucznej inteligencji może dochodzić do ich szkolenia w oparciu o treści cyfrowe zawierające wytwory chronione prawami własności intelektualnej w tym, prawami autorskimi. Mając na względzie powyższe, iż korzystanie z systemów sztucznej inteligencji niekiedy może ingerować w prawa twórców, w dyrektywie Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. (dalej: „Dyrektywa 2019/790")[208], wprowadzono uregulowanie mające na celu zbalansowanie interesów użytkowników technologii sztucznej inteligencji oraz twórców. Zgodnie z art. 4, zatytułowanym „Wyjątki lub ograniczenia w odniesieniu do eksploracji tekstów i danych", państwa członkowskie Unii Europejskiej wprowadzają przepisy ograniczające prawa własności intelektualnej[209] „w odniesieniu do zwielokrotnień i pobrań dostępnych zgodnie z prawem utworów i innych przedmiotów objętych ochroną do celów eksploracji tekstów i danych".

W motywie 8 Dyrektywy 2019/790 zauważa się, że „nowe technologie umożliwiają automatyczną matematyczną analizę informacji w postaci cyfrowej, takich jak

[205] W motywie 18 Dyrektywy 2019/790 (zob. przypis 17) wskazuje się, że „oprócz znaczenia dla badań naukowych, techniki eksploracji tekstów i danych są szeroko wykorzystywane także przez podmioty prywatne i publiczne do analizowania dużych ilości danych w różnych sferach życia codziennego i do różnych celów, w tym przez służby państwowe, do podejmowania złożonych decyzji biznesowych oraz do rozwijania nowych aplikacji i technologii".

[206] Zob. A. Niewęgłowski, *Prawo autorskie. Komentarz*..., op.cit., s. 334.

[207] A. Niewęgłowski, *Prawo autorskie. Komentarz*..., op.cit., s. 334.

[208] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz. U. UE. L. z 2019 r. Nr 130, str. 92).

[209] Przepis Dyrektywy 2019/790 precyzuje, iż chodzi o prawa przewidziane w „art. 5 lit. a) i art. 7 ust. 1 dyrektywy 96/9/WE, art. 2 dyrektywy 2001/29/WE, art. 4 ust. 1 lit. a) i b) dyrektywy 2009/24/WE oraz art. 15 ust. 1 niniejszej dyrektywy".

teksty, dźwięki, obrazy lub dane, powszechnie określaną jako eksploracja tekstów i danych (...). W niektórych przypadkach eksploracja tekstów i danych może obejmować czynności chronione prawem autorskim lub prawem do bazy danych *sui generis*, w szczególności zwielokrotnianie utworów lub innych przedmiotów objętych ochroną lub pobieranie treści z bazy danych, co ma miejsce na przykład w przypadku normalizacji danych podczas eksploracji tekstów i danych". Jednocześnie w powyższym motywie podkreśla się, że taka eksploracja tekstów i danych może przynosić szczególne korzyści dla rozwoju nauki i kultury. Użycie technologii sztucznej inteligencji może sprzyjać rozwojowi instytucji naukowych, badawczych, dziedzictwa kulturowego, jak również okazać się przydatne jednostkom, w tym naukowcom. Konieczne jest zatem stworzenie możliwości dla takiej eksploracji tekstów i danych, również w sytuacji, gdy mogą one ingerować w prawa twórców i innych podmiotów uprawnionych z praw własności intelektualnej. „Jeżeli nie znajduje zastosowanie wyjątek lub ograniczenie, konieczne jest uzyskanie zezwolenia na dokonanie takich czynności od podmiotów uprawnionych" – czytamy dalej z motywu 8 Dyrektywy 2019/790. Użycie bowiem technologii sztucznej inteligencji musi następować z poszanowaniem praw tych podmiotów. Mając na względzie powyższe, konieczne okazuje się wprowadzenie ograniczeń lub wyjątków od sfery wyłączności praw własności intelektualnej, które pozwolą na nieskrepowane użycie technologii generatywnej sztucznej inteligencji.

Wydaje się, że zwrócenie uwagi na jej zastosowanie nie tylko jednostkowe, ale mające znaczenie również dla organizacji, prowadzi do wniosku o zasadności odwołania się do instytucji dozwolonego użytku publicznego. Ja zważano na początku, dozwolony użytek publiczny obejmuje przypadki, kiedy korzystanie z utworu, bez zezwolenia twórcy, może następować nie tylko przez osoby fizyczne, ale wszelkie podmioty, w tym jednostki organizacyjne.

Zgodnie z art. 4 ust. 1 Dyrektywy 2019/790 możliwe jest zwielokrotnianie (pobieranie) utworu, jeżeli służy procesowi szkolenia technologii sztucznej inteligencji. Zwielokrotnianie stanowi jedną z postaci eksploatacji utworu składającą się na treść wyłącznych autorskich praw majątkowych twórcy[210]. Tym samym zwielokrotnianie z założenia wymaga zezwolenia twórcy. Ponadto, w świetle art. 4 ust. 2 Dyrektywy 2019/790, zwielokrotnienia i pobrania mogą być przechowywane tak długo, jak jest to konieczne do celów eksploracji tekstów i danych.

Niekiedy przepisy przewidują możność zwielokrotniania utworu bez zezwolenia twórcy oraz bez zapłaty z tego tytułu stosownego wynagrodzenia właśnie w ramach przepisów o dozwolonym użytku utworu. Szczególnie gdy wyłączenie takie

[210] Zob. J. Szczotka w: M. Poźniak-Niedzielska, J. Szczotka (red.), *Prawo autorskie. Zarys problematyki*, Warszawa 2020, s. 81. E. Traple, [w:] *Ustawa o prawie autorskim i prawach pokrewnych*. Komentarz, J. Barta, R. Markiewicz (red.), Warszawa 2011, s. 333-334.

może to być uzasadnione interesem społecznym. Taką postacią dozwolonego użytku jest analizowany art. 4 Dyrektywy 2019/790. Jednakże w ust. 3 przepis ten zastrzega, że wprowadzenie wyjątku (lub ograniczenia) w sferze uprawnienia do zwielokrotniania utworu (lub innych przedmiotów objętych ochroną) może nastąpić tylko wówczas, gdy „korzystanie z utworów i innych przedmiotów objętych ochroną (...) nie zostało wyraźnie zastrzeżone przez podmioty uprawnione w odpowiedni sposób, na przykład za pomocą środków nadających się do odczytu maszynowego w przypadku treści, które zostały podane do publicznej wiadomości w Internecie". W powyższym zastrzeżeniu chodzi o tzw. instytucję *opt-out'u*. Zakłada ona możliwość po stronie podmiotu uprawnionego (w tym twórcy), dokonania zastrzeżenia, wedle którego podmiot ten nie wyraża zgody na korzystanie z jego utworu na potrzeby eksploracji tekstów i danych. Takie zastrzeżenie *de facto* powinno skutkować wykluczeniem utworu (lub innego przedmiotu objętego ochroną) spod regulacji dozwolonej eksploatacji utworu, o które mowa w art. 4 Dyrektywy 2019/790.

Dozwolony użytek TDM w świetle ustawy o prawie autorskim i prawach pokrewnych

Dnia 20 września 2024 r. weszły w życie art. 26^2 oraz 26^3 upapp, które stanowią efekt implementacji art. 4 Dyrektywy 2019/790[211]. W literaturze wskazuje się, że art. 26^2 upapp reguluje tzw. dozwolony użytek w celu eksploracji tekstów i danych (ang. *text end data mining;* w skrócie - TDM) w odniesieniu do badań naukowych, zaś 26^3 upapp dozwolony użytek TDM dla celów komercyjnych[212]. Obie postacie dozwolonego użytku pomyślane zostały w związku z zapewnieniem możliwości używania technologii generatywnej sztucznej inteligencji[213]. Odnoszą się do przypadków dozwolonego użytku publicznego utworu. Przy czym, art. 26^2 upapp, jako przewidziany dla celów badań naukowych, w ust. 1 wyraźnie określa podmioty, które mogą korzystać z danej postaci dozwolonego użytku. W świetle tego przepisu są to „instytucje dziedzictwa kulturowego, a także podmioty, o których mowa w art. 7 ust. 1 pkt 1, 2 i 4-8 ustawy z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce". Podmiotom tym zapewnia się nieco szerszy zakres dozwolonego użytku (niż wynika to art. 26^3 upapp), bowiem nie ma on służyć celom komercyjnym, lecz

[211] Analogiczne uregulowania znalazły się również ustawie z dnia 27 lipca 2001 r. o ochronie baz danych (t.j. Dz. U. z 2024 r. poz. 1769), a mianowicie art. 8a oraz 8b. Przedmiotem dalszych rozważań będą przepisy ustawy prawnoautorskiej.

[212] J. Ożegalska-Trybalska, B. Widła, *Komentarz do wybranych przepisów ustawy o prawie autorskim i prawach pokrewnych*,, [w:] *Prawo autorskie. Komentarz do znowelizowanych 26 lipca 2024 r. przepisów ustaw: o prawie autorskim i prawach pokrewnych, o ochronie baz danych, o zbiorowym zarządzaniu prawami autorskimi i prawami pokrewnymi,* N. Ghazal, M. Markiewicz, A. Matlak, E. Nowińska, S. Stanisławska-Kloc, T. Targosz, M. Wyrwiński, J. Ożegalska-Trybalska, B. Widła, Warszawa 2025, s. 156.

[213] A. Niewęgłowski, *Prawo autorskie. Komentarz*..., op.cit., s. 334.

badawczym. Artykuł 26^2 ust. 1 upapp wyraźnie stanowi, że powyższe podmioty utwory mogą zwielokrotniać „w celu eksploracji tekstów i danych do celów badań naukowych, jeżeli czynności te nie są dokonywane w celu osiągnięcia bezpośredniej lub pośredniej korzyści majątkowej". Dodatkowo art. 26^2 ust. 1 upapp stanowi, że tak zwielokrotnione utworu mogą być przechowywane zarówno do celów badań naukowych, jak również do weryfikacji wyników tych badań.

Z kolei druga postać dozwolonego użytku TDM, uregulowana w art. 26^3 upapp, ograniczeń podmiotowych nie wprowadza[214]. Na marginesie, należy zauważyć, że oznacza to, iż na taką postać dozwolonego użytku mogą powoływać się również ww. instytucje dziedzictwa kultury oraz wskazane podmioty, o których mowa w ustawie – Prawo o szkolnictwie wyższym[215]. Pomimo, że w literaturze przyjęto nazywać tę postać dozwolonego użytku utworu „komercyjnym", to może odgrywać on również istotną rolę w działalności organów administracji publicznej[216]. Co również ważne, powyższa postać dozwolonego użytku odnosi się do każdego rodzaju utworów[217].

Art. 26^3 ust. 1 upapp przewiduje, że „wolno zwielokrotniać rozpowszechnione utwory w celu eksploracji tekstów i danych, chyba że uprawniony zastrzegł inaczej". Jednocześnie art. 6 ust. 1 pkt. 22 upapp definiuje pojęcie eksploracji tekstów i danych wskazując, że jest to „analiza wyłącznie przy zastosowaniu zautomatyzowanej techniki służącej do analizowania tekstów i danych w postaci cyfrowej w celu wygenerowania określonych informacji, obejmujących w szczególności wzorce, tendencje i korelacje". Co charakterystyczne dla przypadków dozwolonego użytku utworów, utwór, który może być zwielokrotniany dla eksploracji tekstów i danych, ma być utworem rozpowszechnionym. W tym miejscu również należy sięgnąć do art. 6 upapp, który definiuje niektóre z pojęć użytych w ustawie. I tak, zgodnie z art. 6 ust. 1 pkt. 3 upapp utworem rozpowszechnionym „jest utwór, który za zezwoleniem twórcy został w jakikolwiek sposób udostępniony publicznie". Definicja ta wskazuje na bardzo istotną okoliczność, a mianowicie, że z rozpowszechnieniem utworu mamy do czynienia wówczas, gdy na udostępnienie publiczne

[214] A. Niewęgłowski, *Prawo autorskie. Komentarz...*, op.cit., s. 334.

[215] Ustawa z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2024 r. poz. 1571 ze zm.).

[216] Jak trafnie stwierdza A. Niewęgłowski, w kontekście art. 26^3 upapp, to w przypadku wyrażonej w nim postaci dozwolonego użytku utworu „eksploracja może nastąpić zarówno w celu komercyjnym, jak i niekomercyjnym" (A. Niewęgłowski, *Prawo autorskie. Komentarz...*, op.cit., s. 335). W doktrynie nie budzi wątpliwości, że na przedmiotową postać dozwolonego użytku mogą powoływać się również instytucje państwowe (P. Ruchała, *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, J. Kępiński (red.), Warszawa 2025, Legalis, s. 508).

[217] Wart zauważenia jest fakt, że art. 77 upapp wyłącza zastosowanie względem programów komputerowych tylko dozwolony użytek z art. 26^2 upapp (dozwolony użytek TDM dla celów badań naukowych). Powyższe prowadzi do wniosku, że programy komputerowe mogą być przedmiotem zwielokrotnienia w celu eksploracji tekstów i danych na podstawie art. 26^3 upapp (Zob P. Ruchała, *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz...*, op.cit., s. 507).

utworu zezwolił twórca[218]. Tytułem przykładu, jeżeli utworów zostałby udostępniony publicznie w Internecie bez zezwolenia twórcy, to wówczas nie mamy do czynienia z jego rozpowszechnieniem[219]. *Ergo*, w takim przypadku również utwór nie może być eksploatowany w ramach dozwolonego użytku TDM.

Kolejny bardzo istotnym fragmentem art. 26^3 ust. 1 upapp stanowi, że podmiot uprawniony może wyłączyć zastosowanie regulacji dozwolonego użytku utworu dla celów eksploracji tekstów i danych, co wyraża się w sformułowaniu „chyba że uprawniony zastrzegł inaczej". Instytucja ta – jak wskazano powyżej - znana w pod ang. nazwą *opt-out*, wywołuje wiele kontrowersji, zarówno teoretyków prawa, jak również specjalistów w dziedzinie techniki[220]. Zarzuca się jej przy tym trudności w realizacji od strony technicznej. Artykuł 26^3 ust. 2 upapp w zdaniu pierwszym stanowi, iż powyższego zastrzeżenia dokonuje się „wyraźnie i odpowiednio do sposobu, w jaki utwór został udostępniony". Wykluczone jest zatem złożenie takiego oświadczenia w sposób dorozumiany (por. art. 60 Kodeksu cywilnego[221])[222]. W zdaniu drugim wskazuje na oczekiwania natury technicznej, którym odpowiadać powinno takie zastrzeżenie. W wypowiedziach specjalistów w dziedzinie techniki wskazuje się, że „fundamentalny problem procedury *opt-out* z technicznego punktu widzenia polega na tym, że narzędzia do jej egzekwowania praktycznie nie istnieją. Pliki robots.txt powstały jako reakcja na kontrowersje związane z indeksowaniem treści przez wyszukiwarki i stanowią jedynie sugestię dla aplikacji indeksujących, którą można całkowicie legalnie zignorować (...). W przypadku wyszukiwarek łatwo jest sprawdzić, czy strona została zaindeksowana. W przypadku generatywnej AI niemal niemożliwe jest ustalenie, czy dany utwór został użyty do treningu modelu, dopóki wynik pracy modelu nie przypomina istniejącego utworu „zbyt bardzo""[223].

---

218 Prawo do decydowania o pierwszym udostępnieniu utworu publiczności, jest jednym z autorskich praw osobistych, *expressis verbis* wymienionym w art. 16 pkt 3 upapp. Przy tym, w świetle tego przepisu twórca nie może zrzec się tego prawa. To oznacza, że - co do zasady - tylko twórca może decydować o tym, kiedy jego utwór dojrzał do tego, aby być prezentowany publiczności.

219 W literaturze wskazuje się również na inne przypadki bezprawnego uzyskania dostępu do utworu: „sztuczna inteligencja nie może przełamywać zabezpieczeń w celu dotarcia do utworów, które są przechowywane w poufności. Generalnym warunkiem wolnego użytku jest zresztą korzystanie z dzieła rozpowszechnionego" (A. Niewęgłowski, *Prawo autorskie. Komentarz...*, op.cit., s. 335). Ponadto P. Ruchała zauważa, że: „polski ustawodawca nie wysłowił wprost wyrażonego w art. 4 ust. 1 Dyrektywy 2019/790, by wykorzystywane utwory były „dostępne zgodnie z prawem". Sam fakt rozpowszechnienia utworu nie oznacza jeszcze, że w danym przypadku użytkownik uzyskuje do niego dostęp zgodnie z prawem" (P. Ruchała, *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz...*, op.cit., s. 507).

220 Zob. szerzej: J. Ożegalska-Trybalska, B. Widła, *Komentarz do wybranych przepisów ustawy o prawie autorskim i prawach pokrewnych...*, op.cit, s. 158-159.

221 Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2025 r. poz. 1071 ze zm.).

222 P. Ruchała, *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz...*, op.cit., s. 508.

223 G. Piwowarek w: M. Miernik-Grzesiowska, *Procedura opt-out TDM czyli jak chronić swoją twórczość przed trenowaniem genAI?*, https://lookreatywni.pl/baza-wiedzy/o-procedurze-opt-out-jak-chronic-swoja-tworczosc-przed-trenowaniem-genai/ (dostęp: 22.01.2026 r.).

Zastrzeżenie z art. 26^3 ust. 1 upapp stanowi jednostronne oświadczenie woli podmiotu uprawnionego. Podmiot, któremu przyznaje się uprawnienia do dokonania tego zastrzeżenie został ujęty szeroko. Nie obejmuje on bowiem wyłącznie twórcy, ale również inne podmiotu uprawnione z tytułu autorskich praw majątkowych[224]. Wydaje się tak dlatego, że zwielokrotnienie jest jedną z postaci eksploatacji utworu, składających się na treść autorskich praw majątkowych (zob. art. 17 oraz 50 upapp, por. art. 2 dyrektywy 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r.[225]). To oznacza, że również inni uprawnieni z autorskich praw majątkowych niż twórca, mogą dokonywać powyższego zastrzeżenia, np. pracodawca, producent lub wydawca, czy nawet nabywca na podstawie umowy o przeniesienie autorskich praw majątkowych. To oznacza, że jeżeli twórca dokonał zastrzeżenia w rozumieniu art. 26^3 ust. 1 upapp, to podmiot, który nabył od niego następnie autorskie prawa majątkowe, może takie zastrzeżenie odwołać. Ewentualnie – odwrotnie, jeżeli twórca nie dokonał zastrzeżenia, to nabywca następnie oświadczanie o takim zastrzeżeniu może złożyć (np. pracodawca twórcy). Dodatkowo mając na względzie wynikający z art. 41 ust. 2 upapp obowiązek specyfikacji pól eksploatacja, który nakazuje w umowach praw autorskiego, w tym umowach przenoszących, wskazywanie pól eksploatacji (odpowiadających uprawnieniom cząstkowym skradającym się na autorskie prawa majątkowe), to ustalenie *a casu* podmiotu uprawnionego może niekiedy nastręczać daleko idące problemy. W ramach niniejszej pracy niestety nie ma miejsc na całościowe omówienie podniesionego problemu, ale należy zwrócić uwagę, że w zakresie samego zwielokrotniana utworu wyróżniamy najróżniejsze postacie eksploatacji – w zależności od techniki zwielokrotnia – np. zwielokrotnienie utworu techniką drukarską, zwielokrotnienie utworu techniką cyfrową (por. art. 50 pkt 1 upapp). W doktrynie precyzuje się, że art. 26^3 upapp (jak również art. 26^2 upapp) odnosi się do zwielokrotniania utworów techniką cyfrową[226].

Ponadto w doktrynie prawa słusznie zwraca się uwagę, że nie tylko utwory rozpowszechnione cyfrowo mogą być przedmiotem zwielokrotnienia na podstawie art.

[224] A. Niewęgłowski, *Prawo autorskie. Komentarz...*, op.cit., s. 336.

[225] Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz. U. UE. L. z 2001 r. Nr 167, str. 10 z późn. zm.). Pojęcie pól eksploatacji utworu z art. 50 upapp odpowiada pojęciu uprawnień cząstkowych, składających się na treść autorskich praw majątkowych, ujętych w definicji syntetycznej w art. 17 upapp (zob. E. Traple, [w:] *Prawo autorskie. System Prawa Prywatnego*, t. 13, J. Barta (red.), Warszawa 2017, s. 175). I tak, zwielokrotnianie może być na gruncie polskiego prawa autorskiego utożsamiane z uprawnieniem węższym składającym się na autorskie prawa majątkowe. Z kolei w prawie Unii Europejskiej nie posłużono się pojęciem pól eksploatacja. Za K. Klafkowska-Waśniowska można wskazać, że „w prawie Unii Europejskiej określa się zakres uprawnień wyłącznych przez odwołanie do określonego, nazwanego sposobu eksploatacji, np. prawo do zwielokrotniania" (K. Klafkowska-Waśniowska, *Komentarz do ustawy o prawie autorskim i prawach pokrewnych*, [w]: *Ustawy autorskie. Komentarze*, t. I, R. Markiewicz (red.), Warszawa 2021, s. 1195). I tak też prawo do zwielokrotniania ujmuje art. 2 ww. dyrektywy.

[226] P. Ruchała, *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz...*, op.cit., s. 508.

26^3 upapp. Zwielokrotnienie, o którym mowa w art. 26^3 upapp, jak również 26^2 upapp, pozwalają na digitalizację fizycznie dostępnych egzemplarzy utworów[227].

Wreszcie art. 26^3 ust. 3 upapp reguluje jak długo mogą być przechowywane zwielokrotnione utworu na podstawie dozwolonego użytku TDM. W świetle tego przepisu mogą być one przechowywane tak długo jak jest to konieczne do osiągnięcia cel eksploracji tekstów i danych.

Wnioski. Nie tylko „komercyjny" dozwolony użytek TDM

Od 20 września 2024 r. w polskim prawie autorskim obowiązują dwie nowe postacie dozwolonego użytku utworu. Reguluje je art. 26^2 i 26^3 upapp. Stanowią efekt implementacji Dyrektywy 2019/790. Motywem ich przyjęcia było zapewnienie możności korzystania z technologii generatywnej sztucznej inteligencji przy poszanowaniu prawa autorskich do utworów. W kontekście działalności organów administracji publicznej szczególną uwagę zwraca art. 26^3 upapp. Przepis ten dozwala na zwielokrotniania rozpowszechnionych utworów w celu eksploracji tekstów i danych, a mianowicie umożliwia określoną eksploatację utworów na potrzeby szkolenia systemów sztucznej inteligencji. Należy bowiem pamiętać, że w procesie szkolenia tychże systemów dostarczane lub pobierane są dane i materiały mogące obejmować chronione prawem autorskim utwory. Artykuł 26^3 upapp należy do przepisów regulujących tzw. dozwolony użytek publiczny utworu. Powyższe oznacza, że mogą się na niego powoływać najróżniejsze podmioty, w tym organy administracji publicznej. Ustawa o prawie autorskim i prawach pokrewnych przewiduje wiele postaci dozwolonego użytku utworów, które mają na celu zapewnienie nieskrępowanego funkcjonowania organów administracji publicznej, w tym wykonywania ciążących na nich ustawowych zadań. Przypisy te w znacznej części należą do regulacji dozwolonego użytku publicznego utworów. Artykuł 26^3 upapp wzbogaca powyższy arsenał środków z obszaru dozwolonego użytku publicznego utworu, na który mogą powoływać się organy administracji publicznej. Pomimo, że określa się go niekiedy mianem „komercyjnego" dozwolonego użytku utworu TDM, to przepis nie ogranicza jego zastosowania wyłącznie do takich celów. Tym samym służyć może z powodzeniem wielu uczestnikom obrotu prawnego, w tym organom administracji publicznej.

[227] W kontekście art. 26^2 upapp J. Ożegalska-Trybalska oraz B. Widła zauważają, że „na podstawie art. 26^2 pr. aut. dozwolone jest zwielokrotnianie utworów. Chodzi tu nie tylko o „proste" kopiowanie utworu w niezmienionej postaci, ale także zwielokrotnienia wymagane w toku analizy, prowadzące np. do przetworzenia pierwotnej kopii. W braku rozróżnienia należy przyjąć, że chodzi tu nie tylko o poddanie automatycznej analizie kopii, które mają już postać cyfrową. Na podstawie art. 26^2 pr. aut. dozwolona jest także digitalizacja, czyli wytworzenie cyfrowych kopii na podstawie fizycznych egzemplarzy, np. zeskanowanie drukowanej książki i uzyskanie cyfrowej kopii tekstu przy pomocy technik optycznego rozpoznawania znaków (OCR)" (J. Ożegalska-Trybalska, B. Widła *Komentarz do wybranych przepisów ustawy o prawie autorskim i prawach pokrewnych*..., op. cit., s. 148).

Bibliografia:

Akty prawne

1) Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2025 r. poz. 1071 z późn. zm.).
2) Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2025 r. poz. 24 ze zm.).
3) Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych (t.j. Dz. U. z 2024 r. poz. 1769).
4) Ustawa z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (t.j. Dz. U. z 2024 r. poz. 1571 ze zm.).
5) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz. U. UE. L. z 2019 r. Nr 130, str. 92).
6) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji) (Dz. U. UE. L. z 2024 r. poz. 1689).
7) Ustawa z dnia 26 lipca 2024 r. o zmianie ustawy o prawie autorskim i prawach pokrewnych, ustawy o ochronie baz danych oraz ustawy o zbiorowym zarządzaniu prawami autorskimi i prawami pokrewnymi (Dz. U. poz. 1254).

Literatura

1) Auleytner A., Stępień M.J., *Dostęp do sztucznej inteligencji – równość i inne aspekty prawne dostępu do systemów sztucznej inteligencji*, „Monitor Prawniczy" 2019, nr 21.
2) Bar A., *Obrazy generowane z wykorzystaniem sztucznej inteligencji. Status prawnoautorski*, Warszawa 2025.
3) Barta J. (red.), *Prawo autorskie. System Prawa Prywatnego* t. 13, Warszawa 2017.
4) Barta J., Markiewicz R. (red.), *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz,* Warszawa 201.1
5) Błeszyński J., *Prawo autorskie*, Warszawa, 1988..
6) Czajkowska-Dąbrowska M., Ćwiąkalski Z., Felchner K., Traple E., Barta J., Markiewicz R., *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, Warszawa 2011.
7) Flisak D. (red.), *Prawo autorskie i prawa pokrewne. Komentarz*, Warszawa 2015.

8) Ghazal N., Markiewicz M., Matlak A., Nowińska E.,. Stanisławska-Kloc S., Targosz T., Wyrwiński M., Ożegalska-Trybalska J., Widła B., *Komentarz do wybranych przepisów ustawy o prawie autorskim i prawach pokrewnych*, [w:] *Prawo autorskie. Komentarz do znowelizowanych 26 lipca 2024 r. przepisów ustaw: o prawie autorskim i prawach pokrewnych, o ochronie baz danych, o zbiorowym zarządzaniu prawami autorskimi i prawami pokrewnymi*, Warszawa 2025.
9) Kępiński J. (red.), *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, Warszawa 2025.
10) Markiewicz R. (red.), *Komentarz do ustawy o prawie autorskim i prawach pokrewnych*, [w:] *Ustawy autorskie. Komentarze*, t. I, Warszawa 2021.
11) Niewęgłowski A., *Prawo autorskie. Komentarz*, Warszawa 2025.
12) Poźniak-Niedzielska M., Szczotka J. (red.), *Prawo autorskie. Zarys problematyki*, Warszawa 2020.
13) Stępień M.J., *Rzeczpospolita Polska w stosunkach prawnoautorskich*, [w:] *Prawo i państwo: księga jubileuszowa 200-lecia Prokuratorii Generalnej Rzeczypospolitej Polskiej*, L. Bosek (red.), Warszawa 2017.

Orzecznictwo

1) Wyrok Sądu Apelacyjnego w Gdańsku z dnia 30 września 2020 r., sygn. akt V AGa 74/19, LEX nr 3102186.
2) Wyrok Sądu Apelacyjnego w Poznaniu z dnia 20 grudnia 2022 r., sygn. akt I AGa 89/22, LEX nr 3488150.

Inne źródła

1) Piwowarek G., [w:] M. Miernik-Grzesiowska, *Procedura opt-out TDM czyli jak chronić swoją twórczość przed trenowaniem genAI?*, https://lookreatywni.pl/baza-wiedzy/o-procedurze-opt-out-jak-chronic-swoja-tworczosc-przed-trenowaniem-genai/ (dostęp: 22.01.2026 r.).

dr Paweł Świtał
Uniwersytet Radomski im. Kazimierza Pułaskiego
e-mail: p.swital@uthrad.pl
ORCID: 0000-0002-7404-5143

dr Damian Witczak
Uniwersytet Radomski im. Kazimierza Pułaskiego
adres e-mail: d.witczak@urad.edu.pl
ORCID: 0009-0003-3012-731X

Obraźliwa infografika jako przedmiot postępowania dyscyplinarnego – ocena odpowiedzialności dyscyplinarnej studenta uczelni mundurowej za naruszenie etosu służby i dobrego imienia wykładowcy

Offensive infographic as the subject of disciplinary proceedings –assessment of the disciplinary responsibility of a student at a uniformed services university for violating the ethos of service and the good name of a lecturer

Streszczenie

Rozdział podejmuje analizę prawną konsekwencji stworzenia oraz rozpowszechnienia obraźliwej infografiki przez studenta uczelni mundurowej, kwalifikowanej jako przejaw hejtu internetowego skierowanego wobec wykładowcy wyższego stopniem pełniącego funkcję przełożonego. W pierwszej części omówiono zagadnienie naruszenia dóbr osobistych. Następnie przedstawiono rolę postępowania dyscyplinarnego w środowisku uczelni mundurowej jako mechanizmu ochrony etosu służby, hierarchii oraz autorytetu kadry dydaktycznej. Szczegółowej analizie poddano konstrukcję przewinienia dyscyplinarnego, ze szczególnym uwzględnieniem wymogu zawinienia, charakteru naruszonego dobra prawnego oraz skutków działania dla prawidłowego funkcjonowania formacji. W ramach studium przypadku oceniono stopień naruszenia dobrego imienia wykładowcy oraz wpływ czynu na funkcjonowanie formacji, z uwzględnieniem kryteriów wynikających z orzecznictwa sądów administracyjnych dotyczącego odpowiedzialności funkcjonariuszy służb mundurowych. Rozdział dowodzi, że obraźliwa infografika publikowana w przestrzeni cyfrowej, nawet w grupie pozornie zamkniętej, może stanowić poważne naruszenie służby i uzasadniać zastosowanie kar dyscyplinarnych o charakterze represyjnoprewencyjnym. Wyniki analizy wskazują na konieczność wzmacniania świadomości prawnej oraz odpowiedzialności komunikacyjnej osób przygotowujących się do pełnienia zawodów zaufania publicznego.

Wstęp

Celem rozdziału jest wieloaspektowa analiza odpowiedzialności dyscyplinarnej studenta uczelni mundurowej, który opublikował w internecie obraźliwą infografikę dotyczącą wykładowcy, naruszając tym samym zarówno jego dobra osobiste, jak i standardy etosu służby sprzeniewierzając się treści roty ślubowania. Zjawisko hejtu w sieci, szczególnie w środowisku kształcącym przyszłych funkcjonariuszy służb mundurowych, nabiera szczególnego znaczenia, ponieważ dotyka nie tylko relacji interpersonalnych w ramach wspólnoty akademickiej, lecz także fundamentalnych wartości związanych z odpowiedzialnością, lojalnością i kulturą służby publicznej. Publikacja obraźliwych treści przez studenta uczelni mundurowej rodzi pytania o granice wolności wypowiedzi w sieci, zakres ochrony dóbr osobistych wykładowców oraz obowiązki wynikające z regulaminów służby, a także ustaw pragmatycznych.

W niniejszej pracy przedstawiono szczegółowe ramy prawne odpowiedzialności dyscyplinarnej, wynikające z przepisów regulujących funkcjonowanie uczelni mundurowych, w tym obowiązek przestrzegania zasad etyki zawodowej i godnego zachowania w służbie i poza nią. Dokonano analizy stanu faktycznego zakończonego już postępowania dyscyplinarnego odnoszącego się do naruszenia obowiązków służbowych oraz znieważenia osoby będącej funkcjonariuszem pożarnictwa i jednocześnie wykładowcą na uczelni mundurowej. Szczególną uwagę poświęcono relacji między odpowiedzialnością dyscyplinarną a karną oraz możliwości ich równoległego stosowania.

Wnioski płynące z analizy podkreślają konieczność wypracowania spójnych i skutecznych procedur reagowania na przejaw naruszania dóbr osobistych w sieci w instytucjach mundurowych, a także potrzebę wzmacniania edukacji prawnej, etycznej i cyfrowej studentów przygotowujących się do pełnienia odpowiedzialnych ról w służbie publicznej. Rozdział wskazuje, że przeciwdziałanie cyberprzemocy w środowisku uczelni mundurowych jest nie tylko kwestią ochrony dóbr osobistych, lecz także elementem budowania profesjonalizmu i kultury organizacyjnej służb mundurowych.

Naruszenie dóbr osobistych

W myśl art. 23 ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny[228] ochronie prawnej podlegają dobra osobiste człowieka, do których zalicza się m.in. zdrowie, wolność, cześć, swobodę sumienia, nazwisko lub pseudonim, wizerunek, tajemnicę korespondencji, nietykalność mieszkania oraz twórczość naukową, artystyczną,

[228] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2025 r. poz. 1071 ze. zm.), dalej: k.c.

wynalazczą i racjonalizatorską. Katalog ten ma charakter otwarty, co oznacza, że również inne wartości niemajątkowe – o ile wykazują indywidualnie doniosłe znaczenie dla jednostki i jej relacji społecznych – mogą być kwalifikowane jako dobra osobiste[229]. Ochrona przewidziana w art. 23 k.c. ma wymiar powszechny i rozciąga się na wszystkie sfery aktywności człowieka: prywatną, zawodową i publiczną. Dobra osobiste mają naturę niemajątkową, ale ich naruszenie bezpośrednio godzi w poczucie godności oraz społeczną akceptację jednostki[230]. Skutkuje to nie tylko ujemnymi następstwami psychologicznymi, lecz także rodzi konsekwencje prawne, uruchamiając środki ochrony przewidziane w prawie cywilnym. Zarówno doktryna, jak i judykatura podkreślają, że zakres dóbr osobistych nie jest statyczny: ewoluuje wraz ze zmianami społecznymi i technologicznymi. Zjawiska współczesne, takie jak cyberprzemoc czy nieuprawnione udostępnianie treści w Internecie, wymuszają elastyczną interpretację i rozpoznawanie nowych postaci dóbr wymagających ochrony[231].

Hejt, przemoc słowna lub fizyczna, a także upublicznienie wizerunku bez zgody należą do typowych sytuacji, które – na gruncie art. 23 k.c.– mogą stanowić podstawę dochodzenia ochrony[232]. Do naruszenia dochodzi wtedy, gdy działanie bądź zaniechanie osoby trzeciej zagraża lub uderza w prawnie chronione wartości, takie jak godność, dobre imię, prywatność czy wizerunek. Elementem konstytutywnym odpowiedzialności jest bezprawność zachowania, rozumiana jako brak usprawiedliwienia w przepisach prawa bądź w zasadach współżycia społecznego[233]. W orzecznictwie akcentuje się, że do stwierdzenia naruszenia nie jest konieczny zamiar sprawcy – wystarczające jest, aby obiektywnie doszło do wkroczenia w sferę cudzego dobra osobistego.

Szczegółowy opis czynu dyscyplinarnego

W pierwszych miesiącach 2020 r. jeden z podchorążych uczelni mundurowej opublikował w zamkniętej grupie na portalu społecznościowym grafikę przedstawiającą jedną z osób pełniących funkcję dowódcy kompanii szkolnej oraz wykładowcy. Grafika miała charakter prześmiewczy i zawierała liczne komentarze opisujące rzekome zachowania przełożonej, w tym wiele wulgaryzmów oraz treści ośmieszających. Dodatkowo stopień służbowy widoczny na grafice został celowo odwrócony,

[229] A. Sylwestrzak [w:] *Kodeks cywilny. Komentarz aktualizowany*, M. Balwicka-Szczyrba (red.), LEX/el. 2024, art. 23, pkt 2.5.

[230] M. Dobrowolska, A. Goebel, *Czy możemy skutecznie chronić dobra osobiste przed zagrożeniami, jakie niesie za sobą współczesna technologia?*, „Palestra" 2025, nr 1, s. 209-223.

[231] T. Zalewski, U. Zdanowicz, *Realność ochrony dóbr osobistych naruszonych za pośrednictwem Internetu a konstytucyjna gwarancja prawa do sądu*, „Palestra" 2025, nr 1, s. 182-184.

[232] B. Hołyst, *Kryminologiczna ocena agresji werbalnej*, „Ius Novum" 2020, nr 2, s. 26-27.

[233] J. Mucha-Kujawa, *W kierunku ochrony prywatności w erze społeczeństwa informacyjnego*, „Palestra" 2024, nr 8, s. 17-35.

co miało symboliczny wymiar deprecjonujący. Publikacja była podpisana indywidualnym *nickiem* autora, co wykluczało anonimowość. Grupa, w której zamieszczono grafikę, liczyła około 90 członków – głównie studentówpodchorążych. Choć formalnie była to grupa zamknięta, organy dyscyplinarne uznały, że nie można traktować jej jako przestrzeni prywatnej, ponieważ liczba odbiorców oraz charakter komunikacji wskazywały na publiczny wymiar przekazu. Po publikacji grafika zaczęła krążyć wśród studentów, a jej treść – zdaniem komisji – przyczyniła się do powstania hejtu i mowy nienawiści wobec osoby przedstawionej, podważając jej autorytet jako przełożonej odpowiedzialnej za kształtowanie postaw przyszłych funkcjonariuszy. W toku postępowania dyscyplinarnego podchorąży przyznał się do stworzenia i opublikowania grafiki. Wyjaśnił, że działał pod wpływem narastających negatywnych emocji związanych z zachowaniem przełożonej, które – w jego ocenie – miało być niezgodne z regulaminem. Nie skorzystał jednak z żadnej z przewidzianych formalnych ścieżek zgłaszania zastrzeżeń, takich jak rozmowa z dowódcą pododdziałów, psychologiem szkolnym czy rektoremkomendantem. Zamiast tego zdecydował się na publiczne ośmieszenie przełożonej w internecie.

Komisja dyscyplinarna pierwszej instancji uznała, że czyn podchorążego naruszył przepisy ustawy regulującej funkcjonowanie formacji oraz zasady etyki zawodowej, w szczególności obowiązek okazywania szacunku przełożonym, dbania o ich autorytet oraz zachowania godnego funkcjonariusza. Podkreślono, że publikacja godziła nie tylko w dobra osobiste konkretnej osoby, lecz także w dobre imię formacji i w etos służby, który stanowi fundament kształcenia w uczelni mundurowej. Komisja orzekła wobec podchorążego karę wydalenia ze służby. Obwiniony złożył odwołanie, zarzucając m.in. błędną ocenę dowodów, niewłaściwe ustalenia faktyczne, brak przeprowadzenia niektórych dowodów oraz niewspółmierność kary. Organ odwoławczy utrzymał jednak orzeczenie w mocy, wskazując, że czyn miał wysoki stopień społecznej szkodliwości, a kara wydalenia jest adekwatna zarówno z punktu widzenia prewencji indywidualnej, jak i generalnej[234].

Prawna ochrona prawidłowego wykonywania ustawowych zadań przez Państwową Straż Pożarną realizowana jest na wielu płaszczyznach, z których jedną z kluczowych stanowi odpowiedzialność dyscyplinarna. Można określić ją jako instrument wewnętrznego nadzoru służbowego, wdrażany wówczas, gdy dochodzi do nienależytego bądź zawinionego naruszenia obowiązków służbowych przez funkcjonariusza pożarnictwa. W ujęciu dogmatycznym odpowiedzialność ta obejmuje reakcję na czyny naruszające obowiązki zawodowe, zachowania sprzeczne z zasadami deontologii oraz postawy etycznie naganne, które uchybiają godności zawodu strażaka.

[234] Wyrok Naczelnego Sądu Administracyjnego z dnia 17 stycznia 2024 r., sygn. akt III OSK 7613/21 LEX nr 3755645 oraz Wyrok Wojewódzkiego Sadu Administracyjnego w Warszawie z dnia 31 sierpnia2021 r., sygn. akt II SA/Wa 111/21, LEX nr 3319598.

Istotą odpowiedzialności dyscyplinarnej jest wprowadzenie sankcji o charakterze represyjnym za czyn stanowiący przewinienie dyscyplinarne. Konstrukcja ta została jednoznacznie podkreślona w orzecznictwie Trybunału Konstytucyjnego, który w wyroku z dnia 27 lutego 2001 r. wskazał, że postępowanie dyscyplinarne w odniesieniu do zawodów zaufania publicznego bądź zawodów o szczególnej doniosłości społecznej jest ukierunkowane na ochronę honoru, godności oraz dobra wykonywanego zawodu[235]. Tym samym deontologia tych postępowań pełni rolę nie tylko porządkującą, lecz także gwarancyjną dla prawidłowego funkcjonowania formacji mundurowej.

W literaturze przedmiotu podkreśla się, że każde przewinienie dyscyplinarne godzi w określone dobro prawne, naruszając jednocześnie relacje służbowe oraz zaburzając funkcjonowanie organizacji, w ramach której funkcjonariusz realizuje swoje obowiązki. W doktrynie utrwaliło się stanowisko, że najczęściej spotykanymi kategoriami przewinień dyscyplinarnych w formacjach mundurowych są zachowania przedstawiające lekceważący stosunek do przełożonych lub funkcjonariuszy starszych stopniem. Wskazuje się na szczególne znaczenie podporządkowania i hierarchiczności dla prawidłowego przebiegu służby[236].

W formacjach takich jak Państwowa Straż Pożarna odpowiedzialność dyscyplinarna pełni zatem podwójną funkcję: z jednej strony zapewnia sankcjonowanie zachowań sprzecznych z obowiązkami służbowymi, a z drugiej – chroni prawidłowe funkcjonowanie formacji poprzez wzmacnianie postaw zgodnych z etosem służby. W konsekwencji reżim ten ma charakter systemowy, a jego znaczenie wykracza poza indywidualny wymiar odpowiedzialności funkcjonariusza, obejmując również dbałość o sprawność, autorytet i wiarygodność służby jako instytucji publicznej.

Rola postępowania dyscyplinarnego w strukturach Państwowej Straży Pożarnej

Mając na uwadze pożywszy stan faktyczny należy dokonać jego oceny przez pryzmat odpowiedzialności dyscyplinarnej wynikającej z ustawy pragmatycznej jaką w tym przypadku jest ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej[237] oraz zasad etyki zawodowej funkcjonariuszy Państwowej Straży Pożarnej[238]. Na wstępie należy wskazać, że w myśl art. 115 ust. 1 , strażak odpowiada dyscy-

[235] Wyrok Trybunału Konstytucyjnego z dnia 27 lutego 2001 r.,sygn. akt K 22/00, OTK 2001, nr 3, poz. 48.

[236] J. Muszyński, *Przestępstwo wojskowe a przewinienie dyscyplinarne w polskim prawie wojskowym*, Warszawa 1967, s. 69; D. Witczak, *Wpływ statusu funkcjonariusza pożarnictwa na zakres jego ochrony i odpowiedzialności karnej*, Warszawa 2017, s. 41.

[237] Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (t.j. Dz. U. z 2025 r. poz. 1312ze zm.. zm.), dalej: ustawa o PSP.

[238] Zasady etyki zawodowej funkcjonariuszy Państwowej Straży Pożarnej, Komenda Główna Państwowej Straży Pożarnej, Warszawa 2014.

plinarnie za zawinione, nienależyte wykonywanie obowiązków służbowych oraz za czyny sprzeczne ze złożonym ślubowaniem. Z kolei ust. 2 stanowi, że strażak odpowiada dyscyplinarnie również za popełnione przestępstwa lub wykroczenia, niezależnie od odpowiedzialności karnej.

Odpowiedzialność dyscyplinarna strażaków opiera się w polskim systemie prawnym na zasadzie winy, co jednoznacznie potwierdza zarówno doktryna[239], jak i judykatura. W ramach tego reżimu odpowiedzialności nie jest wystarczające samo ustalenie faktu naruszenia obowiązków służbowych czy stwierdzenie zachowania sprzecznego ze złożonym ślubowaniem. Konieczne jest również wykazanie, że działanie strażaka nosiło znamiona zawinienia. Jak podkreślił Naczelny Sąd Administracyjny w wyroku z dnia 11 lutego 2010 r. tylko czyn popełniony w sposób zawiniony może stanowić podstawę przypisania odpowiedzialności dyscyplinarnej. Stanowisko to wprowadza do postępowania dyscyplinarnego strażaków wyraźny wymóg subiektywnej oceny zachowania, całkowicie odmienny od koncepcji odpowiedzialności obiektywne[240].

W judykaturze sądów administracyjnych podkreśla się, że konstrukcja winy w postępowaniach dyscyplinarnych strażaków nie została przez ustawodawcę unormowana jako autonomiczna względem winy znanej prawu karnemu. W wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 28 września 2010 r. jednoznacznie wskazano, że „nie stworzono odrębnych dla tego rodzaju postępowania postaci winy", a zatem interpretacja pojęcia winy winna odbywać się poprzez stosowanie zasad wypracowanych w prawie karnym. Takie podejście ma istotne konsekwencje praktyczne, gdyż wymaga od organów dyscyplinarnych przeprowadzania pogłębionej analizy elementu podmiotowego zachowania, a nie tylko ustalenia faktu naruszenia norm służbowych[241].

W świetle tej wykładni winę w postępowaniu dyscyplinarnym można przypisać strażakowi w dwóch podstawowych postaciach – umyślnej oraz nieumyślnej – odpowiadających typologii znanej kodeksowi karnemu. Wina umyślna zachodzi wówczas, gdy strażak obejmuje swoją świadomością i wolą nienależyte wykonanie obowiązków służbowych[242]. Oznacza to, że po pierwsze, może on chcieć wykonać te obowiązki w sposób sprzeczny z prawem lub zasadami etyki zawodowej,

[239] M. Rogalski [w:] *Państwowa Straż Pożarna. Komentarz*, P. Szustakiewicz, M. Wieczorek (red.), LEX/el. 2024, art. 115; K. Kwapisz-Krygel [w:] *Ustawa o Państwowej Straży Pożarnej. Komentarz*, Warszawa 2014, art. 115; S. Maj [w:] *Komentarz do niektórych przepisów ustawy o Państwowej Straży Pożarnej* [w:] *Postępowanie dyscyplinarne w służbach mundurowych. Komentarz*, Warszawa 2008, art. 115.

[240] Wyrok Naczelnego Sądu Administracyjnego z dnia 11 lutego 2010 r., sygn. akt I OSK 1044/09, LEX nr 1611986.

[241] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 28 września 2010 r., sygn. akt II SA/Wa 756/10, LEX nr 755416.

[242] Szerzej M. Zelek, *Wina w prawie karnym i prawie deliktów – przyczynek do dyskusji na temat tożsamości pojęcia winy w prawie polskim*, „Acta Iuris Stetinensis" 2019, nr 26, s. 109-126.

a po drugie – godzić się na takie zachowanie, przewidując możliwość jego zaistnienia. W pierwszym przypadku mamy do czynienia z tzw. zamiarem bezpośrednim, w drugim zaś z zamiarem ewentualnym, analogicznie jak w prawie karnym.

Druga postać winy – nieumyślność – obejmuje zarówno lekkomyślność, jak i niedbalstwo. Lekkomyślność występuje, gdy strażak przewidywał możliwość nienależytego wykonania obowiązków, lecz – nie znajdując ku temu racjonalnych podstaw – przypuszczał, że do tego nie dojdzie[243]. Z kolei niedbalstwo polega na tym, że funkcjonariusz nie przewidział możliwości naruszenia obowiązków, mimo że przy zachowaniu wymaganej od niego w danych warunkach staranności mógł i powinien ją przewidzieć. Ocena ta ma charakter obiektywno-subiektywny – odwołuje się zarówno do konkretnych kwalifikacji i doświadczenia strażaka, jak i do abstrakcyjnego wzorca należytej staranności wymaganego od funkcjonariusza Państwowej Straży Pożarnej.

W praktyce organów dyscyplinarnych zasada winy pełni funkcję gwarancyjną dla strażaków, zapobiegając przypisywaniu im odpowiedzialności wyłącznie na podstawie skutków naruszenia. Konstrukcja ta chroni przed obciążaniem funkcjonariuszy odpowiedzialnością w sytuacjach, w których do zdarzenia doszło w sposób niezawiniony – na przykład na skutek okoliczności od nich niezależnych, działania sił przyrody czy braku dostępu do informacji niezbędnych do prawidłowej oceny np. sytuacji operacyjnej. Zasada winy nakłada na poszczególne komisje dyscyplinarne rozpoznające poszczególne sprawy dyscyplinarne wnikliwe ustalenie zarówno przebiegu zdarzenia, jak i motywacji, świadomości oraz staranności strażaka[244]. Należy podkreślić, że konsekwentne stosowanie reguł prawa karnego w zakresie winy nie oznacza przenoszenia do postępowania dyscyplinarnego całego systemu karnego wraz z jego zasadami, lecz jedynie wykorzystanie dorobku doktryny i judykatury dotyczącego rozumienia winy jako elementu odpowiedzialności. Zasada ta pozwala na zachowanie spójności systemu prawa oraz zapewnia jednolite standardy oceny zachowania funkcjonariuszy służb mundurowych.

Ocena czynu dyscyplinarnego polegającego na zamieszczeniu obraźliwej infografiki w sieci

Oceniając przywołany wyżej stan faktyczny należy wskazać, że analizowana publikacja nie miała charakteru spontanicznego ani emocjonalnego wzburzenia, lecz była efektem świadomego, zaplanowanego i wieloetapowego działania. Jej

[243] M. Dąbrowska-Kardas, P. Kardas [w:] *Kodeks karny. Część szczególna, t. III. Komentarz do art. 278-363 k.k., wyd. V*, W. Wróbel, A. Zoll (red.), Warszawa 2022.

[244] K. Nowak, *Postępowania dyscyplinarne w służbach mundurowych podległych Ministrowi Spraw Wewnętrznych i Administracji w szczególności na tle ustawy o Państwowej Straży Pożarnej oraz ustawy o Straży Granicznej*, „Zeszyty Naukowe SGSP" 2020, nr 75, 241-259.

przygotowanie obejmowało zarówno selekcję treści, jak i ich graficzne opracowanie, co – zgodnie z wyjaśnieniami podchorążego – zajęło kilkadziesiąt minut. Zaangażowany czas oraz konieczność podjęcia decyzji co do formy, treści i przekazu przesądzają o braku elementu gwałtowności. W konsekwencji czyn obwinionego należy kwalifikować jako działanie w zamiarze bezpośrednim, obejmującym zarówno świadomość treści, jak i przewidywalnych konsekwencji ich rozpowszechnienia. Taki stan rzeczy odpowiada klasycznemu rozumieniu winy umyślnej w prawie karnym. Ponadto, istotnym elementem ocenianego zachowania była pełna świadomość treści zamieszczonych w infografice[245]. Autor grafiki zapoznał się z każdym użytym sformułowaniem, w tym z wyrażeniami o charakterze wulgarnym, obraźliwym i deprecjonującym. Nie działał on instynktownie ani pod przymusem chwili – przeciwnie, jego działanie cechowało się rozwagą i intencjonalnością. W realiach sprawy świadomość ta wynikała z samej natury procesu tworzenia grafiki: dobór poszczególnych słów wymagał ich przeczytania, przemyślenia oraz podjęcia decyzji o ich wykorzystaniu. Tym samym autor nie tylko znał charakter znaczeniowy użytych zwrotów, ale również musiał zdawać sobie sprawę z ich obraźliwego potencjału oraz z możliwości naruszenia godności osoby przedstawionej. Tego rodzaju świadomość nadaje czynowi wyraźnie zawiniony charakter i przesądza, że nie sposób mówić o działaniu nieumyślnym lub wynikającym z niedbalstwa.

Treść grafiki zawierała liczne wulgaryzmy oraz elementy ośmieszające. Charakter przekazu był jednoznacznie obraźliwy – obejmował sformułowania nacechowane ironią, pogardą i wulgarnością, przekraczające nie tylko granice dopuszczalnej krytyki, lecz także minimalne standardy kultury osobistej wymaganej od osób aspirujących do pełnienia służby w formacji mundurowej. Zawarte sformułowania godziły bezpośrednio w kobietę jak i w każdego człowieka. Działanie studenta szkoły pożarniczej polegało na zaatakowaniu w zasadzie bez celu, bez przyczyny dowódcy kompanii szkolnej. Rolą postępowania dyscyplinarnego jest wyciągnięcie konsekwencji za konkretny czyn. Treści tego rodzaju nie tylko naruszają dobra osobiste osoby przedstawionej w grafice, ale także godzą w powagę i autorytet formacji mundurowej, podważając standardy działalności formacji oraz poszanowania hierarchii[246]. W środowisku funkcjonariuszy, dla którego etos służby opiera się na szacunku, lojalności i odpowiedzialności, użycie podobnych treści stanowi naruszenie o szczególnie wysokim stopniu społecznej szkodliwości.

Autorytet przełożonego stanowi jeden z kluczowych filarów funkcjonowania wszystkich formacji mundurowych. Konstrukcja ta wynika z samej istoty służby

[245] M. Peno, *Problem sposobu pojmowania i roli winy w prawie karnym (od dogmatyki do wartości)*, „Czasopismo Prawa Karnego i Nauk Prawnych" 2016, nr 3, s. 109-130.

[246] Szerzej M. Cenin, *Psychospołeczne podstawy tworzenia ustaw o ochronie przeciwpożarowej i Państwowej Straży Pożarowej*, „Przegląd Prawa i Administracji" 2016, nr 106, s. 293-306.

opartej na hierarchii, dyscyplinie i zasadzie bezwzględnego wykonywania rozkazów. W takich strukturach autorytet nie jest wyłącznie kategorią socjologiczną, lecz pełni funkcję normatywną oraz organizacyjną – jego naruszenie przekłada się *a priori* na obniżenie sprawności działania całej jednostki oraz osłabienie zdolności do realizacji ustawowych zadań[247].

Kolejnym istotnym elementem postępowania dyscyplinarnego prowadzonego w przedmiotowym stanie faktycznym była ocena charakteru samej publikacji. Pomimo że grafika została zamieszczona w grupie określanej jako „zamknięta", liczba jej członków wynosiła około 90 osób, to w praktyce wykluczała możliwość uznania przekazu za prywatny. Należy mieć na względzie, że przy tak szerokim kręgu odbiorców ryzyko dalszego rozpowszechniania treści było zarówno realne, jak i w pełni przewidywalne. W świetle ustalonych faktów autor musiał liczyć się z tym, że grafika dotrze do osób spoza grupy, w tym do samej zainteresowanej przełożonej. W Słowniku Języka Polskiego znaczenie słowa „publiczny" zostało określonego jako „dotyczący całego społeczeństwa lub jakiejś zbiorowości", „dostępny lub przeznaczony dla wszystkich", „związany z jakimś urzędem lub z jakąś instytucja nieprawną", oraz „odbywający się przy świadkach"[248]. W rezultacie publikacja miała charakter zbliżony do publicznego co znacząco zwiększało ciężar gatunkowy czynu oraz zakres jego negatywnych konsekwencji.

Szczególnie istotnym elementem ocenianego postępowania jest to, że czyn doprowadził do podważenia autorytetu wykładowcy, osoby odpowiedzialnej za kształtowanie postaw przyszłych oficerów, funkcjonariusza wyższego stopniem służbowym. Ponadto, doszło do sprzeniewierzenia się treści roty ślubowania i zasad etyki służby. Podchorążowie, składając ślubowanie, zobowiązują się m.in. do godnego zachowania, poszanowania przełożonych oraz dbania o dobre imię formacji[249]. Publikacja o uwłaczającym charakterze pozostaje w sprzeczności z każdym z tych zobowiązań, co dodatkowo pogłębia zawiniony charakter czynu i przemawia za jego szczególnie negatywną oceną. Osoba przedstawiona na grafice pełniła funkcję przełożonej odpowiedzialnej za kształtowanie postaw przyszłych funkcjonariuszy. Publiczne jej ośmieszenie w środowisku podchorążych w sposób oczywisty utrudniało wykonywanie przez nią obowiązków, osłabiało jej autorytet oraz

[247] S. Fiodorów, M. Kowalska, *Rola autorytetu w grupach dyspozycyjnych*, „Wiedza Obronna" 2019, nr 1-2, s. 203-225; W. Ołdyński, *Motywacja i przywództwo w służbach mundurowych na przykładzie Policji*, „Wiedza `obronna" 2015, nr 13, s. 255-263.

[248] https://sjp.pwn.pl/so/publicznie.html (dostęp: 12.01.2026 r.).

[249] Art. 30 ust. 1 ustawy o PSP stanowi: Podejmując służbę w Państwowej Straży Pożarnej, strażak składa ślubowanie według następującej roty: *„Ja, obywatel Rzeczypospolitej Polskiej, świadom podejmowanych obowiązków strażaka, uroczyście ślubuję być ofiarnym i mężnym w ratowaniu zagrożonego życia ludzkiego i wszelkiego mienia - nawet z narażeniem życia. Wykonując powierzone mi zadania, ślubuję przestrzegać prawa, dyscypliny służbowej oraz wykonywać polecenia przełożonych. Ślubuję strzec tajemnic związanych ze służbą, a także honoru, godności i dobrego imienia służby oraz przestrzegać zasad etyki zawodowej."*.

naruszało zasady hierarchii, która stanowi jeden z kluczowych filarów funkcjonowania wszystkich formacji mundurowych. Działanie tego rodzaju jawi się jako sprzeczne z wartościami służby, w której nadrzędną rolę odgrywają dyscyplina, poszanowanie przełożonych i respektowanie zasad współżycia służbowego.

Czyn dyscyplinarny popełniony przez funkcjonariusza pożarnictwa noszący znamiona przestępstwa

Zgodnie z art. 115 ust. 2 ustawy o Państwowej Straży Pożarnej strażak odpowiada dyscyplinarnie również za popełnione przestępstwa lub wykroczenia, niezależnie od odpowiedzialności karnej. Przepis ten wskazuje na dualny model reakcji prawnej na czyny naruszające porządek prawny oraz odnoszące się do etosu pełnionej służby tj. odpowiedzialność karną o charakterze publicznoprawnym oraz odpowiedzialność dyscyplinarną o charakterze służbowym. Z uwagi na bliskie relacje prawa karnego z prawem dyscyplinarnym w doktrynie prawo dyscyplinarne ujmowane było jako odmiana rodzajowa prawa karnego. Argumentowano to zbliżonym celem jakim jest reakcja na naruszenie norm oraz podobnych zasad gwarancyjnych m.in. zasada winy czy określoność przewinienia dyscyplinarnego[250]. Pomimo tych podobieństw odpowiedzialność karna i dyscyplinarna pozostają odrębnymi reżimami. Różnią się one przede wszystkim podstawą aksjologiczną, dobrem chronionym czy bezpośrednim celem kary. Trybunał Konstytucyjny w wyroku z dnia 27 lutego 2001 r. podkreślił, że *„deontologia postępowania dyscyplinarnego jest inna niż postępowania karnego. Łączy się ona przede wszystkim ze specyfiką wykonywania niektórych zawodów oraz zasadami funkcjonowania konkretnych korporacji zawodowych. Ukształtowane w ich ramach reguły deontologiczne ukierunkowane są przede wszystkim na obronę honoru i dobra zawodu. […] Stąd też odpowiedzialność dyscyplinarna związana może być z czynami, które nie podlegają odpowiedzialności karnej"*[251].

Zgodnie z art. 115 §18 kodeksu karnego[252], który znajduje zastosowanie w postępowaniu dyscyplinarnym odpowiednio do realiów służby, przez *rozkaz* należy rozumieć służbowe polecenie podjęcia określonego działania albo powstrzymania się od niego, skierowane do strażaka przez przełożonego bądź innego uprawnionego funkcjonariusza starszego stopniem. W świetle art. 318 kodeksu karnego, również stosowanego odpowiednio, strażak nie ponosi odpowiedzialności za czyn zabroniony, którego dopuścił się w wyniku wykonania rozkazu, chyba że realizując go, umyślnie popełnia przestępstwo. Z kolei art. 344 § 1 k.k. stanowi, że strażak nie odpowiada za niewykonanie rozkazu, o którym mowa w art. 343 k.k., jeżeli rozkaz

250 M. Cieślak, *Polskie prawo karne. Zarys systemowego ujęcia*, Warszawa 1994, s. 22–23.

251 Wyrok Trybunału Konstytucyjnego z dnia 27 lutego 2001 r., sygn., akt K 22/00, OTK 2001/3, poz. 48.

252 Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2025 r. poz. 383 ze . zm.), dalej: k.k.

ten nakazywałby popełnienie przestępstwa, a funkcjonariusz odmówił jego wykonania albo powstrzymał się od jego realizacji. Jeżeli jednak strażak wykonuje taki rozkaz niezgodnie z jego treścią w celu istotnego ograniczenia szkodliwości czynu, sąd – na podstawie art. 344 § 2 k.k. – może zastosować nadzwyczajne złagodzenie kary albo całkowicie odstąpić od jej wymierzenia[253].

Na gruncie ustawy o Państwowej Straży Pożarnej odpowiednie regulacje przewiduje art. 116 ust. 2, który wprowadza wyjątek od zasady odpowiedzialności dyscyplinarnej. Zgodnie z tym przepisem, strażak, który popełnia wykroczenie w związku z wykonaniem polecenia służbowego, ponosi wyłącznie odpowiedzialność dyscyplinarną – chyba że w toku realizacji polecenia działał umyślnie, dopuszczając się czynu stanowiącego wykroczenie. W takiej sytuacji ochrona wynikająca z wykonywania rozkazu zostaje uchylona, a funkcjonariusz ponosi pełną odpowiedzialność przewidzianą przepisami.

Odpowiedzialność karna i dyscyplinarna strażaka są wzajemnie niezależne, dlatego też możliwe jest jednoczesne pociągnięcie go do odpowiedzialności karnej oraz dyscyplinarnej – za ten sam czyn oceniany w różnych dziedzinach prawnych. Ustawodawca jednoznacznie przesądził, że w relacji pomiędzy postępowaniem karnym a dyscyplinarnym nie obowiązuje zakaz *ne bis in idem*. Stanowisko to zostało ocenione jako zgodne z Konstytucją, co uzasadniono odmiennością przedmiotu ochrony i celów obu dziedzin: prawo karne służy ochronie porządku prawnego i dóbr prawnych w wymiarze publicznym, prawo dyscyplinarne zaś – ochronie ładu organizacyjnego i etosu służby[254].

Należy podzielić stanowisko Wojewódzkiego Sądu Administracyjnego w Gliwicach, zgodnie z którym postępowanie dyscyplinarne stanowi tryb samodzielny i autonomiczny względem postępowania karnego, a funkcjonariusz podlega odpowiedzialności dyscyplinarnej niezależnie od odpowiedzialności karnej. Dwutorowość ta determinuje jednak, że w każdym z tych postępowań organy orzekające zobowiązane są do dokonania własnych ustaleń faktycznych oraz przeprowadzenia odrębnej oceny zgromadzonego materiału. Niedopuszczalne jest zatem redukowanie aktywności dowodowej organu dyscyplinarnego do wykorzystania materiału z innego, odrębnego postępowania bez podjęcia pełnego, adekwatnego do celu postępowania, postępowania dowodowego[255].

---

253 M. Rogalski [w:] *Państwowa Straż Pożarna. Komentarz*... op.cit., art. 116; D. Korczyński, *Zbieg odpowiedzialności dyscyplinarnej z odpowiedzialnością karną lub za wykroczenie*, [w:] *Odpowiedzialność dyscyplinarna w Policji*, P. Jóźwiak, W.S. Majchrowicz (red.), Piła 2011, s. 59.

254 por. wyrok Trybunału Konstytucyjnego z dnia 8 października 2002 r., sygn. akt K 36/00, OTKA 2002/5, poz. 63.

255 Wyrok Wojewódzkiego Sądu Administracyjnego w Gliwicach z dnia 30 października 2009 r., sygn. akt IV SA/Gl 560/09, LEX nr 574086.

Postępowanie dyscyplinarne służy bowiem weryfikacji odpowiedzialności innego rodzaju niż odpowiedzialność karna. Choć w praktyce te same zachowania strażaka mogą stanowić podstawę zarówno do odpowiedzialności dyscyplinarej, jak i karnej, to każda z nich musi zostać udowodniona przez właściwy organ, w odrębnym trybie, z wykorzystaniem takich środków dowodowych, które – z perspektywy celu i funkcji danego postępowania – są niezbędne i wystarczające do rozstrzygnięcia. Autonomia reżimów pociąga za sobą nie tylko rozdział kompetencyjny, lecz także samodzielność metodologiczną w zakresie gromadzenia, oceny i wnioskowania z dowodów, adekwatną do specyfiki ochrony dóbr i wartości właściwych dla każdego z tych postępowań.

Zakończenie

Przeprowadzona w rozdziale analiza prowadzi do konkluzji, że odpowiedzialność dyscyplinarna w środowisku uczelni mundurowej stanowi autonomiczny i komplementarny względem odpowiedzialności karnej środek ochrony takich wartości jak etos służby czy dobra osobiste poszczególnych funkcjonariuszy. Dualizm reżimów – karny oraz dyscyplinarny – znajduje uzasadnienie w odmienności chronionych dóbr i celów reakcji prawnej: podczas gdy prawo karne zabezpiecza porządek publiczny i dobra prawne w wymiarze powszechnym, odpowiedzialność dyscyplinarna koncentruje się na należytym wykonywaniu obowiązków służbowych oraz postępowaniu zgodnym z treścią złożonego ślubowania.

W realiach formacji mundurowych autorytet przełożonego ma charakter zarówno aksjologiczny, jak i organizacyjny. Jego naruszenie nie jest wyłącznie indywidualnym konfliktem osób, lecz zjawiskiem systemowym, które godzi w system dowodzenia czy zaufanie i obniża gotowość do wykonywania poleceń, a więc realnie zagraża sprawności realizacji zadań ustawowych. Z tego powodu treści ośmieszające, wulgarne, deprecjonujące – zwłaszcza gdy dotyczą osoby odpowiedzialnej za kształtowanie postaw przyszłych funkcjonariuszy – przekraczają granice dopuszczalnej krytyki i uruchamiają reżim ochronny właściwy dla postępowania dyscyplinarnego.

Konkludując, przypadek obraźliwej infografiki stanowi przejaw konfliktu między wolnością wypowiedzi a ochroną dóbr osobistych i etosu służby w warunkach służby mundurowej. Analizowany czyn był dokonany w sposób umyślny i zawiniony, naruszał dobra osobiste konkretnej osoby oraz podważał powagę formacji mundurowej. W takich okolicznościach zastosowanie surowej sankcji dyscyplinarnej jest usprawiedliwione zarówno w wymiarze indywidualnym, jak i generalnym. Warto wskazać, że skuteczność takiego modelu ochrony wymaga jednak równoległego inwestowania w edukację komunikacyjną i etyczną przyszłych funkcjonariuszy, konsekwentnego egzekwowania standardów oraz budowy kultury służbowej, w której zgłaszanie zastrzeżeń odbywa się kanałami instytucjonalnymi, a nie za pośrednictwem treści deprecjonujących w przestrzeni cyfrowej.

Bibliografia:

Akty prawne

1) Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2025 r. poz. 1071 ze. zm.).
2) Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej (t.j. Dz. U. z 2025 r. poz. 1312 ze zm.).
3) Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2025 r. poz. 383 ze zm.).

Literatura

1) Cenin M., *Psychospołeczne podstawy tworzenia ustaw o ochronie przeciwpożarowej i Państwowej Straży Pożarowej*, „Przegląd Prawa i Administracji" 2016, nr 106.
2) Cieślak M., *Polskie prawo karne. Zarys systemowego ujęcia*, Warszawa 1994.
3) Dąbrowska-Kardas M., Kardas P. [w:] *Kodeks karny. Część szczególna, t. III. Komentarz do art. 278-363 k.k., wyd. V*, W. Wróbel, A. Zoll (red.), Warszawa 2022.
4) Dobrowolska M., Goebel A., *Czy możemy skutecznie chronić dobra osobiste przed zagrożeniami, jakie niesie za sobą współczesna technologia?*, „Palestra 2025", nr 1.
5) Fiodorów S., Kowalska M., *Rola autorytetu w grupach dyspozycyjnych*, „Wiedza Obronna" 2019, nr 1-2.
6) Hołyst B., *Kryminologiczna ocena agresji werbalnej*, „Ius Novum" 2020, nr 2.
7) Korczyński D., *Zbieg odpowiedzialności dyscyplinarnej z odpowiedzialnością karną lub za wykroczenie*, [w:] *Odpowiedzialność dyscyplinarna w Policji*, P. Jóźwiak, W.S. Majchrowicz (red.), Piła 2011.
8) Kwapisz-Krygel K. [w:] *Ustawa o Państwowej Straży Pożarnej. Komentarz*, Warszawa 2014.
9) Maj S. [w:] *Komentarz do niektórych przepisów ustawy o Państwowej Straży Pożarnej [w:] Postępowanie dyscyplinarne w służbach mundurowych. Komentarz*, Warszawa 2008.
10) Mucha-Kujawa J., *W kierunku ochrony prywatności w erze społeczeństwa informacyjnego*, „Palestra" 2024, nr 8.
11) Muszyński J., *Przestępstwo wojskowe a przewinienie dyscyplinarne w polskim prawie wojskowym*, Warszawa 1967.
12) Nowak K., *Postępowania dyscyplinarne w służbach mundurowych podległych Ministrowi Spraw Wewnętrznych i Administracji w szczególności na tle ustawy o Państwowej Straży Pożarnej oraz ustawy o Straży Granicznej*, „Zeszyty Naukowe SGSP" 2020, nr 75.
13) Ołdyński W., *Motywacja i przywództwo w służbach mundurowych na przykładzie Policji*, „Wiedza Obronna" 2015, nr 13.

14) Peno M., *Problem sposobu pojmowania i roli winy w prawie karnym (od dogmatyki do wartości)*, „Czasopismo Prawa Karnego i Nauk Prawnych" 2016, nr 3.
15) Rogalski M. [w:] *Państwowa Straż Pożarna. Komentarz*, P. Szustakiewicz, M. Wieczorek (red.), LEX/el. 2024.
16) Sylwestrzak A. (w:) *Kodeks cywilny. Komentarz aktualizowany*, M. Balwicka-Szczyrba (red.), LEX/el. 2024.
17) Witczak D., *Wpływ statusu funkcjonariusza pożarnictwa na zakres jego ochrony i odpowiedzialności karnej*, Warszawa 2017,.
18) Zalewski T., Zdanowicz U., *Realność ochrony dóbr osobistych naruszonych za pośrednictwem Internetu a konstytucyjna gwarancja prawa do sądu*, „Palestra" 2025, nr 1.
19) Zasady etyki zawodowej funkcjonariuszy Państwowej Straży Pożarnej, Komenda Główna Państwowej Straży Pożarnej, Warszawa 2014.
20) Zelek M., *Wina w prawie karnym i prawie deliktów – przyczynek do dyskusji na temat tożsamości pojęcia winy w prawie polskim*, „Acta Iuris Stetinensis" 2019, nr 26.

Orzecznictwo

1) Wyrok Trybunału Konstytucyjnego z dnia 27 lutego 2001 r., sygn. akt. K 22/00, OTK 2001, nr 3, poz. 48.
2) Wyrok Trybunału Konstytucyjnego z dnia 8 października 2002 r., sygn. akt K 36/00, OTKA 2002/5, poz. 63.
3) Wyrok Naczelnego Sądu Administracyjnego z dnia 11 lutego 2010 r., sygn. akt I OSK 1044/09, LEX nr 1611986.
4) Wyrok Naczelnego Sądu Administracyjnego z dnia 17 stycznia 2024 r., sygn. akt III OSK 7613/21 LEX nr 3755645.
5) Wyrok Wojewódzkiego Sądu Administracyjnego w Gliwicach z dnia 30 października 2009 r., sygn. akt IV SA/Gl 560/09, LEX nr 574086.
6) Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 28 września 2010 r., sygn. akt II SA/Wa 756/10, LEX nr 755416).
7) Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 31sierpnia 2021 r., sygn. akt II SA/Wa 111/21, LEX nr 3319598.

Inne źródła

1) https://sjp.pwn.pl/so/publicznie.html (dostęp: 12.01.2026 r.).

Redaktorzy naukowi

Dominika Skoczylas – doktor w dziedzinie nauk społecznych w dyscyplinie nauki prawne. Adiunkt na Wydziale Prawa i Administracji Uniwersytetu Szczecińskiego, członek Zespołu Badawczego Prawa Administracyjnego, Nowych Technologii i Prawa Kosmicznego. Specjalizuje się przede wszystkim w zagadnieniach z zakresu prawa administracyjnego i prawa nowych technologii. W kręgu jej zainteresowań badawczych znajdują się: cyberbezpieczeństwo, prawo komunikacji elektronicznej, prawo administracyjne, sztuczna inteligencja, prawo kosmiczne. Autorka licznych publikacji, w tym monografii naukowej, pt. „Krajowy system cyberbezpieczeństwa".

Paweł Świtał – doktor nauk prawnych w zakresie prawa. Adiunkt w Katedrze Prawa Administracyjnego i Nauki o Administracji na Wydziale Prawa i Administracji Uniwersytetu Radomskiego im. Kazimierza Pułaskiego. Specjalizuje się w zagadnieniach z zakresu prawa administracyjnego ze szczególnym uwzględnieniem prawa samorządu terytorialnego, informatyzacji podmiotów publicznych, prawa oświatowego oraz statusu prawnego osób ze szczególnymi potrzebami. Autor licznych publikacji, opinii i referatów. Członek Zarządu Stowarzyszenia Edukacji Administracji Publicznej.

Z recenzji wydawniczej:

Szczegółowa analiza poszczególnych opracowań pozwala stwierdzić, że książka nie zawiera tekstów przypadkowych, a każdy z autorów wnosi istotny, unikalny wkład do omawianej problematyki. Na szczególną aprobatę zasługuje odwaga naukowa redaktorów i autorów w poruszaniu tematów trudnych i niejednoznacznych [...]. Monografia pod redakcją naukową Dominiki Skoczylas i Pawła Świtala stanowi dzieło o wysokich walorach naukowych, poznawczych oraz aplikacyjnych. Książka w sposób spójny i wyczerpujący realizuje postawione we wstępie cele badawcze, trafnie diagnozując stan polskiej administracji publicznej w dobie technologicznego przełomu. Publikacja ta bez wątpienia zainteresuje szerokie grono odbiorców, w tym pracowników naukowych, studentów kierunków prawniczych i administracyjnych, a także urzędników, informatyków i menedżerów odpowiedzialnych za cyfryzację sektora publicznego.

Ks. dr hab. Sławomir Fundowicz
Katolicki Uniwersytet Lubelski
Jana Pawła II w Lublinie