PRZEGLĄD PRAWA ADMINISTRACYJNEGO
(10)2025 • DOI: 10.17951/ppa.2025.10.101-123

UNIWERSYTET WARSZAWSKI
KRZYSZTOF KATKOWSKI
krzysztof.l.katkowski@gmail.com
ORCID ID: https://orcid.org/0000-0001-6816-5125

Prawne formy działania a cyberprzestrzeń. O prawnych formach działania administracji w ramach Krajowego Systemu Cyberbezpieczeństwa*

Legal Forms of Action and Cyberspace: Discussion of Selected Forms of Administration within the National Cybersecurity System

Wprowadzenie

Sieci oraz systemy i usługi informatyczne pełnią ważną rolę w społeczeństwie. Ich niezawodność i bezpieczeństwo mają zasadnicze znaczenie dla działalności gospodarczej i społecznej, zwłaszcza zaś dla funkcjonowania rynku wewnętrznego[1]. Z tego względu ich odpowiednie uregulowanie – na poziomie zarówno

* Według stanu prawnego na dzień 31 maja 2025 r.

[1] Por. 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.Urz. L 194/1, 19.07.2016), dalej: dyrektywa NIS.

prawa wspólnotowego, jak i prawa unijnego – jest jednym z najważniejszych wyzwań stojących przed systemami europejskiego prawa publicznego.

W tym kontekście szczególnego znaczenia nabiera problematyka prawnych form działania administracji publicznej w obszarze cyberbezpieczeństwa. Zgodnie z art. 7 Konstytucji RP każde działanie organów władzy publicznej musi mieć bezpośrednie lub pośrednie oparcie w obowiązujących przepisach prawa, co nabiera szczególnej wagi w sferze dynamicznie rozwijających się technologii informacyjnych. Problematyka prawnych form działania podmiotów administrujących i organów w ramach polskich regulacji dotyczących cyberbezpieczeństwa, a także w kontekście ich potencjalnej kognicji przez sądownictwo administracyjne pozostaje wciąż słabo rozpoznana przez doktrynę. Tymczasem jest to zagadnienie o dużym znaczeniu praktycznym, wynikającym z potrzeby zapewnienia ochrony praw jednostki w ramach nowych regulacji.

Celem artykułu jest próba scharakteryzowania tych problemów w świetle doktryny prawa administracyjnego. W tym zakresie konieczna jest analiza prawnych form działania administracji publicznej w ramach systemu cyberbezpieczeństwa (ze szczególnym uwzględnieniem form wyodrębnionych według kryterium ich funkcji), a także zestawienie uzyskanych wniosków z pojęciami cyberprzestrzeni i cyberbezpieczeństwa w polskim porządku prawnym oraz z odpowiednią literaturą przedmiotu.

Pojęcie cyberbezpieczeństwa

Cyberprzestrzeń została zdefiniowana przez polskiego ustawodawcę jako przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne, określone w art. 3 pkt 3 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne[2], wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. Kluczowym pojęciem w kontekście regulacji cyberprzestrzeni w polskim porządku prawnym jest cyberbezpieczeństwo, rozumiane – zgodnie z art. 1 ust. 1 u.k.s.c.[3] – jako odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Jak słusznie zauważyły J. Taczkowska-Olszewska, K. Chałubińska-Jentkiewicz i M. Nowikowska, definiując pojęcie cyberprzestrzeni,

[2] Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. 2021, poz. 2070).

[3] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018, poz. 1560).

ustawodawca nie odwołuje się do pojęcia cyberbezpieczeństwa[4]. Odwołania te pojawiają się jednak w ustawach dotyczących stanów nadzwyczajnych, związanych z bezpieczeństwem obywateli, co należy interpretować jako świadome podkreślenie przez ustawodawcę ścisłego związku obu pojęć[5].

Warto przy tym zwrócić uwagę, że samo zdefiniowanie pojęcia cyberprzestrzeni w naukach prawnych jest kwestią kontrowersyjną, na co wskazuje A. Szmyt[6]. Podobne uwagi sformułowała M. Berdel-Dudzińska, podkreślając problematyczność tego pojęcia w kontekście prawa unijnego[7]. Propozycja W.Z. Dziomdziory, aby poza definicją legalną używać zaproponowanego przez C. Marcinkowskiego pojęcia cyberbezpieczeństwa jako „sposobu wolnego od zakłóceń gromadzenia, przetwarzania i wymiany informacji utrwalonych i przetwarzanych w sposób cyfrowy"[8], również wydaje się niewystarczająca, co zostanie omówione w analizie działań administracji w tym obszarze.

Ścisłe powiązanie cyberprzestrzeni z cyberbezpieczeństwem przesuwa ciężar regulacji na prawo publiczne. Jest to związane z faktem unarodowienia tych regulacji. Jak zauważył K. Strzępek, prawo międzynarodowe nie zabrania państwu regulowania własnej infrastruktury cyfrowej, ale regulacje te powinny być realizowane z poszanowaniem zasad prawa międzynarodowego[9]. W tym duchu pozostają również postulaty D. Skoczylas dotyczące cybersolidarności oraz M. Siwickiego, który wskazuje na konieczność częstszego odwoływania się do aktów prawa unijnego, a nie wyłącznie do środków harmonizacyjnych[10].

Pojęcie cyberbezpieczeństwa jest ściśle powiązane z cyberprzestępczością, co historycznie sprowadzało refleksję nad tym zagadnieniem do perspektywy

---

[4] J. Taczkowska-Olszewska, K. Chałubińska-Jentkiewicz, M. Nowikowska, *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Warszawa 2019.

[5] *Ibidem*, s. 3–5.

[6] A. Szmyt, *Opinia prawna do przedstawionego przez Prezydenta RP projektu ustawy o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw z dnia 11 lipca 2011 r.*, „Zeszyty Prawnicze Biura Analiz Sejmowych" 2012, nr 33, s. 174.

[7] Por. M. Berdel-Dudzińska, *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, „Przegląd Prawa Publicznego" 2012, nr 2, s. 19–38.

[8] Zob. W.Z. Dziomdziora, *Czym jest cyberbezpieczeństwo?*, [w:] *Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik*, Warszawa 2021, s. 19.

[9] K. Strzępek, *Cyberbezpieczeństwo Rzeczypospolitej Polskiej – podstawy prawne (międzynarodowe i krajowe)*, „Prokuratura i Prawo" 2023, nr 12, s. 152.

[10] D. Skoczylas, *Wzmocnienie zdolności Unii Europejskiej w zakresie cyberbezpieczeństwa – cybersolidarność w kontekście cyberzagrożeń*, „Europejski Przegląd Sądowy" 2024, nr 12, s. 39–44; M. Siwicki, *Kilka uwag na temat ochrony infrastruktury krytycznej w internecie na tle dyrektywy NIS i jej transpozycji do polskiego porządku prawnego*, „Europejski Przegląd Sądowy" 2019, nr 9, s. 20.

prawa karnego[11]. W polskim porządku prawnym powiązanie to uwidacznia się szczególnie poprzez kluczowe pojęcie incydentu – zdarzenia mającego lub mogącego mieć niekorzystny wpływ na cyberbezpieczeństwo, co podkreśla jego funkcję ochronną przed działalnością przestępczą. Ponadto problematyka cyberbezpieczeństwa jest ściśle związana z prawem do prywatności oraz gromadzeniem informacji o obywatelach przez administrację publiczną lub podmioty prywatne zarządzające tymi danymi[12]. W polskiej nauce prawa i administracji można zaobserwować podobne ujęcia, o czym świadczy bogata literatura zarówno z perspektywy prawa karnego[13], jak i praw człowieka[14].

Tendencja ta jednak ulega szybkim zmianom. Coraz większe znaczenie kwestii cyberbezpieczeństwa zauważalne jest również w badaniach prawa samorządowego. Jak wskazuje A. Gryszczyńska, zainteresowanie to wynika z praktycznych problemów, takich jak ułatwione procedury zgłaszania stron podszywających się (np. poprzez przekierowanie wiadomości z hiperlinkiem na specjalny numer telefonu) w połączeniu z szybkim systemem oceny zgłoszeń, co odpowiada na zachowania użytkowników sprzyjające atakom[15]. Istotnym głosem w dyskusji pozostaje także monografia A. Hańderka poświęcona naruszaniu praw autorskich i praw pokrewnych w cyberprzestrzeni[16]. C. Banasiński i M. Rojszczak natomiast zwrócili uwagę na znaczenie cyberbezpieczeństwa w unijnym prawie konsumenckim[17]. Mimo powszechnych stwierdzeń o rosnącej komputeryzacji

---

[11] Por. M. Lukings, A.H. Lashkari, *Understanding Cybersecurity Law and Digital Privacy: A Common Law Perspective*, Cham 2022, s. 59.

[12] Por. M. Rojszczak, *Cyberprzestrzeń jako nowa płaszczyzna budowania relacji społecznych*, [w:] *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019, s. 49–50.

[13] Zob. zwłaszcza: A. Adamski, *Prawo karne komputerowe*, Warszawa 2000; S. Bukowski, *Przestępstwo hackingu*, „Przegląd Sądowy" 2005, nr 4; M. Siwicki, *Cyberprzestępczość*, Warszawa 2013; W. Filipkowski, *Przestępczość z użyciem komputerów i ich sieci*, [w:] E.W. Pływaczewski, S. Redo, E.M. Guzik-Makaruk, K. Laskowska, W. Filipkowski, E. Glińska, E. Jurgielewicz-Delegacz, M. Perkowska, *Kryminologia. Stan i perspektywy rozwoju*, Warszawa 2019.

[14] O praktycznych zagrożeniach związanych z tym aspektem pisał T.M. Miłkowski (*Czynności operacyjno-rozpoznawcze a prawa i wolności jednostki*, Warszawa 2020, s. 315), zwracając uwagę na fakt, że wskutek polskiego ustawodawstwa terrorystycznego nie odnoszą się one bezpośrednio do zakresu kompetencji danej służby, lecz przede wszystkim do zjawiska terroryzmu, co wiąże się z niedookreślonym obszarem działania służb (a w domyśle również administracji publicznej).

[15] A. Gryszczyńska, *Cyberbezpieczeństwo w jednostkach samorządu terytorialnego*, [w:] *System Prawa Samorządu Terytorialnego*, t. 3: *Samodzielność samorządu terytorialnego – granice i perspektywy*, red. I. Lipowicz, Warszawa 2023, s. 664. Ciekawym wątkiem w tej pracy jest próba ustalenia etymologii pojęcia cyberbezpieczeństwa, zwracając uwagę na łacińskie *sine cura* (*ibidem*, s. 670).

[16] A. Hańderek, *Naruszenie praw autorskich i praw pokrewnych w związku z funkcjonowaniem wyszukiwarek internetowych*, Warszawa 2024.

[17] Zob. C. Banasiński, M. Rojszczak, *Cyberbezpieczeństwo smart implantów w kontekście unijnego prawa ochrony konsumentów*, „Państwo i Prawo" 2024, z. 9, s. 19–54.

świata społecznego w literaturze przedmiotu[18], opracowania z zakresu doktryny administracyjnej dotyczące cyberprzestrzeni wciąż nie należą do najczęstszych[19]. W tym kontekście warto wskazać pionierskie prace J. Janowskiego, który starał się nie tylko wprowadzić refleksję nad cyberprzestrzenią do polskich nauk prawnych i nauk o administracji, lecz także osadzić ją w szerszym, społecznym kontekście[20].

W przypadku dokonywania typologii prawnych form działania administracji celem jest umożliwienie objęcia szerszej problematyki kognicją sądów administracyjnych oraz organów kontrolnych. Rzetelne omówienie form działania organów i podmiotów tworzących Krajowy System Cyberbezpieczeństwa jest więc niezbędne. Jednocześnie ma to istotne znaczenie z perspektywy ochrony praw podmiotowych jednostki, w szczególności prawa do prywatności, a pośrednio wpisuje się też w szerszy nurt badań nad informatyzacją oraz prywatyzacją zadań publicznych. Prawne formy działania stanowią podstawową formę działań władczych administracji publicznej w Polsce, realizując przy tym konstytucyjną zasadę legalizmu. Zgodnie z definicją K.M. Ziemskiego prawna forma działania administracji to „wyodrębniony bądź dający się wyodrębnić, prawem określony, o utrwalonych cechach typ czynności konwencjonalnej bądź faktycznej, bądź zespół takich czynności określonego, powołanego do wykonywania zadań z zakresu administracji publicznej podmiotu (bądź zespołu podmiotów) w celu wypełnienia zadań z zakresu administracji publicznej"[21].

Mając na uwadze klasyczną typologię prawnych form działania administracji zaproponowaną przez J. Starościaka[22], a także szczególne prawne formy działania wskazane przez M. Stahl[23], w niniejszym artykule omówione będzie ich możliwe zastosowanie w rozwijaniu doktryny regulacji prawnych cyberprzestrzeni. Formy

[18] K. Chałubińska-Jentkiewicz, *Cyberspace as an Area of Legal Regulation*, [w:] *Cybersecurity in Poland*, eds. K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński, Cham 2022, s. 25.

[19] Dopiero w ostatnich latach, jak się zdaje, możemy obserwować pewien przełom w tej materii. Oprócz cytowanych do tej pory pozycji, warto zwrócić uwagę zwłaszcza na następujące opracowania: C. Banasiński, M. Rojszczak (red.), *Cyberbezpieczeństwo*, Warszawa 2020; D. Skoczylas, *Znaczenie cyberbezpieczeństwa w administracji publicznej*, [w:] *Wzorce i zasady działania współczesnej administracji publicznej*, red. B. Jaworska-Dębska, P. Kledzik, J. Sługocki, Warszawa 2020.

[20] Zob. m.in. J. Janowski, *Technologia informacyjna dla prawników i administratywistów. Szanse i zagrożenia elektronicznego przetwarzania danych w obrocie prawnym i działaniu administracji*, Warszawa 2009.

[21] K.M. Ziemski, *Indywidualny akt administracyjny jako forma prawna działania administracji*, Poznań 2001, s. 138.

[22] Zob. J. Starościak, *Prawne formy działania administracji*, Warszawa 1957. Co do zasady typologia ta współcześnie jest akceptowana i przytaczana w podręcznikach akademickich. Por. J. Jagielski, M. Wierzbowski (red.), *Prawo administracyjne*, Warszawa 2020, s. 343–381.

[23] Zob. M. Stahl, *Szczególne prawne formy działania administracji*, [w:] *System Prawa Administracyjnego*, t. 5: *Prawne formy działania administracji*, red. A. Błaś, J. Boć, M. Stahl, K.M. Ziemski, Warszawa 2013, s. 318–401.

te, związane przede wszystkim z zagadnieniami prawa publicznego, stanowią – jak stwierdzili hiszpańscy teoretycy C.M. Galán i C. Galán Cordero – logiczną implikację zasady rządów prawa oraz podstawową gwarancję ochrony praw podmiotowych w cyberprzestrzeni[24]. W tym sensie można zgodzić się z tezą K. Chałubińskiej-Jentkiewicz, według której cyberbezpieczeństwo jest zadaniem publicznym administracji, a kontrola i nadzór nad cyberprzestrzenią stanowią jeden z jej kluczowych obowiązków[25]. Należy przy tym pamiętać, że jest to stosunkowo nowy obszar regulacji, często funkcjonujący na nowych zasadach, co uzasadnia potrzebę dokładnych badań teoretycznoprawnych.

Na potrzeby niniejszego opracowania przyjęto, że definicje operacyjne mają przede wszystkim odzwierciedlać praktyczne działania administracji publicznej w cyberprzestrzeni oraz wiązać je z obowiązującymi regulacjami prawnymi. W odróżnieniu od definicji legalnych, które określają pojęcia w sposób formalny i abstrakcyjny, definicje operacyjne uwzględniają organizacyjno-techniczny wymiar zagrożeń.

Cyberbezpieczeństwo definiuje się tutaj jako odporność systemów teleinformatycznych na zagrożenia, zapewniającą poufność, integralność, dostępność i autentyczność danych oraz usług, wspieraną przez działania administracji publicznej w sferze prawnej, organizacyjnej, technicznej i informacyjnej. Incydent cyberbezpieczeństwa to zdarzenie rzeczywiste lub potencjalne, które negatywnie wpływa lub może wpłynąć na funkcjonowanie systemów teleinformatycznych oraz wymaga reakcji administracyjnej lub technicznej. Prawna forma działania administracji to typ czynności określony prawem, mający na celu realizację zadań publicznych w obszarze cyberbezpieczeństwa (są to np. decyzje, akty nadzoru, akty kontroli, akty współdziałania).

Podstawy prawne regulacji dotyczących cyberbezpieczeństwa – obszary analizy

Krajowy System Cyberbezpieczeństwa (KSC) został utworzony na mocy ustawy o krajowym systemie cyberbezpieczeństwa, będącej implementacją dyrektywy NIS. Celem ustawy jest – jak wskazano w uzasadnieniu do jej projektu – „próba kompleksowego uregulowania krajowego systemu cyberbezpieczeństwa, z jednej strony, będąca odpowiedzią na stale rosnące i dynamicznie się zmieniające cyberzagrożenia

[24] Zob. C.M. Galán, C. Galán Cordero, *La ciberseguridad pública como garantía del ejercicio de derechos*, "Derecho & Sociedad" 2016, núm. 47, s. 293.

[25] Zob. K. Chałubińska-Jentkiewicz, *Cybersecurity as a Public Task in Administration*, [w:] *Cybersecurity in Poland…*; eadem, *Bezpieczeństwo cyberprzestrzeni jako zadanie publiczne w systemie bezpieczeństwa narodowego RP*, „Zeszyty Naukowe AON" 2014, nr 3, s. 20–35.

mogące godzić w bezpieczeństwo państwa, gospodarki i społeczeństwa, a z drugiej strony, stanowiąca implementację przedstawionej wyżej dyrektywy NIS"[26].

Krajowy System Cyberbezpieczeństwa opiera się na współpracy podmiotów prywatnych – w tym spółek skarbu państwa – oraz podmiotów publicznych, przy czym do zadań tych ostatnich należy przede wszystkim sprawowanie nadzoru i kontroli, wskazane w art. 4 u.k.s.c. Do podmiotów prywatnych należą: operatorzy usług kluczowych, dostawcy usług cyfrowych, spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej w rozumieniu art. 1 ust. 2 ustawy o gospodarce komunalnej, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, a także wybrane jednostki sektora finansów publicznych.

Przedstawicielami administracji publicznej w KSC są m.in. Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego Ministerstwa Obrony Narodowej (CSIRT MON), Krajowy Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (CSIRT NASK), Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Agencję Bezpieczeństwa Wewnętrznego (CSIRT GOV), sektorowe zespoły cyberbezpieczeństwa, instytuty badawcze, Narodowy Bank Polski, Bank Gospodarstwa Krajowego, Urząd Dozoru Technicznego, Polska Agencja Żeglugi Powietrznej, Polskie Centrum Akredytacji, Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej (NFOŚiGW), wojewódzkie fundusze ochrony środowiska i gospodarki wodnej, organy właściwe do spraw cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa, Pełnomocnik Rządu ds. Cyberbezpieczeństwa, Kolegium ds. Cyberbezpieczeństwa. W niniejszej pracy omówione zostaną prawne formy działania podmiotów należących do tej drugiej grupy, ze szczególnym uwzględnieniem działań CSIRT oraz organów właściwych do spraw cyberbezpieczeństwa.

Dla lepszego zrozumienia znaczenia podmiotów w KSC warto dokonać ich podziału. Dostawcy usług kluczowych przejmują część obowiązków administracji publicznej, co w doktrynie określa się jako prywatyzację zadań publicznych. W niniejszym opracowaniu koncentrujemy się jednak na podmiotach i organach administracji publicznej. W tym kontekście można wyróżnić: organy administracyjne, nietypowe organy administracyjne oraz podmioty administrujące. Organy właściwe do spraw cyberbezpieczeństwa zaliczane są do organów administracyjnych, natomiast instytucje takie jak NFOŚiGW – zgodnie z typologią J. Jagielskiego – do nietypowych organów administracyjnych[27]. Trudniejszą kwestią

[26] W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019, s. 19.

[27] J. Jagielski, *Z problematyki organów administracyjnych*, [w:] *Problemy współczesnego ustrojoznawstwa. Księga jubileuszowa Profesora Bronisława Jastrzębskiego*, red. J. Dobkowski, Olsztyn 2007.

jest klasyfikacja CSIRT-ów i sektorowych zespołów cyberbezpieczeństwa. Przyjmujemy, że stanowią one podmioty administrujące, ponieważ zostały powołane do wykonywania funkcji administracji publicznej, nie będąc jednak organami administracji *par excellence*.

Podmioty te działają poprzez odpowiednie prawne formy działania, obejmujące zarówno klasyczne instrumenty administracyjne, jak i nowe, szczególne formy, często pozostające poza kognicją sądów administracyjnych.

Jednocześnie warto podkreślić, że KSC jest subsystemem norm w fazie dynamicznego rozwoju. Już po rozpoczęciu pełnoskalowej inwazji Federacji Rosyjskiej na Ukrainę ustawodawca wprowadził szereg nowych regulacji, w tym np. takie jak: możliwość wyznaczenia jednego organu wiodącego do sprawowania nadzoru nad podmiotami kluczowymi i ważnymi, w tym w sektorach finansowym, telekomunikacyjnym i energetycznym; ustanowienie procedury kontroli doraźnych, możliwych m.in. po zgłoszeniu potencjalnych naruszeń przez urzędnika monitorującego; zmiany w zasadach nakładania kar pieniężnych, których wysokość zależy od charakteru i skali naruszenia, czasu jego trwania, sytuacji finansowej podmiotu oraz poziomu współpracy z organami nadzoru; złagodzenie przepisów dotyczących kar okresowych; uregulowanie statusu urzędnika monitorującego, którego działania ograniczono do okresu nieprzekraczającego jednego miesiąca przy obowiązku uprzedniego powiadomienia nadzorowanego podmiotu o planowanych oględzinach systemów IT; przyspieszenie tworzenia sektorowych zespołów cyberbezpieczeństwa oraz umożliwienie włączenia centrów wymiany informacji i analiz (ISAC) do krajowego systemu cyberbezpieczeństwa.

Prawne formy działania administracji wobec cyberprzestrzeni

Do prawnych form działania administracji zalicza się m.in. akty normatywne administracji, akty administracyjne (np. decyzje), ugody, porozumienia administracyjne, umowy cywilnoprawne, czynności faktyczne oraz działania społeczno-organizatorskie, natomiast tzw. milczenie administracji pozostaje kategorią dyskusyjną[28]. Jak trafnie zauważyła M. Stahl, „żaden z proponowanych katalogów nie może być uznany za pełny, przystający do współczesnych zadań administracji, do nowych dostosowanych do nich środków działania, do rozbudowującego się katalogu podmiotów administrujących”[29]. Autorka podkreśliła, że pojawiają się nowe prawne formy działania, których nie da się zakwalifikować do żadnej

[28] J. Jagielski, M. Wierzbowski (red.), *op. cit.*, s. 343–381.

[29] M. Stahl, *op. cit.*, s. 319–320.

z tradycyjnie wyodrębnianych kategorii, a ustawodawca nie podejmuje prób ich formalnej definicji ani adaptacji do istniejących schematów.

Wyróżnienie prawnych form działania ma doniosłe znaczenie z co najmniej dwóch powodów. Po pierwsze, administracja realizuje swoje zadania przede wszystkim poprzez te formy. Po drugie, ich wyraźne scharakteryzowanie umożliwia objęcie ich kognicją przez sądy administracyjne, co przekłada się na lepszą ochronę praw jednostki. Typologia prawnych form działania, jaką zaproponował J. Starościak[30], opisuje je bardzo ogólnie i stwarza trudności w identyfikacji nowych, szczególnych form. Wychodząc z założenia M. Stahl, że określenie nowej prawnej formy działania administracji wymaga analizy zmian w sposobach realizacji zadań publicznych[31], należy stwierdzić, że regulacje dotyczące KSC mogą stanowić cenny przyczynek do dalszych badań nad szczególnymi formami działania administracji. Równocześnie system ten funkcjonuje na czterech wzajemnie powiązanych poziomach: prawnym, organizacyjnym, technicznym oraz informacyjnym. Każdy z tych poziomów warunkuje dobór określonych form działania administracji oraz wyznacza granice możliwych interwencji w sferę publiczną i prywatną.

Poziom prawny stanowi fundament całego KSC. To właśnie normy prawne, w szczególności ustawa o krajowym systemie cyberbezpieczeństwa oraz akty wykonawcze, określają strukturę, zadania i kompetencje organów, a także relacje między nimi. Na tym poziomie dominują formy władcze: decyzje administracyjne (np. uznanie podmiotu za operatora usługi kluczowej, nałożenie kar pieniężnych), akty nadzoru oraz niektóre akty kontroli. Prawny wymiar funkcjonowania KSC realizuje wprost konstytucyjną zasadę legalizmu (art. 7 Konstytucji RP) oraz wyznacza granice działania administracji publicznej wobec podmiotów prywatnych. Jednocześnie zakres normatywnego ujęcia cyberbezpieczeństwa jest dynamiczny i fragmentaryczny, dlatego wymaga ciągłej reinterpretacji form działania administracji w świetle zmieniających się realiów technologicznych oraz bezpieczeństwa informacyjnego.

Poziom organizacyjny dotyczy układu instytucjonalnego KSC oraz mechanizmów współdziałania pomiędzy jego uczestnikami. To tutaj materializują się formy współdziałania (koordynacji), porozumienia administracyjne, akty planowania i akty polityki. System KSC opiera się na sieciowym modelu współpracy pomiędzy podmiotami publicznymi (takimi jak CSIRT MON, CSIRT GOV, CSIRT NASK, organy właściwe ds. cyberbezpieczeństwa) oraz prywatnymi (jak operatorzy usług kluczowych, dostawcy usług cyfrowych, podmioty świadczące usługi z zakresu cyberbezpieczeństwa). Taki model wymaga stosowania form niewładczych, opartych na zaufaniu i wymianie informacji, co czyni klasyczną doktrynę form admi-

[30] *Ibidem*.

[31] *Ibidem*, s. 326.

nistracyjnych niewystarczającą dla pełnego opisu tego typu relacji. W praktyce na poziomie organizacyjnym dominują akty współpracy i koordynacji, które pełnią funkcję spajającą cały system oraz zapewniają jego operacyjną integralność.

Poziom techniczny odnosi się do infrastruktury teleinformatycznej, narzędzi, standardów i procedur technicznych, które umożliwiają realizację zadań publicznych w obszarze cyberbezpieczeństwa. Działania administracji na tym poziomie przybierają często postać czynności materialno-technicznych, aktów kontroli technicznej czy też rekomendacji eksperckich. Z racji swej natury formy działania na tym poziomie są z reguły nietypowe i trudne do jednoznacznej klasyfikacji w ramach klasycznych form prawa administracyjnego, wymagają bowiem współdziałania z ekspertami technicznymi, stosowania narzędzi analizy ryzyka czy systemów monitorowania incydentów, a także podejmowania decyzji w czasie rzeczywistym. Często przybierają charakter *soft law* – zaleceń, wytycznych i standardów, które formalnie nie są wiążące, ale faktycznie kształtują zachowania uczestników systemu.

Poziom informacyjny dotyczy zarządzania wiedzą, wymiany danych oraz komunikacji pomiędzy uczestnikami systemu. W ramach tego poziomu pojawiają się takie formy działania jak: akty informacji i akty wiedzy, raporty o incydentach, ostrzeżenia, rekomendacje. Załóżmy więc, że jest to sfera szczególnie wrażliwa z punktu widzenia ochrony praw jednostki, zwłaszcza zaś prawa do prywatności i ochrony danych osobowych. Działania na poziomie informacyjnym często mają charakter pozaprawny, ale normatywnie istotny – tworzą nowe obowiązki faktyczne oraz kształtują praktykę funkcjonowania administracji w cyberprzestrzeni.

W tym sensie wymiar informacyjny KSC wyznacza granice współczesnej administracji cyfrowej, w której informacja staje się nie tylko narzędziem, lecz także celem działań publicznych. Podział ten umożliwia również dalszą analizę prawnych form działania administracji, zarówno tych uznawanych za typowe, jak i tych nazywanych w doktrynie „nietypowymi". I tak na poziomie prawnym dominują decyzje administracyjne oraz akty formalne, takie jak kontrola i nadzór, przy czym obowiązuje tutaj zasada legalizmu, determinująca konieczność działania organów w granicach prawa. Poziom organizacyjny obejmuje przede wszystkim akty współdziałania i nadzoru, które zapewniają sieciową strukturę systemu oraz koordynację działań podmiotów publicznych i prywatnych. Na poziomie technicznym kluczową rolę odgrywają akty kontroli oraz akty wiedzy, odpowiadające na potrzebę działań eksperckich i operacyjnych w zakresie cyberbezpieczeństwa. Wreszcie poziom informacyjny wykorzystuje miękkie instrumenty, takie jak rekomendacje, zalecenia czy akty informacji, które umożliwiają prewencyjny i koordynacyjny wpływ na funkcjonowanie podmiotów bez stosowania władztwa.

Decyzje administracyjne

Decyzje administracyjne, będące jedną z postaci aktów administracyjnych[32], należą do typologii form działania administracji wiązanej z propozycjami J. Starościaka. Mimo to należą do najczęściej wykorzystywanych form działania administracji. Są definiowane jako oparte na przepisach prawa administracyjnego władcze, jednostronne oświadczenia woli organu administracji publicznej, kształtujące sytuację prawną konkretnie wskazanego adresata w indywidualnie oznaczonej sprawie. Jednocześnie pozostają jedynymi formami działania administracji w ramach KSC, które do 2021 r. zajmowały jakkolwiek polskie sądownictwo administracyjne[33]. Kwestia decyzji administracyjnych pojawiła się na późniejszym etapie jedynie w dwóch sprawach. W sprawie o sygn. VI SA/Wa 2293/20 Wojewódzki Sąd Administracyjny w Warszawie oddalił skargę na decyzję odmawiającą stwierdzenia wygaśnięcia wcześniejszej decyzji uznającej podmiot za operatora usługi kluczowej, wydanej na podstawie art. 6 ust. 2 u.k.s.c. Druga ze spraw znalazła swój finał przed Naczelnym Sądem Administracyjnym – mowa o wyroku w sprawie o sygn. II GSK 557/21. Dotyczyła ona samego uznania podmiotu za operatora usługi kluczowej.

W każdym przypadku poszczególne osoby prawne lub jednostki organizacyjne zaskarżały właściwe organy, m.in. na podstawie art. 5 ust. 2 u.k.s.c., który daje organom właściwym do spraw cyberbezpieczeństwa kompetencję do wydawania decyzji o uznaniu podmiotu za operatora usługi kluczowej. Uznanie za operatora usługi kluczowej oznacza nałożenie odpowiednich obowiązków na daną osobę prawną czy też jednostkę organizacyjną, co reguluje rozdział 3 ustawy o krajowym systemie cyberbezpieczeństwa. Orzecznictwo z pewnością doprecyzowuje

[32] Oczywiście ustawa o krajowym systemie cyberbezpieczeństwa zawiera również przepisy blankietowe, a więc na jej podstawie wydawane są akty generalne (rozporządzenia właściwych ministrów).

[33] Są to: wyrok WSA w Warszawie z dnia 14 stycznia 2021 r., VI SA/Wa 2293/20; wyrok WSA w Warszawie z dnia 22 października 2020 r., VI SA/Wa 2666/19; wyrok WSA w Warszawie z dnia 3 września 2020 r., VI SA/Wa 2151/19; wyrok WSA w Warszawie z dnia 5 sierpnia 2020 r., VI SA/Wa 2667/19; wyrok WSA w Warszawie z dnia 11 grudnia 2019 r., VI SA/Wa 1436/19. Jedna ze spraw była następnie rozważana przez Naczelny Sąd Administracyjny (postanowienie NSA z dnia 23 kwietnia 2020 r., II GZ 97/20). Pozostałe orzeczenia nie odnoszą się bezpośrednio do form działania administracji publicznej, a z pewnością nie w takim zakresie, który uzasadniałby ich szczegółowe omówienie w ramach niniejszej analizy dogmatycznej. Wyroki Wojewódzkiego Sądu Administracyjnego w Warszawie w sprawach II SAB/Wa 673/23 oraz II SA/Wa 2386/23 dotyczą jedynie zagadnień powiązanych z ustawą o krajowym systemie cyberbezpieczeństwa, w szczególności zaś bezczynności Komendanta Policji w zakresie przyznania dodatku teleinformatycznego. Wyrok w sprawie VIII SA/Wa 76/22 dotyczy natomiast kwestii przyznania wsparcia ze środków unijnych i nie odnosi się wprost do problematyki analizowanej w niniejszym opracowaniu.

warunki uznania podmiotu za operatora usługi kluczowej, co praktycznie znacząco ogranicza władzę dyskrecjonalną organów administracji w tym zakresie.

Drugą podstawą prawną do wydawania indywidualnych aktów administracyjnych przez organy właściwe do spraw cyberbezpieczeństwa jest art. 74 u.k.s.c., który upoważnia je do nakładania kar pieniężnych na operatorów usług kluczowych, którzy nie wywiązują się z należnych im obowiązków (jak np. przeprowadzanie systematycznego szacowania ryzyka).

W obu przypadkach organy właściwe do spraw cyberbezpieczeństwa są związane prawem i działają zgodnie z zasadą legalizmu. Jest to decyzja identyfikacyjna, stanowiona w zgodzie z wytycznymi dyrektywy NIS, a postępowanie w przedmiocie identyfikacji prowadzone jest według kodeksu postępowania administracyjnego[34]. Warto przy tym pamiętać, że możliwe jest świadczenie przez podmioty działające w sektorach i podsektorach, o których mowa w dyrektywie NIS, zarówno usług kluczowych, jak i usług innych niż kluczowe, przy czym Polska ustanowiła wykaz usług, które uważa za kluczowe (taki wykaz został określony w załączniku 1 do ustawy o krajowym systemie cyberbezpieczeństwa)[35].

Analogicznie w komentarzach do ustawy o krajowym systemie cyberbezpieczeństwa bezspornie decyzje wydawane na podstawie art. 74 u.k.s.c. uważa się za decyzje administracyjne, pomimo zaznaczenia pewnych wątpliwości, jeśli chodzi o kolizję z art. 189f § 2 i 3 k.p.a.[36]. Kontrowersji nie budzi też wydawanie decyzji na podstawie art. 76 u.k.s.c., zgodnie z którym kara może zostać nałożona również w przypadku, gdy podmiot zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę, jeżeli organ właściwy do spraw cyberbezpieczeństwa uzna, że przemawia za tym czas trwania, zakres lub skutki naruszenia. Art. 75 u.k.s.c. wskazuje zaś, że jeśli kara zostaje wymierzona kierownikowi operatora usługi kluczowej, to może być wymierzona w kwocie nie większej niż 200% jego miesięcznego wynagrodzenia.

Akty nadzoru

Ewentualne problemy natury praktycznej pojawiają się przy analizie szczególnych, nietypowych form działania administracji. Pierwszą formą, bardzo istotną dla funkcjonowania KSC, są akty nadzoru. W doktrynie są one łączone z aktami kierownictwa, zwłaszcza w sferze wewnętrznej[37]. Definiuje się je jako

[34] Zob. K. Czaplicki, A. Gryszczyńska, G. Szpor (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019, s. 79–99.

[35] W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz (red.), *op. cit.*, s. 335.

[36] *Ibidem*.

[37] M. Stahl, *op. cit.*, s. 335–336.

ingerencję organów administracji w działalność innych podmiotów wykonujących zadania administracji publicznej, podejmowaną na podstawie wyraźnego umocowania ustawowego w celu zlikwidowania skutków naruszenia prawa[38]. Nie są przy tym tożsame z decyzjami administracyjnymi, ponieważ nie są podejmowane w sprawach indywidualnych z zakresu administracji; są one raczej związane ze sprawowaniem kontroli nad samorządami[39]. Ingerencja nadzorcza może przybierać różne formy[40]. W doktrynie całość środków nadzoru zalicza się do czterech grup. Są to środki: informacyjne, ostrzegawcze, represyjne oraz z zakresu jurysdykcji administracyjnej[41].

Co istotne, akty nadzoru stosowane są w systemie administracji zdecentralizowanej wobec samodzielnych na płaszczyźnie prawnej podmiotów administrujących, które wykonują zadania publiczne. Na tym aspekcie ma się zasadzać także wymiar podmiotowy tej formy prawnej, co przejawia się w tym, że akty nadzoru są podejmowane przez podmioty administracji publicznej w stosunku do innych podmiotów administrujących, samodzielnie realizujących przekazane im zadania publiczne[42]. Prowadzi to do wymieniania aktów nadzoru jako charakterystycznych dla relacji między administracją wyższego szczebla a samorządami lokalnymi, zawodowymi czy specjalnymi.

Refleksja nad regulacjami ustawy o krajowym systemie cyberbezpieczeństwa pozwala na szersze spojrzenie na pojęcie aktów nadzoru[43]. Jak wskazano w art. 1 pkt 2 u.k.s.c., ustawa ta określa również sposób sprawowania nadzoru i kontroli w zakresie stosowania jej przepisów. Same regulacje ustawowe także szeroko obejmują problematykę aktów nadzoru, co widać zwłaszcza w możliwości form działania podejmowanych wobec operatorów usług kluczowych oraz dostawców usług cyfrowych przez CSIRT-y i zespoły właściwe do spraw cyberbezpieczeństwa. Ich charakter jest ściśle związany z aktami kontroli i aktami współdziałania (koordynacji). Razem współtworzą one podstawy działania administracji w ramach KSC. Co istotne, mamy tutaj do czynienia z nową formą administracji zdecentralizowanej, w tym wypadku jednak łączącej sektor publiczny i prywatny, nieopierający się – na czym do tej pory skupiała się doktryna – przede wszystkim na problematyce samorządowej.

Operatorzy usług kluczowych są zobligowani do przeprowadzania aktów kontroli na własną rękę (poprzez powoływanie struktur wewnętrznych lub zawarcie

[38] *Ibidem*, s. 341.
[39] *Ibidem*, s. 338–339.
[40] *Ibidem*, s. 342.
[41] *Ibidem*, s. 341–342.
[42] *Ibidem*, s. 339–340.
[43] I to nie tylko jako analogia z pozostałymi formami, takimi jak rekomendacje Komisji Nadzoru Finansowego. Zob. *ibidem*, s. 346–347.

umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa, co reguluje art. 14 u.k.s.c.) lub poprzez ustawowo określone podmioty (chodzi tutaj zwłaszcza o przeprowadzanie audytów, co reguluje m.in. art. 15 u.k.s.c.). Wiąże się to z obowiązkiem bądź z możliwością informowania organów właściwych do spraw cyberbezpieczeństwa, właściwych CSIRT-ów i sektorowych zespołów cyberbezpieczeństwa o zawieraniu umów z podmiotami świadczącymi usługi z zakresu cyberbezpieczeństwa. Dostawcy usług cyfrowych, również zobligowani do prowadzenia pewnych form samokontroli niezależnie od aparatu administracji państwowej, mają zgłaszać incydenty niezwłocznie do odpowiedniego podmiotu administracji publicznej. Podobnie podmioty publiczne, o których mowa w art. 4 pkt 7–15 u.k.s.c., zobligowane są do przeprowadzania licznych form samokontroli.

Co istotne, wszystkie akty w ramach KSC pozostają pod nadzorem właściwych CSIRT-ów. Zgodnie z art. 26 ust. 3 pkt 1 u.k.s.c. do ich zadań należy monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym, realizowane poprzez liczne akty nadzoru. Wynikają one przede wszystkim z kompetencji do występowania do operatorów usług kluczowych, podmiotów publicznych wskazanych w art. 4 pkt 7–15 u.k.s.c. oraz dostawców usług cyfrowych o informacje związane z ochroną systemów teleinformatycznych. Poprzez obsługę incydentów i ich klasyfikowanie uwidacznia się władczy charakter CSIRT-ów, który stanowi podstawę do wydawania aktów nadzoru. Aby uniknąć nadmiernego formalizmu, są one realizowane w formie rozstrzygnięć nadzorczych, a nie decyzji administracyjnych. Istotnym elementem działań CSIRT-ów są też opinie, rekomendacje oraz różnego rodzaju niewiążące zalecenia, stanowiące formę „miękkiego prawa" i jednocześnie nadzoru nad podlegającymi im podmiotami.

Nadzór sprawują także organy właściwe do spraw cyberbezpieczeństwa. Realizują go m.in. poprzez prowadzenie kontroli operatorów usług kluczowych i dostawców usług cyfrowych oraz – podobnie jak CSIRT-y – występowanie o udzielenie informacji od poszczególnych podmiotów. Istotne kompetencje posiada również Prezes Rady Ministrów, uregulowane w art. 67 ust. 1–2 u.k.s.c. Na podstawie rekomendacji Kolegium ds. Cyberbezpieczeństwa Prezes Rady Ministrów może wydawać wiążące wytyczne dotyczące zapewnienia cyberbezpieczeństwa na poziomie krajowym, funkcjonowania KSC oraz obsługi incydentów krytycznych, w tym wskazywać CSIRT odpowiedzialny za ich obsługę. Są to formy nadzoru sprawowanego nad niższymi w hierarchii przedstawicielami administracji publicznej oraz podmiotami prywatnymi.

Reasumując, akty nadzoru pełnią w ramach KSC funkcję scalającą działalność systemu, podkreślając jego hierarchiczną strukturę. Opierają się one na aktach kontroli oraz aktach współdziałania (koordynacji).

Akty kontroli

O ile pojęcie nadzoru można zamknąć w pewne ramy, określając je poprzez formy rekomendacji czy też rozstrzygnięć nadzorczych, o tyle sytuacja w przypadku tzw. aktów kontroli wydaje się bardziej złożona. Jak wskazuje M. Stahl, w ramach nadzoru materialnoprawnego podstawową formą działania administracji pozostaje klasyczny akt administracyjny, lecz w fazie kontroli, poprzedzającej akty o charakterze formalnym, możliwe jest wydawanie aktów nieformalnych[44]. Aktami kontroli mogą być zatem dokumenty zawierające uwagi, wnioski, zalecenia, projekty, wystąpienia oraz wystąpienia pokontrolne, przy czym władczy charakter tych aktów pozostaje kwestią dyskusyjną[45]. Jak podkreśla D. Wacinkiewicz, samo poddanie się kontroli stanowi w praktyce pewne podporządkowanie się władzy podmiotu kontrolującego[46]. Akty kontroli mogą przyjmować również formę decyzji administracyjnych, wydawanych na podstawie ustaleń kontroli lub innych aktów administracyjnych o władczym charakterze, rozstrzygających sprawy indywidualne określonych podmiotów oraz podlegających zaskarżeniu, co znajduje potwierdzenie w orzecznictwie[47].

Akty kontroli niebędące decyzjami administracyjnymi również pełnią istotną rolę w KSC. Kontrole podejmowane są przede wszystkim przez CSIRT-y, co regulują w szczególności art. 32–33 oraz rozdział 11 u.k.s.c. Według art. 32 ust. 1 u.k.s.c. CSIRT MON, CSIRT NASK i CSIRT GOV mogą wykonywać niezbędne działania techniczne związane z analizą zagrożeń oraz koordynacją obsługi incydentu poważnego, incydentu istotnego i incydentu krytycznego, co ustawodawca wiąże z możliwością występowania przez CSIRT-y o udzielenie odpowiednich informacji do badanych podmiotów. Art. 33 u.k.s.c. przewiduje możliwość przeprowadzania przez właściwy CSIRT badania urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, co może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Są to działania o tyle istotne, że ustawodawca wiąże z nimi wydawanie aktów pokontrolnych, przyjmujących często postać aktów nadzoru. Według art. 33 ust. 3 u.k.s.c. w przypadku identyfikacji podatności, o której mowa w ust. 1, CSIRT MON, CSIRT NASK

[44] *Ibidem*, s. 349.

[45] *Ibidem*.

[46] D. Wacinkiewicz, *Kontrola i nadzór w prawie komunalnym*, Warszawa 2006, s. 136. Co istotne, autor pisze o tym w kontekście wystąpień pokontrolnych, które również są bardzo istotne w ramach Krajowego Systemu Cyberbezpieczeństwa.

[47] M. Stahl, *op. cit.*, s. 355.

lub CSIRT GOV składa wniosek w sprawie rekomendacji, udzielanej następnie przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa.

Akty kontroli, połączone z aktami nadzoru, mogą być prowadzone również przez organy cyberbezpieczeństwa w zakresie opisanym w art. 53 ust. 1 pkt 2 u.k.s.c.[48] oraz ministra właściwego do spraw informatyzacji w zakresie spełniania przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa wymogów, o których mowa w art. 14 ust. 2 u.k.s.c.[49]. Sprawowanie nadzoru może być realizowane poprzez nakładanie administracyjnych kar pieniężnych oraz – co istotniejsze – poprzez kontrolę zakończoną wystawieniem wiążących zaleceń pokontrolnych[50].

Osoba przeprowadzająca czynności kontrolne wobec podmiotów ma w myśl art. 55 u.k.s.c. m.in. prawo do: swobodnego wstępu i poruszania się po terenie podmiotu kontrolowanego bez obowiązku uzyskiwania przepustki; wglądu do dokumentów dotyczących działalności podmiotu kontrolowanego; pobierania za pokwitowaniem oraz zabezpieczania dokumentów związanych z zakresem kontroli, z zachowaniem przepisów o tajemnicy prawnie chronionej. Osoba ta ma najpierw ustalić stan faktyczny na podstawie dowodów zebranych w toku kontroli, a następnie przedstawić przebieg prowadzonej kontroli w protokole kontroli, który podpisuje osoba prowadząca czynności kontrolne oraz osoba reprezentująca podmiot kontrolowany.

Art. 59 ust. 1 u.k.s.c. daje organowi właściwemu do spraw cyberbezpieczeństwa lub ministrowi właściwemu do spraw informatyzacji kompetencję zdecydowania – w wypadku naruszenia przepisów ustawy przez podmiot kontrolowany – o przekazaniu zaleceń pokontrolnych dotyczących usunięcia nieprawidłowości.

---

[48] Zakres ten ma się sprowadzać do kwestii związanych z wykonywaniem przez operatorów usług kluczowych, wynikających z ustawy obowiązków dotyczących przeciwdziałania zagrożeniom cyberbezpieczeństwa i zgłaszania incydentów poważnych oraz spełniania przez dostawców usług cyfrowych wymogów bezpieczeństwa świadczonych przez nich usług cyfrowych, określonych w rozporządzeniu wykonawczym 2018/151, oraz wykonywania wynikających z ustawy obowiązków dotyczących zgłaszania incydentów istotnych. Ponadto w myśl art. 54 ust. 1–2 u.k.s.c. stosuje się wobec kontrolowanych podmiotów będących przedsiębiorcami przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców, a wobec podmiotów niebędących przedsiębiorcami stosuje się przepisy ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej, określające zasady i tryb przeprowadzania kontroli.

[49] Należy zaznaczyć, że w myśl art. 54 ust. 1 u.k.s.c. do tego rodzaju kontroli stosuje się przepisy rozdziału 5 ustawy z dnia 6 marca 2018 r. – Prawo przedsiębiorców.

[50] Warto zwrócić uwagę, że istnieją również inne regulacje i formy ochrony podmiotów kontrolowanych, wynikające m.in. z dyrektywy NIS. Jak piszą autorzy jednego z komentarzy, „podjęcie czynności kontrolnych bądź służących nałożeniu kary pieniężnej może nastąpić dopiero po uzyskaniu dowodu, iż dany podmiot nie spełnia wymogów określonych w rozporządzeniu wykonawczym 2018/151 lub nie wykonuje wynikających z ustawy obowiązków dotyczących zgłaszania incydentów istotnych" (K. Czaplicki, A. Gryszczyńska, G. Szpor (red.), *op. cit.*, s. 428–429).

Co wydaje się kontrowersyjne, w myśl art. 59 ust. 2–3 od zaleceń tych nie przysługują środki odwoławcze, a podmiot kontrolowany jedynie zobligowany jest do poinformowania o sposobie wykonywania zaleceń.

Jak zauważają komentatorzy tego przepisu, „wydaje się (…), iż ustawodawcy chodziło przede wszystkim o wyłączenie możliwości weryfikacji zaleceń pokontrolnych w następstwie skargi do sądu administracyjnego”[51], zwłaszcza w myśl art. 3 ust. 2 pkt 4 ustawy Prawo o postępowaniu przed sądami administracyjnymi. Ci sami autorzy wskazują na możliwość ograniczenia prawa do sądu przez tę regulację[52]. Zwrócenie uwagi na potrzebę zachowania bezstronności, którą proponują autorzy innego komentarza, wydaje się jednak kontrfaktyczne, wszak chodzi o władcze działania administracji[53]. Kontrowersyjne może wydawać się również pozostawianie bez kognicji sądów administracyjnych licznych aktów kontroli i czynności materialno-technicznych, które podejmowane są podczas przeprowadzania kontroli. Co istotne, w żadnym z wymienionych przypadków nie są to decyzje administracyjne, a jedynie akty w rozumieniu art. 3 ust. 2 pkt 4 ustawy Prawo o postępowaniu przed sądami administracyjnymi. Funkcjonariusze publiczni bądź organy nie są więc w tym przypadku związani zasadą legalizmu, tylko zasadą praworządności – to znaczy, że mają działać nie na podstawie prawa, lecz w granicach określonych przez porządek prawny. Stanowi to kolejny problem dla doktryny prawa administracyjnego, jako że podobne stosunki pozaprawne, lecz w pewien sposób determinowane prawem, łączono raczej z problematyką władztwa fachowego w zakładzie administracyjnym[54]. Jak w takim razie prawo administracyjne powinno rozumieć tak nowy twór, jakim jest KSC, w ramach którego mają współdziałać zarówno podmioty administracji publicznej, jak i podmioty prywatne? W tym sensie problematyka nie tylko aktów kontroli, lecz także towarzyszących im czynności materialno-technicznych funkcjonariuszy czy organów administracji wychodzi poza samą problematykę ochrony praw jednostki.

Akty współdziałania (koordynacji)

Akty współdziałania (koordynacji) to ostatnia z kategorii nietypowych prawnych form działania administracji, które M. Stahl wytypowała według kryterium funkcji. Głównym celem tej formy działania jest harmonizowanie wykonywania zadań publicznych przez różne podmioty. Za przykład może posłużyć chociażby koordynacja niektórych aspektów działalności samorządu terytorialnego przez

[51] *Ibidem*, s. 448–451.
[52] *Ibidem*.
[53] Por. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz (red.), *op. cit.*, s. 315.
[54] *Ibidem*, s. 357.

podmioty administracji państwowej w celu „zapewnienia współdziałania”[55]. Co istotne, może to być również koordynacja w ramach współdziałania na poziomie międzynarodowym.

Formy te są bardzo istotne także w ramach KSC, który opiera się na harmonijnym współdziałaniu różnych podmiotów, zarówno na szczeblu krajowym, jak i międzynarodowym; dotyczy to też podmiotów z sektora prywatnego oraz publicznego. Na szczeblu krajowym chodzi zwłaszcza o koordynację prowadzoną przez podmioty administracji rządowej, jak chociażby Pełnomocnik (któremu art. 60 u.k.s.c. przyznaje kompetencję do koordynowania działań i realizowania polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w Rzeczypospolitej Polskiej) oraz Kolegium, które ma wydawać opinie, będące również formą harmonizacji funkcjonowania KSC. Są to kwestie o tyle istotne, że umożliwiają koordynację działań na poziomie krajowym (jak chociażby wynikająca z art. 36 u.k.s.c. współpraca CSIRT-ów z odpowiednimi organami ścigania, nie mówiąc już o porozumieniach tych podmiotów administrujących między sobą) oraz międzynarodowym. Oprócz współpracy z Unią Europejską, dotyczy to także NATO, a na podstawie umów o partnerstwie strategicznym z krajami spoza Unii, np. z Japonią[56]. W żadnym wypadku akty te nie powinny wywoływać kontrowersji, wiążą bowiem przede wszystkim podmioty administracji publicznej i w bezpośredni sposób nie dotyczą praw jednostki.

Pozostałe formy

Oczywiście to krótkie omówienie nie wyczerpuje wszystkich form działania administracji, które funkcjonują w ramach KSC. Jeśli chodzi o nietypowe, szczególne formy działania administracji, to istotne miejsce zajmują akty planowania (polityki), akty organizacji, akty wiedzy, akty informacji, akty etyki oraz akty certyfikacji. Aktem planowania jest zwłaszcza Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej, wydawana przez ministra właściwego do spraw informatyzacji na podstawie art. 45 u.k.s.c. Aktami organizacji (przy czym to pojęcie w doktrynie jest kontrowersyjne[57]) są chociażby regulaminy czy statuty poszczególnych podmiotów administrujących, a także akty wydawane przez właściwe organy, jak np. rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów

[55] *Ibidem*, s. 360.

[56] Zob. umowa o partnerstwie strategicznym między Unią Europejską i jej państwami członkowskimi, z jednej strony, a Japonią, z drugiej strony (Dz.Urz. L 216/1, 24.08.2018).

[57] Zob. M. Stahl, *op. cit.*, s. 372–374.

usług kluczowych odpowiedzialnych za cyberbezpieczeństwo[58]. Akty wiedzy czy akty informacji są istotne zwłaszcza przy okazji postępowań czy też czynności kontrolnych – są to nieomawiane w ramach ustawy o krajowym systemie cyberbezpieczeństwa ekspertyzy odpowiednich specjalistów.

Ciekawym zjawiskiem wydaje się istotność aktów etyki w ramach KSC. Zdaniem K. Świtały normy etyczne stanowią zbiór dobrych praktyk istotnych, choć niepodlegających żadnemu usankcjonowaniu, w ramach sektora IT[59]. Wreszcie ważne w ramach KSC są akty certyfikacji. Są to certyfikaty wydawane na podstawie obwieszczeń ministra cyfryzacji w sprawie włączenia odpowiednich kwalifikacji rynkowych do Zintegrowanego Systemu Kwalifikacji.

Zakończenie

Słowem podsumowania, warto podkreślić, że KSC stanowi nową, zorganizowaną formę działania administracji publicznej w Polsce. Uprawnienia przyznawane administracji w ramach KSC uzupełniają dotychczasowe ustalenia doktryny dotyczące prawnych form działania administracji. Istotnym aspektem jest wprowadzenie nowych form aktów nadzoru dotyczących podmiotów, które nie należą do administracji państwowej. Dotychczas refleksja doktrynalna koncentrowała się głównie na samorządach, natomiast obecnie problematyka władztwa administracyjnego rozciąga się także na podmioty prywatne.

W efekcie powstają nowe, specyficzne stosunki administracyjnoprawne, przyznające uprawnienia zarówno organom państwowym, jak i podmiotom administrującym, takim jak CSIRT-y czy sektorowe zespoły do spraw cyberbezpieczeństwa. Kontrowersyjną kwestią pozostaje fakt, że na niektóre akty administracyjne nie przysługuje odwołanie, co zostało wyraźnie zastrzeżone przez ustawodawcę. Problematyczne wydaje się również przeprowadzanie kontroli w podmiotach prywatnych. Obecne regulacje mogą nie zapewniać w pełni ochrony praw zarówno przedsiębiorców, jak i jednostek funkcjonujących w ich ramach. Warto jednak zaznaczyć, że na skutek przepisów unijnych, w tym dyrektywy RODO, ochrona danych osobowych obywateli pozostaje w teorii na wysokim poziomie. Jednocześnie poleganie na dotychczasowych przepisach regulujących kontrole w podmiotach prywatnych wydaje się niewystarczające w kontekście dynamicznie rozwijającej się cyberprzestrzeni.

---

[58] Dz.U. 2019, poz. 2479.

[59] K. Świtała, *Bezpieczeństwo sieci i usług w projekcie nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa*, „Monitor Prawniczy" 2020, nr 23, s. 1241. Podobnie stwierdził M. Rojszczak (*Zarządzanie incydentami a ustawa o krajowym systemie cyberbezpieczeństwa*, [w:] *Cyberbezpieczeństwo…*, s. 41), zwracając uwagę na istotność tzw. dobrych praktyk.

Nawet jeżeli zestawimy je z regulacjami dotyczącymi zarządzania kryzysowego czy ustawodawstwa antyterrorystycznego, warto mieć na uwadze, że obsługa incydentów dotyczy zupełnie nowego obszaru regulacji – cyberprzestrzeni. Pomimo definicji legalnych, nie istnieje jednak w doktrynie praktycznie jakakolwiek dyskusja na temat ich zasadności, a nieliczne propozycje, jak ta przytoczona przez W.Z. Dziomdziorę, są bardzo ogólnikowe i nie pozwalają lepiej obejmować interesującego nas obszaru badania. Nawiązując do typologii definicji zaproponowanej przez L. Petrażyckiego (omówionej przez J. Winczorka[60]), można stwierdzić, że są to definicje „kulawe"[61] – jest to przypadek, kiedy definiendum nie obejmuje wszystkich przypadków, które powinny znaleźć się w definiensie, co czyni definicję nieadekwatną. Modyfikacje w tym obszarze, a przynajmniej dyskusja doktryny, są konieczne również w obecnej sytuacji społeczno-politycznej, gdyż coraz częściej mówi się o „wojnach informacyjnych". Podstawą do przeprowadzenia kontroli jest wszakże nie tylko podstawa prawna, lecz także akty wiedzy odpowiednich ekspertów w kwestiach problemów systemów teleinformatycznych. Co również problematyczne, w ich wypadku nie ma mowy o możliwościach ich odpowiedniej kontroli przez sądownictwo. Definicje operacyjne, które zostały zaproponowane w tekście, mogą stanowić punkt wyjścia do dalszej dyskusji.

Nie można polegać jedynie – i to przez cały czas obowiązywania ustawy o krajowym systemie cyberbezpieczeństwa – na gwarancjach płynących z odpowiednich regulacji unijnych. Wydaje się, że obecnie konieczne jest przede wszystkim przeprowadzenie dyskusji na temat nowych form działania administracji w ramach tego systemu, a następnie wydanie szczegółowych aktów prawnych (bądź odpowiednich nowelizacji obecnych aktów prawnych), które będą gwarantować przejrzyste, ustalone wytyczne tych procedur.

Jednocześnie warto już w tym miejscu zaznaczyć konieczność dalszych studiów nad prawnymi formami działania administracji w ramach KSC. Mianowicie dobór form działania administracji nie jest przypadkowy, lecz warunkowany jest strukturą systemu i charakterem jego zadań. Poziom prawny wymusza stosowanie form władczych, poziom organizacyjny – współdziałanie i koordynację, poziom techniczny – czynności faktyczne i akty eksperckie, poziom informacyjny – formy oparte na wymianie danych i komunikacji. Wszystkie te poziomy tworzą złożony, wielowarstwowy model działania administracji publicznej w cyberprzestrzeni,

[60] Zob. J. Winczorek, *Czy istnieje etyka prawnicza? Kilka uwag ze stanowiska socjologicznej teorii norm*, [w:] *Etyka prawnicza. Stanowiska i perspektywy 2*, red. H. Izdebski, P. Skuczyński, Warszawa 2011, s. 33.

[61] Analogicznie propozycja W.Z. Dziomdziory (*op. cit.*) jest „skacząca", czyli definicja jest nieadekwatna przez zbyt obszerny definiens. Ponadto propozycja ta pokrywa się w wielu aspektach z definicją legalną, dlatego nie przynosi zbyt wielu walorów natury poznawczej. Warto ją jednak odnotować jako próbę doprecyzowania tej definicji legalnej.

w którym granice między formami klasycznymi i szczególnymi ulegają zatarciu. Z perspektywy doktryny prawa administracyjnego oznacza to konieczność przyjęcia otwartego katalogu prawnych form działania administracji, elastycznego i zdolnego do adaptacji w świecie zmieniających się technologii. Dynamika rozwoju technologicznego sprawia bowiem, że utrzymanie sztywnej typologii form działania staje się niemożliwe. Elastyczna interpretacja pojęcia formy działania administracji – otwarta na procesy cyfryzacji, automatyzacji i współdzielenia kompetencji – staje się warunkiem efektywnego funkcjonowania państwa w cyberprzestrzeni oraz ochrony praw jednostki w warunkach społeczeństwa informacyjnego.

Bibliografia

Adamski A., *Prawo karne komputerowe*, Warszawa 2000.

Banasiński C., Rojszczak M., *Cyberbezpieczeństwo smart implantów w kontekście unijnego prawa ochrony konsumentów*, „Państwo i Prawo" 2024, z. 9.

Banasiński C., Rojszczak M. (red.), *Cyberbezpieczeństwo*, Warszawa 2020.

Berdel-Dudzińska M., *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*, „Przegląd Prawa Publicznego" 2012, nr 2.

Bukowski S., *Przestępstwo hackingu*, „Przegląd Sądowy" 2005, nr 4.

Chałubińska-Jentkiewicz K., *Bezpieczeństwo cyberprzestrzeni jako zadanie publiczne w systemie bezpieczeństwa narodowego RP*, „Zeszyty Naukowe AON" 2014, nr 3.

Chałubińska-Jentkiewicz K., *Cybersecurity as a Public Task in Administration*, [w:] *Cybersecurity in Poland*, eds. K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński, Cham 2022.

Chałubińska-Jentkiewicz K., *Cyberspace as an Area of Legal Regulation*, [w:] *Cybersecurity in Poland*, eds. K. Chałubińska-Jentkiewicz, F. Radoniewicz, T. Zieliński, Cham 2022.

Czaplicki K., Gryszczyńska A., Szpor G. (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019.

Dziomdziora W., *Czym jest cyberbezpieczeństwo?*, [w:] *Cyberbezpieczeństwo w samorządzie terytorialnym. Praktyczny przewodnik*, Warszawa 2021.

Filipkowski W., *Przestępczość z użyciem komputerów i ich sieci*, [w:] E.W. Pływaczewski, S. Redo, E.M. Guzik-Makaruk, K. Laskowska, W. Filipkowski, E. Glińska, E. Jurgielewicz-Delegacz, M. Perkowska, *Kryminologia. Stan i perspektywy rozwoju*, Warszawa 2019.

Galán C.M., Galán Cordero C., *La ciberseguridad pública como garantía del ejercicio de derechos*, "Derecho & Sociedad" 2016, núm. 47.

Gryszczyńska A., *Cyberbezpieczeństwo w jednostkach samorządu terytorialnego*, [w:] *System Prawa Samorządu Terytorialnego*, t. 3: *Samodzielność samorządu terytorialnego – granice i perspektywy*, red. I. Lipowicz, Warszawa 2023.

Hańderek A., *Naruszenie praw autorskich i praw pokrewnych w związku z funkcjonowaniem wyszukiwarek internetowych*, Warszawa 2024.

Jagielski J., *Z problematyki organów administracyjnych*, [w:] *Problemy współczesnego ustrojoznawstwa. Księga jubileuszowa Profesora Bronisława Jastrzębskiego*, red. J. Dobkowski, Olsztyn 2007.

Jagielski J., Wierzbowski M. (red.), *Prawo administracyjne*, Warszawa 2020.
Janowski J., *Technologia informacyjna dla prawników i administratywistów. Szanse i zagrożenia elektronicznego przetwarzania danych w obrocie prawnym i działaniu administracji*, Warszawa 2009.
Kitler W., Taczkowska-Olszewska J., Radoniewicz F. (red.), *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019.
Lukings M., Lashkari A.H., *Understanding Cybersecurity Law and Digital Privacy: A Common Law Perspective*, Cham 2022.
Miłkowski T.M., *Czynności operacyjno-rozpoznawcze a prawa i wolności jednostki*, Warszawa 2020.
Rojszczak M., *Cyberprzestrzeń jako nowa płaszczyzna budowania relacji społecznych*, [w:] *Ochrona prywatności w cyberprzestrzeni z uwzględnieniem zagrożeń wynikających z nowych technik przetwarzania informacji*, Warszawa 2019.
Rojszczak M., *Zarządzanie incydentami a ustawa o krajowym systemie cyberbezpieczeństwa*, [w:] *Cyberbezpieczeństwo*, red. C. Banasiński, M. Rojszczak, Warszawa 2020.
Siwicki M., *Cyberprzestępczość*, Warszawa 2013.
Siwicki M., *Kilka uwag na temat ochrony infrastruktury krytycznej w internecie na tle dyrektywy NIS i jej transpozycji do polskiego porządku prawnego*, „Europejski Przegląd Sądowy" 2019, nr 9.
Skoczylas D., *Wzmocnienie zdolności Unii Europejskiej w zakresie cyberbezpieczeństwa – cybersolidarność w kontekście cyberzagrożeń*, „Europejski Przegląd Sądowy" 2024, nr 12.
Skoczylas D., *Znaczenie cyberbezpieczeństwa w administracji publicznej*, [w:] *Wzorce i zasady działania współczesnej administracji publicznej*, red. B. Jaworska-Dębska, P. Kledzik, J. Sługocki, Warszawa 2020.
Stahl M., *Szczególne prawne formy działania administracji*, [w:] *System Prawa Administracyjnego*, t. 5: *Prawne formy działania administracji*, red. A. Błaś, J. Boć, M. Stahl, K.M. Ziemski, Warszawa 2013.
Starościak J., *Prawne formy działania administracji*, Warszawa 1957.
Strzępek K., *Cyberbezpieczeństwo Rzeczypospolitej Polskiej – podstawy prawne (międzynarodowe i krajowe)*, „Prokuratura i Prawo" 2023, nr 12.
Szmyt A., *Opinia prawna do przedstawionego przez Prezydenta RP projektu ustawy o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw z dnia 11 lipca 2011 r.*, „Zeszyty Prawnicze Biura Analiz Sejmowych" 2012, nr 33.
Świtała K., *Bezpieczeństwo sieci i usług w projekcie nowelizacji ustawy o Krajowym Systemie Cyberbezpieczeństwa*, „Monitor Prawniczy" 2020, nr 23.
Taczkowska-Olszewska J., Chałubińska-Jentkiewicz K., Nowikowska M., *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Warszawa 2019.
Wacinkiewicz D., *Kontrola i nadzór w prawie komunalnym*, Warszawa 2006.
Winczorek J., *Czy istnieje etyka prawnicza? Kilka uwag ze stanowiska socjologicznej teorii norm*, [w:] *Etyka prawnicza. Stanowiska i perspektywy 2*, red. H. Izdebski, P. Skuczyński, Warszawa 2011.
Ziemski K.M., *Indywidualny akt administracyjny jako forma prawna działania administracji*, Poznań 2001.

Abstract: This article discusses the proposed typology of legal forms of public administration activity within the framework of the Polish National Cybersecurity System. By juxtaposing research findings with definitional challenges related to the concept, attention is drawn to potential risks and controversies arising from the current legal regulations. Particularly controversial may be atypical, special forms of administrative action within this system, which remain unrecognized by legal doctrine or are even explicitly excluded by the legislator from judicial review in administrative courts.

Keywords: legal forms of administrative action; public administration; cybersecurity

Abstrakt: W artykule omówiono zaproponowaną typologię prawnych form działania administracji publicznej w ramach Krajowego Systemu Cyberbezpieczeństwa. Poprzez zestawienie wyników badań z problemami definicyjnymi tego pojęcia zwrócono uwagę na potencjalne niebezpieczeństwa i kontrowersje, które mogą być spowodowane przez obecne regulacje ustawowe. Kontrowersyjne mogą być zwłaszcza nietypowe, szczególne formy działania administracji w ramach tego systemu, które pozostają nierozpoznane przez doktrynę lub są wręcz wyłączone przez ustawodawcę z możliwości zaskarżania ich do sądów administracyjnych.

Słowa kluczowe: prawne formy działania administracji; administracja publiczna; cyberbezpieczeństwo