



CYFRYZACJA INFORMATYZACJA CYBERBEZPIECZEŃSTWO

PERSPEKTYWY, SZANSE I ZAGROŻENIA DLA ADMINISTRACJI PUBLICZNEJ

red. naukowa
Dominika Skoczylas, Paweł Śwital

Recenzje naukowe

dr hab. prof. US Aleksandra Monarcha-Matlak (Uniwersytet Szczeciński)

dr hab. prof. URad. Joanna Smarż (Uniwersytet Radomski im. K. Pułaskiego)

Redakcja techniczna: dr Emilia Gulińska

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

eISBN: 978-83-7789-774-4

Radom-Szczecin 2024

Monografia naukowa została wydana jedynie w wersji elektronicznej.

© Autorzy rozdziałów

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	4
dr hab. Maciej Błażewski, dr hab. Monika Tenenbaum-Kulig	
Bezpieczeństwo głosowania w kolegialnych organach administracyjnych w procesie rozstrzygania w drodze decyzji administracyjnej z zastosowaniem prywatnych systemów teleinformatycznych.....	6
mgr Mariusz Dubowski	
Zwiększenie dostępności cyfrowej nakierowanej na klienta – kazus Kuratorium Oświaty w Szczecinie.....	21
dr Marta Grabowska	
Status polskiego społeczeństwa na przykładzie dostępu do usług użyteczności publicznej	29
dr Emilia Gulińska	
Elektroniczne zarządzanie dokumentacją w kontekście informatyzacji administracji publicznej	36
Dr Aleksandra Puczek	
Wpływ cyfryzacji administracji publicznej na obowiązek ochrony tajemnicy skarbowej przez Krajową Administrację Skarbową.....	47
dr Dominika Skoczylas	
Kompetencje cyfrowe i polityka cyberbezpieczeństwa jako warunki <i>sine qua non</i> funkcjonowania elektronicznej administracji.....	59
prof. UAM dr hab. Lucyna Staniszevska	
Wykorzystanie chatbotów w polskiej administracji publicznej – wizja czy rzeczywistość	71
dr Jarosław Stasiak LL.M. Münster	
Zbywanie i oddawanie w użytkowanie wieczyste nieruchomości należących do podmiotów publiczno-prawnych – doświadczenia z czasów pandemii i ich aktualność po jej zakończeniu	83
dr Marcin Jan Stępień	
Sztuczna inteligencja a cyberbezpieczeństwo – wybrane aspekty regulacji cyberbezpieczeństwa w projekcie Aktu ws. Sztucznej Inteligencji w wersji zaproponowanej przez Parlament Europejski	95
dr Paweł Śwital	
Elektroniczne konsultacje społeczne.....	108

Wprowadzenie

Transformacja cyfrowa przyczyniła się do zmian w zakresie funkcjonowania administracji publicznej. Innymi słowy, nowoczesne technologie informacyjno-komunikacyjne zmodernizowały dotychczasowy sposób świadczenia usług publicznych, wprowadzono bowiem nowy sposób zarządzania sprawami publicznymi pod postacią e-administracji. E-usługi, e-zarządzanie i dostępność cyfrowa stanowią obecnie niezwykle istotne zagadnienia, szczególnie w kontekście informatyzacji, cyfryzacji a także cyberbezpieczeństwa administracji publicznej. Przedmiotowa problematyka stała się języczkiem u wagi prawników, administratywistów i przedstawicieli doktryny przede wszystkim podczas pandemii COVID-19, aktualnie zaś stanowi pole do dyskusji w aspekcie zastosowania systemów sztucznej inteligencji w działaniach podejmowanych przez administrację publiczną.

W dniu 4 lipca 2023 r. w wersji hybrydowej odbyła się I Ogólnopolska Konferencja Naukowa pt. „Cyfryzacja - informatyzacja - cyberbezpieczeństwo. Perspektywy, szanse i zagrożenia dla administracji publicznej”. Konferencja została zorganizowana przez Wydział Prawa i Administracji Uniwersytetu Szczecińskiego oraz Wydział Prawa i Administracji Uniwersytetu Technologiczno-Humanistycznego im. Kazimierza Pułaskiego w Radomiu (aktualnie: Uniwersytet Radomski im. Kazimierza Pułaskiego). Celem konferencji była wymiana poglądów środowiska naukowego na temat aktualnych wyzwań i problemów w zakresie zastosowania nowych technologii informacyjno-komunikacyjnych w sektorze publicznym. Podczas konferencji dokonano pogłębionej analizy legislacyjnych, społecznych i technologicznych uwarunkowań cyfryzacji, informatyzacji i cyberbezpieczeństwa w administracji publicznej. Poruszono wiele interesujących zagadnień m.in. w obszarze dostępności cyfrowej, elektronicznego zarządzania dokumentacją czy kompetencji cyfrowych użytkowników e-administracji. Niezwykle ważną tematykę stanowiły kwestie dotyczące polityki cyberbezpieczeństwa oraz wykorzystania chatbotów w administracji publicznej. Zważywszy na wzrost zainteresowania systemami sztucznej inteligencji, omówione zostały także wybrane aspekty regulacji cyberbezpieczeństwa w projekcie Aktu ws. Sztucznej Inteligencji. Adresatami konferencji byli prawnicy, administratywiści, ale również wszyscy zainteresowani tematyką cyfryzacji, informatyzacji i cyberbezpieczeństwa administracji publicznej.

Niniejsza książka stanowi pokłosie Konferencji Naukowej pt. „Cyfryzacja - informatyzacja - cyberbezpieczeństwo. Perspektywy, szanse i zagrożenia dla administracji

publicznej”. Umieszczone w monografii opracowania obejmują bardzo różnorodne aspekty cyfryzacji, informatyzacji i cyberbezpieczeństwa w administracji publicznej. Autorzy rozdziałów w interdyscyplinarny sposób odnieśli się do aktualnych perspektyw, szans i wyzwań w obszarze e-modernizacji sektora usług publicznych. Szczególne miejsce zajmują m.in. aspekty związane z polityką cyberbezpieczeństwa, dostępnością cyfrową czy sztuczną inteligencją. Monografia zawiera 10 rozdziałów, w których poruszone zostały następujące zagadnienia: „Bezpieczeństwo głosowania w kolegialnych organach administracyjnych w procesie rozstrzygania w drodze decyzji administracyjnej z zastosowaniem prywatnych systemów teleinformatycznych” (Maciej Błażewski, Monika Tenenbaum-Kulig); Zwiększenie dostępności cyfrowej nakierowanej na klienta – kazus Kuratorium Oświaty w Szczecinie (Mariusz Dubojski); Status polskiego społeczeństwa na przykładzie dostępu do usług użyteczności publicznej (Marta Grabowska); Elektroniczne zarządzanie dokumentacją w kontekście informatyzacji administracji publicznej (Emilia Gulińska); Wpływ cyfryzacji administracji publicznej na obowiązek ochrony tajemnicy skarbowej przez Krajową Administrację Skarbową (Aleksandra Puczeko); Kompetencje cyfrowe i polityka cyberbezpieczeństwa jako warunki *sine qua non* funkcjonowania elektronicznej administracji (Dominika Skoczylas); Wykorzystanie chatbotów w polskiej administracji publicznej – wizja czy rzeczywistość (Lucyna Staniszevska); Zbywanie i oddawanie w użytkowanie wieczyste nieruchomości należących do podmiotów publiczno – prawnych – doświadczenia z czasów pandemii i ich aktualność po jej zakończeniu (Jarosław Stasiak); Sztuczna inteligencja a cyberbezpieczeństwo – wybrane aspekty regulacji cyberbezpieczeństwa w projekcie Aktu ws. Sztucznej Inteligencji w wersji zaproponowanej przez Parlament Europejski (Marcin Jan Stępień); Elektroniczne konsultacje społeczne (Paweł Śwital).

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

Głównym założeniem monografii jest podjęcie debaty na temat pełnej cyfryzacji sektora publicznego oraz dyskusji w zakresie wprowadzenia zmian natury organizacyjno-prawnej, społecznej i technologicznej w celu rozwoju administracji publicznej. Książka skierowana jest do osób zajmujących się informatyzacją, cyfryzacją i cyberbezpieczeństwem oraz wszystkich zainteresowanych przedmiotową tematyką. Zapraszamy do lektury monografii „Cyfryzacja – informatyzacja – cyberbezpieczeństwo. Perspektywy, szanse i zagrożenia dla administracji publicznej”.

*dr Dominika Skoczylas
dr Paweł Śwital*

Szczecin-Radom 2024

dr hab. Maciej Błazewski

Uniwersytet Wrocławski

ORCID: 0000-0003-2812-8199

Adres email: maciej.blazewski@uwr.edu.pl

radca prawny

dr hab. Monika Tenenbaum-Kulig

Uniwersytet Wrocławski

ORCID: 0000-0001-7539-6351

Adres email: monika.tenenbaum-kulig@uwr.edu.pl

radca prawny

Bezpieczeństwo głosowania w kolegialnych organach administracyjnych w procesie rozstrzygania w drodze decyzji administracyjnej z zastosowaniem prywatnych systemów teleinformatycznych

Security of voting in collegial administrative authorities in the process of decision in the administrative procedure with technical means of communication.

Streszczenie

Stosowanie środków komunikacji elektronicznej w procesie rozstrzygania przez kolegialne organy administracji publicznej wymaga zachowania standardów bezpieczeństwa. Standardy te powinny być uwzględnione w umowie licencyjnej, której przedmiotem jest prawo organu administracji publicznej do stosowania programów komputerowych. Wymogi prawne dotyczą także sanacji naruszeń tych standardów, której skutkiem może być eliminacja z obrotu prawnego decyzji administracyjnej zawierającej rozstrzygnięcie o zniekształconej treści.

Wprowadzenie

Sposób działania administracji publicznej, w zakresie regulowanym przepisami prawa, uwzględnia osiągnięcia postępu technicznego, co odnosi się także do stosowania środków komunikacji elektronicznej. Organy administracji publicznej stosując te środki powinny uwzględniać standardy techniczne, w tym odnoszące się do wymogów bezpieczeństwa. Częścią złożonej problematyki zapewniania bezpieczeństwa stosowania środków komunikacji elektronicznej jest stosowanie środków komunikacji elektronicznej w kolegialnych organach administracji publicznej w procesie rozstrzygania w drodze decyzji administracyjnej.

Celem opracowania jest określenie stopnia adekwatności obowiązujących przepisów prawa, regulujących proces rozstrzygania drogą elektroniczną w kolegiальnym organie administracji publicznej, względem potencjalnych zagrożeń dla tego procesu, które mogą skutkować zniekształceniem treści rozstrzygnięcia tego organu. W opracowaniu zastosowano metodę analityczno-dogmatyczną, która opiera się na analizie obowiązujących przepisów prawa, z uwzględnieniem dorobku nauki prawa.

Proces rozstrzygania w drodze decyzji administracyjnej w kolegiальных organach administracji publicznej

Stosowanie środków komunikacji elektronicznej przez organy administracji publicznej w toku postępowania administracyjnego wymaga wyrażnej podstawy prawnej, co oznacza, że prawodawca dopuszcza drogę elektroniczną jedynie w oznaczonych przypadkach. Wymóg ten obejmuje także proces rozstrzygania w kolegiальных organach administracji publicznej, który odnosi się do głosowania, a także ustalenia liczby i treści głosów. Przyczyną ustanowienia takiej możliwości są względy organizacyjne. Podjęcie rozstrzygnięcia drogą elektroniczną ułatwia wykonanie tej czynności przez kolegialne organy administracji publicznej, szczególnie w przypadku znaczącego składu ich członków. Prawodawca dopuszcza możliwość podjęcia w drodze elektronicznej uchwał zawierających rozstrzygnięcia administracyjne m.in. przez organy szkół wyższych¹, a w okresie obowiązywania stanu zagrożenia epidemicznego albo stanu epidemii także przez zarząd powiatu, zarząd województwa oraz regionalne izby obrachunkowe i samorządowe kolegia odwoławcze².

¹ Zgodnie z art. 178 ust. 1a w zw. z art. 178 ust. 1 ustawy z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce, t.j. Dz. U. z 2024 r., poz. 124 ze zm., posiedzenia organów uczelni wyższej, a także rady naukowej instytutu PAN, instytutu badawczego oraz instytutu międzynarodowego, w których toku nadaje się w drodze decyzji administracyjnej stopień naukowy albo stopień w zakresie sztuki, mogą być przeprowadzane przy użyciu środków komunikacji elektronicznej.

² W świetle art. 15zxx ust. 1 ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, t.j. Dz. U. z 2024 r., poz. 340 ze zm., w okresie obowiązywania stanu zagrożenia epidemicznego albo stanu epidemii organy stanowiące jednostek samorządu terytorialnego oraz działające kolegialnie organy: wykonawcze w jednostkach samorządu terytorialnego, w związkach jednostek samorządu terytorialnego, w związku metropolitalnym, w regionalnych izbach obrachunkowych, samorządowych kolegiach odwoławczych oraz w organach pomocniczych jednostek samorządu terytorialnego mogą zwoływać i odbywać obrady, sesje, posiedzenia, zgromadzenia lub inne formy działania właściwe dla tych organów, a także podejmować rozstrzygnięcia, w tym uchwały, z wykorzystaniem środków porozumiewania się na odległość lub korespondencyjnie. Zaznaczenia wymaga, że zarząd województwa oraz zarząd powiatu są organami właściwymi do wydawania decyzji administracyjnej na podstawie przepisów szczególnych (*a contrario* art. 46 ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa, z 2024 r., poz. 566, dalej u.s.w., oraz *a contrario* art. 38 ust. 1 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym, t.j. Dz. U. z 2024 r., poz. 107 ze zm., dalej u.s.p.). Zgodnie z art. 25 pkt. 1 w zw. z art. 26 ust. 1 pkt. 15 w zw. z art. 14lp ust. 6 pkt. 1 ustawy z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju, t.j. Dz. U. z 2024 r., poz. 324 ze zm., dalej u.z.p.p.r. zarząd województwa jest organem właściwym do wydania decyzji administracyjnej w rozumieniu k.p.a., której przedmiotem jest zwrot środków przekazanych na realizację programów, projektów lub zadań przepisów u.z.p.p.r. W świetle art. 45 ust.

Kolegialny organ administracji publicznej stanowi grupę jego członków, jako całość posiadającą podmiotowość publicznoprawną³. Członkami tego organu są osoby fizyczne. Ze względu na wielość członków kolegialnego organu administracji publicznej, ma miejsce swoisty związek pomiędzy czynnościami członków tego organu, a czynnościami organu. Związek ten dotyczy rozstrzygnięcia tego organu, które zapada w formie uchwały⁴. Rozstrzygnięcie administracyjne, w przypadku gdy jest podejmowane w drodze decyzji administracyjnej, jest orzeczeniem organu administracji publicznej obejmującym normy prawne o charakterze indywidualnym i konkretnym⁵. Uchwała organu kolegialnego, która zawiera to rozstrzygnięcie, stanowi prawnie istotną, jednostronną czynność konwencjonalną tego organu obejmującą złożenie jego oświadczenia woli⁶. Zaznaczenia wymaga, że wydanie rozstrzygnięcia przez kolegialny organ administracji publicznej jest konsekwencją

1 w zw. z art. 4 pkt. 9 ustawy z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami, z 2024 r., poz. 1145 ze zm., zarząd województwa oraz zarząd powiatu są organami właściwymi do wydania decyzji administracyjnej w sprawie ustanowienia trwałego zarządu na rzecz jednostki organizacyjnej w odniesieniu do nieruchomości stanowiącej własność odpowiednio województwa oraz powiatu.

³ W literaturze prawa administracyjnego przyjmuje się podział według kryterium składu osobowego organów, na organy jednoosobowe oraz organy kolegialne. Zob. E. Ura, *Prawo administracyjne*, Warszawa 2021, s. 79; J. Boć, *Podmioty administrujące*, [w:] *Prawo administracyjne*, (red.) J. Boć, Wrocław 2007, s. 131. W nauce prawa administracyjnego podkreśla się, że organy administracji publicznej stanowią podmioty publicznoprawne. Jak zauważają M. Wierzbowski oraz A. Wiktorowska organem administracji publicznej jest podmiot posiadające kompetencje z zakresu prawa administracyjnego. M. Wierzbowski, A. Wiktorowska, *Rodzaje jednostek organizacyjnych w systemie administracji publicznej*, [w:] *Prawo administracyjne*, (red.) M. Wierzbowski, Warszawa 2017, s. 94. Zdaniem J. Zimmermanna, organem administracji publicznej jest podmiot działający za państwo. J. Zimmermann, *Prawo administracyjne*, Warszawa 2014, s. 140.

⁴ J. Wróblewski zaproponował model stosowania prawa obejmujący 6 etapów, którymi są: 1. ustalenie obowiązku przepisu prawa; 2. ustalenie znaczenia przepisu prawa; 3. uznanie za udowodnione fakty sprawy; 4. subsumpcja; 5. ustalenie konsekwencji prawnych udowodnionych faktów; 6. wydanie finalnej decyzji. J. Wróblewski, *Sądowe stosowanie prawa*, Warszawa 1988, s. 43. Orzecznictwo sądowo-administracyjne stosuje uproszczoną wersję tego modelu obejmującą 4 etapy, którymi są 1) ustalenie treści normy prawnej, 2) ustalenie stanu faktycznego, 3) subsumpcję, 4) ustalenie konsekwencji prawnych stanu faktycznego na podstawie stosowanej normy prawnej. Zob. uchwała NSA z dnia 26 października 2009 r., I OPS 10/09, CBOSA; wyrok NSA z dnia 10 stycznia 2012 r., II FSK 1304/10, CBOSA. Wydanie rozstrzygnięcia jest właściwe ostatniemu etapowi uproszczonego modelu, czyli ustalenie konsekwencji prawnych stanu faktycznego na podstawie stosowanej normy prawnej.

⁵ Badane rozstrzygnięcie administracyjne przybiera formę aktu administracyjnego. Jak wskazuje W. Dawidowicz, akt administracyjny stanowi orzeczenie organu administracji publicznej, które wywiera wiążące skutki prawne względem indywidualnego podmiotu, w konkretnej sprawie. W. Dawidowicz, *Polskie prawo administracyjne*, Warszawa 1978, s. 47.

⁶ Jak podkreśla A. Wróbel, decyzja administracyjna jest jednostronną czynnością z zakresu prawa administracyjnego, która dochodzi do skutku poprzez złożenie oświadczenia woli przez organ administracji publicznej. A. Wróbel, *Komentarz do art. 104*, [w:] *Komentarz aktualizowany do Kodeksu postępowania administracyjnego*, (red.) M. Jaśkowska, M. Wilbrandt-Gotowicz, A. Wróbel, LEX/el. 2023, teza 1. Zdaniem A. Skóry, decyzja administracyjna, w ujęciu materialnym stanowi władcze i jednostronne oświadczenie woli organu administracji publicznej podjęte na podstawie przepisów prawa administracyjnego, którego przedmiotem są normy indywidualne i konkretne. A. Skóra, *Komentarz do art. 104*, [w:] *Kodeks postępowania administracyjnego. Komentarz do art. 61-126. Tom II*, (red.) M. Karpiuk, P. Krzykowski, Olsztyn 2020, LEX/el., teza III.2. Poglądy te można odnieść także do innych rozstrzygnięć administracyjnych.

oddania głosów przez członków tego organu. Czynności te stanowią elementy procesu rozstrzygnięcia.

Proces rozstrzygnięcia w kolegiальnym organie administracji publicznej obejmuje trzy etapy. Są nimi czynności związane ze: złożeniem oświadczenia woli w formie głosu przez członków organu, zbiorczym ustaleniem liczby i treści oddanych głosów oraz złożeniem oświadczenia woli kolegiального organu⁷. Kolejny etap procesu rozstrzygnięcia jest konsekwencją poprzedniego etapu. Złożenie oświadczenia woli w formie głosów przez członków organu determinuje wynik zbiorczego ustalenia liczby i treści oddanych głosów. Wynik ten determinuje treść oświadczenia woli kolegiального organu administracji publicznej. Rozstrzygnięcie kolegiального organu administracji publicznej wymaga spójności tych etapów.

Etap pierwszy obejmuje wyrażenie głosu przez członka kolegiального organu. Członkiem tym jest osoba fizyczna, która wchodzi w skład zespołu osób fizycznych wspólnie tworzących kolegiálny organ administracji publicznej. Członek tego organu wyrażając swój głos składa oświadczenie woli, którego przedmiotem jest treść przyszłego rozstrzygnięcia administracyjnego.

Etap drugi obejmuje zbiorcze ustalenie liczby i treści oddanych głosów. Jest to czynność materialno-techniczna służąca przetworzeniu indywidualnych głosów wyrażonych przez członków kolegiального organu administracji publicznej w jednolitą treść oświadczenia woli tego organu.

Etapem trzecim jest złożenie oświadczenia woli przez kolegiálny organ administracji publicznej. Przedmiotem tego oświadczenia jest rozstrzygnięcie administracyjne. Jednolita treść tego oświadczenia oznacza, że w sposób kategoryczny określa swoje skutki prawne.

Wymogi względem prywatnych systemów teleinformatycznych dotyczące bezpieczeństwa przeprowadzenia głosowania w toku procedur służących podejmowaniu rozstrzygnięć w drodze decyzji administracyjnych

Ustawodawca w obowiązującym porządku prawnym nie przewidział *expressis verbis* wymogów, jakie muszą spełniać prywatne systemy teleinformatyczne, wykorzystywane przez organy administracji publicznej do przeprowadzania głosowań. Pomimo tego określone wnioski dotyczące cech, jakie powinny mieć takie

⁷ Zdaniem Naczelnego Sądu Administracyjnego, rozpatrującego problematykę wydania decyzji administracyjnej przez Samorządowe Kolegium Odwoławcze, wydanie decyzji administracyjnej przez organ kolegiálny nie następuje w chwili sporządzenia i podpisania protokołu z głosowania, lecz w chwili sporządzenia decyzji administracyjnej, co obejmuje podpisanie tej decyzji (wyrok NSA z dnia 11 lipca 2007 r., I OSK 1292/06, CBOSA). Naczelny Sąd Administracyjny w tym wyroku rozróżnił zatem etap głosowania od etapu sporządzania decyzji administracyjnej.

systemy, można wyprowadzić z cech prawidłowo podjętej uchwały. Mianowicie skoro z prawidłowo podjętą uchwałą mamy do czynienia wówczas, gdy jest ona efektem swobodnie przejawionej woli osób wchodzących w skład określonego organu, efektywny system teleinformatyczny służący do przeprowadzania głosowań musi zapewniać, że głosy oddane w toku procedury służącej do podjęcia uchwały zostaną oddane wyłącznie przez uprawnione do tego osoby, będące członkami organu kolegialnego oraz że uwzględnieniu będą podlegały wyłącznie rzeczywiście oddane głosy uprawnionych do udziału w głosowaniu, tj. że w toku podejmowania uchwały nie dojdzie do sfałszowania oddanych głosów wskutek wadliwości systemu, bądź niedozwolonej ingerencji osoby trzeciej. Adekwatny system teleinformatyczny powinien także zapewniać tajność głosowania, ponieważ w określonych przez ustawodawcę przypadkach uchwały są podejmowane w głosowaniu tajnym (np. w sprawach osobowych).

Niektóre rodzaje niedozwolonej ingerencji w proces podejmowania uchwały przez kolegialne organy administracji publicznej mogą nastąpić w konsekwencji przełamania zabezpieczeń leżących po stronie podmiotu udzielającego licencji, w efekcie którego dochodzi do bezprawnej modyfikacji programu komputerowego. W takich przypadkach wiedzę o nieuprawnionej ingerencji osoby trzeciej może mieć przede wszystkim podmiot udzielający licencji. Ze względu na to, że z postanowień przedmiotowo istotnych umowy licencyjnej ani z ustawy o prawie autorskim i prawach pokrewnych⁸ nie wynika obowiązek licencjodawcy poinformowania licencjobjorcy o każdym wiadomym licencjodawcy przypadku niedozwolonej ingerencji w program komputerowy, w interesie licencjobjorcy leży zastrzeżenie takiego obowiązku licencjodawcy w umowie licencyjnej⁹. Mimo różnicy zdań przedstawicieli doktryny należy uznać, że umowa licencyjna stanowi umowę obligacyjną¹⁰. Zgodnie z art. 67 ust. 1 ustawy o prawie autorskim i prawach pokrewnych umowa licencyjna polega bowiem na „upoważnieniu do korzystania z utworu na wymienionych w umowie polach eksploatacji z określeniem

⁸ Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, t.j. Dz. U. z 2022 r., poz. 2509 ze zm.

⁹ Zob. szerzej abstrakt referatu pt. „Postanowienia umowy licencyjnej jako środek zabezpieczający prawidłowe funkcjonowanie administracji publicznej” wygłoszonego przez M. Tenenbaum-Kulig dnia 25 maja 2023 r. na II Międzynarodowej Konferencji Naukowo-Praktycznej „Cyberbezpieczeństwo instytucji państwowych i przewidywanie sytuacji kryzysowych”, zorganizowanej przez Narodowy Uniwersytet Techniczny Ukrainy, Kijowski Instytut Politechniczny im. Igora Sikorskiego i Uniwersytet Wrocławski, w druku.

¹⁰ Tak np.: A. Kopff, w: S. Grzybowski, A. Kopff, J. Serda, Zagadnienia prawa autorskiego, Warszawa 1973, s. 205-211. Warszawa 1973; A. Niewęglowski, Komentarz do art. 41, [w:] Prawo autorskie. Komentarz, WKP 2021, Lex/el., Nb. 40. Wypada jednak zaznaczyć, że charakter prawny umowy licencyjnej, w tym jej zobowiązujący, rozporządzający bądź upoważniający skutek jest sporny. Wyrażany jest także pogląd, że udzielenie licencji stanowi obciążenie prawa podmiotowego. Zob. szerzej np. M. Kępiński, [w:] System Prawa Prywatnego, t. 13, Prawo autorskie, (red.) J. Barta, Warszawa 2017, s. 752 i n.; M. Załucki, Licencja na używanie znaku towarowego, Studium prawnoporównawcze, Warszawa 2008, s. 284 i n.; A. Niewęglowski, Komentarz do art. 41, op. cit., Nb. 40; B. Giesen, Umowa licencyjna w prawie autorskim, Struktura i charakter prawny, Warszawa 2013, s. 143 i n.

zakresu, miejsca i czasu tego korzystania” (art. 67 ust. 1 ustawy o prawie autorskim i prawach pokrewnych), a zważywszy na to, że nie sposób uznać umowy licencyjnej za czynność prawną upoważniającą¹¹, wypada opowiedzieć się za jej zobowiązującym charakterem. Uznanie umowy licencyjnej za umowę obligacyjną powoduje, że strony tej umowy mogą na podstawie zasady swobody umów (art. 353¹ k.c.¹²) zastrzec opisany wyżej obowiązek. Pożądane jest również ustanowienie w umowie licencyjnej kary umownej na wypadek każdorazowego niewywiązania się przez licencjodawcę z tego obowiązku (art. 483 k.c.)¹³. Zawarcie w umowie licencyjnej opisanych wyżej postanowień jest istotne nie tylko z tego powodu, że powzięcie przez organ administracji publicznej wiedzy o wywarcu przez osobę trzecią nieuprawnionego wpływu na proces podejmowania uchwały stanowi warunek weryfikacji, czy podjęta uchwała jest ważna – a w razie jej nieważności podjęcia odpowiednich kroków służących sanacji naruszeń prawa. Wzbogacenie umowy licencyjnej o opisany wyżej obowiązek licencjodawcy, jako warunkujące powzięcie wiedzy przez organ administracji publicznej o niedozwolonej ingerencji osoby trzeciej, jest także niezbędne dla umożliwienia realizacji przez organ administracji publicznej jego uprawnień wynikających z wadliwości fizycznej programu komputerowego. Przyjmuje się bowiem, że wadliwość programu komputerowego jest związana z zakłóceniami dotyczącymi: istnienia w programie wszystkich uzgodnionych modułów, wykonywania przez program wszystkich określonych w dokumentacji funkcji, zasadniczej bezbłędności wykonywania przez program jego podstawowych funkcji, ergonomiczności pracy programu, zdolności programu do pracy w określonym przez twórcę systemie operacyjnym i przy określonych wymaganiach sprzętowych, czy też z zakłóceniami dotyczącymi spełniania przez program określonej funkcji, jaką ma on spełniać u nabywcy¹⁴. Dopóki organ administracji publicznej nie ma wiedzy o wadliwości programu, nie może zrealizować przysługujących mu uprawnień, natomiast w interesie licencjodawcy nie leży dobrowolne (niewynikające z obowiązku prawnego) informowanie licencjobiorcy o nieuprawnionej ingerencji osoby trzeciej w program, która nastąpiła wskutek przełamania zabezpieczeń leżących po stronie licencjodawcy. Pożądane jest zatem umowne ustanowienie takiego obowiązku i obwarowanie go odpowiednio dotkliwą karą umowną.

¹¹ Czynność prawną upoważniającą definiuje się jako „polegającą na tym, że podmiot dokonujący jej (A) wyznacza innemu podmiotowi (B) kompetencję do dokonania jakiejś czynności konwencjonalnej (w szczególności czynności prawnej) ze skutkiem dla siebie – to znaczy dla A” – tak: Z. Radwański/J. Grykiel, [w:], System Prawa Prywatnego, t. 2, Prawo cywilne – część ogólna, (red.) Z. Radwański, A. Olejniczak, Warszawa 2019, s. 287.

¹² Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny, t.j. Dz. U. z 2024 r., poz. 1061 ze zm.

¹³ Tak: M. Tenenbaum-Kulig, w abstrakcie referatu pt. „Postanowienia umowy licencyjnej jako środek zabezpieczający prawidłowe funkcjonowanie administracji publicznej”, w druku.

¹⁴ A. Stuglik, Odpowiedzialność licencjodawcy za wady fizyczne programu komputerowego, s. 3, <https://kbzlegal.pl/wp-content/uploads/2018/10/1.pdf> [data dostępu 31.08.2023 r.]; J. Barta, R. Markiewicz, Główne problemy prawa komputerowego, Warszawa 1993, s. 186.

Zagrożenia dla głosowania prowadzonego w toku procedury służącej podejmowaniu rozstrzygnięć w drodze decyzji administracyjnej

Prawnie doniosła uchwała musi opierać się na podstawie prawnej zawartej w ustawie lub w akcie wewnętrznym (statucie, bądź umowie) regulującym działanie określonej zbiorowości¹⁵. W przypadku uchwał organów administracji publicznej wymagana jest podstawa prawna zawarta w ustawie. Uchwała służy do wyrażania wspólnej woli przez dany zespół osób. Do podjęcia uchwały wymagane jest wyrażenie zgody przez odpowiednią większość osób, o ile w głosowaniu weźmie udział (lub będzie obecna) określona liczba uprawnionych do głosowania (*quorum*). Po oddaniu we właściwy sposób głosów zostają one zebrane i obliczone przez wyłonioną osobę lub komisję skrutacyjną, która po dokonaniu tych czynności stwierdza, czy spełnione zostały przesłanki konieczne dojścia do skutku uchwały. W razie ich spełnienia uchwała zostaje podjęta¹⁶. W przypadku podejmowania uchwały zdalnie, przy wykorzystaniu systemu teleinformatycznego, zebrania i obliczenia głosów, a także oceny, czy uchwała została podjęta, dokonuje ów system (program komputerowy). Zgodnie z dominującym poglądem, nie odmawia się wszystkim uchwałom charakteru oświadczeń woli lub czynności prawnej (choć – co należy podkreślić - nie wszystkie uchwały mogą mieć charakter czynności prawnej)¹⁷. Natomiast oświadczenie poszczególnej osoby biorącej udział w głosowaniu jest oświadczeniem woli. Wówczas, gdy uchwała ma charakter oświadczenia woli, to jednostkowe oświadczenie osoby biorącej udział w głosowaniu współtworzy oświadczenie woli przypisywane całej zbiorowości na podstawie reguł kompetencyjnych zawartych w ustawie lub w statucie¹⁸. W takich przypadkach suma poszczególnych oświadczeń woli składa się na oświadczenie woli kolektywnego organu osoby prawnej, bądź – w przypadku niniejszych rozważań – organu administracji publicznej.

Zaznaczenia wymaga, że oświadczenia woli członków organu kolegialnego, jak również oświadczenie woli tego organu, w zakresie omawianym w tym opracowaniu, ma charakter administracyjny. Nauka prawa podkreśla, że ze względu na niewyczerpujące unormowanie w prawie administracyjnym instytucji oświadczenia woli, konieczne jest odpowiednie stosowanie przepisów prawa cywilnego regulujących tę instytucję. Odpowiednie stosowanie tych przepisów dotyczy m. in. wad oświadczeń woli¹⁹. Każda osoba biorąca udział w głosowaniu może zatem co do zasady (w braku przepisów szczególnych) w razie spełnienia przesłanek powołać się na wadę złożonego przez siebie oświadczenia woli (art. 82–88 k.c.). Podkreśla się

¹⁵ Z. Radwański/J. Grykiel, op. cit., s. 256.

¹⁶ Ibidem, s. 255 i n.

¹⁷ Ibidem, s. 257 i wskazana tam literatura.

¹⁸ Ibidem.

¹⁹ A. Puczek, Oświadczenie woli w prawie administracyjnym, [w:] Pogranicze prawa administracyjnego, (red.) J. Zimmermann, Warszawa 2019, s. 190.

jednak, że w przypadku głosowania tajnego jest to utrudnione²⁰. Uchylenie się od skutków prawnych złożonego głosu nie powoduje jednak automatycznie nieważności podjętej uchwały, ponieważ co do zasady uchwała nie wymaga podjęcia jej jednogłośnie. Nieważność całej uchwały zachodzi więc wówczas, gdy liczba „nieważnych” głosów (np. oddanych przez osoby nieuprawnione do udziału w głosowaniu, bądź głosów od których skutków prawnych uchyliły się osoby, które oddały te głosy) była tak znaczna, że nie zostało zachowane wymagane *quorum*, bądź nie oddano wymaganej liczby głosów pozytywnych²¹.

W kontekście skuteczności podjęcia uchwały przez organ kolegialny znaczenie ma nie tylko uchylenie się przez poszczególne osoby, biorące udział w głosowaniu, od złożonych przez nie pojedynczych oświadczeń woli (głosów), lecz także problem „sfalszowania głosu” wskutek nieuprawnionej ingerencji osoby trzeciej (np. hakera). Wydaje się, że można wyróżnić dwa podstawowe przypadki takiego „sfalszowania głosu”. Pierwszy polega na tym, że głos w rzeczywistości oddaje osoba nieuprawniona do wzięcia udziału w głosowaniu (np. niewchodząca w skład organu kolegialnego), a równocześnie (w szczególności dla głosującego) zostaje stworzony pozór oddania głosu przez osobę uprawnioną do wzięcia udziału w głosowaniu (np. na monitorze komputera osoby uprawnionej do głosowania, która podjęła czynności zmierzające do oddania głosu, wyświetlony zostaje komunikat, że oddała głos o określonej treści). Tego rodzaju niebezpieczeństwa zachodzą zwłaszcza w toku głosowania na odległość, w szczególności o charakterze tajnym. W opisanym przypadku nie mamy do czynienia z zachowaniem osoby uprawnionej do wzięcia udziału w głosowaniu, lecz z zachowaniem innego podmiotu. W opisanym przypadku nie sposób mówić o zniekształceniu oświadczenia przez posłańca (mającym takie same skutki prawne, jak błąd przy składaniu oświadczenia woli, a więc umożliwiającym uchylenie się od skutków prawnych złożonego oświadczenia – art. 84 w zw. z art. 85 k.c.). Taki wniosek jest zasadny niezależnie od tego, czy podzieli się dominujący w doktrynie pogląd, że zniekształcenie oświadczenia woli przez posłańca polega na przypadkowej zmianie treści oświadczenia powierzonego mu do przekazania, a nie na celowej zmianie jego treści (sfalszowaniu)²². Przychylenie się do tego stanowiska prowadzi do uznania, że

²⁰ Z. Radwański/J. Grykiel, op. cit., s. 258.

²¹ Ibidem.

²² Tak np.: B. Lewaszkiewicz-Petrykowska, [w:] System prawa cywilnego, t. I, Część ogólna, (red.) S. Grzybowski, Wrocław-Warszawa-Kraków-Gdańsk-Łódź 1985, s. 677; też, [w:] Kodeks cywilny, Komentarz, Część ogólna, (red.) M. Pyziak-Szafnicka, P. Księżak, LEX 2014, art. 85, Nb 7; S. Rudnicki, Komentarz do art. 85, [w:] Komentarz do kodeksu cywilnego, Księga pierwsza, Część ogólna, (red.) S. Dmowski, S. Rudnicki, 2011, Lex; A. Jedliński, Komentarz do art. 85, [w:] Kodeks cywilny, Komentarz, t. I, Część ogólna, (red.) A. Kidyba, 2012, Nb 5, LEX; R. Strugała, Komentarz do art. 85, [w:] Kodeks cywilny, Komentarz, (red.) E. Gniewek, P. Machnikowski, Warszawa 2021, Nb. 3; P. Sobolewski, Komentarz do art. 85, [w:] Kodeks cywilny, Komentarz, (red.) W. Borysiak, Nb. 5, 2023, Legalis i wskazana tam literatura. Inaczej: Z. Radwański, M. Gutowski, [w:] System Prawa Prywatnego, t. 2, Prawo cywilne – część ogólna, (red.) Z. Radwański, A. Olejniczak, Warszawa 2019, s. 513; M. Królikowski, Błąd jako wada oświadczenia woli strony umowy, Warszawa 2014, s. 213 i n.; M. Gutowski, Komentarz do art. 85, [w:] Kodeks cywilny, t. I, Komentarz do art. 1-352, (red.) M. Gutowski, 2021, Nb 7, Legalis.

w analizowanym przypadku w istocie nie dochodzi do zniekształcenia oświadczenia osoby uprawnionej do udziału w głosowaniu, lecz do zastąpienia oświadczenia tej osoby oświadczeniem pochodzącym od innego podmiotu. Jednakże wniosek, że w analizowanym przypadku nie zachodzi zniekształcenie oświadczenia przez posłańca, jest zasadny również w razie opowiedzenia się za wyrażonym w nowszej literaturze przez P. Machnikowskiego stanowiskiem, że możliwość zastosowania art. 85 k.c. w przypadku sfalszowania oświadczenia woli zależy m.in. od tego, czy osoba posłańca bądź narzędzie komunikacji zostało narzucone składającemu przez drugą stronę (wówczas zastosowanie art. 85 k.c. jest wykluczone), czy też to składający oświadczenie wybrał pośrednika, a przynajmniej zgodził się na niego (wówczas jest to możliwe, o ile odbiorca potraktował je jako oświadczenie złożone przez składającego i starannie działająca osoba trzecia uczyniłaby tak samo)²³. Przenosząc ten pogląd na grunt analizowanego przypadku należy bowiem uznać, że narzędzie komunikacji zostało narzucone składającemu oświadczenie przez odpowiednią regulację prawną i podjętą na tej podstawie decyzję organu administracji publicznej o odbyciu głosowania w trybie zdalnym, przy zastosowaniu określonego prywatnego systemu teleinformatycznego.

Drugi przypadek „sfalszowania głosu” wskutek nieuprawnionej ingerencji osoby trzeciej (np. hakera) może polegać na następczej modyfikacji (przez osobę trzecią) głosu prawidłowo oddanego przez osobę uprawnioną do udziału w głosowaniu. Wówczas również zniekształcenie jest celowe (a nie jedynie przypadkowe), a narzędzie komunikacji zostało narzucone składającemu oświadczenie przez odpowiednią regulację prawną i podjętą na tej podstawie decyzję organu administracji publicznej o odbyciu głosowania w trybie zdalnym, przy zastosowaniu określonego prywatnego systemu teleinformatycznego. Wydaje się jednak, że w tym przypadku należałoby stosować art. 85 k.c. *per analogiam*²⁴.

W przypadku, gdy w toku procedury służącej podejmowaniu rozstrzygnięć administracyjnych dochodzi do głosowania odbywanego zdalnie z zastosowaniem prywatnych systemów teleinformatycznych, można zatem wyróżnić następujące zagrożenia dla prawidłowości owego głosowania.

Wówczas, gdy wymagane jest głosowanie tajne, zachodzi ryzyko naruszenia tajności głosowania. Może do niego dojść np. wskutek ujawnienia przez osobę zatrudnioną przez organ administracji publicznej (np. informatyka) wbrew jej obowiązkom informacji o tym, jak głosowały poszczególne osoby, czy też wskutek przełamania przez osobę trzecią zabezpieczeń systemu teleinformatycznego i uzyskania wiedzy o treści

²³ P. Machnikowski, [w:] Zobowiązania. Przepisy ogólne i powiązane przepisy Księgi I KC. Tom I. Komentarz, (red.) P. Machnikowski 2022, Nb. 24.

²⁴ Jednak zdaniem R. Strugały w sytuacji celowej zmiany treści oświadczenia (jego sfalszowania) – aczkolwiek dokonanej przez posłańca – zasadne wydaje się stosowanie *per analogiam* art. 103 k.c. – tak: R. Strugała, Komentarz do art. 85, [w:] Kodeks cywilny, Komentarz, (red.) E. Gniewek, P. Machnikowski, Warszawa 2021, Nb. 3.

oddanych głosów, a następnie rozpowszechnienia tej informacji. Kolejne zagrożenia, nawiązując do uwag poczynionych wyżej, są związane z możliwością naruszenia wymogu oddania głosu przez osobę uprawnioną do udziału w głosowaniu (wchodzącą w skład organu administracyjnego), zgodnego z jej wolą. Chodzi zatem o zagrożenie sfalszowania głosu. Może do niego dojść w szczególności wskutek następczej modyfikacji prawidłowo oddanego głosu, albo poprzez oddanie „głosu” – w wyniku ataku hakerskiego – przez osobę do tego nieuprawnioną. Należy przy tym podkreślić, że uzyskanie nieuprawnionego dostępu do systemu teleinformatycznego może nastąpić nie tylko wskutek przełamania przez osobę trzecią zabezpieczeń zastosowanych przez organ administracji publicznej. Wyobrażalna jest także sytuacja, w której osoba trzecia, przełamując zabezpieczenia zastosowane przez licencjodawcę programu do głosowania, dokonuje modyfikacji tego programu, która wskutek aktualizacji programu przez organ administracji publicznej „infekuje” ten program i umożliwia sfalszowanie głosów oddawanych przez osoby uprawnione do głosowania, poprzez faktyczne zablokowanie tych głosów i oddanie „głosów” przez nieuprawnioną do tego osobę trzecią. Należy podkreślić, że – zgodnie z uwagami poczynionymi powyżej – w tym ostatnim przypadku nie mamy do czynienia z nieprawidłowością przy obliczaniu głosów (a więc z naruszeniem wymogu poprawności obliczania głosów), lecz jedynie z pozorem oddania głosu przez określone osoby. Natomiast, gdy głos prawidłowo oddany przez osobę uprawnioną do udziału w głosowaniu zostaje następnie sfalszowany (zmieniony) przez osobę nieuprawnioną (np. hakera), należy stosować *per analogiam* art. 85 k.c., a w konsekwencji art. 84 k.c. Oczywiście wyobrażalne są także inne zagrożenia, np. wywarcie nieuprawnionego wpływu na samą czynność obliczenia głosów, a zatem sfalszowanie działania matematycznego dokonywanego przez system teleinformatyczny.

Sanacja naruszenia prawa skutkującego zniekształceniem treści decyzji administracyjnej ze względu na nieprawidłowe przeprowadzenie głosowania w toku procedury służącej podejmowaniu rozstrzygnięć drogą elektroniczną przez kolegialne organy administracji publicznej

Sanacja naruszenia prawa polegającego na nieprawidłowym ustaleniu liczby i treści oddanych głosów ma miejsce, gdy skutkiem tych nieprawidłowości było zniekształcenie treści oświadczenia woli kolegialnego organu administracji publicznej względem oświadczeń woli członków tego organu, wyrażonych w formie głosu. Celem sanacji tego naruszenia prawa jest przywrócenie rozstrzygnięciu organu treści zgodnej z wynikami głosowania.

Należy wyróżnić dwa rodzaje sanacji tych naruszeń, wyodrębnionych ze względu na kryterium relacji czasu dokonania naruszenia względem działań sanacyjnych. Są nimi sanacja bieżąca oraz sanacja następcza.

Sanacja bieżąca ma miejsce toku procesu rozstrzygnięcia, czyli przed sformułowaniem przez kolegialny organ administracji publicznej treści rozstrzygnięcia w drodze decyzji administracyjnej. Sanacja bieżąca następuje w drodze reasumpcji głosowania. Organ przeprowadza reasumpcję zgodnie z wymogami prawnymi regulującymi jego procedurę uchwałodawczą²⁵. Reasumpcja oznacza powtórne przeprowadzenie głosowania dotyczącego tej samej sprawy²⁶. Powinna mieć ona miejsce zarówno, gdy nieprawidłowe ustalenie liczby lub treści oddanych głosów może skutkować zniekształceniem treści przyszłego rozstrzygnięcia, jak również wtedy gdy nie nastąpi zniekształcenie jego treści.

Drugi rodzaj trybu sanacji ma miejsce po wydaniu rozstrzygnięcia administracyjnego. Sanacja ta jest dokonywana w toku postępowania odwoławczego, postępowania sądowo-administracyjnego lub postępowania w sprawie stwierdzenia nieważności, gdy przedmiotem tych postępowań jest decyzja administracyjna zawierająca rozstrzygnięcie administracyjne o zniekształconej treści. Sanacja ta odnosi się jedynie do sytuacji, gdy skutkiem nieprawidłowego ustalenia liczby i treści oddanych głosów jest zniekształcenie treści rozstrzygnięcia. Jeżeli naruszenie nie skutkuje tymi nieprawidłowościami, sanacja jest zbędna, ponieważ pomimo tych nieprawidłowości treść rozstrzygnięcia ma poprawny charakter. Zaznaczenia wymaga, że zniekształcenie treści stanowi rażące naruszenie prawa, ponieważ decyzja administracyjna kolegialnego organu administracji publicznej powinna opierać się na prawidłowo zebranych głosach, jak również na prawidłowo ustalonym wyniku głosowania członków tego organu. Zniekształcone rozstrzygnięcie stanowi zatem rażące naruszenie przepisów prawa regulujących kolegialne podejmowanie tego rozstrzygnięcia. Skutek stwierdzenia zniekształcenia treści rozstrzygnięcia ze względu na nieprawidłowe zebranie głosów lub nieprawidłowe ustalenie liczby lub treści oddanych głosów, jeżeli były to jedyne naruszenia prawa, jest zależny od rodzaju postępowania. W przypadku postępowania odwoławczego, organ drugiej instancji powinien uchylić decyzję administracyjną i orzec co do istoty sprawy²⁷.

²⁵ W polskim porządku prawnym nie ma jednolitego modelu dotyczącego wymogów prawnych dotyczących procedury uchwałodawczej kolegialnego organu administracji publicznej. W przypadku organów wykonawczych powiatu i samorządu województwa, wymogi te mogą być ustanowione w statucie tych jednostek. Zgodnie z art. 2 ust. 4 u.s.p. o ustroju powiatu stanowi jego statut. W myśl art. 7 ust. 1 u.s.w., ustroj województwa jako jednostki samorządu terytorialnego określa statut województwa uchwalony po uzgodnieniu z Prezesem Rady Ministrów.

²⁶ J. Glinka przedstawia pojęcie reasumpcji na przykładzie głosowania w organach spółkach kapitałowych. J. Glinka, Kilka uwag na tle tak zwanej reasumpcji uchwał organów właścicielskich w spółkach kapitałowych, „Rynek - Społeczeństwo - Kultura” 2016, nr 21, s. 28.

²⁷ Art. 138 § 1 pkt. 2 k.p.a. Zaznaczenia wymaga, że w przypadku omawianych naruszeń prawa, organ odwoławczy nie może uchylić zaskarżonej decyzji w całości i przekazać sprawę do ponownego rozpatrzenia organowi pierwszej instancji. Zgodnie z art. 138 § 2 zd. 1 k.p.a., ten rodzaj decyzji organu odwoławczego jest możliwy, gdy decyzja organu pierwszej instancji została wydana z naruszeniem przepisów postępowania, a konieczny do wyjaśnienia zakres sprawy ma istotny wpływ na jej rozstrzygnięcie. Omawiane naruszenie prawa dotyczy przepisów postępowania, jednakże nie wiąże się z nieprawidłowym wyjaśnieniem zakresu sprawy, ponieważ wyjaśnienie sprawy poprzedza podejmowanie rozstrzygnięcia. Przedmiotem odwołania może być

W przypadku postępowania sądowo-administracyjnego, sąd administracyjny powinien wydać wyrok stwierdzający nieważność decyzji administracyjnej²⁸. W przypadku postępowania w sprawie stwierdzenia nieważności, właściwy organ powinien stwierdzić nieważność decyzji administracyjnej²⁹.

Sanacja następcza zniekształconej treści rozstrzygnięcia nie może nastąpić w drodze sprostowania, ponieważ ten rodzaj naruszenia prawa stanowi istotną wadę decyzji administracyjnej³⁰. Sanacja ta zmierza do zmiany treści rozstrzygnięcia, tak aby odpowiadało ono zbiorczej treści głosów oddanych przez członków kolegiального organu administracji publicznej. Sprostowanie nie może natomiast prowadzić do zmiany treści rozstrzygnięcia³¹.

Podsumowanie

Wymogi prawne dotyczące stosowania środków komunikacji elektronicznej w procesie rozstrzygania w kolegialnych organach administracji publicznej są jedynie częściowo adekwatne względem potencjalnych zagrożeń dla tego procesu. Wymogi te mają dwojaki charakter.

Po pierwsze odnoszą się one do umowy licencyjnej, której przedmiotem jest prawo organu administracji publicznej do korzystania z oprogramowania komputerowego. Ze względu na swobodę umów, organ administracji publicznej zawierając umowę licencyjną samodzielnie powinien zapewnić uwzględnienie w tej umowie

rażące naruszenie prawa, ze względu na prymat odwołania względem żądania stwierdzenia nieważności. Jak zauważa WSA w Krakowie w wyroku z dnia 19 lipca 2012 r., w zbiegu odwołania oraz żądania stwierdzenia nieważności prymat ma odwołanie, ze względu na szerszy zakres uprawnień organu odwoławczego (wyrok WSA w Krakowie z dnia 19 lipca 2012 r., III SA/Kr 1448/11, CBOSA). Jak zauważa B. Adamiak, postępowania nadzwyczajne, w tym postępowanie w sprawie stwierdzenia nieważności, ma służebny charakter względem postępowania głównego. Byt prawny postępowań nadzwyczajnych jest zależny od wydania ostatecznej decyzji - B. Adamiak, Rodzaje, tryby i stadia postępowania administracyjnego i sądowoadministracyjnego, [w:] Postępowanie administracyjne i sądowoadministracyjne, (red.) B. Adamiak, J. Borkowski, Warszawa 2007, s. 99.

²⁸ W świetle art. 145 § 1 pkt. 2 ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi, t.j. Dz. U. z 2024 r., poz. 935, sąd administracyjny uwzględniając skargę na decyzję administracyjną stwierdza jej nieważność w całości lub w części, jeżeli zachodzą przyczyny określone w art. 156 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego, t.j. Dz. U. z 2024 r., poz. 572, dalej k.p.a., lub w innych przepisach.

²⁹ Zgodnie z art. 156 § 1 pkt. 2 k.p.a., organ administracji publicznej stwierdza nieważność decyzji, która m. in. wydana została z rażącym naruszeniem prawa.

³⁰ Zgodnie z art. 113 § 1 k.p.a., organ administracji publicznej może prostować w drodze postanowienia błędy pisarskie i rachunkowe oraz inne oczywiste omyłki w wydanych przez ten organ decyzjach.

³¹ Zob. P. M. Przybysz, Komentarz do art. 113, [w:] Kodeks postępowania administracyjnego. Komentarz aktualizowany, LEX/el. 2023, teza 1. Jak podkreślił NSA w wyroku z dnia 4 maja 1988 r., sprostowanie nie może prowadzić do ponownego rozstrzygnięcia sprawy, o odmiennej treści. Wyrok NSA z dnia 4 maja 1988 r., III SA 1466/87, CBOSA. Zdaniem NSA, wyrażonym w wyroku z dnia 20 czerwca 2012 r., sprostowanie nie może skutkować merytoryczną zmianą decyzji. Wyrok NSA z dnia 20 czerwca 2012 r., I OSK 782/12, CBOSA.

odpowiednich postanowień, umożliwiających zachowanie bezpieczeństwa procesu rozstrzygania z użyciem tego oprogramowania komputerowego. Skutkiem zaniechania tych działań może być niemożność późniejszej weryfikacji naruszeń stosowania środków komunikacji elektronicznej w procesie rozstrzygania. Wymogi prawne dotyczące umów licencyjnych, których stroną jest podmiot publiczny, są niewystarczające względem zagrożenia naruszeniami.

Po drugie wymogi prawne regulują sanację naruszeń skutkujących zniekształceniem treści decyzji administracyjnej. Wymogi te dotyczą sanacji bieżącej odnoszącej się do reasumpcji głosowania, jak również sanacji następczej, która ma miejsce w toku postępowania odwoławczego, postępowania sądowo-administracyjnego lub postępowania w sprawie stwierdzenia nieważności. Wymogi związane z sanacją naruszeń są adekwatne względem potencjalnych zagrożeń dla procesu rozstrzygania, ponieważ zapewniają możliwość eliminacji z obrotu prawnego decyzji administracyjnej zawierającej rozstrzygnięcie o zniekształconej treści.

Bibliografia

Akty prawne

1. Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny, t.j. Dz. U. z 2024 r., poz. 1061 ze zm.
2. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych, t.j. Dz. U. z 2022 r., poz. 2509 ze zm.
3. Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego, t.j. Dz. U. z 2024 r., poz. 572.
4. Ustawa z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, t. j. Dz.U. z 2024 r., poz. 340 ze zm.
5. Ustawa z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce, t.j. Dz. U. z 2024 r., poz. 124 ze zm.
6. Ustawa z dnia 21 sierpnia 1997 r. o gospodarce nieruchomościami, t.j. Dz. U. z 2024 r., poz. 1145 ze zm.
7. Ustawa z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi, t.j. Dz. U. z 2024 r., poz. 935.
8. Ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym, t.j. Dz. U. z 2024 r., poz. 107.
9. Ustawa z dnia 5 czerwca 1998 r. o samorządzie województwa, t.j. Dz. U. z 2024 r., poz. 566.
10. Ustawa z dnia 6 grudnia 2006 r. o zasadach prowadzenia polityki rozwoju, t. j. Dz. U. z 2024 r., poz. 324 ze zm.

Orzecznictwo

1. Uchwała NSA z dnia 26 października 2009 r., I OPS 10/09, CBOSA.
2. Wyrok NSA z dnia 10 stycznia 2012 r., II FSK 1304/10, CBOSA.
3. Wyrok NSA z dnia 11 lipca 2007 r., I OSK 1292/06, CBOSA.
4. Wyrok NSA z dnia 20 czerwca 2012 r., I OSK 782/12, CBOSA.
5. Wyrok NSA z dnia 4 maja 1988 r., III SA 1466/87, CBOSA.
6. Wyrok WSA w Krakowie z dnia 19 lipca 2012 r., III SA/Kr 1448/11, CBOSA.

Literatura

1. Adamiak B., *Rodzaje, tryby i stadia postępowania administracyjnego i sądowniczoadministracyjnego*, [w:] *Postępowanie administracyjne i sądowniczoadministracyjne*, (red.) B. Adamiak, J. Borkowski, Warszawa 2007.
2. Barta J., Markiewicz R., *Główne problemy prawa komputerowego*, Warszawa 1993.
3. Boć J., *Podmioty administrujące*, [w:] *Prawo administracyjne*, (red.) J. Boć, Wrocław 2007.
4. Dawidowicz W., *Polskie prawo administracyjne*, Warszawa 1978.
5. Giesen B., *Umowa licencyjna w prawie autorskim, Struktura i charakter prawny*, Warszawa 2013.
6. Glinka J., *Kilka uwag na tle tak zwanej reasumpcji uchwał organów właścicielskich w spółkach kapitałowych*, „Rynek – Społeczeństwo – Kultura” 2016, nr 21.
7. Gutowski M., *Komentarz do art. 85*, [w:] *Kodeks cywilny, t. I, Komentarz do art. 1-352*, (red.) M. Gutowski, 2021, Legalis.
8. Jedliński A., *Komentarz do art. 85*, [w:] *Kodeks cywilny, Komentarz, t. I, Część ogólna*, (red.) A. Kidyba, 2012, LEX.
9. Kępiński M., [w:] *System Prawa Prywatnego, t. 13, Prawo autorskie*, (red.) J. Barta, Warszawa 2017.
10. Kopff A., [w:] S. Grzybowski, A. Kopff, J. Serda, *Zagadnienia prawa autorskiego*, Warszawa 1973.
11. Królikowski M., *Błąd jako wada oświadczenia woli strony umowy*, Warszawa 2014.
12. Lewaszkiewicz-Petrykowska B., [w:] *System prawa cywilnego, t. I, Część ogólna*, (red.) S. Grzybowski, Wrocław-Warszawa-Kraków-Gdańsk-Łódź 1985.
13. Lewaszkiewicz-Petrykowska B., *Komentarz do art. 85*, [w:] (red.) M. Pyziak-Szafnicka, P. Księżak, *Kodeks cywilny, Komentarz, Część ogólna*, LEX 2014.
14. Machnikowski P., [w:], *Zobowiązania. Przepisy ogólne i powiązane przepisy Księgi I KC. Tom I. Komentarz*, (red.) P. Machnikowski, 2022.
15. Niewęglowski A., *Komentarz do art. 41*, [w:] *Prawo autorskie. Komentarz*, WKP 2021, Lex/el.

16. Przybysz P. M., *Komentarz do art. 113, [w:] Kodeks postępowania administracyjnego. Komentarz aktualizowany*, LEX/el. 2023.
17. Puczek A., *Oświadczenie woli w prawie administracyjnym, [w:] Pogranicze prawa administracyjnego*, (red.) J. Zimmermann, Warszawa 2019.
18. Radwański Z./Grykiel J., [w:], *System Prawa Prywatnego, t. 2, Prawo cywilne – część ogólna*, (red.) Z. Radwański, A. Olejniczak, Warszawa 2019.
19. Radwański Z., Gutowski M., [w:] *System Prawa Prywatnego, t. 2, Prawo cywilne – część ogólna*, (red.) Z. Radwański, A. Olejniczak, Warszawa 2019.
20. Rudnicki S., *Komentarz do art. 85, [w:] Komentarz do kodeksu cywilnego, Księga pierwsza, Część ogólna*, (red.) S. Dmowski, S. Rudnicki, 2011, LEX.
21. Skóra A., *Komentarz do art. 104, [w:] Kodeks postępowania administracyjnego. Komentarz do art. 61-126. Tom II*, (red.) M. Karpiuk, P. Krzykowski, Olsztyn 2020, LEX/el.
22. Sobolewski P., *Komentarz do art. 85, [w:] Kodeks cywilny, Komentarz*, (red.) W. Borysiak, 2023, Legalis.
23. Strugała R., *Komentarz do art. 85, [w:] Kodeks cywilny, Komentarz*, (red.) E. Gniewek, P. Machnikowski, Warszawa 2021.
24. Ura E., *Prawo administracyjne*, Warszawa 2021.
25. Wierzbowski M., A. Wiktorowska, *Rodzaje jednostek organizacyjnych w systemie administracji publicznej, [w:] Prawo administracyjne*, (red.) M. Wierzbowski, Warszawa 2017.
26. Wróbel A., *Komentarz do art. 104, [w:] Komentarz aktualizowany do Kodeksu postępowania administracyjnego*, (red.) M. Jaśkowska, M. Wilbrandt-Gotowicz, A. Wróbel, LEX/el. 2023.
27. Wróblewski J., *Sądowe stosowanie prawa*, Warszawa 1988.
28. Załucki M., *Licencja na używanie znaku towarowego, Studium prawnoporównawcze*, Warszawa 2008.
29. Zimmermann J., *Prawo administracyjne*, Warszawa 2014.

Netografia

1. Stuglik A., *Odpowiedzialność licencjodawcy za wady fizyczne programu komputerowego*, <https://kbzlegal.pl/wp-content/uploads/2018/10/1.pdf> [data dostępu 31.08.2023 r.].

Inne

1. Tenenbaum-Kulig M., abstrakt referatu pt. „Postanowienia umowy licencyjnej jako środek zabezpieczający prawidłowe funkcjonowanie administracji publicznej”, wygłoszonego dnia 25 maja 2023 r. na II Międzynarodowej Konferencji Naukowo-Praktycznej „Cyberbezpieczeństwo instytucji państwowych i przewyżczanie sytuacji kryzysowych”, zorganizowanej przez Narodowy Uniwersytet Techniczny Ukrainy, Kijowski Instytut Politechniczny im. Igora Sikorskiego i Uniwersytet Wrocławski, w druku.

mgr Mariusz Dubojski

Kuratorium Oświaty w Szczecinie

ORCID: 0000-0003-0411-6396

e-mail: mdubojski@kuratorium.szczecin.pl

Zwiększenie dostępności cyfrowej nakierowanej na klienta – kasus Kuratorium Oświaty w Szczecinie

Increasing customer-oriented digital accessibility – a case of the Education Board in Szczecin

Streszczenie

W dzisiejszym dynamicznym świecie technologicznym rola nowoczesnych technologii informacyjno-komunikacyjnych w administracji publicznej nabiera coraz większego znaczenia. Polska nie pozostaje w tyle i stawia na innowacje, które mają na celu usprawnienie i uproszczenie procesów administracyjnych oraz poprawienie dostępności usług publicznych dla obywateli. W rozdziale tym przyjrzymy się, jakie korzyści niesie za sobą digitalizacja w sektorze administracji publicznej w Polsce.

Okres pandemii COVID-19 wywołanej nowym szczepem koronawirusa ciężkiego ostrego zespołu oddechowego SARS-CoV-2 w sposób dynamiczny zmobilizowała wiele sektorów życia publicznego do szybszego i pełniejszego wdrożenia rozwiązań cyfrowych w swojej działalności przez co dostępność obywateli do usług świadczonych przez administrację publiczną zmieniała się ułatwiając ich kontakt z urzędem.

Niniejszy rozdział opisuje podjęte działania ukierunkowane na polepszenie kontaktu klienta z urzędem jakim jest Kuratorium Oświaty w Szczecinie. Opisuje korzyści płynące z wdrożenia informatyzacji procesu załatwiania spraw w zestawieniu do wciąż aktualnych zagrożeń związanych z przestrzenią cyfrową.

Rola technologii cyfrowej w realizacji zadań administracji publicznej w Polsce

Informatyzacja i rosnąca rola technologii cyfrowych w życiu społecznym otwierają nową przestrzeń w administracji publicznej, w tym stają się elementami koniecznymi do wdrożenia a przy okazji usprawnienia komunikacji na linii klient-firma. Powyższe niewątpliwie ma wpływ na poprawę efektywności usług oraz zwiększenie zaufania obywateli do szeroko rozumianej administracji publicznej. Urzędy powinny mieć na uwadze charakter dynamicznych zmian, tym samym poprawić

efektywność załatwiania spraw publicznych oraz zadbać o podniesienie swoich (urzędniczych) kompetencji cyfrowych.

Dzięki informatyzacji, administracja publiczna może oferować bardziej efektywne i dostępne usługi dla obywateli. Elektroniczna obsługa spraw administracyjnych, w tym składanie dokumentów online czy ich odbieranie, ułatwia życie obywatelom zgodnie z § 3 ust. 1 pkt 1 rozporządzenia 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 teleinformatycznych³². Ustawodawca powyższym rozporządzeniem ustanowił sposoby postępowania podmiotu realizującego zadania publiczne w zakresie doboru środków, metod i standardów wykorzystywanych do ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i udoskonalania systemu teleinformatycznego wykorzystywanego do realizacji zadań tego podmiotu. Tym samym aktem prawa ustanowiono procedury organizacyjne, którym przypisano konkretne cele, takie jak: zapewnienie obywatelom dostępności usług świadczonych przez podmioty realizujące zadania publiczne w postaci elektronicznej. Powyższe działanie urzędu powinno mieć realny wpływ na zwiększenie efektywności usług świadczonych przez administrację publiczną, zapewnienie obywatelom i przedsiębiorcom zmniejszenia obciążeń związanych z realizacją uprawnień i obowiązków, zapewnienie podmiotom publicznym redukcji kosztów funkcjonowania oraz zrationalizowanie gospodarowania funduszami publicznymi.

Specyfika pracy organu nadzoru pedagogicznego jakim jest Kuratorium Oświaty w Szczecinie z klientem

Kuratorium Oświaty w Szczecinie jest państwową jednostką budżetową wchodzącą w skład zespolonej administracji rządowej w województwie jako wyodrębniona jednostka organizacyjna³³. Pracami kuratorium kieruje powołany kurator oświaty który zgodnie z artykułem 51 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe³⁴, w imieniu wojewody wykonuje zadania i kompetencje w zakresie oświaty określone w powyższej ustawie oraz przepisach odrębnych na obszarze województwa. Do najważniejszych jego zadań należy w szczególności sprawowanie nadzoru pedagogicznego nad publicznymi i niepublicznymi przedszkolami, innymi formami wychowania przedszkolnego, szkołami, placówkami oraz kolegiami pracowników służb społecznych, które znajdują się na obszarze danego województwa. Ponadto kurator oświaty wydaje decyzje administracyjne, które zostały jasno określone ustawą

³² Dz. U. z 2024 r. poz. 773

³³ §2 ust. 2 ujednoliconego regulaminu Kuratorium Oświaty w Szczecinie, ustalonego zarządzeniem Nr 52/2013 Zachodniopomorskiego Kuratora Oświaty z dnia 21 sierpnia 2013 r.

³⁴ t.j. Dz. U. z 2024 r. poz. 737 z późn. zm., dalej: ustawa Prawo oświatowe.

prawo oświatowe. Jest jednocześnie organem wyższego stopnia w rozumieniu przepisów ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego³⁵ w stosunku do organów jednostek samorządu terytorialnego w sprawach publicznych szkół i placówek zakładanych i prowadzonych przez osoby prawne i osoby fizyczne oraz niepublicznych szkół i placówek wobec dyrektorów szkół w sprawach z zakresu obowiązku szkolnego i obowiązku nauki oraz sprawach skreślenia uczniów z listy uczniów. Kurator oświaty jednocześnie jest osobą odpowiedzialną w województwie za realizację polityki oświatowej państwa³⁶.

Zatem osobami, które mogą stanowić swoistą definicję „klienta” urzędu są w pierwszej kolejności rodzice uczniów pobierających naukę w jednostkach systemu oświaty zlokalizowanych na terenie danego województwa. W dalszej, z pewnością, są to dyrektorzy tych jednostek oraz nauczyciele w nich pracujący. Niekiedy dochodzi do sytuacji, że klientem kuratorium oświaty jest pełnoletni uczeń, który zgodnie z odrębnymi przepisami po osiągnięciu wieku 18 lat może sam decydować o swojej przyszłości, a także rozstrzygać indywidualnie co do spraw z nim związanych. Tak szeroki wachlarz klientów, a zatem osób, obywateli, którzy w pewnym momencie stykają się z koniecznością kontaktu z urzędem, cyfryzacja przychodzi jako rozwiązanie ukierunkowane na polepszenie kontaktu na linii klient - urząd.

Kuratorium Oświaty w Szczecinie stale podnosi swoje kompetencje cyfrowe poprzez wdrażanie coraz to nowszych rozwiązań z dziedziny cyberprzestrzeni. Pozwala to na optymalizację zarządzania danymi z obszaru szeroko rozumianego nadzoru pedagogicznego oraz współpracy organu nadzoru z dyrektorami jednostek systemu oświaty oraz przedstawicielami organów prowadzących, jak również ułatwia współpracę z klientem. Cyfryzacja obiegu dokumentów pozwala na lepsze zarządzanie danymi, ich analizę oraz wykorzystanie w procesach decyzyjnych. Rozbudowanie systemu komunikacji cyfrowej, począwszy od pandemii wywołanej koronawirusem COVID-19 ułatwiło nie tylko kontakt z klientem, ale również przyczyniło się do szybszego i bardziej efektywnego gromadzenia danych dotyczących funkcjonowania jednostek systemu oświaty na terenie województwa zachodniopomorskiego i przekazywania ich odpowiednim służbom sanitarnym oraz Ministerstwu Edukacji i Nauki, które po ich analizie przyjmowało stosowne rozwiązania, a następnie tworzyło rozwiązania ogólnokrajowe ujmowane w stosownych rozporządzeniach. Ten nagły wzrost aktywności w cyberprzestrzeni przełożył się również na współczesny okres po pandemiczny. Wdrożone rozwiązania informatyzacji urzędu zostały dostosowane do współcześnie zmieniającego się świata. Nieustannie dbano o zwiększenie bezpieczeństwa przechowywania oraz przesyłania danych gromadzonych w Kuratorium Oświaty w Szczecinie.

³⁵ t.j. Dz. U. z 2024 r. poz. 572.

³⁶ Art. 51 ust. 1 pkt 1, 2, 4 i 5 ustawy Prawo oświatowe.

Podmiotem, który najczęściej kontaktuje się z organem nadzoru pedagogicznego jakim jest Kuratorium Oświaty w Szczecinie są rodzice dzieci oraz uczniów pobierających naukę na terenie województwa zachodniopomorskiego. Dzięki cyfryzacji urzędu ułatwiono sposób komunikowania się rodzica z właściwą komórką organizacyjną kuratorium. Rodzic, jako klient może w każdej chwili skontaktować się z urzędem wykorzystując najdogodniejszą dla siebie formę kontaktu. Niekiedy jest to kontakt telefoniczny, ale ten ograniczony jest godzinami pracy urzędu lub dostępnością właściwego wizytatora sprawującego bezpośredni nadzór nad daną jednostką systemu oświaty. Ta forma kontaktu z urzędem pozostaje wciąż jedną z najłatwiejszych. Kolejną formą jest droga elektroniczna, w której to klient ma możliwość kontaktu z urzędem drogą elektroniczną wysyłając wiadomość drogą mailową na wskazany adres korespondencji. Ta droga z pewnością jest drogą najpełniejszą, ponieważ umożliwia złożenie pisma wraz z niezbędnymi załącznikami, które rodzic uzna za stosowne, w dogodnej dla niego chwili³⁷. Rodzic dzięki temu rozwiązaniu nie jest ograniczony godzinami pracy urzędu, dostępnością wizytatora lub swoją pracą zawodową. Może dokonać kontaktu w każdej chwili i z każdego miejsca. Kuratorium Oświaty w Szczecinie rozpoznaje takie pisma na równi z pismami wniesionymi drogą tradycyjną, tj. za pośrednictwem usługodawcy pocztowego. Z tą tylko różnicą, że rodzic otrzymuje informacje zwrotną tą samą drogą jaką sprawę wniósł. W tym przypadku stosowne pismo kierowane jest na adres mailowy osoby wnoszącej sprawę. Takie rozwiązanie z pewnością, poza zwiększeniem transparentności pracy urzędu, redukuje w sposób znaczący koszty związane z przesyłaniem odpowiedzi podmiotom wnoszącym. Z kolei z punktu widzenia wnoszącego, otrzymanie odpowiedzi drogą elektroniczną pozwala mu na niezwłoczne zapoznanie się z treścią pisma urzędowego, w czasie i miejscu dogodnym dla klienta. W XXI wieku wielu obywateli korzysta z cyfrowych rozwiązań, choćby poprzez sparowanie poczty elektronicznej z posiadanymi urządzeniami mobilnymi. Otrzymywanie korespondencji tą drogą jest również dbaniem o czas obywatela, który po pierwsze nie musi oczekiwać aż dostawca pocztowy doręczy mu pismo drogą tradycyjną, czyli umieści je w skrzynce pocztowej lub też, w przypadku poważniejszych spraw, a co za tym idzie koniecznością potwierdzenia otrzymania danej korespondencji, nie obliuguje obywatela do osobistego odbioru poczty z urzędu pocztowego.

Kolejną drogą kontaktu z urzędem jest platforma ePUAP, która pozwala na nie tylko szybszą komunikację klienta z urzędem, ale również w sposób precyzyjny umożliwia zidentyfikowanie, a tym samym potwierdzenie tożsamości osoby składającej pismo, która z chwilą jego wysłania otrzymuje automatyczne potwierdzenie jego

³⁷ Zob. Ł. Dragun, K. Kuczyńska, E-mail marketing i jego wpływ na środowisko ludzkie, „Akademia Zarządzania” 2024, vol. 8, no. 1, s. 195-197.

przedłożenia, co pozwala na szybsze załatwienie sprawy istotnej z punktu widzenia tego podmiotu³⁸. Tak samo jak w przypadku drogi elektronicznej, klient uzyskuje odpowiedź tą samą drogą, jaką wykorzystał przy złożeniu stosownej dokumentacji lub wniosku do Kuratorium Oświaty w Szczecinie.

Drugą grupę pod względem liczby kontaktów z kuratorium stanowią dyrektorzy jednostek systemu oświaty znajdujących się na terenie województwa zachodniopomorskiego. Kierowanie jednostką systemu oświaty wymaga często pilnego załatwienia sprawy lub niezwłocznego przekazania niezbędnej dokumentacji lub danych do urzędu sprawującego nadzór pedagogiczny. Wykorzystując technologię cyfrową dyrektor danej jednostki oszczędzając czas oraz pieniądze publiczne coraz częściej kontaktuje się z kuratorium drogą elektroniczną. Warto w tym miejscu zaznaczyć, że zgodnie z ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne³⁹ podmioty te, w tym między innymi przedszkola szkoły i inne placówki oświatowe, zobowiązane są do posiadania elektronicznej skrzynki podawczej na elektronicznej platformie usług administracji publicznej ePUAP⁴⁰. Elektroniczna skrzynka podawcza na tej platformie służy nie tylko do kontaktu na linii obywatel - jednostka administracji publicznej, ale także do kontaktu pomiędzy samymi jednostkami administracji publicznej, w tym przypadku jednostki systemu oświaty z kuratorium oświaty oraz innymi urzędami. Te rozwiązanie z pewnością jest wygodniejsze, szybsze i przede wszystkim nie pociągające za sobą kosztów związanych z przekazywaniem korespondencji. Dzięki cyfrowemu podejściu dyrektor przedszkola, szkoły lub placówki może przekazać do danego urzędu pakiet dokumentów bez konieczności ich drukowania (pierwszy koszt) oraz nadawania pocztą tradycyjną, gdzie koszt nadania przesyłki uzależniony jest od jej wielkości (drugi koszt).

Poza powyżej opisanymi formami kontaktu Kuratorium Oświaty w Szczecinie wdrożono elektroniczny system gromadzenia danych, który wykorzystuje platformy cyfrowe do pozyskiwania kluczowych dla nadzoru pedagogicznego informacji, które następnie są na sposób elektroniczny gromadzone, analizowane i przetwarzane. To rozwiązanie, którego początek miał miejsce w okresie czasowego ograniczenia funkcjonowania jednostek systemu oświaty w związku z pandemią COVID-19 pozostał w urzędzie do dnia dzisiejszego.

Kurator oświaty w swoich zadaniach ma również współpracę z jednostkami samorządu terytorialnego, innymi urzędami oraz przedstawicielami organów prowadzących. Wykorzystanie cyfrowej formy kontaktu oraz cyfrowego załatwiania spraw

³⁸ D. Fleszer, *Funkcjonowanie Elektronicznej Administracji na Przykładzie EPUAP*, „Roczniki Administracji i Prawa” 2012, nr 12, s. 125-131.

³⁹ t.j. Dz. U. z 2024 r. poz. 307

⁴⁰ Art. 16 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

wpływa w sposób bezsporny na skrócenie czasu niezbędnego do ich załatwienie, a także umożliwia wdrożenie oszczędności jednostek samorządu terytorialnego wynikających z elektronicznego przekazywania dokumentacji. Dobrym przykładem tego rozwiązania jest przyjęte w Kuratorium Oświaty w Szczecinie, jak i w wielu innych kuratoriach, przekazywanie elektronicznej wersji arkuszy organizacji jednostek systemów oświaty⁴¹. Dokument ten, opisujący w sposób pełny, organizację nauczania, wychowania, opieki i pracy danej jednostki w danym roku szkolnym niekiedy opiewa na kilkadziesiąt stron. Dyrektor przedszkola, szkoły lub placówki opracowuje arkusz na każdy rok szkolny, który następnie przekazuje do przyjęcia przez organ prowadzący to jest jednostkę systemu oświaty lub osobę prawną która podjęła się zadania prowadzenia publicznej działalności oświatowej. Organ prowadzący przed zatwierdzeniem arkusza organizacji bądź jego zmian wprowadzonych do dnia 30 września danego roku szkolnego na podstawie §18 ust. 7-12 rozporządzenia Ministra Edukacji Narodowej z dnia 28 lutego 2019 r. w sprawie szczegółowej organizacji publicznych szkół i publicznych placówek⁴² zobowiązany jest uzyskać opinie organu sprawującego nadzór pedagogiczny. Przekazanie powyższej dokumentacji w sposób elektroniczny, nie tylko generuje oszczędności finansowe, ale umożliwia sprawniejsze ich załatwienie, to jest szybsze otrzymanie niezbędnej opinii umożliwiającej zatwierdzenie arkusza bądź jego zmian, a co za tym idzie wdrożenia ich w życie. Szczególnie istotnym momentem, niezbędnym do sprawnego przeprowadzenia procesu zatwierdzenia arkusza, są zmiany powstałe w trakcie roku szkolnego i które muszą być wprowadzone do dnia 30 września. Skrócenie okresu oczekiwania, w celu uzyskania wymaganej przepisami prawa opinii, umożliwia poprawę funkcjonowania jednostki systemu oświaty, gdyż zmiany te mogą być szybciej zatwierdzone, a co za tym idzie, wdrożone. Mowa tu choćby o zatrudnieniu nowych nauczycieli, którzy nie mogą rozpocząć pracy do czasu zatwierdzenia arkusza organizacji, gdyż związane jest to z gospodarowaniem finansami publicznymi przez dyrektora.

Zagrożenia płynące z cyfryzacji procesu procedowania spraw w urzędzie administracji publicznej

Omawiając zalety informatyzacji w administracji publicznej oraz jej zadań nie sposób odnieść się do pewnych zagrożeń związanych z tym obszarem. W miarę jak administracja publiczna przechowuje coraz większe ilości danych cyfrowych pojawiają się zagrożenia związane z ich bezpieczeństwem. Obszarem szczególnej

⁴¹ Komunikat w sprawie przesyłania i opiniowania arkuszy organizacji publicznych przedszkoli, szkół i placówek na rok szkolny 2023/2024, <http://www.kuratorium.szczecin.pl/szkoly-i-organy-prowadzace/arkusze-organizacji/komunikat-w-sprawie-przesylania-i-opiniowania-arkuszy-organizacji-publicznych-przedszkoli-szkol-i-placowek-na-rok-szkolny-2023-2024/> [data dostępu 31.08.2023 r.].

⁴² t.j. Dz. U. z 2023 r. poz. 2736.

uwagi jest zabezpieczenie danych przed ich nieuprawnionym wyciekiem lub przed atakiem hackerskim, które mogą narazić na utratę prywatności lub bezpieczeństwa obywateli. Stąd koniecznym jest inwestowanie w coraz to nowsze systemy zabezpieczeń oraz ciągle podnoszenie świadomości i kwalifikacji osób odpowiedzialnych za ten obszar działalności urzędu⁴³.

Cyberbezpieczeństwo to jedno, ale należy pamiętać o dostępności urzędu dla obywatela, który niekiedy w dalszym ciągu pozostaje w sferze wykluczenia cyfrowego. Nie wszyscy obywatele mają dostęp do komputera czy Internetu. Wprowadzenie rozwiązań opartych na technologii może wykluczyć grupy społeczne, które nie są z nimi zaznajomione lub nie posiadają odpowiednich zasobów. Dlatego też w dalszym ciągu nie ma możliwości na pełne przejście w przestrzeń cyfrową przy okazji działalności administracji publicznej, w tym kuratorium oświaty.

Ponadto należy zwrócić uwagę na jeszcze jeden aspekt zagrożeń z informatyzacji na linii klient – urząd, a mianowicie na to, że zarówno pracownicy administracji publicznej jak i obywatele, mogą mieć trudności z dostosowaniem się do nowych technologii i cyfrowych procedur. Technologia cyfrowa w naszym kraju, jak i na całym świecie, rozwija się w sposób bardzo dynamiczny, co poniekąd oblige pracowników do ciągłego podnoszenia swoich umiejętności cyfrowych. Staje się to niezbędne w ich pracy na równi z utrzymaniem wysokiego standardu merytorycznego rozpatrywania spraw. Niezbędnym również staje się podnoszenie świadomości zagrożeń związanych z cyberbezpieczeństwem, które umożliwią lepsze zabezpieczenie danych przez pracownika. Stąd w wielu urzędach powstają i wciąż są aktualizowane procedury postępowania, począwszy od wygaszania monitorów poprzez należyte przechowywanie haseł dostępu, aż do blokowania przyłączania obcych sprzętów do sieci wewnętrznych. Wszystko to ma na celu ochronę danych oraz zapewnienie bezpiecznego funkcjonowania urzędów.

Podsumowanie

Podsumowując, informatyzacja ma potencjał do znaczącej poprawy efektywności administracji publicznej w Polsce, ale niesie również ze sobą pewne zagrożenia, które należy uwzględnić i odpowiednio zarządzać nimi, aby zapewnić bezpieczeństwo danych obywateli oraz dostępność usług dla wszystkich grup społecznych. Informatyzacja i cyberbezpieczeństwo stanowią kluczowe wyzwania oraz szanse dla administracji publicznej w Polsce. Dążenie do efektywności i dostępności usług dla obywateli musi być równoważne z odpowiednią ochroną danych i systemów przed zagrożeniami cybernetycznymi. Świadomość tych kwestii i inwestycje w odpowiednie zabezpieczenia są niezbędne, aby zapewnić pełne korzystanie z korzyści, które

⁴³ Zob. D. Skoczylas, Krajowy System Cyberbezpieczeństwa, Warszawa 2023, s. 327-342.

niewątpliwie płyną z informatyzacji przestrzeni publicznej, a jednocześnie pozostając bezpieczną i niezawodną formą kontaktu na linii klient urząd.

Bibliografia

Akty prawne

1. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, t.j. Dz. U. z 2024 r. poz. 307.
2. Ustawa z dnia 14 grudnia 2016 r. – Prawo oświatowe, t.j. Dz. U. z 2024 r. poz. 737 z późn. zm.
3. Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego, Dz. U. z 2024 r. poz. 572.
4. 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. 2024 r. poz. 773.
5. Rozporządzenie Ministra Edukacji Narodowej z dnia 28 lutego 2019 r. w sprawie szczegółowej organizacji publicznych szkół i publicznych placówek, t.j. Dz. U. z 2023 r. poz. 2736.

Publikacje

1. Dragun Ł., Kuczyńska K., E-mail marketing i jego wpływ na środowisko ludzkie, „Akademia Zarządzania” 2024, vol. 8, no. 1.
2. Fleszer D., Funkcjonowanie Elektronicznej Administracji na Przykładzie EPU-AP, „Roczniki Administracji i Prawa” 2012, nr. 12.
3. Skoczylas D., Krajowy System Cyberbezpieczeństwa, Warszawa, 2023.

Netografia

1. Komunikat Zachodniopomorskiego Kuratora Oświaty z dnia 27 marca 2023 r. w sprawie przesyłania i opiniowania arkuszy organizacji publicznych przedszkoli, szkół i placówek na rok szkolny 2023/2024, <http://www.kuratorium.szczecin.pl/szkoly-i-organy-prowadzace/arkusze-organizacji/komunikat-w-sprawie-przesylania-i-opiniowania-arkuszy-organizacji-publicznych-przedszkoli-szkol-i-placowek-na-rok-szkolny-2023-2024/> [data dostępu 31.08.2023 r.].
2. Elektroniczne Zarządzanie Dokumentacją, <https://ezd.gov.pl/www/index> [data dostępu 31.08.2023 r.].

Inne

1. Ujednolicony regulamin Kuratorium Oświaty w Szczecinie, ustalony zarządzeniem Nr 52/2013 Zachodniopomorskiego Kuratora Oświaty z dnia 21 sierpnia 2013 r.

dr Marta Grabowska

Szkoła Doktorska Uniwersytetu Szczecińskiego

ORCID: 0000-00019812-5570

Adres email: marta.grabowska@phd.usz.edu.pl

Status polskiego społeczeństwa na przykładzie dostępu do usług użyteczności publicznej

The status of Polish society on the example of the use of public services

Streszczenie

Rozwój technologiczny i jego wpływ na funkcjonowanie administracji publicznej na przestrzeni ostatnich lat stał się ciekawym problemem badawczym. Nowe technologie wpływając na większość aspektów życia społecznego, determinują kształt i status polskiego społeczeństwa, które przez pryzmat stopnia korzystania z usług użyteczności publicznej za pomocą technologii mobilnych, ocenić należy jako figurujące na zaawansowanym poziomie z perspektywy jego informacyjności. W tym kontekście zakwalifikować je również można jako społeczeństwo sieci. Mając to na względzie, nie ma wątpliwości, iż nowe technologie wyznaczają trendy i kierunki przeobrażeń społeczeństwa.

Wprowadzenie

Nie ma wątpliwości co do tego, iż postęp technologiczny odnosi bezpośredni wpływ na wszystkie aspekty życia, w tym społecznego, prawnego i gospodarczego. Nowe technologie na gruncie nieustannych przeobrażeń stały się jednym z najbardziej pożądaných dóbr i usług, niejako określając kształt i formę zarówno społeczeństwa, jak również instrumentów przez nie wykorzystywanych. Informatyzacja dostrzegalna jest również w sferze administracji publicznej, formie dostępu do usług użyteczności publicznej, co w konsekwencji wpływa na status społeczeństwa polskiego⁴⁴.

Z uwagi na nieustanny rozwój technologiczny, ciekawym problemem badawczym stał się status polskiego społeczeństwa z perspektywy jego informacyjności. W celu ustalenia i oceny rzeczonoego statusu przeprowadzono badanie ilościowe mające na celu zweryfikowanie stopnia i formy korzystania z usług użyteczności

⁴⁴ D. Cendrowicz, Rozwój e-kompetencji w administracji publicznej na przykładzie pomocy społecznej [w:] Ewolucja elektronicznej administracji publicznej, (red.) E. Kusiak-Winter, J. Korczak, Wrocław 2021, s. 74-78.

publicznej, a także sformułowanie wniosków w tym zakresie z perspektywy społeczeństwa sieci oraz e-kompetencji w administracji publicznej.

Definicja społeczeństwa informacyjnego

Pojawienie się czwartej rewolucji przemysłowej na początku XXI wieku⁴⁵, niejako zapoczątkowało erę przemysłowego internetu rzeczy, sztucznej inteligencji, wirtualnej i poszerzonej rzeczywistości, chmury technologicznej, *blockchain* oraz wykorzystania nowych technologii jako podstawowego przekaznika informacji⁴⁶. Okres ten bezpośrednio również wpłynął na kształt społeczeństwa polskiego ocenianego z perspektywy jego informacyjności.

W celu możliwie kompleksowego omówienia zagadnień stanowiących przedmiot niniejszej pracy, w pierwszej kolejności przytoczyć należy definicję społeczeństwa informacyjnego stanowiącą bazę rozważań w dalszej części pracy. Przyjmuje się, iż społeczeństwo informacyjne to takie, w którym większość aktywnych zawodowo osób zajmuje się przetwarzaniem informacji, a narzędzia informatyczne wykorzystywane są szeroko także w związku z innymi formami aktywności obywateli (komunikacją, konsumpcją, edukacją)⁴⁷. Z uwagi na nieustannie rosnące znaczenie sieci teleinformatycznej jako nośnika danych w doktrynie odnajduje się wiele różnych definicji społeczeństwa informacyjnego, z których każda przykłada największą uwagę do innych – równie ważnych aspektów⁴⁸. W większości definicji jako jedno z najważniejszych determinant tego procesu wymienia się informację i dynamiczny rozwój technologii informacyjno-komunikacyjnych⁴⁹. Społeczeństwo informacyjne jest też coraz częściej postrzegane jeszcze szerzej – z punktu widzenia przemian zachodzących w różnych sferach życia⁵⁰. Jako przykład takiej definicji można wskazać tę zawartą w Strategii rozwoju społeczeństwa informacyjnego w Polsce do roku 2013⁵¹, zgodnie z którą jest to „(...) społeczeństwo, w którym

⁴⁵ Szerzej: J. Blicharz, *Inteligentne miasta i sztuczna inteligencja. Wybrane aspekty teoretycznoprawne*, Wrocław 2023, s. 13 i nast.

⁴⁶ M. Wodnicka, *Wpływ czwartej rewolucji przemysłowej na innowacyjność usługi*, „Optimum Economic Studies” 2021, nr 3(105), s. 52. Także w tej sprawie: B. Zinzuk, op. cit., s. 106.

⁴⁷ G. Szpor, *Urzędnicy w społeczeństwie informacyjnym* [w:] *Prawo administracyjne*, (red.) Z. Niewiadomski, Warszawa 2007, s. 288.

⁴⁸ M. Sokołowski, *Pojęcie usług społeczeństwa informacyjnego* [w:] *Sto lat polskiego prawa handlowego. Księga jubileuszowa dedykowana Profesorowi Andrzejowi Kidybie*, (red.) M. Dumkiewicz, K. Kopczyńska-Pieczniak, J. Szczotka, Warszawa 2020, s. 152-160.

⁴⁹ R. Seweryn, *Technologie informacyjne i komunikacyjne*, Warszawa 2017, s. 14 i nast.

⁵⁰ D. Skoczylas, *Aksjologiczny wymiar administracji i cyberbezpieczeństwa w kontekście potrzeb jednostki i wspólnoty* [w:] *Prawo administracji w służbie jednostki i wspólnoty*, (red.) Z. Duniewska, M. Karcz-Kaczmarek, P. Wilczyński, Warszawa 2022, s. 207 i nast.

⁵¹ *Społeczeństwo informacyjne w Polsce w 2019 roku*, www.stat.gov.pl/obszary-tematyczne [data dostępu: 28.02.2020 r.]

przetwarzanie informacji z wykorzystaniem technologii informacyjnych i komunikacyjnych stanowi znaczącą wartość ekonomiczną, społeczną i kulturową”. Społeczeństwo informacyjne opiera się na komunikacji elektronicznej⁵². Nie ma w zasadzie wątpliwości co do tego, iż rozwój społeczeństwa komunikacyjnego pociąga za sobą konieczność pewnych zmian technologicznych.

W celu ujednolicenia pojęć, które będą wykorzystane w tej pracy, jedynie sygnalizacyjnie, dla potrzeb tych rozważań, wskazać należy, iż przez usługi użyteczności publicznej należy rozumieć usługi o ogólnodostępnym charakterze, służące dobru ogółu społeczeństwa, a mające znaczenie dla interesów społeczno-gospodarczych.

Stopień wykorzystania usług użyteczności publicznej przez polskie społeczeństwo na podstawie przeprowadzonego badania

Jednym z czynników, za pomocą których możliwe jest scharakteryzowanie społeczeństwa przez pryzmat jego informacyjności, jest zasięg korzystania z usług użyteczności publicznej za pośrednictwem technologii mobilnych. Warto wskazać również, że postęp technologiczny wywiera wpływ na rozwój kompetencji cyfrowych odnotowanych w administracji publicznej, między innymi poprzez udostępnienie możliwości cyfrowego załatwiania szeregu spraw urzędowych.⁵³

Aktualnie w Polsce zdecydowana większość spraw przede wszystkim o charakterze administracyjnym, możliwa jest do zrealizowania za pomocą sieci teleinformatycznej. Społeczeństwu udostępniony został szeroki katalog rozwiązań mających na celu przyspieszenia realizacji wielu czynności w kluczowych dziedzinach. Najbardziej popularnymi platformami, których funkcjonowanie przebiega na bardzo wysokim poziomie, posiadającymi zaawansowane struktury i umożliwiającymi realizację szerokiego zakresu czynności w wymiarze usług użyteczności publicznej jest profil zaufany oraz Internetowe Konto Pacjenta. Obie platformy mają status platform rządowych prowadzonych w domenie gov.pl. Na skutek pandemii koronawirusa w Polsce w latach 2020-2022 w sposób znaczny wzrosło zainteresowanie tymi usługami, co wynikało z ograniczenia możliwości bezpośredniego działania w sprawach dotyczących szeroko rozumianego zdrowia jak również dostępu do usług użyteczności publicznych obejmujących możliwość załatwienia spraw urzędowych w dotychczasowej formie. Z uwagi na fakt, iż wiedza w zakresie tych usług ma charakter w zasadzie charakter powszechny, zasygnalizować jedynie należy, iż fakt posiadania konta na profilu zaufanym umożliwia załatwienie spraw, w tym o charakterze urzędowym również na innych platformach oferowanych przez

⁵² A. Monarcha-Matlak, Obowiązki administracji w komunikacji elektronicznej, 2008, s. 48.

⁵³ D. Cendrowicz, Rozwój e-kompetencji w administracji publicznej na przykładzie pomocy społecznej, Wrocław 2021, s. 78.

administrację publiczną. Natomiast Internetowe Konto Pacjenta umożliwia dostęp do informacji dotyczących wystawionych recept, zwolnień, przeprowadzonych zabiegach lekarskich, odbytych wizytach i innych, co bezpośrednio wskazuje na przydatność tych informacji z perspektywy możliwości dostępu do nich na odległość bez konieczności bezpośredniego dostępu do dokumentacji medycznej.

W związku z tym, iż fakt skutecznego obowiązywania usług tego rodzaju niejako determinuje społeczeństwo informacyjne, przeprowadzono badanie ilościowe w dwóch grupach badawczych, z której pierwsza grupa składała się ze 100 członków znajdujących się w wieku produkcyjnym, to jest z osób pełnoletnich od 18 do 68 roku życia, obejmująca zarówno kobiety i mężczyzn, o różnym wykształceniu i statusie zawodowym. Drugą grupę badawczą stanowiły natomiast osoby w wieku szkolnym, to jest do 18 roku życia, również zarówno płci męskiej jak i żeńskiej – także w ilości 100 osób. Wybór grup badawczych podyktowany był koniecznością zapewnienia możliwie maksymalnego zróżnicowania w celu osiągnięcia wymiernych wyników badań. W związku z przeprowadzonym badaniem ilościowym, w ramach kilku pytań w kwestionariuszy ankiety zapytano badanych o korzystanie z usług tego rodzaju, przy czym poruszono również kwestię dostępu i korzystania z bankowości elektronicznej, która w związku z jej szerokim wykorzystaniem może zostać uznana za podobną do wyżej wymienionych usług. Członkowie pierwszej grupy badawczej, w wieku produkcyjnym, w zakresie pytania bezpośrednio odnoszącego się do korzystania z interfejsu bankowości elektronicznej, w 96% zadeklarowali się jako osoby korzystające z tej możliwości, co daje bardzo wysoki wynik, który w zasadzie nie stanowi zaskoczenia, albowiem aktualnie zdecydowana większość operacji finansowych dokonywana jest właśnie w ten sposób. 37% osób ankietowanych wskazało, iż korzysta z Internetowego Konta Pacjenta, a 59% z platformy profilu zaufanego. Zdaje się być to satysfakcjonującą liczbą z uwagi na liczbę osób badanych w ramach tej grupy badawczej. Niemniej jednak wskazać należy, iż ewentualne korzystanie z tych usług bez wątpienia podyktowane jest potrzebą. Oznacza to, że prawdopodobna jest sytuacja, że część osób z grupy badawczej nie znalazła się w sytuacji, w której potrzebowałyby korzystać z tych instrumentów, a gdyby taka sytuacja się zdarzyła – zarejestrowaliby swoje konta. Nadto 47% osób badanych wskazało, iż korzysta z możliwości umówienia wizyt u lekarza, w urzędach i instytucjach użyteczności publicznej przez Internet, co również wskazuje, iż mamy do czynienia bez wątpienia ze społeczeństwem informacyjnym w tym wymiarze na niezwykle zaawansowanym poziomie.

W celu przeprowadzenia analizy porównawczej w tym zakresie, co było bezpośrednim celem badań ilościowych, niezbędne jest przedstawienie wyników badań przeprowadzonych w ramach drugiej grupy badawczej, co dostarczyło pełnego obrazu przeprowadzonych badań i pozwoliło na sformułowanie satysfakcjonujących wniosków w tym zakresie. W zakresie korzystania z usług użyteczności publicznej poprzez technologie mobilne, w przypadku osób poniżej 18 roku życia aż 84% osób

korzysta z bankowości elektronicznej. Zaledwie 13% badanych opowiedziało się za dostępem do Internetowego Konta Pacjenta, 11% korzysta z platformy profilu zaufanego, a 24% osób wykorzystuje sieć teleinformatyczną do umówienia wizyt u lekarza czy w innych instytucjach. Porównując rzeczony wyniki z danymi uzyskanymi na podstawie badania ilościowego przeprowadzonego wśród grupy badawczej w wieku produkcyjnym, jednoznacznie wskazać należy, iż zdecydowanie niższy poziom korzystania z tych usług bezpośrednio podyktowany jest wiekiem grupy badawczej. Nie sposób dopatrzeć się innych okoliczności warunkujących te liczby, albowiem fakt niepełnoletności części grupy badawczej niejako pozbawia ich możliwości korzystania z usług o takim charakterze. Niemniej jednak całościowe rozpatrywanie tego zakresu pytań wprost wskazuje, iż 35% wszystkich członków grup badawczych korzysta z platformy profilu zaufanego oraz 25% z Internetowego Konta Pacjenta, zaś 90% korzysta z usług oferowanych przez bankowość elektroniczną.

Spółeczeństwo sieci

Przeprowadzone badanie wśród licznej grupy badawczej o zróżnicowanych cechach wskazuje, iż bezapelacyjnie odnaleźć w niej można zaawansowane cechy struktury społeczeństwa informacyjnego funkcjonującego na bardzo wysokim poziomie. Rozwój społeczeństwa informacyjnego podyktowany jest rozwojem technologicznym, który określa to społeczeństwo, nadając mu charakterystyczne cechy. Z uwagi na poczynione rozważania oraz przytoczone okoliczności, analizie poddać należy kwestię społeczeństwa sieci. O ile w doktrynie z powodzeniem funkcjonuje pojęcie społeczeństwa sieciowego rozumianego jako jeden z typów społeczeństwa, którego istotą jest sieć relacji społecznych oraz swobodny dostęp do uczestniczenia w różnych organizacjach i grupach społecznych czy kręgach zainteresowań przez jednostkę, o tyle na próżno szukać trafnej i kompleksowej definicji społeczeństwa sieci, które *stricte* związane jest wykorzystaniem nowych technologii przez społeczeństwo.

Przez społeczeństwo sieci należy rozumieć szczególny rodzaj społeczeństwa informacyjnego, w którym najistotniejszym czynnikiem jest w zasadzie nieograniczony dostęp do sieci teleinformatycznej, a w którym podstawowym sposobem komunikacji jest komunikacja elektroniczna. Niewątpliwie społeczeństwo sieci i jego byt uwarunkowane jest nieustannym rozwojem technologicznym, które nadaje mu formę, kształt i pewne cechy. Wśród czynników pozwalających zakwalifikować konkretne społeczeństwo do społeczeństwa sieci wskazać należy rozbudowaną strukturę dostępu do Internetu, którego łączy jest satysfakcjonująco szybkie, prowadzenie komunikacji za pośrednictwem sieci teleinformatycznej, pozyskiwanie w taki sam sposób podstawowych informacji, a także dokonywanie zwykłych, bieżących spraw życia codziennego przy wykorzystaniu usług sieciowych.

Niezależnie od wyżej przytoczonych okoliczności nie pozostawia w zasadzie wątpliwości fakt, iż nowe technologie odnoszą bezpośredni wpływ na sferę administracji publicznej i na poziom jej informatyzacji⁵⁴, a w konsekwencji na ukształtowanie nowych zagadnień w różnych aspektach administracji publicznej. W literaturze słusznie wskazuje się, iż administracja publiczna, aby pozyskać społeczną akceptację w warunkach rozwoju technologicznego, powinna wdrażać procesy mające na celu podwyższenie jej kultury informatycznej, w tym zwłaszcza związane z nabywaniem i rozwojem e-kompetencji⁵⁵.

Podsumowanie

Postęp technologiczny odnotowywany jest we wszystkich aspektach nie tylko życia codziennego, ale również obrotu publicznoprawnego. Niewątpliwie postęp technologiczny odnotowywany jest również wśród zawodów prawniczych, w tym również organów ścigania, które zmagają się z cyberprzestępczością ściśle powiązaną z nowymi technologiami. Niezależnie jednak od powyższego, nowe technologie determinują sposób działania organów administracji publicznej, wyznaczając kierunki jej rozwoju, a także bezpośrednio wpływając na dostęp oraz formę korzystania z usług użyteczności publicznej. Powyżej przytoczone wyniki przeprowadzonego badania ilościowego prowadzą do jednoznacznych wniosków w tym zakresie, dowodząc, iż polskie społeczeństwo w wysokim stopniu wykorzystuje nowe technologie w dostępie do usług użyteczności publicznej, ale również do bankowości elektronicznej. Fakt wysokiego poziomu wykorzystania nowych technologii, zwłaszcza sieci teleinformatycznej, determinuje konieczność analizy pojęcia społeczeństwa sieci, przy pomocy którego również można scharakteryzować polskie społeczeństwo.

Bibliografia

Literatura

1. Blicharz J., *Inteligentne miasta i sztuczna inteligencja. Wybrane aspekty teoretycznoprawne*, Wrocław 2023.
2. Blicharz J., Zacharko L., *Computerization of Public Administration and the Implications for Information Asymmetry* [w:] *Asymmetric Information in*

⁵⁴ J. Blicharz, L. Zacharko, *Computerization of Public Administration and the implications for information asymmetry*, [w:] *Asymmetric Information in Public Administration*, (red.) D. Centrowicz, A. Chrisidu-Budnik, Warszawa 2022, s. 13-21.

⁵⁵ Szerzej: D. Centrowicz, *Rozwój e-kompetencji w administracji publicznej na przykładzie pomocy społecznej w: Ewolucja elektronicznej administracji publicznej*, (red.) R. Kusik-Winter, J. Korczak, Wrocław 2021, s. 73-86.

- Public Administration* (red.) Cendrowicz D., Chrisidu-Budnik A., Warszawa 2022
3. Cendrowicz D., *Rozwój e-kompetencji w administracji publicznej na przykładzie pomocy społecznej*, [w:] Ewolucja elektronicznej administracji publicznej, (red.) Kusik-Winter R., Korczak J., Wrocław 2021.
 4. Monarcha-Matlak A., *Obowiązki administracji w komunikacji elektronicznej*, Wolters Kluwer Polska, Warszawa, 2008.
 5. Seweryn R., *Technologie informacyjne i komunikacyjne*, Warszawa 2017.
 6. Skoczylas D., *Aksjologiczny wymiar e-administracji i cyberbezpieczeństwa w kontekście potrzeb jednostki i wspólnoty* [w:] Duniewska Z. (red.), Karcz-Kaczmarek M. (red.), Wilczyński P. (red.), *Prawo administracyjne w służbie jednostki i wspólnoty*, Warszawa 2022.
 7. Sokołowski M., *Pojęcie usługi społeczeństwa informacyjnego* [w:] Dumkiewicz M. (red.), Kopaczyńska-Pieczniak K. (red.), Szczotka J. (red.), *Sto lat polskiego prawa handlowego. Księga jubileuszowa dedykowana Profesorowi Andrzejowi Kidybie. Tom I*, Warszawa 2020.
 8. Szpor G., *Urzędnicy w społeczeństwie informacyjnym*, [w:] Z. Niewiadomski (red.), *Prawo administracyjne*, Warszawa 2007.
 9. Wodnicka M., *Wpływ czwartej rewolucji przemysłowej na innowacyjność usługi*, „*Optimum Economic Studies*” 2021, nr 3.

Netografia

1. Społeczeństwo informacyjne w Polsce w 2019 r., www.stat.gov.pl/obszary-tematyczne [data dostępu: 28.02.2020 r.]

dr Emilia Gulińska

Uniwersytet Radomski im. Kazimierza Pułaskiego

ORCID: 0000-0002-1106-5067

Adres email: e.gulinska@urad.edu.pl

Elektroniczne zarządzanie dokumentacją w kontekście informatyzacji administracji publicznej

Electronic records management in the context of computerization of public administration

Streszczenie

Elektroniczne zarządzanie dokumentacją to system zapewniający obsługę dokumentów, spraw oraz procesów zachodzących wewnątrz danej instytucji w formie elektronicznej. Dzięki niemu istnieje możliwość szybkiego wyszukiwania przez użytkowników odpowiednich dokumentów, a także zmniejsza on czas potrzebny do przygotowania dokumentacji. Warto także zaznaczyć, że jest to narzędzie usprawniające funkcjonowanie administracji publicznej oraz umożliwiające komunikację pomiędzy organem administracji publicznej a obywatelem. Rozdział ma na celu analizę i ocenę regulacji elektronicznego zarządzania dokumentacją w kontekście informatyzacji administracji publicznej. W związku z tym, w rozdziale, odniesiono się do istoty elektronicznego zarządzania dokumentacją, a następnie przedstawione zostało pojęcie elektroniczne czynności kancelaryjne oraz problematyka wdrażania elektronicznego systemu zarządzania dokumentacją.

Wprowadzenie

Społeczeństwo jako zorganizowana grupa społeczna obejmująca ogół obywateli i inne mniejsze społeczności, na przestrzeni lat podlega nieustannym przeobrażeniom, rozwija się mentalnie, kulturowo, naukowo, tworzone są nowe wynalazki, czy też narzędzia pracy. Człowiek wciąż dąży do polepszenia warunków życiowych, do usprawnienia instrumentów wspomagających sprawne funkcjonowanie społeczeństwa. W kontekście zachodzących przemian upowszechniło się pojęcie społeczeństwa informacyjnego. Określa ono nowy system społeczeństwa, kształtujący się w krajach o wysokim stopniu rozwoju technologicznego, gdzie zarządzanie informacją, jej jakość, szybkość przepływu są zasadniczymi czynnikami konkurencyjności zarówno w przemyśle, jak i usługach, a stopień rozwoju wymaga

stosowania nowych technik gromadzenia, przetwarzania, przekazywania i użytkowania informacji⁵⁶.

Proces zmian technologicznych w administracji jest stale rozwijany i rozszerzany na kolejne obszary jej funkcjonowania, w tym również na zarządzanie dokumentacją. Obieg dokumentów w urzędzie musi odbywać się z zachowaniem wszelkich wymaganych standardów i norm prawnych. Jednocześnie proces ten powinien być możliwie sprawny i szybki. Wraz z rozwojem e-usług w administracji publicznej pojawiły się nowe wyzwania związane z pojawieniem się dokumentów w formie elektronicznej. Spowodowało to trudności z ich odbiorem, przetwarzaniem, przechowywaniem czy archiwizowaniem. Rozwiązaniem tych problemów mają być elektroniczne systemy zarządzania dokumentacją⁵⁷. Celem rozdziału jest analiza i ocena regulacji prawnych dotyczących elektronicznego zarządzania dokumentacją w kontekście informatyzacji administracji publicznej.

Istota elektronicznego zarządzania dokumentacją

System elektroniczne zarządzanie dokumentacją⁵⁸ to system teleinformatyczny umożliwiający elektronicznego zarządzania w nim czynności kancelaryjnych, dokumentowanie przebiegu załatwiania spraw oraz gromadzenie i tworzenie dokumentów elektronicznych⁵⁹. Analogiczne uregulowanie zostało zawarte w art. 6 ust. 1a ustawy o narodowym zasobie archiwalnym i archiwach, w myśl którego elektroniczne zarządzanie dokumentacją to system wykonywania czynności kancelaryjnych, dokumentowania przebiegu załatwiania i rozstrzygania spraw, gromadzenia i tworzenia dokumentacji w postaci elektronicznej z wykorzystaniem systemu teleinformatycznego⁶⁰. Warto także wspomnieć, że elektronicznemu zarządzaniu dokumentacją zostały przypisane trzy zadania. Pierwszym jest wykonywanie czynności kancelaryjnych, przez które należy rozumieć w szczególności przyjmowanie i rejestrowanie wpływającej korespondencji, nadawanie znaków kancelaryjnych sprawom lub pismom, łączenie pism w akta spraw oraz przechowywanie akt spraw zakończonych. Jako drugie zadanie systemu wskazano dokumentowanie przebiegu załatwiania i rozstrzygania spraw. Oznacza to zapewnienie, by na podstawie

⁵⁶ M. Ganczar, A. Sytek, *Informatyzacja administracji publicznej. Skuteczność regulacji*, Wyd. 1, Warszawa 2021, s. 18–19.

⁵⁷ K. Bobowska, *Bariery wdrażania elektronicznych systemów zarządzania dokumentacją w jednostkach administracji publicznej na przykładzie Urzędu Miejskiego w Świebodzicach*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu” 2021, vol. 65, nr 4, 2021, s. 21, https://dbc.wroc.pl/Content/112901/Bobowska_Bariery_wdrazania_elektronicznych_systemow_zarzadzania.pdf [data dostępu: 08.07.2023].

⁵⁸ Dalej: EZD.

⁵⁹ Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych, Dz. U. nr 14, poz. 67 ze zm., § 2 pkt 13.

⁶⁰ Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach, tj. Dz. U. z 2020 r. poz. 164 ze zm.

zarządzanej dokumentacji dało się w wiarygodny sposób odtworzyć przebieg każdej załatwianej sprawy oraz poznać treść i przesłanki podejmowanych w jej ramach rozstrzygnięć. Ostatnim zadaniem jest gromadzenie i tworzenie dokumentacji w postaci elektronicznej. Odnieść to należy nie tylko do dokumentacji, która pierwotnie ma taką postać. Z założenia ze wszystkich wpływających do danej instytucji dokumentów mających postać tradycyjną (najczęściej papierową) tworzone są ich cyfrowe odwzorowania i to one stanowią dokumentację załatwianych przez instytucję spraw oraz uczestniczą w kancelaryjnym obiegu dokumentacji⁶¹.

Należy podkreślić, że system ten służy do postępowania z dokumentami elektronicznymi ewidencjonowanymi i spełnia rolę archiwum zakładowego lub składnicy akt⁶². Zapewnia on integralność treści dokumentów i metadanych polegającą na zabezpieczeniu przed wprowadzaniem zmian, z wyjątkiem tych wprowadzanych w ramach ustalonych i udokumentowanych procedur. Zabezpiecza także przed wprowadzaniem zmian w dokumentach spraw załatwionych oraz przed usunięciem dokumentów z systemu, z wyjątkiem udokumentowanych czynności dokonywanych w ramach ustalonych procedur usuwania dokumentów: dla których upłynął okres przechowywania ustalony w wykazie akt, mylnie zapisanych, mogących stanowić zagrożenie dla prawidłowego funkcjonowania systemu, których usunięcie wymagane jest na podstawie przepisu prawa, prawomocnego orzeczenia sądu lub ostatecznej decyzji organu administracji. Zapewnia on stały i skuteczny dostęp do dokumentów oraz ich wyszukiwanie. Umożliwia odczytanie metadanych dla każdego dokumentu. Identyfikuje użytkowników i dokumentuje dokonywane przez nich zmiany w dokumentach i metadanych. Zapewnia kontrolę dostępu poszczególnych użytkowników do dokumentów i metadanych. Umożliwia odczytanie bez zniekształceń treści dokumentów wytworzonych przez podmiot, w którym działa system. Zachowuje dokumenty i metadane w strukturze określonej w przepisach wydanych na podstawie art. 5 ust. 2a ustawy o narodowym zasobie archiwalnym i archiwach⁶³, łącznie z możliwością prezentacji tej struktury. Zapewnia odtworzenie przebiegu załatwiania i rozstrzygania spraw. Wspomaga czynności

⁶¹ M. Konstankiewicz, Podstawy prawne funkcjonowania elektronicznego zarządzania dokumentacją w instytucjach naukowych i kulturalnych [w:] Rola archiwów w procesie wdrażania systemów elektronicznego zarządzania dokumentacją. Z doświadczeń archiwów szkół wyższych, instytucji naukowych i kulturalnych oraz państwowych i samorządowych jednostek organizacyjnych, (red.) A. Barciak, D. Drzewiecka, K. Peplowska, Wyd. 1, Katowice 2018, s. 18.

⁶² M. Konstankiewicz, Komentarz do art. 6 [w:] Narodowy zasób archiwalny i archiwa. Komentarz, (red.) M. Konstankiewicz, A. Niewęgłowski, Wyd. 1, Warszawa 2016, s. 104–127.

⁶³ Minister właściwy do spraw informatyzacji, po zasięgnięciu opinii Naczelnego Dyrektora Archiwów Państwowych, określi, w drodze rozporządzenia, niezbędne elementy struktury dokumentów elektronicznych powstałych i gromadzonych w organach państwowych i państwowych jednostkach organizacyjnych oraz w organach jednostek samorządu terytorialnego i samorządowych jednostkach organizacyjnych, uwzględniając minimalne wymagania dla rejestrów publicznych i wymiany informacji w formie elektronicznej, a także potrzebę zapewnienia integralności dokumentów elektronicznych.

związane z klasyfikowaniem i kwalifikowaniem oraz grupowaniem dokumentów w akta spraw na podstawie wykazu akt. Wspomaga i dokumentuje proces brakowania dokumentów stanowiących dokumentację niearchiwalną, w tym: wyodrębnia automatycznie dokumenty przeznaczone do brakowania oraz przygotowuje automatycznie spis dokumentacji niearchiwalnej. Wspomaga czynności związane z przygotowaniem dokumentów stanowiących materiały archiwalne i ich metadanych do przekazania do archiwum państwowego, w tym: wyodrębnia automatycznie dokumenty przeznaczone do przekazania, przygotowuje automatycznie spis zdawczo-odbiorczy, w postaci dokumentu elektronicznego, eksportuje dokumenty i ich metadane, jak również oznacza dokumenty przekazane do archiwum państwowego w sposób umożliwiający ich odróżnienie od dokumentów nieprzekazanych. System ten umożliwia także przesyłanie dokumentów do innych systemów teleinformatycznych, w szczególności przez: eksport dokumentów i ich metadanych lub wskazań na te metadane oraz danych dokumentujących dokonane zmiany, z zachowaniem powiązań pomiędzy tymi dokumentami i metadanymi, jak również zapisywanie wyeksportowanych metadanych w formacie XML⁶⁴.

Należy podkreślić, że zarządzanie informacją w systemie EZD wymaga przestrzegania zasad kontroli przetwarzania informacji. Konieczne jest przywracanie spójności informacji, które obejmuje: korygowanie błędów w danych źródłowych i wynikowych realizowane poprzez niedopuszczenie do zapisania nieprawidłowych informacji w zbiorach maszynowych, cofanie nieprawidłowo wykonanych operacji, spowodowanych przez użytkownika, przez neutralizację skutków zakłóceń w toku eksploatacji oraz odtwarzanie zbiorów informacji i stanu systemu na wypadek awarii sprzętu lub oprogramowania przez doprowadzenie do stanu umożliwiającego prawidłową kontynuację dalszych procesów użytkowych⁶⁵.

Elektroniczne czynności kancelaryjne

Zgodnie z Instrukcją kancelaryjną, stanowiącą załącznik do rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r., czynności kancelaryjne w systemie elektronicznego zarządzania dokumentacją polegają na:

1. prowadzeniu rejestru przesyłek wpływających i wychodzących oraz spisów spraw,
2. wykonywaniu dekretacji,
3. wykonywaniu akceptacji, w szczególności przez podpisanie dokumentów elektronicznych odpowiednim podpisem elektronicznym, jeżeli odrębne przepisy

⁶⁴ Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi, Dz. U. nr 206, poz. 1518 ze zm., § 6.

⁶⁵ J. Adamus-Kowalska, Proces informatyzacji administracji publicznej i jego wpływ na kształtowanie narodowego zasobu archiwalnego stanowiącego dziedzictwo kulturowe ludzkości, Wyd. 1, Katowice 2021, s. 161.

- określają, jakiego rodzaju podpisu elektronicznego wymienionego w przepisach o podpisie elektronicznym wymaga się do podpisania danego pisma,
4. prowadzeniu możliwych do zrealizowania w systemie EZD innych potrzebnych rejestrów lub ewidencji, z wyłączeniem rejestrów lub ewidencji prowadzonych w dedykowanych do załatwiania określonych rodzajów spraw systemach teleinformatycznych innych niż EZD,
 5. gromadzeniu przyporządkowanych do właściwych spraw wszelkich dokumentów elektronicznych mających znaczenie dla udokumentowania przebiegu załatwiania i rozstrzygnięcia tych spraw⁶⁶.

Trzeba też wskazać, powtarzając za Ewą Wiktorowską, na obowiązkową rejestrację wiadomości mailowych będących dokumentami ewidencjonowanymi wpływającymi na skrzynki e-mail opublikowane na stronach Biuletynu Informacji Publicznej danego podmiotu. Z wiadomości wpływających na indywidualne skrzynki poczty elektronicznej pracowników jako przesyłki wpływające rejestruje się tylko te istotne dla załatwiania spraw, np. przesyłki wszczynające sprawę lub ją kończące. Wiadomości mailowe o znaczeniu roboczym dołącza się do elektronicznych spraw bez takiej rejestracji. To samo dotyczy maili, które sami wysyłamy w ramach prowadzonych spraw. Jeśli prowadzimy dłuższą roboczą korespondencję, to może, co do zasady, wystarczyć zachowanie ostatniej wiadomości, o ile zawiera ona treść wszystkich poprzednich. Wiadomości poczty elektronicznej wraz z załącznikami dołącza się do spraw jako pliki elektroniczne w oryginalnym formacie (tj. pliki z rozszerzeniami .eml, .msg, .mbx), po ich skopiowaniu z programu pocztowego. Po upływie określonego czasu dokumentacja, zarówno tradycyjna, jak i elektroniczna, jest przejmowana przez archiwum zakładowe, następnie (znow po określonym czasie) materiały archiwalne będą podlegały przekazaniu do archiwum państwowego, a dokumentacja niearchiwalna może być brakowana⁶⁷.

Wdrożenie systemu elektronicznego zarządzania dokumentacją

Problematyka wdrażania elektronicznego zarządzania dokumentacją obejmuje na wstępie podjęcie decyzji przez kierownika podmiotu o wyborze tego systemu jako podstawowego. Oznacza to zmianę dotychczas stosowanego systemu tradycyjnego. Zmiana sposobu wykonywania czynności kancelaryjnych niewątpliwie musi być rozpatrywana w kategoriach dużej zmiany organizacyjnej⁶⁸. Analiza zmiany

⁶⁶ Załącznik nr 1 do rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych, Dz. U. nr 14, poz. 67 ze zm., § 10.

⁶⁷ E. Wiktorowska, Komentarz do art. 10 b [w:] Prawo zamówień publicznych. Komentarz aktualizowany, (red.) E. Wiktorowska, I. Skubiszak-Kalinowska, Warszawa 2020, LEX, [data dostępu: 09.07.2023].

⁶⁸ J. Adamus-Kowalska, Wdrażanie systemu elektronicznego zarządzania dokumentacją w administracji publicznej w kontekście informatyzacji i zarządzania zmianą, „Archeion” 2018, t. 119, s. 150, <https://www.>

organizacyjnej, w ujęciu informatyzacji administracji publicznej obejmuje dwa obszary: wewnętrzny i zewnętrzny. Obszar wewnętrzny dotyczy: wdrożenia narzędzi teleinformatycznych systemu EZD, eliminacji dokumentów papierowych wewnątrz urzędu, wyznaczenia koordynatora czynności kancelaryjnych oraz nadania mu odpowiednich uprawnień w systemie, zmiany wewnętrznych przepisów regulujących sposób prowadzenia spraw, a ponadto przeszkoleń i wdrożenia pracowników do pracy w systemie EZD, jak również ciągłego doskonalenia i motywowania pracowników do pracy w wyżej wskazanym systemie. Natomiast obszar zewnętrzny odnosi się do takich elementów jak:

1. komunikacji z podmiotami zewnętrznymi za pośrednictwem elektronicznych kanałów przepływu informacji,
2. cyfryzacji usług publicznych przez szersze wykorzystanie dedykowanych systemów do obsługi zadań wykonywanych przez administrację,
3. eliminacji dokumentów papierowych wysyłanych na zewnątrz urzędu,
4. tworzenia i wykorzystywania nowoczesnych aplikacji służących do komunikacji z administracją publiczną, w szczególności na urządzenia mobilne,
5. stałego monitorowania poziomu wykorzystania narzędzi elektronicznych do komunikacji administracji publicznej oraz okresową ocenę urzędów pod względem poziomu informatyzacji⁶⁹.

Wprowadzając zmiany w jednostkach organizacyjnych ich kierownicy są zobowiązani realizować zadania oraz nadawać uprawnienia decyzyjne poszczególnym pracownikom instytucji. Zadania, które należy uwzględnić w zarządzaniu zmianą to m.in. ugruntowanie przekonania o konieczności dokonania zmiany, stworzenie zespołu sterującego procesem zmian oraz zespołu realizującego zadania związane z wdrożeniem systemu EZD, wypracowanie wizji oraz strategii, nadanie pracownikom, uczestniczącym w pracach nad zmianą, uprawnień w celu podejmowania określonych działań o wieloaspektowym zakresie decyzyjności, określenie krótkoterminowych korzyści, zespolenie korzyści z początkowej fazy działań, przy równoczesnym zachęcaniu do kolejnych zmian i ostatecznie ugruntowanie wprowadzonych zmian w kulturze organizacyjnej. Cykl zarządzania zmianą można przeprowadzić według ośmiu etapów. Na wstępie należałoby zidentyfikować potrzeby i określić przyczyny zmian. Kolejny etap opierałby się o formalne zaakceptowanie potrzeby zmiany co powinno być wyrażone w zaangażowaniu się osób decyzyjnych w tym procesie. Trzecia faza prac polegać powinna na analizie jednostki organizacyjnej i jej otoczenia celem wskazania aktualnego stanu. Następnym równie istotnym zadaniem jest zaproponowanie wizji przyszłej struktury

ejournals.eu/Archeion/2018/119/art/15715/ [data dostępu: 09.07.2023].

⁶⁹ B. Koszel-Pleskaczuk, K. Pleskaczuk, Elektroniczne zarządzanie dokumentacją jako instrument zarządzania organizacją. Case study uczelni wyższej, „Akademia Zarządzania” 2020, nr 4 (2), s. 224–225, <https://depot.ceon.pl/handle/123456789/18624> [data dostępu: 09.07.2023].

jednostki organizacyjnej poprzez wskazanie celów według zasady SMART i wskazanie oczekiwanych efektów. W etapie piątym należy uzgodnić strukturę jednostki organizacyjnej uwzględniając potrzebę przeprowadzenia modyfikacji obecnej struktury. W dalszych pracach wymagane jest opracowanie planu zmian z użyciem dostępnych narzędzi i technik. Ostatnie etapy odnoszą się do wdrożenia i koordynacji planu zmian, a także umocnienia wprowadzonej zmiany⁷⁰.

Warto także podkreślić, że po wskazaniu systemu EZD jako podstawowego sposobu dokumentowania przebiegu załatwiania i rozstrzygania spraw ponowne wskazanie systemu tradycyjnego jest niedopuszczalne⁷¹. Celem takiego uregulowania jest zabezpieczenie kontynuacji pracy w systemie EZD, tak aby uniknąć możliwości powrotu do systemu tradycyjnego. Założono bowiem, że jeżeli inwestuje się w informatyzację, to po osiągnięciu założonego celu kontynuacja wykorzystywania dzięki temu możliwości jest oczywista. W sposób pośredni przyczynia się to także do stawiania wymagań posiadania umiejętności komputerowych pracownikom urzędów, a także dla samych wójtów, burmistrzów, prezydentów miast, starostów, marszałków województw co najmniej na takim poziomie, by mogli wykonywać przypisane im w systemie czynności kancelaryjne⁷².

W podmiocie, w którym wybrano EZD jako system podstawowy, dokumentacja w postaci papierowej jest skanowana i zatrzymywana w punkcie przyjęć korespondencji w ramach składu chronologicznego. W systemie klasy EZD naturalne dokumenty elektroniczne i odwzorowania cyfrowe dokumentów papierowych są rejestrowane, obsługiwane, gromadzone i przechowywane poprzez pogrupowanie w akta sprawy lub dokumentację nietworzącą akt spraw. Sprawy w całości po stronie podmiotu dokumentowane są w postaci elektronicznej i tak są archiwizowane. System klasy EZD pełni równocześnie funkcję archiwum zakładowego (składnicy akt). Funkcjonują zarówno składy chronologiczne, jak i składy informatycznych nośników danych. Dekretacje i akceptacje dokonywane są w systemie klasy EZD, przy czym w przypadku ostatecznej akceptacji dokumentu jest on podpisywany kwalifikowanym podpisem elektronicznym. Instytucja wykorzystująca w swojej organizacji system EZD może przysyłać dokumenty w postaci papierowej, ale w swoich aktach sprawy zachowuje odpowiednik tego dokumentu w postaci elektronicznej podpisany podpisem elektronicznym⁷³.

W kwietniu 2023 r. w Rządowym Centrum Legislacji został zamieszczony projekt ustawy o zmianie niektórych ustaw w związku z rozwojem e-administracji. Projekt

⁷⁰ Ibidem, s. 225–226.

⁷¹ Załącznik nr 1 do rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r., op. cit., § 1 pkt. 4.

⁷² G. Szpor (red.), Dokumentacja elektroniczna w podmiotach publicznych, Wyd. 1, Warszawa 2013, s. 85.

⁷³ E. Perłakowska, Elektroniczne zarządzanie dokumentacją [w:] Procedury elektronicznego zarządzania dokumentacją, (red.) A. Prasal, E. Perłakowska, G. Abgarowicz, Wyd. 1, Warszawa 2023, s. 130.

ten wprowadza szereg zmian w różnych ustawach, m. in.: w ustawie o narodowym zasobie archiwalnym i archiwach, w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne czy w ustawie o doręczeniach elektronicznych. W ustawie o narodowym zasobie archiwalnym i archiwach zaproponowano nałożenie na podmioty publiczne obowiązku prowadzenia systemu elektronicznego zarządzania dokumentami. Wdrożenie systemu EZD i wykonywanie w nim czynności kancelaryjnych nie jest jednoznaczne z prowadzeniem wszystkich rodzajów spraw w postaci elektronicznej. Wyjątki od EZD określa każdorazowo kierownik danej jednostki, gdy przepisy prawa ustalają sposób dokumentowania przebiegu załatwiania spraw dla określonych rodzajów dokumentacji oraz w sytuacji, gdy istnieją ważne przyczyny organizacyjne i techniczne uniemożliwiające prowadzenie spraw w postaci elektronicznej. Sposoby prowadzenia określonych rodzajów dokumentów zawarte są w przepisach odrębnych i to one określają czy dana dokumentacja będzie prowadzona elektronicznie w systemie EZD czy papierowo. Jednostki organizacyjne uzgadniają przepisy kancelaryjno – archiwalne z właściwymi miejscowo archiwami państwowymi, wprowadzając te przepisy same dla siebie lub mają je narzucone przepisami prawa. Wpływają one również na przyjęty moduł wdrożenia systemu. Zaproponowana zmiana dotyczy EZD jako sposobu wykonywania czynności kancelaryjnych, a nie EZD jako systemu klasy EZD, w którym te czynności są wykonywane co sprowadza się do tego, że część instytucji interpretuje to w ten sposób, iż nie będzie tzw. wyjątków od EZD, czyli spraw dokumentowanych papierowo czy w systemach dziedzicznych lub możliwości postępowania z dokumentacją niejawną zgodnie z przepisami o ochronie informacji niejawnych⁷⁴.

W ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne zaproponowano dodanie komorników sądowych do katalogu podmiotów, wobec których stosowane są przepisy tej ustawy. Druga ze zmian dotyczy przygotowania przez ministra właściwego do spraw informatyzacji strategii transformacji cyfrowej państwa. Strategia uwzględni dotychczas zrealizowane działania oraz poziom zastosowania nowoczesnych technologii w administracji publicznej na rzecz obywateli, weźmie pod uwagę założenia komplementarnych dokumentów strategicznych i programowych rządu w tym obszarze. Projekt wprowadza także rozwiązania wskazujące tryb postępowania, zarówno podmiotów publicznych jak i podmiotów zobowiązanych do wykonania określonych czynności, w przypadku niedostępności systemu teleinformatycznego albo środków komunikacji elektronicznej do przekazywania danych. Proponowane przepisy wprowadzają po stronie podmiotów publicznych obowiązek udostępniania w Biuletynie Informacji Publicznej informacji o zaistniałym zdarzeniu a także możliwość, o ile jest taka potrzeba i rozwiązania techniczne

⁷⁴ Projekt ustawy o zmianie niektórych ustaw w związku z rozwojem e-administracji, <https://www.gov.pl/web/krmc/projekt-ustawy-o-zmianie-niektorych-ustaw-w-zwiazku-z-rozwojem-e-administracji> [data dostępu: 13.07. 2023].

na to pozwalają, wskazania trybu postępowania. Mając jednak na uwadze, że niedostępność systemu może spowodować po stronie podmiotów zobowiązanych do wykonania określonej czynności uchybienie terminu do jej wykonania proponowane przepisy przewidują rozwiązania umożliwiające przywrócenie tego terminu i możliwość odstąpienia od nałożenia kary pieniężnej tak, aby obywatel nie ponosił odpowiedzialności za niedostępność systemu. Celem nowelizacji jest również umocowanie Rejestru Pełnomocnictw Elektronicznych, którego przeznaczeniem jest gromadzenie informacji o pełnomocnictwach udzielanych między osobami fizycznymi posiadającymi numer PESEL. Z punktu widzenia obywatela, wprowadzany rejestr pozwoli na zarządzanie wszystkimi pełnomocnictwami elektronicznymi z poziomu jednego punktu dostępu oraz zagwarantuje mu pewność honorowania takiego pełnomocnictwa jeśli taka możliwość będzie prawnie przewidziana. Proponuje się także dodanie rozdziału „Elektroniczne zarządzanie dokumentacją” w ramach którego wprowadzone zostaną podstawy prawne dla funkcjonowania oprogramowania służącego do elektronicznego zarządzania dokumentacją, umożliwiającego wykonywanie czynności kancelaryjnych, dokumentowanie przebiegu załatwiania i rozstrzygania spraw, gromadzenie i tworzenie dokumentacji w postaci elektronicznej, a także archiwizowanie przetwarzanej dokumentacji⁷⁵.

Natomiast zmiany w ustawie o doręczeniach elektronicznych zmierzają do maksymalnego uproszczenia usług dla obywateli, wprowadzają jednolitą skrzynkę ePUAP i e-Doręczeń, regulują zasady logowania do skrzynki i nadawania adresu elektronicznego oraz wprowadzają możliwość umocowania wielu administratorów. Wprowadzają także kwalifikowalność publicznej usługi rejestrowanego doręczenia elektronicznego (PURDE), dookreślają moment doręczenia wiadomości, a także zakres danych koniecznych do złożenia wniosku, gdzie minister właściwy ds. informatyzacji w wydawanym przez siebie rozporządzeniu określi zakres tych danych⁷⁶.

Podsumowanie

Konkludując, elektroniczne zarządzanie dokumentacją to system zapewniający obsługę dokumentów, spraw oraz procesów zachodzących wewnątrz danej instytucji w formie elektronicznej. Dzięki niemu istnieje możliwość szybkiego wyszukiwania przez użytkowników odpowiednich dokumentów, a także zmniejsza on czas potrzebny do przygotowania dokumentacji. Warto także zaznaczyć, że jest to narzędzie usprawniające funkcjonowanie administracji publicznej oraz umożliwiające komunikację pomiędzy organem administracji publicznej a obywatelem. Zatem proponowane przez ustawodawcę zmiany w ustawie o narodowym zasobie

⁷⁵ Ibidem.

⁷⁶ Ibidem.

archiwalnym i archiwach, w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne oraz w ustawie o doręczeniach elektronicznych, moim zdaniem należy ocenić pozytywnie, gdyż przyczyniają się one do tego, że administracja publiczna staje się bardziej sprawna i przyjazna obywatelowi, co przekłada się także na większe zaufanie podmiotów administrowanych do organu władzy publicznej.

Bibliografia

Akty prawne

1. Ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach, tj. Dz. U. z 2020 r. poz. 164 ze zm.
2. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 30 października 2006 r. w sprawie szczegółowego sposobu postępowania z dokumentami elektronicznymi, Dz. U. nr 206, poz. 1518 ze zm.
3. Rozporządzenie Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych, Dz. U. nr 14, poz. 67 ze zm.

Literatura

1. Adamus-Kowalska J., Proces informatyzacji administracji publicznej i jego wpływ na kształtowanie narodowego zasobu archiwalnego stanowiącego dziedzictwo kulturowe ludzkości, Wyd. 1, Katowice 2021.
2. Ganczar M., Sytek A., Informatyzacja administracji publicznej. Skuteczność regulacji, Wyd. 1, Warszawa 2021.
3. Konstankiewicz M., Komentarz do art. 6 [w:] Narodowy zasób archiwalny i archiwa. Komentarz, (red.) M. Konstankiewicz, A. Niewęglowski, Wyd. 1, Warszawa 2016.
4. Konstankiewicz M., Podstawy prawne funkcjonowania elektronicznego zarządzania dokumentacją w instytucjach naukowych i kulturalnych [w:] Rola archiwów w procesie wdrażania systemów elektronicznego zarządzania dokumentacją. Z doświadczeń archiwów szkół wyższych, instytucji naukowych i kulturalnych oraz państwowych i samorządowych jednostek organizacyjnych, (red.) A. Barciak, D. Drzewiecka, K. Pełowska, Wyd. 1, Katowice 2018.
5. Pełakowska E., Elektroniczne zarządzanie dokumentacją [w:] Procedury elektronicznego zarządzania dokumentacją, (red.) A. Prasał, E. Pełakowska, G. Abgarowicz, Wyd. 1, Warszawa 2023.
6. Szpor G. (red.), Dokumentacja elektroniczna w podmiotach publicznych, Wyd. 1, Warszawa 2013.

Netografia

1. Adamus-Kowalska J., Wdrażanie systemu elektronicznego zarządzania dokumentacją w administracji publicznej w kontekście informatyzacji i zarządzania zmianą, „Archeion” 2018, t. 119, <https://www.ejournals.eu/Archeion/2018/119/art/15715/> [data dostępu: 09.07.2023].
2. Bobowska K, Bariery wdrażania elektronicznych systemów zarządzania dokumentacją w jednostkach administracji publicznej na przykładzie Urzędu Miejskiego w Świebodzicach, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu” 2021, vol. 65, nr 4, 2021, s. 21, https://dbc.wroc.pl/Content/112901/Bobowska_Bariery_wdrazania_elektronicznych_systemow_zarzadzania.pdf [data dostępu: 08.07.2023].
3. Koszel-Pleskaczuk B., Pleskaczuk K., Elektroniczne zarządzanie dokumentacją jako instrument zarządzania organizacją. Case study uczelni wyższej, „Akademia Zarządzania” 2020, nr 4 (2), <https://depot.ceon.pl/handle/123456789/18624> [data dostępu: 09.07.2023].
4. Projekt ustawy o zmianie niektórych ustaw w związku z rozwojem e-administracji, <https://www.gov.pl/web/krmc/-projekt-ustawy-o-zmianie-niektorych-ustaw-w-zwiazku-z-rozwojem-e-administracji>, [data dostępu: 13.07. 2023].
5. Wiktorowska E., Komentarz do art. 10 b [w:] Prawo zamówień publicznych. Komentarz aktualizowany, (red.) Wiktorowska E., Skubiszak-Kalinowska I., Warszawa 2020, LEX, [data dostępu: 09.07.2023].

Inne

1. Załącznik nr 1 do rozporządzenia Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych, Dz. U. nr 14, poz. 67 ze zm.

Wpływ cyfryzacji administracji publicznej na obowiązek ochrony tajemnicy skarbowej przez Krajową Administrację Skarbową

The impact of digitalization in public administration on the duty of protection tax secrets by National Tax Administration

Streszczenie

Rozdział poświęcony jest wyjaśnieniu, czy i jakie skutki wywołała postępująca w organach podatkowych cyfryzacja ich działalności. Podjęto w nim próbę wskazania, co oznacza tajemnica skarbową i jakie dane obejmuje. Następnie też wymieniono jakie narzędzia elektroniczne organy podatkowe wykorzystują, a przez to służą do zbierania i przetwarzania informacji objętych tą tajemnicą. W konsekwencji, jakie zagrożenia wiążą się z ich wykorzystaniem dla ochrony tajemnicy skarbowej.

Wprowadzenie

W obecnych czasach szczególną rolę przede wszystkim w życiu społecznym odgrywa przede wszystkim informacja. Jest ona kluczowym czynnikiem wyznaczającym wiedzę oraz władzę, który również decyduje o bezpieczeństwie organizacji całych państw, jak i o bezpieczeństwie obywateli⁷⁷. Podkreśla to rozwój instrumentów służących jej rozpowszechnianiu, w tym zwłaszcza elektroniki, sieci Internet, powszechność urządzeń dostępu do nich i rozwój sieci społecznościowych⁷⁸. Jednocześnie rozwój społeczeństwa informacyjnego spowodował, że jednocześnie pojawiło się ważne wyzwanie zapewnienia bezpieczeństwa informacji⁷⁹, którego zapewnienie stało się obowiązkiem każdej organizacji będącej w posiadaniu informacji⁸⁰.

⁷⁷ K. Liderman, Bezpieczeństwo informacyjne, wyd. 1, Warszawa 2012, s. 11 i n.

⁷⁸ Ibidem.

⁷⁹ A. Suchorzewska, Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem, LEX/el.

⁸⁰ J. Kowalewski, M. Kowalewski, Polityka bezpieczeństwa informacji w praktyce, wyd. 1, Wrocław 2004, s. 21.

Znaczenie informacji, jej bezpieczeństwa jak i rozwój instrumentów wspomagających jej zbieranie i przetwarzanie, w tym wykorzystywaniem do swojej działalności, nie jest również obojętny dla administracji. Organy administracji publicznej realizując swoje zadania muszą mieć zapewniony dostęp do informacji oraz możliwości jej gromadzenia. Stąd też, postępujący również w administracji publicznej proces cyfryzacji odbywa się na wielu płaszczyznach, w różnorodny sposób dotyka strony stosunków administracyjnych, co powoduje też, że odbywa się wieloma sposobami, zmieniając tym również oblicza w zależności od umieszczonego kontekstu. Cyfryzacja odbywa się zarówno w kierunku poprawienia jakości usług i wykonywania zadań przez organy administracji publicznej, co powoduje, że wywołuje wewnątrz administracji, jak również bez wątpienia oddziałuje na zewnątrz, wpływając na obsługę i realizację praw i obowiązków przez administrowanych. Truizmem jest już stwierdzenie, że w takim ujęciu szeroko ujęta cyfryzacja prowadzi zarówno do negatywnych i pozytywnych skutków. W szczególności ma to znaczenie, gdy podkreślony zostanie związek informacji i informatyzacji i przede wszystkim skupi się na fakcie, że szeroko ujęta cyfryzacja dotyczy w szczególności usprawnienia przepływu informacji.

Z tego też powodu wydaje się, że szczególną uwagę należy skierować tam, gdzie ingerencja organów administracji publicznej w sferę praw i obowiązków jednostki ma z reguły charakter regulacyjno-represyjny oraz związana jest również z zachowaniem niejawności, w tym zwłaszcza z kwestiami tajemnic ustawowo chronionych. Ważnym i jednocześnie ciekawym przykładem dla analizy jest działalność Krajowej Administracji Skarbowej⁸¹, która w swojej działalności nie tyle zajmuje się zarówno ilościowym, jak i jakościowym szerokim zakresem informacji, ale również dysponuje informacjami poufnymi objętymi tajemnicą skarbową. Powoduje to, że proces cyfryzacji jej działalności napotyka na wiele wyzwań, a także prowadzi do wielu skutków i zagrożeń.

Zakres tajemnicy skarbowej w działalności KAS

Zgodnie z art. 129 Ordynacji podatkowej⁸², postępowanie podatkowe jest jawne, ale tylko dla stron. Oznacza to, że organy podatkowe nie mają prawa udzielania jakichkolwiek informacji o okolicznościach faktycznych bądź prawnych toczącej się sprawy komukolwiek poza stronami (jak też ich przedstawicielami bądź pełnomocnikami) prowadzonego postępowania⁸³. Ograniczenia jawności tego postępowania dopuszczalne są wyłącznie na podstawie prawne, jednym z nich jest tajemnica skarbową

⁸¹ Dalej: KAS.

⁸² Ustawa z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa t.j. Dz. U. z 2023 r. poz. 2383 z późn. zm., dalej: „o.p.”.

⁸³ Wyrok WSA w Poznaniu z dnia 11 lipca 2019 r., I SA/Po 357/19, LEX nr 2704635.

uregulowana w art. 293 i n. o.p. z jednej strony służy ona ochronie prywatności podmiotów indywidualnych, z drugiej również interesowi publicznemu. Konieczność jej ochrony wynika również ze ścisłego powiązania z innymi tajemnicami, w tym zwłaszcza bankową, przedsiębiorstwa, przedsiębiorcy, czy handlową. Z tego też względu wskazuje się, że ma ona chronić przede wszystkim podatnika, co powoduje, że związane są ją (jako typem tajemnicy służbowej) w szczególności organy⁸⁴.

Chociaż w o.p. zauważalny jest brak bezpośredniego uregulowania jej istoty, to na zasadzie art. 293 o.p. wskazuje się, że mają to być informacje indywidualne⁸⁵ dotyczące płatników lub inkasentów. Każda tego rodzaju informacja, nawet jeżeli nie dotyczy bezpośrednio obowiązków podatkowych, stanowi tajemnicę skarbową. Dlatego w pełni należy podzielić pogląd, że dane dotyczące podmiotu składającego deklarację są immanentną częścią deklaracji i one także, poza pozostałymi danymi ujętymi w deklaracji, objęte są tajemnicą skarbową⁸⁶. Chodzi tu w szczególności dane osobowe (imiona, nazwisko, nazwisko rodowe, imiona rodziców), PESEL, NIP, stan cywilny, osoby pozostające na ich utrzymaniu⁸⁷, a także źródeł i wysokości osiąganych przychodów oraz rodzajów i wysokości poniesionych wydatków (kosztów), a także zapłaconych zaliczek na podatek⁸⁸ oraz dotyczące spadkodawcy, zapisodawcy, pożyczkodawcy itp.⁸⁹ Poza tym wskazuje się też, że rozciągają się one również na indywidualne dane, czyli fakty, liczby i informacje, dotyczące materiałów służących do ustalania obowiązku podatkowego oraz przekształcenia go w zobowiązanie podatkowe. Powoduje to, że dane odnoszące się do podmiotu składającego deklarację podatkową są nieodłączną częścią deklaracji i one również, oprócz pozostałych zawartych w niej danych, objęte są tajemnicą skarbową⁹⁰.

Powyższe wskazuje, że zakres tajemnicy skarbowej jest wobec tego bardzo szeroki⁹¹. Są to wszystkie informacje przekazywane organom podatkowym w sprawach

⁸⁴ Wyrok WSA we Wrocławiu z dnia 27 czerwca 2012 r., IV SA/Wr 154/12, Legalis.

⁸⁵ Jak się zauważa, brzmienie przepisu art. 293 o.p. oznacza, że w trybie ustawy o dostępie do informacji publicznej mogą być udzielane jedynie informacje zbiorcze o podatnikach, nie mogą być natomiast udzielane żadne informacje indywidualne (por. wyrok NSA z dnia 2.02.2005 r., OSK 1060/04, CBOSA).

⁸⁶ Wyrok NSA z dnia 20 lutego 2020 r., I OSK 1844/18, LEX nr 3022094.

⁸⁷ Wyrok NSA z dnia 20 kwietnia 2017 r., I OSK 1785/15, Legalis.

⁸⁸ Wyrok NSA z 3 lutego 2022 r., III OSK 4926/21, LEX nr 3331078.

⁸⁹ Por. J. Brolik i in., *Ordynacja podatkowa. Komentarz*, Warszawa 2013, LEX/el, Komentarz do art. 293.

⁹⁰ Por. wyr. NSA z dnia 20 lutego 2020 r., I OSK 1844/18, Legalis.

⁹¹ B. Adamiak, J. Borkowski, R. Mastalski, J. Zubrzycki, *Ordynacja podatkowa*, Warszawa 2009, s. 1106. Jak stwierdził WSA we Wrocławiu w wyroku z dnia 27.6.2012 r. (IV SA/Wr 154/12, Legalis): „Taką tajemnicą ustawowo chronioną jest tajemnica skarbową, jako szczególny rodzaj tajemnicy służbowej, zatem jej granice muszą być zakreślone szeroko. Z opodatkowaniem związane są bowiem zjawiska gospodarcze, a niejednokrotnie wiąże się ono z indywidualnymi przejawami życia jednostki, co wymaga ścisłego przestrzegania zawodowej dyskrecji dotyczącej wszelkich informacji, jakie pozyskiwane są dla potrzeb stosowania prawa podatkowego. Pozyskiwanie informacji oraz ich przekazywanie innym podmiotom, musi się poza tym odbywać z poszanowaniem prawa dla ochrony prywatności, zważywszy że indywidualne dane zawarte w składanych

daninowych i w sprawach karnych skarbowych, bez względu na podmiot, który je przekazuje, objęte są tajemnicą skarbową. Przekłada się to też na jej przedmiot, który w art. 293 o.p. uregulowano w sposób kazuistyczny, przez co obejmuje ona wszystkie indywidualne dane zawarte we wszelkich dokumentach składanych przez podatników, płatników i inkasentów⁹². Oznacza to, że tajemnicą objęte są informacje zawarte w każdym dokumencie będącym w posiadaniu organu podatkowego, który pozwala zidentyfikować konkretny podmiot i który został do organu podatkowego przekazany w trybie określonym przepisami prawa⁹³. Są to wobec tego dane wynikające w szczególności z deklaracji, przez które rozumieć też należy zeznania, wykazy, zestawienia i informacje, czyli każdy dokument, pozwalający zidentyfikować konkretny podmiot, przekazany przez podatnika, płatnika czy inkasenta, objęty jest tajemnicą skarbową⁹⁴.

Poza tym, zgodnie z art. 293 § 2 o.p. tajemnicą skarbową objęte są też, dane zawarte w informacjach podatkowych przekazywanych organom podatkowym przez osoby i podmioty wymienione m. in. w art. 82-82b o.p., jak również informacje uzyskane przez organy podatkowe z banków i innych źródeł niż wymienione w art. 293 § 1 lub w § 2 pkt 1, np. z takich instytucji finansowych, jak: domy maklerskie, towarzystwa funduszy powierniczych, towarzystwa funduszy inwestycyjnych, dobrowolne fundusze emerytalne, banki prowadzące działalność maklerską, ale też Najwyższej Izby Kontroli czy innych organów kontroli i ochrony prawa, będą również objęte tajemnicą skarbową.

Precyzując znaczenie tajemnicy skarbowej w celu rozwiania wątpliwości w działalności organów administracji publicznej, Minister Finansów w piśmie z dnia 26 marca 1998 r., FB 1/235/CH/98⁹⁵ wskazał, że tajemnicą skarbową objęte są: dane zawarte w deklaracjach oraz innych dokumentach składanych przez podatników, płatników lub inkasentów oraz uzyskane z innych źródeł (art. 293 § 1 i 2 pkt 1 i 4 o.p.); akta spraw prowadzonych przez organy podatkowe i organy kontroli skarbowej (art. 293 § 2 pkt 2 i 3 o.p. oraz art. 34a ust. 3 ustawy o kontroli skarbowej); informacje sporządzane i przetwarzane w ramach kontroli skarbowej (art. 34 ust.

przez nich dokumentach podatkowych zawierają wiele informacji ze sfery prywatności. Każdy przypadek udostępniania danych zawartych we wszelkich dokumentach podatkowych jest ściśle unormowany, tak co do podmiotów, którym można udostępniać te dane, jak i zakresu, w jakim to może nastąpić. Regułą jest wykorzystywanie informacji znajdujących się w posiadaniu organu podatkowego tylko wewnątrz jego struktur organizacyjnych i wyłącznie dla potrzeb podatkowych, natomiast wszelkie wyjątki muszą być *expressis verbis* określone przepisami prawa”.

⁹² Por. S. Babiarz, B. Dauter, B. Gruszczyński, R. Hauser, A. Kabat, M. Niezgódka - Medek, *Ordynacja podatkowa. Komentarz*, Warszawa 2009, s. 977.

⁹³ A. Biegalski, M. Kuciewicz, *Prawo do prywatności a systemy wymiany informacji w sprawach podatkowych*, cz. II, *Prokuratura i Prawo*, 2008, nr 9, s. 17-22.

⁹⁴ Ibidem, a także: Wyrok NSA z dnia 3 lutego 2022 r., III OSK 4926/21, LEX nr 3331078.

⁹⁵ Pismo z dnia 26.03.1998 r., wydane przez: Ministerstwo Finansów, FB 1/235/Ch/98, *Tajemnica skarbowa. Udostępnienie akt, „Prawo Przedsiębiorcy”* 1998, nr 33-34, str. 19.

1 i art. 7 ustawy o kontroli skarbowej)); informacje przekazane organom podatkowym przez osoby prawne, jednostki organizacyjne niemające osobowości prawnej oraz osoby fizyczne prowadzące działalność gospodarczą lub wykonujące wolny zawód o zdarzeniach wynikających ze stosunków cywilnoprawnych albo z prawa pracy, mogących mieć wpływ na powstanie obowiązku podatkowego lub wysokość zobowiązania podatkowego osób lub jednostek, z którymi zawarto umowę, oraz o umowach zawartych z osobami zagranicznymi (art. 82 § 1 o.p.); wystąpienia naczelników urzędów skarbowych, Generalnego Inspektora Kontroli Skarbowej i dyrektorów urzędów kontroli skarbowej do banków, domów (biur) maklerskich, towarzystw funduszy powierniczych i towarzystw funduszy inwestycyjnych o udzielenie informacji i uzyskane tą drogą informacje (art. 182 i 184 § 2 i 4 o.p. oraz art. 33 i 33a ustawy o kontroli skarbowej); informacje o powstaniu zobowiązań podatkowych przekazane organom podatkowym przez sądy, komorników sądowych i notariuszy oraz wystąpienia i informacje z zakresu działalności gospodarczej i informacje uzyskane tą drogą przez dyrektora urzędu kontroli skarbowej od wydawców i redaktorów (art. 84 o.p. i art. 35 ustawy o kontroli skarbowej); wystąpienia o informacje oraz otrzymane tą drogą informacje dotyczące numerów rachunków bankowych osób prawnych, jednostek organizacyjnych nieposiadających osobowości prawnej oraz osób fizycznych prowadzących działalność gospodarczą lub wykonujących wolny zawód oraz danych umożliwiających identyfikację posiadaczy tych rachunków (art. 82 § 2 i 3 o.p.); wystąpienia do instytucji finansowych o udzielenie informacji o zdarzeniach stanowiących podstawę do skorzystania przez podatnika z ulg podatkowych, jeżeli zostały wykazane w deklaracjach złożonych przez podatnika, i informacje uzyskane tą drogą (art. 275 § 2 i 3 o.p.). Oznacza to, że objęte są nią dane zawarte w dokumentacji wszystkich procedur prowadzonych przez organy podatkowe, ich rachunkowości, jak również w aktach postępowań w sprawach karnych skarbowych⁹⁶, a to w postępowaniach: podatkowych, kontrolnych, kontrolach celno-skarbowych, czynnościach sprawdzających, czy postępowań w sprawach o wykroczenia i przestępstwa skarbowe prowadzone w oparciu o k.k.s.

Powyższe oznacza, że organy podatkowe dysponują szeregiem informacji, dotyczących osób fizycznych, podmiotów gospodarczych, pozyskanych z różnych źródeł, w tym m. in. z banków oraz instytucji finansowych. W zależności też od rodzaju danych objętych tą tajemnicą, jak i podmiotu od którego pochodzą, odmiennie kształtowane są sposoby zarówno jej udostępniania, jak i chronienia⁹⁷. Bez wyjątku jednak dane te w chwili obecnej są objęte cyfryzacją.

⁹⁶ M. Niezgódka-Medek [w:] *Ordynacja podatkowa. Komentarz*, (red.) S. Babiarsz, B. Dauter, R. Hauser, A. Kabat, J. Rudowski, M. Niezgódka-Medek, Warszawa 2019, art. 293.

⁹⁷ J. Serwacki, *Tajemnica skarbowa* [w:] *Państwo demokratyczne, prawne i socjalne: księga jubileuszowa dedykowana profesorowi Zbigniewowi Antoniemu Maciągowi*, (red.) M. Grzybowski, Kraków 2014, s. 361 i n.

Objęcie cyfryzacją danych objętych tajemnicą skarbową

Podstawowymi aktami, które mają znaczenie dla postępującej cyfryzacji administracji publicznej, w tym KAS, są m. in. ustawa z dnia 8 czerwca 2022 r. o zmianie niektórych ustaw w celu automatyzacji załatwiania niektórych spraw przez Krajową Administrację Skarbową⁹⁸, jak również ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne⁹⁹. Poza tym nie sposób pominąć, że wpływ na informatyzację KAS mają też realizowane na wskazanych wyżej podstawach prawnych i współfinansowane z Unią Europejską projekt e-Podatki, w tym też realizowany jego ostatni moduł projekt „Czynności kontroli elektronicznej, VAT – Plik” (CVP), obejmujący: rozwój katalogu usług cyfrowych KAS; podniesienie poziomu wsparcia informatycznego w procesach kontroli podatkowej i celno-skarbowej z wykorzystaniem Jednolitych Plików Kontrolnych oraz innych informacji gromadzonych w KAS; cyfryzację sprawozdań finansowych¹⁰⁰.

Zmiany te spowodowały, że w istocie doszło do przeniesienia całej komunikacji z organami podatkowymi, jak również wykonywania czynności materialno-technicznych oraz prawnych do rzeczywistości wirtualnej. W chwili obecnej na gruncie o.p. wykorzystanie technologii cyfrowych nie jest wyłącznie prawem, czy możliwością organów i administrowanych, ale obowiązkiem stron stosunków podatkowych. W formie elektronicznej w rozumieniu, jako formy podstawowej odbywa się m. in. korespondencja z organem (m. in. art. 144 o.p.), składanie deklaracji podatkowych (art. 80 o.p.), a także przekazywanie mu dokumentacji rachunkowej (art. 193a o.p.), zgodnie z obecnym brzmieniem ustawy odbywają się w formie elektronicznej. Powoduje to, że zakres usług cyfrowych realizowanych i oferowanych przez KAS rozszerza się. W drodze elektronicznej możliwe jest złożenie deklaracji podatkowych, wysłanie elektronicznego pisma do organów podatkowych, a także elektroniczne pobieranie zaświadczeń, odbierania pism doręczanych przez organy KAS; wnoszenie pism, a także przeglądanie danych objętych tajemnicą skarbową dotyczących osoby fizycznej, w tym też zapoznavanie się z aktami sprawy. M. in. dokonano też automatyzacji obsługi wniosków komorników sądowych o udostępnienie informacji. Przekazywane przez nich informacje mają formę cyfrową oraz są gromadzone oraz przetwarzane przy użyciu narzędzi elektronicznych. Dokumenty papierowe pełnią w o.p. wyłącznie rolę subsydiarną i ich wymiana jest możliwa dopiero kiedy zachowanie formy dokumentu elektronicznego jest niemożliwe

⁹⁸ Dz. U. poz. 1301 z późn. zm.

⁹⁹ T.j. Dz. U. z 2023 r. poz. 57 z późn. zm, dalej „ustawa o informatyzacji”.

¹⁰⁰ Projekt CVP, <https://www.gov.pl/web/kas/projekt-cvp>, [data dostępu: 1.07.2023 r.]; zob. także: A. Bielawska, D. Pauch, Jednolity plik kontrolny jako sposób przekazywania informacji podatkowej, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach”, Katowice 2016, nr 282, s. 17-25.

(art. 144 § 1 c o.p.). Informacje o podatnikach i inkasentach, są wobec tego zarówno przez nich samych w celu uszczelnienia systemu podatkowego¹⁰¹, jak i organy KAS gromadzone i przetwarzane wyłącznie w formie cyfrowej.

W konsekwencji, chociaż w żadnym miejscu regulacji prawne determinujące cyfryzację organów podatkowych nie posługują się pojęciem tajemnicy skarbowej, to nie ulega wątpliwości, że w sposób ścisły jej dotyczą. Chociaż pierwotnie nie było to takie jednoznaczne i pojawiały się głosy wykluczające uznanie, że dokumenty w formie elektronicznej są nią objęte¹⁰². Zasadne znaczenie dla zrozumienia tej kwestii ma tu jednak orzecznictwo, zgodnie z którym, dane są objęte tajemnicą skarbową z mocy prawa, a nie wskutek decyzji organu. Tym samym, tajemnica skarbową rozciąga się na dane automatycznie, niezależnie od opatrzenia stosowną klauzulą dokumentów, które jest jedynie czynnością o charakterze deklaratoryjnym i potwierdzającą cechę wynikającą z ustawy¹⁰³.

Wykorzystanie nowych technologii przez KAS nie wpłynęło wobec tego na samo znaczenie tajemnicy skarbowej, w tym zwłaszcza na zakres danych nią objętych. Rozszerzyły one jednak jej przedmiot, a także rozszerzyły obowiązek jej ochrony. W kontekście cyfryzacji działania administracji publicznej, w tym zwłaszcza organów podatkowych, zauważyć należy, że przekłada się ona na: (i) objęcie tajemnicą skarbową również dokumentów w postaci elektronicznej, (ii) umożliwienie przekazania danych objętych tajemnicą skarbową w formie elektronicznej, jak również (ii) zapewnienie instrumentów ochrony przed ujawnieniem tajemnicy skarbowej w ramach korzystania z technologii informatycznych.

Zagrożenia związane cyfryzacją gromadzenia i przetwarzania danych objętych tajemnicą skarbową

Z istoty tajemnicy skarbowej wynika, że samo udostępnienie administracji skarbowej informacji przez osobę, której dane dotyczą, nakłada na tę administrację (w tym też osoby w niej pracujące) obowiązek zachowania tych informacji w sekrecie. Powoduje to, że w z jednej strony wyłączenia jawności wynikającego z tajemnicy skarbowej nie można traktować rozszerzająco. Jest ona wynikiem od zasady jaką jest jawność postępowania podatkowego i dostęp do informacji. Z drugiej strony jest ona środkiem ochrony informacji, przez co jest argumentem za wzmocnieniem ochrony danych, w tym danych osobowych podatników. Powiązany jest

¹⁰¹ A. Bielawska, D. Pauch, *Jednolity...*, op.cit., s. 24 i n.

¹⁰² Ł. Zalewski, Wszystkie dokumenty elektroniczne objęte tajemnicą skarbową, *Dziennik Gazeta Prawna* z dnia 23 listopada 2021 r., <https://podatki.gazetaprawna.pl/artykuly/8297568,dokumenty-elektroniczne-objete-tajemnica-skarbowa.html> [data dostępu: 1.08.2023].

¹⁰³ Postanowienie NSA z dnia 3 września 2013 r., II FSK 1271/13, *Legalis*.

z nią w tym wypadku obowiązek organu, jak i jego pracowników zachowania w dyskrekcji informacji, w szczególności podatkowych, przetwarzanych w związku z realizacją zadań publicznych przez organy podatkowe i kontrolę skarbową¹⁰⁴. Jest to szczególnie ważne również z perspektywy zrozumienia obecnej wartości informacji. W obecnych czasach informacja zarówno jawna, jak i niejawna ma znaczenie strategiczne i jest towarem, który należy chronić przed nieuprawnionym ujawnieniem¹⁰⁵. Informacja staje się przez to podstawowym warunkiem wyznaczającym wiedzę, władzę, ale i determinującym bezpieczeństwo państw, jak i obywateli¹⁰⁶.

Jak zostało wykazane we wcześniejszych rozważaniach, dane objęte tajemnicą skarbową w bardzo szerokim zakresie są obecnie gromadzone i przetwarzane przy użyciu urządzeń elektronicznych. Oznacza to, że do rozszerzeniu uległy zagrożenia informacyjne, które obecnie związane są też z rozwiązaniami technologicznymi¹⁰⁷. Z tego też względu po stronie organów podatkowych zwiększony został zakres ich obowiązków w zakresie ochrony informacji, jaki można opisać, jako zapewnienie bezpieczeństwa informacyjnego. Za K. Lidermanem można zauważyć, że jest to zaufanie podmiotu (człowieka, czy organizacji) do jakości (tj. otrzymanie informacji o odpowiedniej jakości) oraz dostępności informacji (tj. bezpieczeństwo zasobów informacji)¹⁰⁸. W chwili obecnej jest ono wobec tego zagrożone wieloma cyber-zagrożeniami, które ewoluują wraz z postępem technologicznym. Jak się wskazuje w normie ISO 27001: „zachowanie poufności, integralności i dostępności informacji; dodatkowo mogą być brane pod uwagę inne własności takie, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność”¹⁰⁹. W ramach tego można wyodrębnić też bezpieczeństwo teleinformatyczne, które obejmuje procesy przetwarzania informacji przy użyciu technologii informatycznych w sieciach, systemach i bazach danych¹¹⁰.

Na obecnym etapie bezpieczeństwo informacyjne regulowane jest przez szereg aktów prawnych, które mają na celu zbudowanie systemów jego ochrony. Jednym z podstawowych jest wydane na podstawie ustawy o informatyzacji Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych¹¹¹.

¹⁰⁴ P. Krawczyk, Czy tajemnica skarbową jest potrzebna? [w:] Ordynacja podatkowa. Wokół nowelizacji, R. Dogwier (red.), Warszawa 2009, s. 63–65.

¹⁰⁵ J. Pałgan, Co warto wiedzieć o tajemnicach prawnie chronionych w Polsce, „Wiedza Obronna” 2009, nr 1, s. 76.

¹⁰⁶ K. Liderman, Bezpieczeństwo..., s. 11.

¹⁰⁷ P. Bączek, Zagrożenia informacyjne a bezpieczeństwo państwa polskiego, Toruń 2006, s. 7.

¹⁰⁸ K. Liderman, Bezpieczeństwo... op.cit., s. 22.

¹⁰⁹ PN-ISO/IEC 27001 – Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, PKN, Warszawa 2007, s. 9.

¹¹⁰ K. Liderman, Analiza ryzyka i ochrona informacji w systemach komputerowych, Warszawa 2009, s. 25.

¹¹¹ T.j. Dz. U. z 2017 r. poz. 2247, dalej: „KRI”.

Zgodnie z § 20 ust. 1 KRI, organy podatkowe mają opracowywać i ustanawiać, wdrażać i eksploatować, monitorować i przeglądać oraz utrzymywać i doskonalić system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Podstawą dla zapewnienia bezpieczeństwa informacyjnego jest cykliczność opisanych powyższej działań, jak i spełnianie przez kierownictwo podmiotu publicznego warunków wyszczególnionych w ust. 2 możliwe jest osiągnięcie pożądanego bezpieczeństwa¹¹². § 20 KRI, obejmuje nie tylko wymogi bezpośrednio dotyczące systemów teleinformatycznych, ale wywiera wpływ na całokształt procesów informacyjnych występujących w sektorze publicznym, tworząc standard bezpieczeństwa. Jednocześnie też zapewnienie bezpieczeństwa w danym podmiocie nie może następować bez uwzględnienia wymogów indywidualnych. Stąd zapewnienie bezpieczeństwa teleinformatycznego zależy od konkretnego systemu w konkretnym podmiocie. Umożliwia to dostosowywanie rozwiązań do wyników analiza ryzyka i ewentualnego ustanawiania dodatkowych zabezpieczeń, o czym jest mowa w § 20 ust. 4 KRI.

Nadal jednak uznać należy, że nie da się zapewnić pełnej ochrony i kontroli nad gromadzeniem i przetwarzaniem danych. Z jednej strony wynika to z ciągle postępującego rozwoju technologicznego, z czym idzie również ewolucja cyber-zagrożeń, jak również z ich różnorodnej natury. W literaturze wskazuje się, że źródłami zagrożeń dla bezpieczeństwa informacyjnego są przede wszystkim siły natury, błędy ludzi i a w tym też błędy i niewłaściwości procedur determinujących ich działania, a także celowe i szkodliwe działanie ludzi oraz awarie sprzętu komputerowego oraz oprogramowania¹¹³. W ich ramach można wyróżnić zagrożenia o charakterze technologicznym, czyli powstałe na skutek niedostatecznych zabezpieczeń przed atakami na gromadzone i przetwarzane informacje oraz osobowym, tj. związane udostępnianiem (celowym, czy też przez niedbałość) danych objętych tajemnicą skarbową przez osoby zobowiązane do jej przestrzegania. Poza tym można tu mówić o zagrożeniach zewnętrznych, tj. atakach na integralność, poufność, rozliczalność i dostępność danych spoza sieci w danym urzędzie oraz zagrożeniach wewnętrznych tj. powstałych w sieci lokalnej danego urzędu. W ramach zagrożeń o charakterze technologicznym o charakterze zewnętrznym, można zwłaszcza wymienić można wirusy, ale też formy wyłudzenia danych jak phishing, czy pharming¹¹⁴. Do zagrożeń wewnętrznych należą zwłaszcza te

¹¹² K. Światała, Prawnoadministracyjne aspekty problematyki bezpieczeństwa informacji w podmiotach publicznych, „Przegląd Prawa Publicznego” 2013, nr 10, s. 24.

¹¹³ K. Liderman, Bezpieczeństwo..., s. 155.

¹¹⁴ D. Wiśniewski, Bezpieczeństwo informacji oraz ochrona przed ich wyciekami na przykładzie wybranego Urzędu Miejskiego, „Przedsiębiorczość i Zarządzanie” 2014, t. 15, z. 9, cz. 1, E-biznes i ochrona danych osobowych, s. 135 i n.

o charakterze osobowym, wśród nich wskazuje się brak świadomości oraz wiedzy pracowników, w tym też ich podatność na instrumenty inżynierii społecznej¹¹⁵.

Powyższe wskazuje, że ulepszenia wobec tego systemu zabezpieczenia ochrony tajemnicy skarbowej powinny być podejmowane na wielu płaszczyznach. Na płaszczyźnie prawnej przez rozwijanie nowych warstw obowiązku jej ochrony, ale też zmianę dotychczasowych uregulowań zmniejszających bezpieczeństwo danych (jak np. ograniczenie jawności procedur przetargowych na oprogramowania zabezpieczające dostęp do tych danych, w celu ograniczenia możliwości wytwarzania dedykowanych instrumentów dla ich nielegalnego pozyskania). Na poziomie technologicznym przez tworzenie nowych oraz coraz bardziej efektywnych rozwiązań chroniących dane. Na poziomie osobowym przez tworzenie i udoskonalanie mechanizmów zarówno doboru oraz szkolenia kadry urzędniczej, zwłaszcza w zakresie zwiększania świadomości wagi danych objętych tajemnicą skarbową oraz konieczności wszechstronnej ich ochrony.

Podsumowanie

Zaprezentowana analiza stanowi jedynie ułamek bogatego i wieloaspektowego zagadnienia jakim jest cyfryzacja działalności administracji publicznej. W jej ramach podjęto próbę wykazania, że zwiększenie roli narzędzi informatycznych w działalności KAS wpłynęło na sposób ochrony tajemnicy skarbowej. Chociaż rozważania prowadzą do wniosków, iż cyfryzacja działań organów podatkowych nie wpłynęła zasadniczo na zakres i znaczenie tajemnicy skarbowej, to jednak miała wpływ na określenie jej przedmiotu. Wskutek zwiększenia wykorzystania nowych technologii w procedurach prowadzonych przez organy podatkowe, również elektroniczne dokumenty, zbiory danych, skutki przetwarzania informacji oraz procesy do nich prowadzące, zostały objęte tajemnicą skarbową. W konsekwencji miało to wpływ na zakres obowiązku ochrony tajemnicy skarbowej przez KAS. Tradycyjne metody ochrony informacji podatkowych są niewystarczające w realiach rewolucji technologicznej, cyfrowej, z którą oprócz bezspornych korzyści wynikających z wykorzystania narzędzi informatycznych, jednocześnie wynikają nowe zagrożenia.

Liczba oraz różnorodność tych zagrożeń stwarza konieczność podejmowania ciągłych działań w celu ulepszania istniejących oraz tworzenia nowych systemów zabezpieczeń na poziomie technologicznym, ale także nowych rozwiązań prawnych, a także kadrowych i etycznych zapewniających bezpieczeństwo informacyjne (w tym teleinformacyjne). W konsekwencji, podsumowując całość analiz dokonanych w rozdziale uznać należy, że chociaż treść i zakres tajemnicy skarbowej nie uległy zasadniczym zmianom, to jednak zwiększona została potrzeba ich zabezpieczenia i związane z tym obowiązki organów podatkowych.

¹¹⁵ Ibidem, s. 136 i n.

Bibliografia

Akty prawne

1. Ustawa z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa, t.j. Dz. U. z 2023 r. poz. 2383 z późn. zm.
2. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. z 2024 r. poz. 307.
3. Ustawa z dnia 8 czerwca 2022 r. o zmianie niektórych ustaw w celu automatyzacji załatwiania niektórych spraw przez Krajową Administrację Skarbową, Dz. U. poz. 1301 z późn. zm.
4. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych, t.j. Dz. U. z 2017 r. poz. 2247.

Orzecznictwo

1. Wyrok NSA z dnia 2 lutego 2005 r., OSK 1060/04, CBOSA
2. Wyrok NSA z dnia 20 kwietnia 2017 r., I OSK 1785/15, Legalis
3. Wyrok NSA z dnia 20 lutego 2020 r., I OSK 1844/18, LEX nr 3022094
4. Wyrok NSA z dnia 3 lutego 2022 r., III OSK 4926/21, LEX nr 3331078
5. Postanowienie NSA z dnia 3 września 2013 r., II FSK 1271/13, Legalis
6. Wyrok WSA w Poznaniu z dnia 11 września 2019 r., I SA/Po 357/19, LEX nr 2704635
7. Wyrok WSA we Wrocławiu z dnia 27 czerwca 2012 r., IV SA/Wr 154/12, Legalis

Literatura

1. Adamiak B., Borkowski J., Mastalski R., Zubrzycki J., *Ordynacja podatkowa*, Warszawa 2009.
2. Babiarz S., Dauter B., Gruszczyński B., Hauser R., Kabat A., Niezgódka-Medek M., *Ordynacja podatkowa. Komentarz*, Warszawa 2009.
3. Bączek P., *Zagrożenia informacyjne a bezpieczeństwo państwa polskiego*, Toruń 2006.
4. Biegalski A., Kucewicz M., *Prawo do prywatności a systemy wymiany informacji w sprawach podatkowych*, cz. II, „Prawo i Prokuratura” 2008, nr 9.
5. Bielawska A., Pauch D., *Jednolity plik kontrolny jako sposób przekazywania informacji podatkowej*, „Studia Ekonomiczne. Zeszyty Naukowe Uniwersytetu Ekonomicznego w Katowicach” 2016 r., nr 282.
6. Brolik J. i in., *Ordynacja podatkowa. Komentarz*, Warszawa 2013, LEX/el.
7. Kowalewski J., Kowalewski M., *Polityka bezpieczeństwa informacji w praktyce*, Wrocław 2004.

8. Krawczyk P., *Czy tajemnica skarbową jest potrzebna?* [w:] *Ordynacja podatkowa. Wokół nowelizacji*, (red.) Dowgier R., Warszawa 2009.
9. Liderman K., *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2009.
10. Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2012.
11. Pałgan J., *Co warto wiedzieć o tajemnicach prawnie chronionych w Polsce*, „Wiedza Obronna” 2009, nr 1.
12. Serwacki J., *Tajemnica skarbową* [w:] *Państwo demokratyczne, prawne i socjalne: księga jubileuszowa dedykowana profesorowi Zbigniewowi Antoniemu Maciągowi*, (red.) M. Grzybowski, Kraków 2014.
13. Suchorzewska A., *Rozdział I. Społeczeństwo w dobie rozwoju sieci teleinformatycznych. Pkt 6. Współczesne zagrożenia informacyjne* [w:] Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*, LEX/el.
14. Świata K., *Prawoadministracyjne aspekty problematyki bezpieczeństwa informacji w podmiotach publicznych*, PPP 2013, nr 10.
15. Wiśniewski D., *Bezpieczeństwo informacji oraz ochrona przed ich wyciekiem na przykładzie wybranego Urzędu Miejskiego*, *Przedsiębiorczość i Zarządzanie* 2014, t. 15, z. 9, cz. 1 E-biznes i ochrona danych osobowych.

Netografia

1. Zalewski Ł., *Wszystkie dokumenty elektroniczne objęte tajemnicą skarbową*, *Dziennik Gazeta Prawna* z dnia 23 listopada 2021 r., <https://podatki.gazeta-prawna.pl/artykuly/8297568,dokumenty-elektroniczne-objete-tajemnica-skarbowa.html> [data dostępu: 1.08.2023].
2. Projekt CVP, <https://www.gov.pl/web/kas/projekt-cvp> [data dostępu: 1.07.2023].

Inne

1. Pismo z dnia 26.03.1998 r., wydane przez: Ministerstwo Finansów, FB 1/235/Ch/98, *Tajemnica skarbową. Udostępnienie akt*, *Pr.Przeds.* 1998, nr 33-34.
2. PN-ISO/IEC 27001 – Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania, PKN, Warszawa 2007.

Kompetencje cyfrowe i polityka cyberbezpieczeństwa jako warunki *sine qua non* funkcjonowania elektronicznej administracji

Digital competences and cybersecurity policy as sine qua non conditions functioning of e-government

Streszczenie

Z całą pewnością należy stwierdzić, że współcześnie zarządzanie sprawami publicznymi nie jest możliwe bez zastosowania nowoczesnych rozwiązań teleinformatycznych. Znamienne jest to, że cyfryzacja sektora publicznego sprzyja efektywności i skuteczności realizacji zadań publicznych, a także kreuje wizerunek administracji przyjaznej i otwartej na potrzeby obywateli. Jednakże prawidłowe funkcjonowanie elektronicznej administracji wymaga zapewnienia zarówno bezpieczeństwa prawnego, jak i technologicznego. Nie bez znaczenia są także kwestie społeczne, przede wszystkim rozwój podstawowych i zaawansowanych kompetencji cyfrowych wśród profesjonalnych i nieprofesjonalnych użytkowników e-administracji.

Celem rozdziału jest przedstawienie niezbędnych warunków prawidłowego funkcjonowania elektronicznej administracji. Przedmiot badania obejmuje wskazanie celowości zapewnienia polityki cyberbezpieczeństwa i rozwoju kompetencji cyfrowych w zakresie bezpiecznego i efektywnego świadczenia usług publicznych na odległość. Analiza tematu, pozwoli odpowiedzieć na następujące pytanie: „czy kompetencje cyfrowe i politykę cyberbezpieczeństwa należy uznać za warunki *sine qua non* funkcjonowania elektronicznej administracji?”. W pierwszej części pracy oprócz charakterystyki elektronicznej administracji, wskazano warunki cyberbezpieczeństwa w e-administracji oraz zasadność wdrożenia tzw. polityki cyberbezpieczeństwa. Druga część koncentruje się na zagadnieniach związanych ze wzrostem poziomu umiejętności cyfrowych, w tym wsparcia rozwoju edukacji cyfrowej społeczeństwa informacyjnego.

Wprowadzenie

Dostępność usług publicznych jest istotnym elementem prawidłowego działania administracji publicznej. Efektywnie funkcjonująca e-administracja zapewnia sprawną realizację zadań publicznych, cechuje się transparentnością, umożliwia racjonalne gospodarowanie zasobami publicznymi, pozwala aktywnie uczestniczyć obywatelom w procesach dotyczących zarządzania publicznego i koncentruje się na świadczeniu usług zgodnie z ich oczekiwaniami¹¹⁶. W tym miejscu należy zaznaczyć, że w związku z modernizacją sektora publicznego, *stricte* wprowadzenia modelu e-administracji na znaczeniu zyskały określone determinanty świadczenia e-usług. Oprócz, tak istotnych aspektów jak chociażby szybki i łatwy sposób załatwienia spraw za pomocą właściwego systemu teleinformatycznego danego organu administracji publicznej, w centrum uwagi znalazły się kwestie bezpieczeństwa (cyberbezpieczeństwa) i wsparcia użytkowników w zakresie odpowiedniego korzystania z e-administracji. Jacek Jankowski zauważył, że „dane elektroniczne i elektroniczna transmisja, są podatne na zarządzanie”, a „zarządzanie przetwarzaniem i transmisją danych odbywa się w coraz bardziej zaprogramowany sposób”¹¹⁷. W nawiązaniu do powyższego poglądu, można stwierdzić, że szczególnie niepokojącą sytuacją będzie ta, w której mechanizmy odpowiedzialne za zarządzanie, przetwarzanie danych, komunikację czy też wspieranie procesów decyzyjnych staną się obiektami cyberataków (cyberzagrożeń¹¹⁸). W takim przypadku może dojść do ograniczenia czy też uniemożliwienia (czasowego bądź trwałego) dystrybucji informacji lub świadczenia usług. Zważywszy na fundamentalną rolę administracji publicznej i jej wpływ na rozwój społeczno-gospodarczy, a jednocześnie intensyfikację cyberzagrożeń w sektorze publicznym, na mocy Dyrektywy NIS 2¹¹⁹, podmioty administracji publicznej uznano za tzw. podmioty kluczowe i przypisano im szczególne zadania w zakresie cyberbezpieczeństwa. Ekspozowanie polityki cyberbezpieczeństwa systemów publicznych jest bezsprzecznie koniecznym elementem prawidłowego funkcjonowania e-administracji w XXI wieku.

¹¹⁶ S. Żuczek, E-administracja, a konkurencyjność na arenie międzynarodowej, [w:] Międzynarodowa Innowacyjność i Konkurencyjność w XXI w. Aspekty Innowacyjne, (red.) R. Luft, Lublin 2022, s. 50-51.

¹¹⁷ J. Janowski, Wpływ technologizacji na informację o prawie, [w:] Modele dostępu do informacji o prawie, (red.) G. Szpor, Warszawa 2014, s. 19.

¹¹⁸ Art. 2 pkt 8 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz.Urz. UE L 151 z 7.6.2019 r., s. 15, stanowi, że cyberzagrożenie oznacza wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób.

¹¹⁹ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) Nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylającą dyrektywę (UE) 2016/1148, Dz.Urz. UE L Nr 333, s. 80.

Niewątpliwie kluczową rolę w procesie cyfryzacji administracji publicznej odgrywają potrzeby społeczeństwa informacyjnego. W ślad za Bolesławem Szafrąnskim należy wskazać, że dąży ono do „niemal natychmiastowego, nieodpłatnego i w praktyce nieograniczonego dostępu do wskazanych przez siebie informacji gromadzonych i przetwarzanych w zasobach administracji publicznej” (...) „większej otwartości, interoperacyjności i elastyczności systemów administracji publicznej”¹²⁰. Niemniej jednak, można zauważyć, że pomimo wzrastających potrzeb, społeczeństwo informacyjne nie osiągnęło w pełnym zakresie właściwych umiejętności i kompetencji cyfrowych. Tym samym, ze względu na brak odpowiedniej edukacji cyfrowej, użytkownicy Internetu nie są wystarczająco świadomi potencjalnych cyberzagrożeń, nie potrafią ocenić i wyselekcjonować informacji prawdziwych i nieprawdziwych, brakuje im podstawowych i zaawansowanych umiejętności cyfrowych (nie mogą sobie poradzić z incydentami o mniej bądź bardziej negatywnych skutkach). Nie można pominąć tego, że przede wszystkim to na podmiotach zaangażowanych w realizację zadań publicznych spoczywają istotne obowiązki związane z bezpiecznym świadczeniem e-usług (administracja publiczna jako gwarant realizacji zadań publicznych). Jednocześnie, wysoki poziom umiejętności cyfrowych powinien charakteryzować również pozostałych użytkowników e-administracji – czyli obywateli. Powyższe stwierdzenia potwierdzają słowa Agnieszki Ziółkowskiej, która jasno daje do zrozumienia, że: „miernikiem postępu procesu cyfryzacji administracji publicznej nie powinna bowiem być jedynie skala wdrażania technologii cyfrowych w świadczeniu usług publicznych, lecz również stopień dojrzałości cyfrowej pracowników administracji i obywateli”¹²¹. W dalszej części pracy zostaną omówione warunki cyberbezpieczeństwa w e-administracji oraz zasadność wdrożenia tzw. polityki cyberbezpieczeństwa, a także zagadnienia związane z rozwojem kompetencji cyfrowych pracowników administracji publicznej i społeczeństwa informacyjnego. Powyższe pozwoli odpowiedzieć na pytanie: „czy kompetencje cyfrowe i politykę cyberbezpieczeństwa należy uznać za warunki *sine qua non* funkcjonowania elektronicznej administracji?”.

Cyberbezpieczeństwo e-administracji. Polityka cyberbezpieczeństwa

Transformacja cyfrowa odgrywa coraz większe znaczenie zarówno w relacjach międzyludzkich, jak i w świadczeniu usług publicznych. Pojęcie cyfryzacji nie ogranicza się wyłącznie do wykorzystywania narzędzi teleinformatycznych (głównie

¹²⁰ B. Szafrąński, Główne wyzwania związane z modernizacją funkcjonowania państwa, „Roczniki Kolegium Analiz Ekonomicznych” 2013, nr 29, s. 311.

¹²¹ A. Ziółkowska, Wrażliwość społeczna władzy w kontekście dostępności cyfrowej administracji publicznej, [w:] Obywatel w centrum działań e-administracji w Unii Europejskiej, (red.) S. Dudzik, I. Kawka, R. Śliwa, Kraków 2023, s. 124.

komputerów) w procesach przetwarzania danych, czy digitalizacji. Cyfryzacja jest bowiem terminem wieloznacznym, ma szczególne konsekwencje społeczne (usieciowienie społeczeństwa, dostępność cyfrowa), gospodarcze (wytwarzanie i oferowanie produktów online) i *stricte* technologiczne (rozwój infrastruktury teleinformatycznej, zastosowanie sztucznej inteligencji)¹²². Zgodnie z art. 5 Konstytucji Rzeczypospolitej Polskiej jednym z podstawowych zadań państwa (organów administracji publicznej) jest zapewnienie bezpieczeństwa obywateli¹²³, którego szczególnym rodzajem z uwagi na powszechną cyfryzację jest cyberbezpieczeństwo. W rezultacie należy je uznać za determinantę funkcjonowania elektronicznej administracji.

Kluczowym elementem bezpieczeństwa e-informacji, infrastruktury teleinformatycznej i świadczenia e-usług publicznych jest opracowanie zasad (polityki) cyberbezpieczeństwa. W tym kontekście konieczne jest określenie zarówno katalogu chronionych dóbr i usług (aspekt przedmiotowy), jak i podmiotów narażonych na cyberzagrożenia (aspekt podmiotowy). Małgorzata Ganczar wskazuje, że działania w ramach cyberbezpieczeństwa muszą uwzględniać „osiąganie celów informatycznych w sposób bezpieczny i niezawodny przy zachowaniu prywatności”¹²⁴, a zatem odzwierciedlać potrzeby osób fizycznych, przedsiębiorców i instytucji publicznych. Cele polityki cyberbezpieczeństwa można wywnioskować z definicji, która wskazuje, że przez cyberbezpieczeństwo należy rozumieć odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy¹²⁵. Aktywność administracji publicznej w przedmiocie kierowania cyberbezpieczeństwem w organizacji powinna koncentrować się zatem na zagadnieniach związanych z ochroną danych i informacji (w tym informacji niejawnych), dostępem do usług publicznych (jakość i stabilne świadczenie usług) i bezpieczeństwem użytkownika końcowego. Wzmocnienie odporności systemów teleinformatycznych administracji publicznej wymaga dookreślenia priorytetów cyberbezpieczeństwa w odniesieniu do potencjalnych incydentów¹²⁶ czy cyberzagrożeń. W efekcie wdrożenie odpowiedniej polityki cyberbezpieczeństwa wymusza spojrzenie na tzw. wrażliwe elementy, czyli takie które są szczególnie narażone na awarie, cyberataki czy innego rodzaju incydenty.

¹²² G. Szpor, Cyfryzacja, [w:] Wielka Encyklopedia Prawa, tom XXII. Prawo informatyczne, (red.) G. Szpor, L. Grochowski, Warszawa 2021, s. 94.

¹²³ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. nr 78, poz. 483 ze zm.

¹²⁴ M. Ganczar, Umowne partnerstwo publiczno-prywatne w kontekście bezpieczeństwa sieci i informacji administracji publicznej, [w:] Internet. Strategie bezpieczeństwa, (red.) G. Szpor, A. Gryszczyńska, Warszawa 2017, s. 85.

¹²⁵ Art. 2 pkt 4 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. z 2024 r. poz. 1077,1222, dalej: u.k.s.c.

¹²⁶ Zgodnie z art. 2 pkt 5 u.k.s.c. incydent to zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo. W u.k.s.c. dokonano ich klasyfikacji, należą do nich incydenty: krytyczne (art. 2 pkt 6 u.k.s.c), poważne (art. 2 pkt 7 u.k.s.c), istotne (art. 2 pkt 8 u.k.s.c), w podmiocie publicznym (art. 2 pkt 9 u.k.s.c).

Za Włodzimierzem Nowakiem należy odnotować, że katalog szkodliwych czynników jest bardzo szeroki. Zalicza się do niego m.in. awarie sieci, błędy oprogramowań, brak autoryzacji dostępu, celowe działania hakerów (kradzież, nielegalne przetwarzanie danych), błędy ludzkie (operatorów, administratorów, użytkowników)¹²⁷. Najważniejszym elementem prawidłowego funkcjonowania e-administracji pozostaje kwestia ustanowienia rozwiązań prawnych odpowiadających warunkom technologicznym i społeczno-gospodarczym. Kazus pandemii COVID-19 ugruntował znaczenie świadczenia usług drogą elektroniczną. W tym czasie zarówno administracja rządowa, jak i samorządowa zintensyfikowała działania online, urzędy wprowadziły zdalny tryb funkcjonowania, dzięki czemu obywatele mogli załatwiać sprawy na odległość¹²⁸. Powyższy przypadek uświadomił jak wiele jest jeszcze wyzwań i problemów związanych z efektywnym funkcjonowaniem e-administracji, szczególnie w aspekcie cyberbezpieczeństwa i dostępności świadczenia e-usług. Nie dziwi zatem, że ze względu na kluczową rolę administracji publicznej w świadczeniu e-usług publicznych, w tym wzrost incydentów i cyberzagrożeń, a także doświadczenia postpandemiczne, na poziomie Unii Europejskiej zdecydowano się wprowadzić nowe rozwiązania w zakresie cyberbezpieczeństwa dotyczące także podmiotów administracji publicznej. Oczywiście, warto odnotować, że dla wzmocnienia cyberbezpieczeństwa niezbędne są także inwestycje w cyfrową infrastrukturę i wykorzystanie technologii nowej generacji, w tym sztucznej inteligencji.

Jak można zauważyć za wdrożeniem tzw. polityki cyberbezpieczeństwa w działaniach administracji publicznej aktualnie przemawiają dwie kwestie. Po pierwsze niezbędność opracowania określonych zasad cyberbezpieczeństwa wynika z przepisów prawa, które jednoznacznie wskazują, które podmioty powinny wzmocnić (zapewnić) ochronę systemów teleinformatycznych. Tendencja cyfryzacji administracji publicznej jest priorytetem Unii Europejskiej. W odniesieniu do powyższego, można powiedzieć, że o zdolnościach administracyjnych i efektywności administracji publicznej świadczy stopień cyfryzacji, który wymaga zapewnienia cyberbezpieczeństwa świadczenia usług publicznych. Polityka cyberbezpieczeństwa jest warunkiem *sine qua non* funkcjonowania elektronicznej administracji ponieważ pozwala na bezpieczne świadczenie usług on-line i przetwarzanie danych osobowych (ochrona przed cyberzagrożeniami), zapewnia transparentność informacji, umożliwia identyfikację elektroniczną, gwarantuje transgraniczną dostępność usług¹²⁹. Po drugie celowość polityki cyberbezpieczeństwa w e-administracji

¹²⁷ W. Nowak, Ochrona infrastruktury krytycznej w cyberprzestrzeni, [w:] Cyberbezpieczeństwo. Zarys wykładu, (red.) C. Banasiński, Warszawa 2018, s. 182-183.

¹²⁸ Jacek Wojnicki, Modernizacja administracji publicznej w Polsce w XXI wieku – założenia teoretyczne i praktyka administracyjna, „Studia Politologiczne” 2022, vol. 64, s. 40.

¹²⁹ I. Kawka, Kompetencje Unii Europejskiej w zakresie cyfryzacji administracji publicznej państw członkowskich, [w:] Obywatel w centrum działań e-administracji w Unii Europejskiej, (red.) S. Dudzik, I. Kawka, R. Śliwa, Kraków 2023, s. 184-185.

związana jest z intensyfikacją cyberzagrożeń w sektorze publicznym. Obok takich działań jak *spamming* czy *phishing* cyberprzestępcy coraz chętniej posługują się sztuczną inteligencją, która powinna być nie zagrożeniem ale technologią wspierającą działania administracji publicznej. Stąd też, „dobrą koncepcją jest m.in. stworzenie polityki cyberbezpieczeństwa, określającej odpowiednie środki zapobiegawcze i ochronne, w tym zasady obsługi tzw. incydentów”¹³⁰.

Literalna wykładnia przepisów prawa dotychczas nie pozwalała na umiejscowienie usług świadczonych przez administrację publiczną w katalogu tzw. usług kluczowych. Sytuacja zmieniła się w momencie opracowania nowej unijnej polityki w sprawie osiągnięcia środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii Europejskiej. Na mocy tzw. dyrektywy NIS 2 podmioty administracji publicznej¹³¹ uznano za tzw. podmioty kluczowe. Innymi słowy, zważywszy na kluczową rolę administracji publicznej w obszarze świadczenia usług użyteczności publicznej, ustawodawca unijny dostrzegł, że działalność takich podmiotów wymaga wprowadzenia szczególnych zasad cyberbezpieczeństwa. Dyrektywa NIS 2 zawiera katalog skoordynowanych ram w zakresie cyberbezpieczeństwa podmiotów administracji publicznej. Do najważniejszych zadań należy niewątpliwie wprowadzenie odpowiednich i proporcjonalnych środków zarządzania ryzykiem w cyberbezpieczeństwie. Polityka cyberbezpieczeństwa administracji publicznej powinna uwzględniać, tj. przewidywać ryzyka dla bezpieczeństwa systemów informatycznych, ale również zwracać uwagę na takie komponenty jak obsługa incydentu czy bezpieczeństwo łańcucha dostaw, zapewniać ciągłość działania usługi, określać: polityki i procedury służące ocenie skuteczności środków zarządzania ryzykiem w cyberbezpieczeństwie i zasady cyberhigieny, zawierać zasady stosowania zaawansowanych metod kryptografii czy szyfrowania a także uwzględniać bezpieczeństwa zasobów ludzkich¹³². Na podmioty administracji publicznej zostały również nałożone obowiązki w zakresie zgłaszania incydentów poważnych (art. 23 dyrektywy NIS 2). Dyrektywa NIS 2 sformułowała warunki cyberbezpieczeństwa w administracji publicznej, jednocześnie podkreśliła znaczenie elektronicznej administracji dla rozwoju społeczno-gospodarczego.

¹³⁰ D. Skoczyła, Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe, „Prawo w działaniu. Sprawy karne” 2023, nr 53, s.110.

¹³¹ Art. 2 ust 2 lit. f dyrektywy NIS 2 stanowi, że podmiot jest podmiotem administracji publicznej zarówno na poziomie rządu centralnego, zdefiniowanym przez państwo członkowskie, zgodnie z prawem krajowym; lub na poziomie regionalnym, zdefiniowanym przez państwo członkowskie zgodnie z prawem krajowym, który zgodnie z oceną opartą na analizie ryzyka świadczy usługi, których zakłócenie mogłoby mieć znaczący wpływ na krytyczną działalność społeczną lub gospodarczą.

¹³² Zob. art. 21 dyrektywy NIS 2.

Kompetencje cyfrowe i rozwój edukacji cyfrowej.

Program Rozwoju Kompetencji Cyfrowych

Analizując zagadnienie funkcjonowania elektronicznej administracji, należy podkreślić znaczenie rozwoju kompetencji cyfrowych pracowników administracji publicznej i użytkowników e-usług. Nie ulega wątpliwości, że cyberprzestępcy chętnie wykorzystują błędy ludzkie w celu uzyskania łatwego dostępu do konkretnych baz danych czy systemów teleinformatycznych. Jest to sytuacja szczególnie niebezpieczna ponieważ użytkownik często nie jest świadomy, że wykonując określone ruchy w sieci pozwala na nieskrępowany dostęp osób trzecich do informacji, w tym danych wrażliwych czy prywatnych. Wawrzyniec Świącicki stawia tezę, że osoby korzystające z Internetu lekceważą zasady cyberbezpieczeństwa, nie chcą (bądź nie potrafią) zastosować ich w praktyce, czy też uważają, że ryzyko cyberzagrożeń ich nie dotyczy. Autor wprost wskazuje, że w ocenie użytkowników sieci „ryzyko, że padną ofiarą cyberprzestępstwa jest na tyle niskie, że nie warto utrudniać sobie życia wprowadzaniem nowych skomplikowanych procedur”¹³³. Rolę kompetencji cyfrowych w aspekcie wspierania procesu cyfrowej transformacji przedstawiono w programie Cyfrowa Europa na lata 2021–2027¹³⁴. Z jego treści wynika, że rozwój zaawansowanych umiejętności cyfrowych jest konieczny w celu m.in. analizy dużych zbiorów danych, czy korzystania ze sztucznej inteligencji. Co istotne, wskazano również na relację występującą pomiędzy cyberbezpieczeństwem a kompetencjami cyfrowymi. W kontekście pracowników administracji publicznej rozwój kompetencji cyfrowych jest możliwy dzięki stałemu dostępowi do szkoleń zawodowych, czy kursów w zakresie korzystania z zaawansowanych technologii cyfrowych. Zaawansowane kompetencje cyfrowe kadry pracowniczej należy traktować jako warunek sine qua non funkcjonowania elektronicznej administracji w sposób zarówno bezpieczny jak i efektywny. Z kolei użytkownik posiadający odpowiednie umiejętności cyfrowe jest w stanie co najmniej przewidzieć potencjalne zagrożenie, ma wiedzę o tym w jaki sposób i do jakiego podmiotu zgłosić incydent – w ten sposób może ograniczyć negatywne skutki cyberataku. Należy nadmienić, że program Cyfrowa Europa wskazuje kluczową rolę tzw. europejskich centrów innowacji cyfrowych¹³⁵.

Unowocześnienie administracji publicznej (usług publicznych) i dostęp do wysokiej jakości usług cyfrowych wymaga intensyfikacji działań w zakresie rozwoju edukacji cyfrowej. Znaczenie kompetencji cyfrowych dla funkcjonowania elektronicznej administracji w Polsce odzwierciedlają założenia rządowego Programu Rozwoju

¹³³ W. Świącicki, Wykorzystanie infografiki w kształtowaniu cyberhigieny wśród użytkowników przestrzeni cyfrowej, [w:] Internet. Hacking, (red.) A. Gryszczyńska, G. Szpor, W. R. Wiewiórowski, Warszawa 2023, s. 320.

¹³⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z dnia 29 kwietnia 2021 r. ustanawiające program „Cyfrowa Europa” oraz uchylające decyzję (UE) 2015/2240, Dz. Urz. UE L Nr 166, s. 1, dalej: Program Cyfrowa Europa.

¹³⁵ Zob. art. 16 Programu Cyfrowa Europa.

Kompetencji Cyfrowych¹³⁶. Niewątpliwie wpływ na jego powstanie miał unijny program polityki „Droga ku cyfrowej dekadzie” do 2030 r.¹³⁷ Jednym z celów ogólnych programu jest wzmocnienie zbiorowej odporności państw członkowskich i niwelowanie przepaści cyfrowej. W tym przypadku podkreślono aspekt osiągnięcia równowagi płci i równowagi geograficznej w drodze promowania stale dostępnych wszystkim osobom możliwości w zakresie rozwijania podstawowych i zaawansowanych umiejętności i kompetencji cyfrowych. Wskazano, że kluczowe jest odpowiednie kształcenie i szkolenie zawodowe, w tym wspieranie rozwoju wysoce wydajnych cyfrowych zdolności w ramach horyzontalnych systemów kształcenia i szkolenia¹³⁸. Unijny ustawodawca zaznacza istotę uczenia się przez całe życie. Za jeden z podstawowych celów cyfrowych uznano zaś stworzenie wykwalifikowanego cyfrowo społeczeństwa i wysoko wykwalifikowanych profesjonalistów w dziedzinie cyfrowej, z dbałością o osiągnięcie równowagi płci, przy założeniu, że co najmniej 80 % osób w wieku 16–74 lat posiadać będzie przynajmniej podstawowe umiejętności cyfrowe (art. 4 ust. 1 pkt 1 lit. a programu polityki Droga ku cyfrowej dekadzie).

Rządowy Program Rozwoju Kompetencji Cyfrowych wskazuje, że w skład kompetencji cyfrowych wchodzi kompetencje informatyczne, informacyjno-komunikacyjne oraz funkcjonalne. Zgodnie z powyższą klasyfikacją wszystkie z nich uznano za równie ważne w kontekście rozwoju podstawowych i zaawansowanych umiejętności i kompetencji cyfrowych oraz edukacji cyfrowej. Nie bez znaczenia jest również to, że rozwój kompetencji cyfrowych zmniejsza bariery w zakresie dostępności cyfrowej (przepaść cyfrową), zwiększa także świadomość wystąpienia cyberzagrożeń. Do kompetencji informatycznych zaliczono te związane z obsługą komputera, urządzeń elektronicznych, bezpiecznym korzystaniem z sieci, aplikacji, oprogramowań, nowych inteligentnych technologii cyfrowych. W ramach kompetencji informacyjno-komunikacyjnych wskazano umiejętności obejmujące przetwarzanie informacji oraz komunikację na odległość. Z kolei za kompetencje funkcjonalne uznano te, które umożliwiają wykorzystanie powyższych kompetencji w różnych sferach codziennego życia, takich jak np. finanse, praca i rozwój zawodowy, utrzymywanie relacji, zdrowie, zaangażowanie obywatelskie¹³⁹. Istotnym elementem Programu Rozwoju Kompeten-

¹³⁶ Uchwała nr 24 Rady Ministrów z dnia 21 lutego 2023 r. w sprawie ustanowienia programu rządowego pod nazwą „Program Rozwoju Kompetencji Cyfrowych”, M.P. 2023 poz. 318, dalej: Program Rozwoju Kompetencji Cyfrowych.

¹³⁷ Decyzja Parlamentu Europejskiego i Rady (UE) 2022/2481 z dnia 14 grudnia 2022 r. ustanawiająca program polityki „Droga ku cyfrowej dekadzie” do 2030 r., Dz. Urz. UE L Nr 323, s. 4, dalej: program polityki Droga ku cyfrowej dekadzie.

¹³⁸ Zob. art. 3 ust. 1 lit. b programu polityki Droga ku cyfrowej dekadzie.

¹³⁹ Zob. załącznik do uchwały nr 24 Rady Ministrów z dnia 21 lutego 2023 r. w sprawie ustanowienia programu rządowego pod nazwą „Program Rozwoju Kompetencji Cyfrowych”, M.P. 2023 poz. 318. W Programie Rozwoju Kompetencji Cyfrowych zdefiniowano pojęcie kompetencji przyszłości, do których zaliczono kompetencje techniczne, poznawcze i społeczne (zwłaszcza krytyczne myślenie, kreatywność, komunikację i kooperację) oraz postawy ułatwiające funkcjonowanie w warunkach przyspieszonej zmiany społecznej i gospodarczej (w tym elastyczność, wytrzymałość oraz nastawienie na uczenie się przez całe życie).

cji Cyfrowych jest to, że jego beneficjentami są wszyscy obywatele - użytkownicy technologii cyfrowych, tj. dzieci w wieku przedszkolnym i uczniowie, studenci, nauczyciele (również akademicy), osoby stawiające pierwsze kroki w świecie cyfrowym, w tym seniorzy, osoby z niepełnosprawnościami, osoby pracujące, specjaliści ICT, przedsiębiorcy i osoby zarządzające i pracownicy sektora publicznego. Grażyna Szpor stwierdza, że należy szczególne zadbać o edukację cyfrową wśród absolwentów szkół wyższych. Autorka zaznacza, że: „(...) dla sprostania wyzwaniom współczesności wszyscy absolwenci szkół wyższych powinni posiadać podstawową wiedzę i umiejętności z zakresu informatyki oraz prawnych aspektów wykorzystania nowych technologii”¹⁴⁰. Umiejętności nabyte podczas tego typu zajęć mogą zdecydowanie ułatwić funkcjonowanie na rynku pracy (także w sektorze publicznym), gdzie obecnie znajomość ICT jest niezbędna.

Program Rozwoju Kompetencji Cyfrowych kładzie nacisk na rozwój edukacji cyfrowej, zapewnienie każdemu możliwości rozwoju kompetencji cyfrowych, wsparcie kompetencji cyfrowych osób pracujących, rozwój zaawansowanych kompetencji cyfrowych, wzmocnienie zarządzania i koordynacji działań w zakresie rozwoju kompetencji cyfrowych. W treści programu wskazano, że rozwój kompetencji cyfrowych pracowników administracji publicznej, jest równie istotny jak pozostałych użytkowników ICT. Nie bez przyczyny zwrócono uwagę na potrzebę osiągnięcia określonych celów szczegółowych w sektorze publicznym, takich jak: promocja rozwoju kompetencji cyfrowych wśród pracowników sektora publicznego, upowszechnienie kursów rozwoju kompetencji cyfrowych, cyberbezpieczeństwa i etyki cyfrowej w sektorze publicznym, opracowanie systemu szkoleń online dla sektora publicznego w zakresie rozwoju kompetencji cyfrowych i cyberbezpieczeństwa, wspieranie rozwoju kompetencji cyfrowych wśród pracowników sektora publicznego. Określony został również katalog działań w przedmiotowym obszarze, np. szkolenie pracowników JST z otwierania danych publicznych, e-Kompetencje w obszarze cyberbezpieczeństwa czy Przyjazny urząd – szkolenia z zakresu dostępności cyfrowej ¹⁴¹. Aleksandra Monarcha-Matlak podkreśla znaczenie e-learningu w kontekście podnoszenia kwalifikacji pracowników administracji publicznej. Zaznacza jednak, że „efektywność takiego szkolenia zależy jednak od: technologii informacyjno-komunikacyjnych, treści przekazanych w ramach szkolenia oraz od usług wspierających”¹⁴². Zważywszy na przedstawione powyżej zagadnienia, rozwój kompetencji cyfrowych i edukacja cyfrowa należy uznać za warunki *sine qua non* funkcjonowania elektronicznej administracji.

¹⁴⁰ G. Szpor, Model podnoszenia kompetencji cyfrowych, [w:] Internet. Hacking, (red.) A. Gryszczyńska, G. Szpor, W. R. Wiewiórowski, Warszawa 2023, s. 334.

¹⁴¹ Zob. załącznik do uchwały nr 24 Rady Ministrów z dnia 21 lutego 2023 r. w sprawie ustanowienia programu rządowego pod nazwą „Program Rozwoju Kompetencji Cyfrowych”.

¹⁴² A. Monarcha-Matlak, E-learning w administracji publicznej, [w:] Internet. Prawno-informatyczne problemy sieci, portali i e-usług, (red.) G. Szpor, W. R. Wiewiórowski, Warszawa 2012, s. 374.

Podsumowanie

Nie ulega wątpliwości, że współcześnie kompetencje cyfrowe i polityka cyberbezpieczeństwa to warunki *sine qua non* funkcjonowania elektronicznej administracji. Powyższe wynika z dwóch podstawowych kwestii, po pierwsze konieczności zapewnienia bezpiecznego świadczenia usług na odległość, utożsamianego z ochroną przed cyberzagrożeniami. Po drugie dotyczy rozwoju kompetencji cyfrowych użytkowników nowych technologii, co pozwala zmniejszyć bariery w zakresie dostępności cyfrowej i zwiększyć świadomość wystąpienia cyberzagrożeń.

Prawidłowe funkcjonowanie e-administracji nie jest możliwe bez uszczegółowienia zasad bezpieczeństwa e-informacji, infrastruktury teleinformatycznej i świadczenia e-usług publicznych. W tym celu niezbędne jest opracowanie zasad (polityki) cyberbezpieczeństwa. Należy jednak wskazać, że polityka cyberbezpieczeństwa powinna przede wszystkim uwzględniać takie aspekty jak ochrona danych i informacji, nieprzerwany dostęp do usług i bezpieczeństwo użytkownika końcowego. Na jej kształt wpływ ma również profil danej organizacji, a także potencjalne incydenty czy cyberzagrożenia, które mogą wystąpić w związku ze świadczeniem usług publicznych. Fundamentalne znaczenie odporności systemów teleinformatycznych na cyberzagrożenia, zauważyła Unia Europejska. Na mocy dyrektywy NIS 2 podmioty administracji publicznej uznano za tzw. podmioty kluczowe. Wskazano zatem, że świadczenie e-usług przez te podmioty wymaga wprowadzenia szczególnych zasad cyberbezpieczeństwa.

Istotnym komponentem funkcjonowania elektronicznej administracji są kompetencje cyfrowe zarówno pracowników administracji publicznej, jak i użytkowników e-usług. Niezwykle ważna jest także edukacja cyfrowa wśród wszystkich grup społecznych, dzieci, uczniów, studentów, nauczycieli, seniorów, osób z niepełnosprawnościami, osób pracujących, specjalistów ICT, przedsiębiorców i osób zarządzających i pracowników sektora publicznego. Program Cyfrowa Europa, program polityki „Droga ku cyfrowej dekadzie” do 2030 r a także rządowy Programu Rozwoju Kompetencji Cyfrowych akcentują znaczenie kompetencji cyfrowych w kontekście bezpiecznego i skutecznego świadczenia usług na odległość. Krajowy Program Rozwoju Kompetencji Cyfrowych do kompetencji cyfrowych zalicza kompetencje informatyczne, informacyjno-komunikacyjne oraz funkcjonalne, wskazuje istotę rozwoju podstawowych i zaawansowanych umiejętności i kompetencji cyfrowych oraz edukacji cyfrowej oraz wagę dostępności cyfrowej. Podniesiono w nim potrzebę rozwoju kompetencji cyfrowych wśród pracowników sektora publicznego, w tym zasadność przeprowadzania szkoleń i kursów, cyberbezpieczeństwa i etyki cyfrowej w sektorze publicznym. Reasumując, mając na uwadze powyższe należy jednoznacznie stwierdzić, że kompetencje cyfrowe i polityka cyberbezpieczeństwa to warunki *sine qua non* funkcjonowania elektronicznej administracji.

Bibliografia:

Akty prawne

1. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. nr 78, poz. 483 ze zm.
2. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz. U. z 2024 r. poz. 1077,1222.
3. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie), Dz. Urz. UE L 151 z 7.6.2019 r., s. 15.
4. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/694 z dnia 29 kwietnia 2021 r. ustanawiające program „Cyfrowa Europa” oraz uchylające decyzję (UE) 2015/2240, Dz. Urz. UE L Nr 166, s. 1.
5. 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, Dz.Urz. UE L Nr 333, s. 80.
6. Decyzja Parlamentu Europejskiego i Rady (UE) 2022/2481 z dnia 14 grudnia 2022 r. ustanawiająca program polityki „Droga ku cyfrowej dekadzie” do 2030 r., Dz. Urz. UE L Nr 323, s. 4.
7. Uchwała nr 24 Rady Ministrów z dnia 21 lutego 2023 r. w sprawie ustanowienia programu rządowego pod nazwą „Program Rozwoju Kompetencji Cyfrowych”, M.P. 2023 poz. 318.

Literatura

1. Ganczar M., Umowne partnerstwo publiczno-prywatne w kontekście bezpieczeństwa sieci i informacji administracji publicznej, [w:] Internet. Strategie bezpieczeństwa, (red.) G. Szpor, A. Gryszczyńska, Warszawa 2017.
2. Janowski J., Wpływ technologizacji na informację o prawie, [w:] Modele dostępu do informacji o prawie, (red.) Grażyna Szpor, Warszawa 2014.
3. Kawka I., Kompetencje Unii Europejskiej w zakresie cyfryzacji administracji publicznej państw członkowskich, [w:] Obywatel w centrum działań e-administracji w Unii Europejskiej, (red.) S. Dudzik, I. Kawka, R. Śliwa, Kraków 2023.
4. Monarcha-Matlak A., E-learning w administracji publicznej, [w:] Internet. Prawno-informatyczne problemy sieci, portali i e-usług, (red.) G. Szpor, W. R. Wiewiórowski, Warszawa 2012.
5. Nowak W., Ochrona infrastruktury krytycznej w cyberprzestrzeni, [w:] Cyberbezpieczeństwo. Zarys wykładu, (red.) C. Banasiński, Warszawa 2018.

6. Skoczylas D., Cyberzagrożenia w cyberprzestrzeni. Cyberprzestępczość, cyberterroryzm i incydenty sieciowe, „Prawo w działaniu. Sprawy karne” 2023.
7. Szafrąński B., Główne wyzwania związane z modernizacją funkcjonowania państwa, „Roczniki Kolegium Analiz Ekonomicznych” 2013, nr 29.
8. Szpor G. Cyfryzacja, [w:] Wielka Encyklopedia Prawa, tom XXII. Prawo informatyczne, (red.) G. Szpor, L. Grochowski, Warszawa 2021.
9. Szpor G., Model podnoszenia kompetencji cyfrowych, [w:] Internet. Hacking, (red.) A. Gryszczyńska, G. Szpor, W. R. Wiewiórowski, Warszawa 2023.
10. Świącicki W., Wykorzystanie infografiki w kształtowaniu cyberhigieny wśród użytkowników przestrzeni cyfrowej, [w:] Internet. Hacking, (red.) A. Gryszczyńska, G. Szpor, W. R. Wiewiórowski, Warszawa 2023.
11. Wojnicki J., Modernizacja administracji publicznej w Polsce w XXI wieku – założenia teoretyczne i praktyka administracyjna, „Studia Politologiczne” 2022, vol. 64.
12. Ziółkowska A., Wrażliwość społeczna władzy w kontekście dostępności cyfrowej administracji publicznej, [w:] Obywatel w centrum działań e-administracji w Unii Europejskiej, (red.) S. Dudzik, I. Kawka, R. Śliwa, Kraków 2023.
13. Żuczek S., E-administracja, a konkurencyjność na arenie międzynarodowej, [w:] Międzynarodowa Innowacyjność i Konkurencyjność w XXI w. Aspekty Innowacyjne, (red.) R. Luft, Lublin 2022.

Wykorzystanie chatbotów w polskiej administracji publicznej – wizja czy rzeczywistość

The use of chatbots in polish public administration - vision or reality

Streszczenie

Komunikacja człowieka z maszynami współcześnie rozwija się w porażającym tempie. Aby zredukować zbędne obciążenie pracą człowieka zwłaszcza w powtarzalnych czynnościach dotyczące obsługi zarówno klientów jak i petentów rozbudowane programy komputerowe zastępują człowieka. Stają się one narzędziem dialogu i komunikacji. Narzędzie do dialogu, takie jak Chatbot, który obsługuje jednostki, udziela informacji, służy pomocą, przekazuje dane, stwarza możliwość skierowania zasobów ludzkich do „zadań niemechanicznych”.

Biorąc pod uwagę, że Chatboty wymieniają wiadomości bezpośrednio także pomiędzy podmiotami ze strefy publicznej, mogą zbierać wymagane informacje i dane. Dane te trzeba zabezpieczyć z perspektywy norm prawnych gwarantujących zabezpieczenie danych osobowych, czy praw własności intelektualnej. Pomimo pomocy człowieka we wprowadzaniu baz danych ich aktualizacji i monitorowaniu, program komputerowy działa powtarzalnie, automatycznie, może poprawić efektywność administrowania.

Wprowadzenie

Nowe narzędzia sztucznej inteligencji, które mogą szybko generować teksty pisanne, obrazy, filmy i nie tylko mogą znaleźć w przyszłości zastosowanie w prawnych formach działania administracji jak i metodach jej działania. Przypomnieć należy, że przez prawną formę działania administracji rozumieć 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

publicznej¹⁴³. Natomiast metodą działania administracji jest polityka stosowania pewnych środków pozostających w dyspozycji organów administracyjnych¹⁴⁴. Skoro zarówno formy jak i metody działania, z których korzystają organy administracji publicznej zmierzają do jednego celu jakim jest efektywna realizacja zadań, to każde narzędzie, które może owe działania usprawniać i jest ono legalne może zostać zaadaptowane na potrzeby administrowania. Omawiane w niniejszym rozdziale narzędzie jakim jest chatGPT czyli tzw. chatbot to program komputerowy, które pozwala na interakcję z użytkownikami poprzez interfejs konwersacyjny i użycie języka naturalnego¹⁴⁵. Narzędzie to umożliwia generowanie odpowiedzi na dane wprowadzane przez użytkownika, jest współcześnie jednym z najbardziej zaawansowanych narzędzi do uczenia maszynowego poprzez przetwarzanie języka naturalnego, które zostało opracowane na dużych zbiorach danych w grudniu 2022 roku. Zaledwie miesiąc po jego udostępnieniu dla społeczeństwa narzędzie dotarło do ponad 100 milionów aktywnych użytkowników¹⁴⁶. ChatGPT odpowiada na pytania użytkowników w sposób konwersacyjny i ma możliwość angażowania się w dialogi, przyznania się do błędów w poprzednich odpowiedziach oraz odmowy odpowiedzi na pytanie. Przy jego wykorzystaniu można napisać nie tylko krótkie treści tekstowe lecz całe eseje, książki, czy poezję, a w konsekwencji także i uzasadnienia rozstrzygnięć organów administracji publicznej. Obecnie interfejsy konwersacyjne służą komunikacji między podmiotami gospodarczymi a klientami, lecz w przyszłości równie dobrze co w biznesie mogą sprawdzić się w administrowaniu przez organy administracji publicznej.

Rozwój technologii informatycznej w administracji publicznej

Pandemia Covid-19 przyspieszyła informatyzację w wielu dziedzinach, także w administracji publicznej, zaistniała bowiem potrzeba zdalnej komunikacji z organami administracyjnymi stron postępowania, a także komunikacji pomiędzy samymi organami za pomocą systemów elektronicznych. W organach centralnych zwłaszcza na szczeblu ministerialnym priorytetem stała się cyfryzacja a także automatyzacja rutynowych zadań. Opracowano w 2020 roku strategię „Informatyzacji Państwa – Plan Działań Ministra Cyfryzacji” przedstawiający plan zintegrowanych działań Ministra

¹⁴³ K. Ziemiński, Indywidualny akt administracyjny jako forma prawna działania administracji, Poznań 2005, s. 138.

¹⁴⁴ J. Starościcki, Prawo administracyjne, Warszawa 1975, s. 226.

¹⁴⁵ P. Gatzoufa, V. Saprikis, A literature review on users behavioral intention toward chatbots adoption. Appl Comput Inform. 2022, <https://www.emerald.com/insight/content/doi/10.1108/ACI-01-2022-0021/full/html> [data dostępu: 10.10.2024].

¹⁴⁶ J. Cordero, L.B. Guaman, F. Guam, Use of chatbots for customerservice in MSMEs an Department of Ciencias de la Computacion y Electronica Universidad Tecnica Particular de Loja, Loja, Ecuador, Applied Computing and Informatics Emerald Publishing Limited 2022, s. 30 i n.

Cyfryzacji, których celem jest usprawnienie działania administracji publicznej, a co za tym idzie funkcjonowania państwa polskiego dzięki informatyzacji. Zgodnie z założeniami tego dokumentu, obywatel jest głównym beneficjentem działań administracji, a administracja pełni rolę służebną wobec obywateli, dlatego tak upodobnia się relację pomiędzy public „administrative bodies” a „citizen” do relacji „business” a „client”, w której z powodzeniem wykorzystywane są chatboty. Chatboty są atrakcyjne, ponieważ są zawsze dostępne dla klientów, petentów, czy też stron postępowania. Udzielają niezbędnych odpowiedzi, mogą służyć petentom do jako pomoc w sporządzeniu wniosków, zgłoszeń podatkowych. Organy administracji publicznej mogą wykorzystywać chatboty do obniżania kosztów personelu, usprawniania procesów wewnętrznych i identyfikowania potrzeb w zakresie poprawy relacji z wnioskodawcami. Testy użyteczności wykonane dla tych urządzeń pokazują, że chatboty mogą automatyzować zadania, dostarczać informacji i pomagać w kontaktach ze stronami postępowania, a także w relacjach wewnątrz administracji¹⁴⁷.

Przenosząc się na grunt rzeczywistości polskiej, wskazać należy, że informatyzacja administracji publicznej zakłada takie działania jak: a) pełne zintegrowanie rozproszonych zasobów informatycznych państwa i zapewnienie ich interoperacyjności, a także b) ustandaryzowanie informacji publicznej na rzecz budowy państwa usługowego, w którym obywatele będą mogli korzystać z usług e-administracji w sposób cyfrowy przy zapewnieniu interaktywności komunikacji z urzędem i elektronicznego sposobu załatwiania spraw. Usługi e-administracji są projektowane z zachowaniem standardów dostępności dla osób niepełnosprawnych a dane publiczne są udostępniane w formatach otwartości umożliwiającym automatyczne przetwarzanie maszynowe (bez konieczności składania wniosków). Chociaż przywołana strategia z 2020 roku nie przyniosła od razu zamierzonych to w 2022 roku została ona poddana ewaluacji, zaktualizowana i uzupełniona o konkretne działania, projekty¹⁴⁸. Planowane do realizacji są takie projekty jak: 1) wprowadzenie eID – krajowego oraz paneuropejskiego schematu identyfikacji elektronicznej – narzędzia, które umożliwi obywatelom i przedsiębiorcom dostęp do usług publicznych na Portalu Rzeczypospolitej Polskiej oraz na portalach publicznych (rządowych i samorządowych), a urzędnikom autoryzację, otwierającą dostęp do zasobów informacyjnych państwa, b) wprowadzenie SRP – systemu rejestrów państwowych, wyposażonego w referencyjny model tworzenia i utrzymywania kluczowych rejestrów państwa oraz – dla uproszczenia i automatyzacji procesów administracyjnych – mechanizmy udostępniania gromadzonych w nim informacji, c) wprowadzenie EZD RP – jednolitego systemu elektronicznego zarządzania dokumentacją administracji rządowej, a więc usprawniania działań urzędów oraz integracji systemów dziedzinowych, d) wprowadzenie

¹⁴⁷ J.R. Lewis, The system usability scale: past, present, and future, „International Journal of Human-Computer Interaction” 2018 nr 34(7), s. 577–590.

¹⁴⁸ <https://www.gov.pl/web/cyfryzacja> [data dostępu: 13.10.2024].

Platformy Integracji Usług i Danych – narzędzia odpowiedzialnego za utrzymywanie centralnego rejestru usług, techniczną integrację systemów oraz centralne monitorowanie i raportowanie dostępności usług oraz danych udostępnianych przez poszczególne systemy administracji.

Realizacja postulatu państwa przejrzystego i otwartego na potrzeby obywateli wymaga uporządkowania sposobów komunikacji obywateli z administracją. Administracja informacyjna obsługująca wszystkie kluczowe procesy i realizująca usługi publiczne, w tym usługi cyfrowe, powinna być dla obywateli i przedsiębiorców dostępna w nierozproszonej, jednolitej formie. Automatyzacja skupiać ma funkcje od informacyjnych po usługowe. Na takich założeniach opiera się projekt Portalu Rzeczypospolitej Polskiej, jednolitej bramy informacyjno-usługowej państwa polskiego, która nie tylko zjednoczy rozproszone dotąd kanały informacyjne poszczególnych jednostek administracji publicznej, ale również będzie oferowała cały katalog usług państwowych. Ważnym elementem usprawniania e-usług jest udostępnienie w sposób przejrzysty i atrakcyjny dla usługodawców oraz obywateli danych przestrzennych. Dzięki temu obywatel będzie miał dostęp do przeglądania i wyszukiwania oraz wizualizacji aktualnych zbiorów i danych przestrzennych, usługodawcy zaś uzyskają możliwość korzystania z tych danych i uatrakcyjnienia świadczonych usług.

Korzystanie z instrumentów elektronicznych zwiększa efektywność oraz usprawnia operacje, zarządzanie i administrowanie. Po pierwsze, chatboty mogą być one wykorzystywane z powiedzeniem w komunikacji strony z organem administracji publicznej. Po drugie, mogą być wykorzystywane jako zaplecze helpdesku poprzez odpowiednie udzielanie odpowiedzi na pytania administrowanych.

Chociaż ich użyteczność może okazać się nie do przecenienia dostrzec można także poważne ryzyka. Po pierwsze, są to ograniczenia merytoryczne, nie zawsze jego odpowiedzi czy teksty będą spójne i logiczne, a nadto może prowadzić mogą do naruszeń danych osobowych, czy też własności intelektualnej. Budzi także wątpliwości natury etycznej wykorzystywanie maszyny do zastępowania pracy ludzkiej. Niekiedy maszyna ma wyższe kompetencje aniżeli wykwalifikowany personel ludzki. Zadać można pytanie, czy urządzenie takie jak chatGPT czy jemu podobne mogą znaleźć zastosowanie do sprawowania władzy wykonawczej przez administrację publiczną jak i o granice tego zastosowania.

Czym jest chatGPT i jakie są sposoby jego wykorzystania

ChatGPT to najnowsza technologia uczenia maszynowego, która może generować tekst. Jest to więc jedna z klas technologii, które mogą wykonywać proste zadania pisarskie, obsługiwać bazy danych a także tworzyć uzasadnienia do rozstrzygnięć

administracji publicznej. ChatGPT tworzy tekst, który ma cechy oryginalności i może być przekonujący dla adresata. ChatGPT może być idealnym urządzeniem do odpowiedzi na prawdopodobnie większość pytań, w ramach współdziałania organów poszukujących danych z baz innych organów administracji publicznej. Technologia może wchodzić w interakcje z ludźmi i dostarczać użytecznych informacji. Eric Schmidt powiedział wiele lat temu, że użyteczne są nie same wyszukiwarki baz danych ale takie algorytmy, które generują odpowiedzi, polega na przetwarzaniu danych i przeprowadzeniu tych wyszukiwań, a następnie przygotowanie odpowiedzi¹⁴⁹. Czasami wyniki są prawidłowe, a czasem nie. Jeśli zatem mechanizm jest dobrze opracowany, jeśli dobrze wyselekcjonuje dane to wiele łatwiej będzie prowadzić postępowanie dowodowe, czy wykonywać czynności techniczne i organizatorskie w administracji. Oczywiście jakość odpowiedzi, czy przygotowanego tekstu zależy także od tego w jaki sposób się porozumiemy z maszyną. Podobnie jak w przypadku wyszukiwarek wpisując odpowiednie hasła zapewniamy precyzyjność efektu poszukiwań tak i poddanie danych sztucznej inteligencji będzie jednym z gwarantów jakości wyników. Zatem maszyna ucząca się musi być obsługiwana przez człowieka, który poda/wprowadzi jej niezbędne bazy danych. Sztuczna inteligencja nauczy jej użytkowników zadawać pytania w określony sposób, aby uzyskali odpowiedzi, których potrzebują. Można więc sobie wyobrazić, że organ administracji publicznej podaje dane faktyczne a urządzenie przygotowuje podsumowanie czy też filtruje dane a zatem i nadaje im znaczenie. Maszyna ucząca posiada zatem zdolność do tworzenia sensu. Jakie to jednak niesie niebezpieczeństwa lub ograniczenia? Jakie są więc niebezpieczeństwa, gdy sztuczna inteligencja się myli? A jak często się to zdarza? To są tylko wybrane pytania, na których odpowiedź determinuje użytkowanie takich systemów przez organy administracji publicznej.

Wskazać można, że chatyboty to technologia uczenia maszynowego. Zważywszy, że zwykle mówi się o sztucznej inteligencji myśląc o uczeniu maszynowym, ponieważ to są technologie statystyczne, a te statystyki muszą skądś pochodzić. Zatem wprowadza je człowiek z dostępnych baz danych. Tak wiele jednak zagrożeń wiąże się z podstawowym zestawem danych i znaczeniem tych danych, które są wprowadzane do maszyny. W rezultacie informacje czy teksty, które uzyskuje się z ChatGPT lub innego modelu maszyny uczącej się, będą zawierały patologie właściwe dla Internetu. Rodzaj wprowadzonych baz danych będzie determinował odpowiedzi, odpowiedzi będą wypadkową poglądów użytkowników komputerów. Poglądy te w przypadku stosowania chatuGPT do podejmowania aktów administracyjnych wypełniałyby miejsce dyskrecjonalności organów zarówno w zakresie

¹⁴⁹ <https://www.komputerswiat.pl/aktualnosci/internet/eric-schmidt-moim-najwiekszym-bledem-w-google-bylo/s6p5xkt> [data dostępu: 11.08.2023].

wyboru możliwych rozstrzygnięć, jak i wykładni pojęć nieostrych. Rodzi to zagrożenie braku wyważania wartości i poglądów do której zdolny jest człowiek¹⁵⁰. Nie można zapomnieć jak trafnie wskazuje Chris Hoofnagle internet jest użytkowany przez określoną grupę społeczną, ludzi młodych i w średnim wieku, najczęściej zamożnych wszystko to będzie wpływać na wytwory ChatuGPT, a zatem będzie istniała polityka leżąca u podstaw odpowiedzi ChatGPT¹⁵¹. Problemem jest kwestia weryfikacji informacji podanych w ChatGPT.

Sztuczna inteligencja

Pojęcie sztucznej inteligencji nie ma definicji legalnej jest to bardzo mylący termin, ponieważ oznacza bardzo różnorodne zjawiska. Niektórzy używają pojęcia sztucznej inteligencji do definiowania technologii, takich jak kalkulatory, komputery czy różnego rodzaju czytniki, czy też roboty zastępujące pracę ludzką. Sztuczna inteligencja znana jest z tego, że potrafi wykorzystując swoje zasoby szybciej niż człowiek. Może sprawnie czytać, liczyć. Jest także wąskie ujęcie sztucznej inteligencji odwołuję się ono do technologii uczenia maszynowego, dokonującego analiz statystycznych i ujednolicająca pewne ustalenia. Przetwarzanie statystyk jest zależne od tego, co jest dostępne dla maszyny uczącej się. Jeśli dane wprowadza ktoś o poglądach konserwatywnych czy liberalnych odpowiedzi będą tym determinowane. Rodzi to pytanie w jaki sposób możemy zagwarantować, że te narzędzia wykorzystujące uczenie maszynowe będą wywarzać wartości i nie zaostrzą systemowych nierówności i uprzedzeń społecznych. Skąd musiałyby pochodzić dane, na pewno muszą one mieć najwyższy poziom i jakość. Takie dane zawarte w opracowaniach, książkach są chronione prawem autorskim. Niezbędne będą osoby, które będą monitorować co umieszczane jest w systemach informatycznych. Przykładowo jeśli zamieszczane dane będą miały wydźwięk rasistowski czy antysemitowski to urządzenie uczące się nauczy się tego, i może np. zaprzeczać takim zdarzeniom jak Holocaust. Istnieje także w przypadkach spraw prawnych duże ryzyko zaciągania danych o nieaktualnym stanie prawnym dostępnych przecież na masową skalę w źródłach internetowych. Prawdziwym wyzwaniem dla komputerów nie jest zrozumienie słów, ale zrozumienie także kontekstów, w których te słowa są używane. Dlatego chatboty naśladują ludzką osobowość, zachowanie i dialogi, aby zapewnić użytkownikom wyjątkowe wrażenia obcowania z żywą istotą. Innymi

¹⁵⁰ H. Fakhruddin, The Other Side Of Chatbots. Risks & Disadvantages 2017, at: <http://teks.co.in/site/blog/the-other-side-of-chatbots-risksdisadvantages/> [data dostępu: 10.10.2024].

¹⁵¹ Ch. Hoofnagle, The Capabilities and Limitations of ChatGPT with Professor Chris Hoofnagle, <https://btlj.org/2023/02/berkeley-technology-law-journal-podcast-the-capabilities-and-limitations-of-chatgpt-with-professor-chris-hoofnagle/> [data dostępu: 10.10.2024].

słowy, odpowiadają użytkownikom w kontekście konwersacji. Chatboty pozwalają użytkownikowi na swobodną interakcję i prowadzenie prawdziwej dyskusji. Użytkownik może wpisać zdanie, a bot może przeanalizować szereg parametrów, aby zrozumieć jego intencję i reakcję, jednak z wykorzystaniem wprowadzonych do niej danych¹⁵².

Oznacza to w praktyce, że owej automatyzacji nie można w całości zautomatyzować, bowiem należy dokonywać przeglądu treści zaciąganych do maszyn uczących się i to poprzez stałą weryfikację. Oczywiście dotąd algorytm w pewnym sensie także był wykorzystany, przykładowo w procesie aplikacji na studia, czy ubiegania się o pracę, są to procedury od dawna zautomatyzowane. Jednostki powinny mieć jednak pełne prawo do kwestionowania tego, co zostało ustalone przez maszynę, a ustalenia automatycznie powinny być na skutek zakwestionowania od razu kasowane. To organ miałby obowiązek wykazania, że zaprezentowane treści są przeanalizowane i prawidłowe.

Ponieważ podejmowanie decyzji przez komputer zaczyna dominować w coraz szerszych sferach życia ludzkiego, społeczeństwa będą musiały podejmować decyzje gdzie może to znaleźć zastosowanie, tak aby nie działa się krzywda jednostkom czy niesprawiedliwość. Kadry prawnicze i pracowników administracji będzie należało uczyć wysoko wykwalifikowanych programów takich jak: Python, który jest językiem programowania wysokiego poziomu z bardzo rozbudowanym pakietem bibliotek i baz danych. Dzięki temu znalazł on zastosowanie w wielu dziedzinach związanych m. in. z analizą danych. Niewątpliwie nastąpi rewolucja karierze zawodowej prawników i administratywistów, komputery będą wykorzystywane do wykonywania zadań prawnych. Oznacza to zmianę rozmieszczenia zadań kadry urzędniczej konieczność zdobycia umiejętności zadawania pytań, czy rozpoznania nowych sposobów wyszukiwania informacji.

Niewątpliwie nowe technologie jednak mogą wkraczać w prawa autorskie. Można sobie wyobrazić technologie generatywne wykorzystywane przez artystę do rozwijania koncepcji. Głównymi pytaniami, które pojawiają się w dyskusji, jest to, czy model uczenia maszynowego lub algorytm może uzyskać prawa autorskie. Profesor Samuelson, poruszył ten problem już w 1985 roku, badając, czy komputer może posiadać prawa autorskie wskazując, że współczesny model ochrony praw autorskich na to nie pozwala¹⁵³.

¹⁵² J. Wong, What is a chat bot, and should I be using one?, The Guardian, 6 kwietnia 2016, <https://www.theguardian.com/technology/2016/apr/06/what-is-chat-bot-kik-bot-shop-messaging-platform> [data dostępu: 13.10.2024], a także, A.M. Turing, Computing machinery and intelligence, „Mind”, Volume LIX, Issue 236, 1950, s. 433–460.

¹⁵³ P. Kuczma Dane z internetu. Rola rafinacji informacji sieciowej w kampaniach wyborczych, niepublikowana rozprawa doktorska, Warszawa 2016, s. 210 i n.

Cybernetyka a administrowanie

Cybernetyka jako pojęcie zostało wykorzystane po raz pierwszy w fizyce przez francuskiego uczonego André-Marie Ampère w eseju „*Essai sur la philosophie des sciences*” w 1834 r., w jego treści odniósł cybernetykę do nauki o zarządzaniu i służeniu¹⁵⁴. Zatem w sposób bliskoznaczny pojęciu administrowania¹⁵⁵. Bronisław Trentowski pod pojęciem cybernetyka definiował sztukę rządzenia narodem przez organy państwa¹⁵⁶. Pionierem badań nad cybernetyką był Norbert Wiener, który wskazywał, że jest to komunikacja maszynowa między podmiotami, których to działanie dotyczy¹⁵⁷. Według N. Winera konsekwencją cybernetycznego podejścia do kierowania państwem jest stworzenie automatycznego systemu (aplikacji), która analizuje różne scenariusze działania i na podstawie danych wybiera te najbardziej korzystne pod kątem zaprogramowanego celu. Umożliwia tenże system zastępowanie działań ludzkich dla bardziej wyważonych, zapewniających zasadę równości trafnych rozstrzygnięć władzy publicznej. Co więcej na początku XX w. dokonano nazwania takiej aplikacji „maszyną do rządzenia”. Maszyna do rządzenia byłaby tworem bardzo skomplikowanym, wymagającym olbrzymiej ilości i różnego rodzaju danych dostarczanych w czasie rzeczywistym, przez człowieka. Jednak już wówczas dostrzegano pewne zagrożenia, które sprowadzają się do jej dążenia do przejęcia władzy od ludzi. N. Wiener podkreślał możliwość wykorzystania maszyn do zarządzania przez polityków o złych zamiarach¹⁵⁸. Do zaprogramowania wspomnianej maszyny do rządzenia konieczne są odpowiednie bowiem kryteria, które pozwalałyby wspomnianej maszynie do rządzenia podejmować odpowiednie decyzje lub podpowiadać najlepsze scenariusze ludziom, na których taka odpowiedzialność ciąży.

Narzędzia technologiczne mają także pewną moc wpływania na partycypację społeczeństwa w administrowaniu poprzez ułatwienie kontaktu z administracją. Jeśli państwo ma z informatyzowane dostęp do danych, może stworzyć ramy prawno-instytucjonalne do udzielania ich społeczeństwu i zachęcania do udziału w administrowaniu¹⁵⁹. Państwo znajduje się w określonym otoczeniu, na które składają się podmioty wewnątrz aparatu państwa czyli administracja jak i zewnątrz czyli społeczeństwo. Zarządzanie danymi w państwie musi uwzględniać istotne relacje między nimi. Chociaż wizja państwa i jego organów zarządzanego przez komputer

¹⁵⁴ P. R. Masani, Norbert Wiener 1894–1964, seria „*Vita Mathematica*”, Vol. 5, 1990, s. 252.

¹⁵⁵ S. Gomołka, *Cybernetyka w zarządzaniu organizacją*, Warszawa 2000, s. 92.

¹⁵⁶ B. Trentowski, *Stosunek filozofii do cybernetyki, czyli sztuki rządzenia narodem. Rzecz treści politycznej*, Poznań 1974, s. 203.

¹⁵⁷ N. Wiener, *Cybernetics, or control and communication in the animal and the machine*, Cambridge, Massachusetts, „*The Technology Press*”; New York 1948, s. 53.

¹⁵⁸ N. Wiener, op. cit., s. 68.

¹⁵⁹ B. McLeish, M. Berkowitz, P. Joseph, *The Zeitgeist Movement Defined*, 2013, s. 251.

wyduje się być dziś wizją utopijną i niemożliwą do przeprowadzenia to były w historii próby wprowadzania jej w życie. Jednym z przykładów jest projekt Cybersyn wdrażany w latach siedemdziesiątych w Chile za rządów prezydenta Salvadora Allende. Zakładający próbę zbudowania system komputerowego sprawującego w czasie rzeczywistym kontrolę administracji nad przedsiębiorcami w różnych aspektach ich działalności. Był to projekt innowacyjny, a jego pomysłodawcą był brytyjski teoretyk w dziedzinie zarządzania, Stafford Beer. Przedsiębiorcy zostali zobowiązani do połączenia z siecią pozwalającą na przepływ danych ich działalności. Obserwować można dzisiaj to na gruncie rodzimym w Polsce, chociażby przy okazji regulacji kontroli Inspekcji Ochrony Środowiska wobec przedsiębiorców z branży odpadowej poddany monitorowaniu 24 h na dobę. Owa sieć Cybernet, bo tak została nazwana, była siecią informacyjną między przedsiębiorcami a rządem.

Współcześnie cyfryzacja w administrowaniu doskonale rozwija się w Korei Południowej internet jest technologią wszechobecną w tym państwie. Obywatele Korei mają dostęp do usług publicznych z każdego miejsca w kraju za pomocą sieci Broadband Convergence Networks (BcN). Dzięki temu państwo kreuje nowe usługi publiczne, informuje obywateli o zagrożeniach środowiskowych. Wdrożony już w 2016 roku został program Inteligentnego Rządu (Smart Government), ułatwiający obywatelom komunikację z organami administracji w każdej sprawie online. Europejskim liderem społeczeństwa cyfrowego i administracji cyfrowej jest Estonia. Dostęp do internetu w tym kraju jest definiowany jako prawo człowieka przynależne każdemu obywatelowi¹⁶⁰. Począwszy od 2012 Estonia jest członkiem inicjatywy Partnerstwo Otwartego Rządu prowadzącego repozytorium otwartych danych¹⁶¹. Strategią państw cyfrowych jest dostęp do danych. Państwa regulujące dostęp do tzw. otwartych danych komunikuje się z obywatelami celem poprawy jakości administrowania.

W Polsce także wykorzystywanie informacji sektora publicznego nie jest nowym zagadnieniem prawnym. Regulacja ustanawiająca ramy prawne dla dalszego wykorzystywania informacji pochodzących z sektora publicznego obowiązywała w krajowym porządku prawnym już od 2011 r. Jednakże dopiero ustawa o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, która weszła w życie 8.12.2021 r.¹⁶², otworzyła nowy rozdział w obszarze praw informacyjnych obywateli. Stało się tak za sprawą wprowadzenia do polskiego porządku prawnego normatywnie znaczenie otwartych danych, wyodrębnienia pojęcia danych o wysokiej wartości, danych dynamicznych czy danych badawczych. Ustawa

¹⁶⁰ C. Woodard, Estonia, where being wired is a human right, In a once-crumbling former Soviet republic, even the farmers have broadband Internet access, 1.07.2003, csmonitor.com/2003/0701/p07s01-woeu.html.

¹⁶¹ opendata.riik.ee [data dostępu: 10.10.2024].

¹⁶² Ustawa o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego z dnia 11 sierpnia 2021 r., Dz.U. z 2023 r. poz. 1524.

zabezpieczyła zaplecze instytucjonalne dla realizacji polityki państwa w obszarze otwierania danych. Na pozytywną ocenę zasługuje regulacja funkcji pełnomocnika do spraw otwartości danych czy portalu danych. Znacząco wzrosła rola zautomatyzowanej dystrybucji informacji za pomocą interfejsów programistycznych aplikacji, co więcej prowadzono możliwość udostępniania kodu źródłowego programu komputerowego w celu dalszej eksploatacji przez każdego zainteresowanego użytkownika czy stosowania otwartych standardowych licencji. Sprawia to, że ustawa o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego ma szerszy zakres stosowania od przepisów dyrektywy Unijnej 2019/1024¹⁶³, którą implementuje do polskiego porządku prawnego.

Jednak aby dostęp do danych publicznych był w Polsce w pełni realizowany postulować należałoby także o wyklarowanie definicji legalnej informacji publicznej. Powinna ona dotyczyć wszystkich materiałów znajdujących się w zasobach instytucji publicznych albo przechowywanych w ich imieniu, niezależnie od tego, w jakim formacie są utrwalone i kto je wytworzył, bez wyjątku wszystkich instytucji publicznych i wykonujących funkcje publiczne lub finansowanych ze środków publicznych.

Ponadto, stworzenie w każdym państwie pełnej elektronizacji procesów administrowania na różnych szczeblach wymaga posiadania infrastruktury, narzędzi i know-how jest to projekt wymagający i skomplikowany, łączy on w sobie zarówno aspekty polityczne, prawne, technologiczne jak i finansowe. Wiele pomysłów jest w fazie testowania, analizowania co do skutków społecznych. Sprawna elektronizacja wymaga sprawnie działającej infrastruktury – serwerów pozwalających na magazynowanie i przetwarzanie wielkich zasobów danych, oprogramowania oraz osób, które wiedzą, jak postępować z danymi. Nerozerwalnie wiąże się to z koniecznością ochrony przed ryzykami cyberataków, wpływania na proces rządzenia czy zarządzania przez podmioty do tego nieuprawnione – np. cyberatak na strony samorządowe czy rządowe, wyciekami danych osobowych, czy o charakterze strategicznym dla państwa.

Podsumowanie

Nowe urządzenia takie jak chatboty produkowane przez największe podmioty informatyczne wykorzystywane obecnie przez podmioty prywatne mogą posłużyć także państwu, samorządom i ich organom. Pomogą korzystać z danych i mogą zachęcić do zaangażowania obywateli z jednej strony, ale również

¹⁶³ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (przekształcenie) PE/28/2019/REV/1, OJ L 172, 26.6.2019, p. 56–83.

dostosowywać swój sposób funkcjonowania do nowych relacji komunikacyjnych z drugiej strony. Wykorzystanie chatbotów może być wieloaspektowe, poczynając od komunikowania centralnego w stronę wielokierunkowych konsultacji społecznych i realnego wpływu obywateli na uchwalane prawo i podejmowane decyzje po ułatwienia w stanowieniu prawa czy rozstrzyganiu spraw. Rosnąca popularności elektronicznych form korzystania z usług publicznych (w tym administracji publicznej) potwierdza wdrożenie chatbotów do administrowania. Otwartość danych i dostęp do informacji publicznej jako prawa kluczowe dla obywateli może być wzmocnione za pomocą tego typu technologii informacyjnych. Administracja w państwie wyposażonym w odpowiednie narzędzia technologiczne umożliwiające zaistnienie otwartego rządu i otwartego społeczeństwa, a w konsekwencji cyberpaństwa, z ochroną cybernetyczną działać sprawniej i bliżej jednostki pozostając z nią w stałym kontakcie, budując tym samym zaufanie do administracji publicznej. Oczywiście wielu aspektów zarządzania państwem da się poddać automatyzacji, eliminując obecność człowieka – urzędnika, który może uzyskany w ten sposób czas przeznaczyć na zajmowanie się tylko sprawami wymagającymi czynnika ludzkiego, np. myśleć nad polityką administrowania. Ponadto, w przyszłości decyzje podejmowane przez maszyny będą musiały być w pewnym stopniu weryfikowane przez człowieka, jego rolą będzie także tworzenie i wprowadzanie danych do baz obsługiwanych przez maszyny uczące się. Człowieka nie da się wyeliminować czy w pełni zastąpić, maszyny uczące się mają być narzędziem w jego rękach. Mają podpowiedzieć najlepsze, najbardziej efektywne rozwiązanie, ale w administrowaniu zapewnić racjonalność i efektywność realizacji powierzonych jej zadań.

Bibliografia

Akty prawne

1. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (przekształcenie) PE/28/2019/REV/1, OJ L 172, 26.6.2019.
2. Ustawa o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego z dnia 11 sierpnia 2021 r. (Dz.U. z 2023 r. poz. 1524).

Literatura

1. Cordero J., Guaman L.B., Guam F., Use of chatbots for customerservice in MS-MEs an Department of Ciencias de la Computacion y Electronica Universidad Tecnica Particular de Loja, Loja, Ecuador, Applied Computing and Informatics Emerald Publishing Limited 2022.
2. Gatzidoufa P., Saprikis V., A literature review on users behavioral intention toward chatbots adoption. Appl Comput Inform. 2022, <https://www.emerald.com/insight/content/doi/10.1108/APCI-01-2022-0001/full#ftoc>.

- com/insight/content/doi/10.1108/ACI-01-2022-0021/full/html, [data dostępu: 10.10.2024].
3. Gomółka S., *Cybernetyka w zarządzaniu*, Warszawa 2000.
 4. Hoofnagle Ch., *The Capabilities and Limitations of ChatGPT with Professor Chris Hoofnagle*, <https://btlj.org/2023/02/berkeley-technology-law-journal-podcast-the-capabilities-and-limitations-of-chatgpt-with-professor-chris-hoofnagle/> [data dostępu: 10.10.2024].
 5. Lewis J.R., *The system usability scale: past, present, and future*. *Int J Human-computer Interact*, 2018; 34(7).
 6. Kuczma P., *Dane z internetu. Rola rafinacji informacji sieciowej w kampaniach wyborczych*, niepublikowana rozprawa doktorska, Warszawa 2016.
 7. Masani P. R., *Norbert Wiener 1894–1964*, seria „Vita Mathematica”, Vol. 5, 1990.
 8. McLeish B., Berkowitz M., Joseph P., *The Zeitgeist Movement Defined*, 2013.
 9. Starościak J., *Prawo administracyjne*, Warszawa 1975,
 10. Trentowski B., *Stosunek filozofii do cybernetyki, czyli sztuki rządzenia narodem. Rzecz treści politycznej*, Poznań 1974.
 11. Wiener N., *Cybernetics, or control and communication in the animal and the machine*, Cambridge, Massachusetts, „The Technology Press”; New York 1948.
 12. Wong J., *What is a chat bot, and should I be using one?*, *The Guardian*, 6 kwietnia 2016, <https://www.theguardian.com/technology/2016/apr/06/what-is-chat-bot-kik-bot-shop-messaging-platform> [data dostępu: 13.10.2024.], a także, A.M. Turing, *Computing machinery and intelligence*, *Mind*, Volume LIX, Issue 236, 1950,
 13. Woodard C., *Estonia, where being wired is a human right*, In a once-crumbling former Soviet republic, even the farmers have broadband Internet access, 1.07.2003, csmonitor.com/2003/0701/p07s01-woeu.html [data dostępu: 13.10.2024.].
 14. Ziemiński K., *Indywidualny akt administracyjny jako forma prawna działania administracji*, Poznań 2005.

Zbywanie i oddawanie w użytkowanie wieczyste nieruchomości należących do podmiotów publiczno-prawnych – doświadczenia z czasów pandemii i ich aktualność po jej zakończeniu

Sale and granting permanent usufruct of real estate owned by public and legal entities – experience from the time of pandemic and its relevance today

Streszczenie

Rozdział opisuje specyficzną działalność administracji publicznej, jaką jest gospodarowanie nieruchomości stanowiącym własność Skarbu Państwa i jednostek samorządu terytorialnego oraz problemy prawne z jakimi zetknęła się ona podczas pandemii. Zawiera kilka wypracowanych w 2020 roku rozwiązań prawnych mających na celu ochronę ludzkiego życia i zdrowia. Zachowują one częściową aktualność również w czasach postpandemicznych.

Wprowadzenie

Cyfryzacja i informatyzacja różnych sfer działalności administracji publicznej jest zjawiskiem narastającym i nieuniknionym. Warto, jednakże zauważyć, iż dotyczy różnych zakresów działania administracji w odmiennym stopniu i tempie. Jednym z obszarów, w którym zmiany następowały dość powoli i zdawały się nie nadążać za zmianami technicznymi było zarządzanie nieruchomościami, do których prawa rzeczowe przysługują podmiotom publiczno-prawnym – Skarbowi Państwa i jednostkom samorządu terytorialnego.

Dla porównania wykorzystanie nowych technologii zarówno w prowadzeniu postępowań administracyjnych, jak i udziale organu w postępowaniu sądowo-administracyjnym było przedmiotem licznych zmian ustawodawczych. Zamiarem ustawodawcy w tym zakresie jest np. wprowadzenie obowiązkowego wykorzystania narzędzi informatycznych w komunikacji pomiędzy organami administracyjnymi na

podstawie art. 106 KPA¹⁶⁴, a także pomiędzy nimi a uczestnikami postępowania administracyjnego na skutek wejścia w życie ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych¹⁶⁵ w toku toczących się postępowań administracyjnych¹⁶⁶. Podobnie zauważalnym jest stopniowy wzrost znaczenia narzędzi elektronicznych w procesach partycypacji społecznej w jednostkach samorządu terytorialnego. Choć nadal mimo zastosowania nowych narzędzi komunikacji elektronicznej udział obywateli w tych rodzajach działalności administracji publicznej oceniany jest jako znikomy¹⁶⁷. Na tym tle działania administracji publicznej dotyczące gospodarowania nieruchomością, przez długi czas nie były przedmiotem szerszego zainteresowania ustawodawcy dążącego do cyfryzacji administracji publicznej. Sytuację zmieniła nieco pandemia COVID-19 i konieczność realizacji zadań przez urzędników w warunkach drastycznego ograniczenia możliwości bezpośredniego kontaktu z osobami spoza aparatu administracji publicznej. Można nawet zauważyć, iż w okresie spadku wpływów podmiotów publicznoprawnych z innych źródeł, presja osób kierujących poszczególnymi sektorami administracji publicznej na pozyskiwanie dochodów z gospodarki nieruchomościami, w tym ich sprzedaży, stała się nawet silniejsza. Wypracowane w owym czasie rozwiązania prawne warto poddać ocenie. Wiele z nich pozwala na przyjęcie ich aktualności również po zakończeniu stanu epidemii oraz stanu zagrożenia epidemiologicznego. Inne zaś warto odrzucić jako potencjalne źródło inspiracji dla ustawodawcy, w procesie dalszej cyfryzacji i informatyzacji administracji publicznej.

Specyfika działalności administracji w zakresie gospodarowania nieruchomościami

Niewątpliwie gospodarka nieruchomościami publicznymi nie jest pierwszym skojarzeniem, gdy pomyślimy o relacjach na linii administracja-obywatel. Przepisy w oparciu, o które administracja realizuje swoje zadania w opisywanym zakresie z reguły nie posiadają typowej cechy prawa publicznego jaką jest podporządkowanie obywatela władzy publicznej. Mają charakter prawa prywatnego, jednakże z bardzo istotnymi ograniczeniami z uwagi na konieczność transparentnego gospodarowania mieniem publicznym. Dotyczą części tej sfery działalności państwa i jednostek władzy publicznej, która odbywa się w sferze *dominium* nie zaś *imperium*. W opisywanym zakresie funkcjonowanie

¹⁶⁴ Tj. Ustawa z 14 czerwca 1960 r. - Kodeks postępowania administracyjnego, t.j. Dz. U. z 2024 r. poz. 572.

¹⁶⁵ Dz. U. z 2020 r., poz. 2320.

¹⁶⁶ D. Kościuk, Informatyzacja współdziałania organów administracji po nowelizacji kodeksu postępowania administracyjnego związanej z wejściem w życie ustawy o doręczeniach elektronicznych, „Acta Universitatis Resoviensis Folia Juridica” 2021, nr 3, s. 148

¹⁶⁷ P. Świtał, Wykorzystanie środków komunikacji elektronicznej w procesach partycypacji społecznej, „Acta Universitatis Resoviensis Folia Juridica” 2021, nr 3, s. 352.

administracji publicznej upodabnia się nieco do działalności gospodarczej. Obie sfery działalności są równie ważne, przy czym pierwsza z nich najszerszy wymiar przybiera na najniższym szczeblu samorządu terytorialnego¹⁶⁸. Gospodarowanie nieruchomościami winno bowiem prowadzić, szczególnie w wypadku gmin do uzyskiwania środków, które mogą zostać wykorzystane na realizację innych zadań publicznych¹⁶⁹.

Podstawowym aktem prawnym regulującym działania podmiotów publicznych w opisywanym zakresie jest ustawa z 21 sierpnia 1997 r. o gospodarce nieruchomościami¹⁷⁰. Spośród szeregu zagadnień z różnych dziedzin prawa nieruchomości funkcjonujących w przepisach opisywanej ustawy największa część regulacji dotyczy zasad gospodarowania nieruchomościami przez Skarb Państwa i jednostki samorządu terytorialnego (Dział II). Wspomnieć również wypada, iż redakcja przepisów u.g.n. prowadzi do zdecydowanego wniosku, że określone w nich zasady gospodarowania nieruchomościami stanowiącyymi własność Skarbu Państwa oraz własność jednostek samorządu terytorialnego, w tym również zasady sprzedaży tych nieruchomości, nie mają zastosowania do gruntów należących do innych - poza Skarbem Państwa - państwowych osób prawnych, jak również innych - poza jednostkami samorządu terytorialnego - samorządowych osób prawnych¹⁷¹. Zauważyć również trzeba, iż zgodnie z art. 10 ust. 4 u.g.n.¹⁷² jeśli nieruchomość jest przedmiotem współwłasności Skarbu Państwa lub jednostek samorządu terytorialnego i osób trzecich przepisy o gospodarce nieruchomościami publicznymi stosuje się wyłącznie do gospodarowania udziałem Skarbu Państwa lub jednostek samorządu terytorialnego w nieruchomości. Zasadą jest, iż do czynności prawnych związanych z wspomnianymi nieruchomościami stosuje się przepisy kodeksu cywilnego po ich modyfikacji przez u.g.n., która stanowi w tym zakresie *lex specialis*. Nieruchomości należące do podmiotów publicznych mogą być, zgodnie z art. 13. ust. 1 u.g.n., przedmiotem obrotu. W szczególności ustawodawca dopuszcza ich sprzedaż, zamianę, zrzeczenie się, oddanie w użytkowanie wieczyste, oddanie w najem dzierżawę lub użyczenie a także w trwały zarząd. Mogą być również obciążane ograniczonymi prawami rzeczowymi, wnoszone jako wkłady niepieniężne (aporty) do spółek jak i przekazywane jako wyposażenie dla tworzonych przedsiębiorstw publicznych oraz majątek tworzonych fundacji.

¹⁶⁸ J. Kotlińska, Niekomercyjna działalność gospodarcza gminy - zrozumieć zmysły ustawodawcy, „Finanse Komunalne” 2010, nr 6, s. 6.

¹⁶⁹ C. Kosikowski, Działalność gospodarcza gmin, Białystok 1992, s. 11.

¹⁷⁰ tj.: Dz. U. z 2023 r., poz. 344 ze zm.

¹⁷¹ C. Kociński, Zbycie nieruchomości gruntowej przez Ośrodek Sportu i Rekreacji Spółkę z o.o., „Nowe Zeszyty Samorządowe” 2014, nr 3, s. 45.

¹⁷² Ustawa z 21 sierpnia 1997 r. o gospodarce nieruchomościami, tj: Dz. U. z 2024 r., poz. 1145 ze zm. dalej: u.g.n.

Zbywanie i oddawanie w użytkowanie wieczyste nieruchomości należących do podmiotów publicznoprawnych

Jedną z centralnych instytucji działu II u.g.n. są przepisy regulujące przetargi na zbycie nieruchomości lub oddanie ich w użytkowanie wieczyste. Aktem prawnym o podstawowym znaczeniu dla powyższych czynności jest rozporządzenie z 14 września 2004 r. w sprawie sposobu i trybu przeprowadzenia przetargów i rokowań na zbycie nieruchomości¹⁷³. Wspomniany akt prawny pochodzi sprzed niemal 20 lat i choć był parokrotnie nowelizowany, żadna ze zmian do czasu rozpoczęcia pandemii COVID-19 nie była nakierowana na wykorzystanie nowych narzędzi informatycznych dla usprawnienia procedur, w szczególności przetargów na zbycie nieruchomości.

Ustawodawca traktuje bezprzetargowe zbywanie nieruchomości przez podmioty publicznoprawne jako sytuację potencjalnie korupcjogenną. Założenie to pozwala na przyjęcie, iż jest ono dopuszczalne absolutnie wyjątkowo w wypadkach uregulowanych w art 37 ust.2 u.g.n. Spośród zaś wprowadzonych w w/w przepisie wyjątków największe praktyczne znaczenie ma zbywanie nieruchomości na rzecz właściciela albo użytkownika wieczystego nieruchomości przyległej wobec braku możliwości samodzielnego jej zagospodarowania. Formą domniemaną przez ustawodawcę pozostaje natomiast przetarg, najbardziej transparentny ze sposobów sprzedaży, ale charakteryzujący się również najbardziej rozbudowaną siecią kontaktów międzyludzkich, do których dochodzi podczas jego przeprowadzenia.

Organizator przetargu ma prawo wyboru jednej z jego form zgodnie z art. 40 u.g.n. przetargu ustnego nieograniczonego, przetargu ustnego ograniczonego, przetargu pisemnego nieograniczonego czy też przetargu pisemnego ograniczonego. Przetarg ustny ma za zadanie uzyskanie jak najwyższej ceny, zaś wybór zwycięzcy przetargu pisemnego odbywa się według najkorzystniejszej oferty. Przetarg ograniczony wchodzi w rachubę wówczas, gdy warunki przetargowe mogą być spełnione tylko przez określone osoby¹⁷⁴. W praktyce również w przetargu ustnym jest możliwość zastrzeżenia dodatkowych kryteriów wyboru oferty. Treść tych postanowień nie podlega oczywiście licytacji, jest jednakowa dla każdego oferenta - potencjalnego nabywcy, który przez przystąpienie do przetargu godzi się na włączenie tych postanowień do umowy¹⁷⁵. Jeżeli drugi z przetargów dotyczących nieruchomości zakończył się bez wyłonienia nabywcy, otwiera się dla Skarbu Państwa albo jednostki samorządu terytorialnego możliwość zbycia nieruchomości w drodze rokowań, albo też zgodnie z art. 39 ust. 2 u.g.n. podmioty publicznoprawne mogą organizować kolejne przetargi.

¹⁷³ Tj.: Dz. U z 2021 r., poz. 2213 ze zm.

¹⁷⁴ S.Kalus, Z. Marmaj, E. Mzyk, G. Bieniek, Ustawa o gospodarce nieruchomościami. Komentarz, wyd. IV, red. nauk. G. Bieniek, Warszawa 2010, s. 352.

¹⁷⁵ K. Stefaniuk, Wybór formy przetargu i jego ogłoszenie oraz wniesienie wadium w świetle ustawy o gospodarce nieruchomościami, „Rejent” 1999, nr 10, s. 85.

Ceny wywoławcze nieruchomości w przetargach również są określone w ustawie. Zgodnie z art. 67 ust.2 u.g.n. w pierwszym przetargu cena wynosi nie mniej niż wartość oszacowana przez rzeczoznawcę majątkowego, w drugim zaś nie mniej niż 50 % tej wartości. W rokowaniach prowadzonych po drugim przetargu minimalna cena ustalona z nabywcą nie może być niższa niż 40 % jej wartości. Cena sprzedaży gruntu budowlanego podana przez gminę w dokumentacji przetargowej powinna być, co do zasady, powiększona o 22-proc. podatek VAT w stosunku do kwoty wartości rynkowej tego gruntu, wskazanej przez rzeczoznawcę majątkowego, będącej kwotą netto¹⁷⁶.

Uczestnikowi przetargu w ciągu 7 dni od ogłoszenia wyniku przetargu ustnego lub doręczenia mu informacji o zakończeniu przetargu pisemnego przysługuje możliwość wniesienia skargi na czynności związane z zakończoną procedurą zbywania nieruchomości. Po ewentualnym negatywnym rozpatrzeniu skargi, uczestnikowi przysługuje prawo wniesienia do sądu powszechnego powództwa o stwierdzenie nieważności przetargu, względnie o zobowiązanie podmiotu publicznego prawnego do złożenia oświadczenia woli o zawarciu umowy przenoszącej na rzecz powoda umowy zbycia nieruchomości, albo ustanowienia na jego rzecz użytkowania wieczystego¹⁷⁷. Właściwość sądów administracyjnych jest w sprawie zbycia nieruchomości wyłączona, albowiem, pojawiając się pewne ograniczenia o charakterze publicznoprawnym m.in. obowiązek stosowania procedury przetargowej - nie powodują, że spory w tym zakresie tracą cywilnoprawny charakter¹⁷⁸.

Skutki stanu epidemii i zagrożenia epidemiologicznego dla prowadzenia przez Miasto działalności w zakresie sprzedaży i oddawania w użytkowanie wieczyste nieruchomości

W stanie prawnym opisanym poniżej Skarb Państwa i w szerszym zakresie jednostki samorządu terytorialnego były zobowiązane wykonywać swoje zadania również po wprowadzeniu stanu epidemii, co nastąpiło od dnia opublikowania rozporządzeniem Ministra Zdrowia z 20 marca 2020 r.¹⁷⁹

Kolejne utrudnienia w zakresie bezpośrednich kontaktów międzyludzkich wprowadził § 26 pkt 15 Rozporządzenia Rady Ministrów z dnia 6 maja 2020r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku

¹⁷⁶ E. Rogala, Czy oszacowana przez rzeczoznawcę majątkowego wartość rynkowa gminnego gruntu budowlanego to wartość z podatkiem VAT?, „Finanse Komunalne” 2008, nr 7-8, s. 58.

¹⁷⁷ Wyrok Sądu Okręgowego w Poznaniu z dnia 20 września 2016r. XVIII C 845/15, LEX nr 2213100.

¹⁷⁸ Postanowienie NSA z dnia 31 marzec 2011 r., I OSK 492/11, LEX nr 1079780.

¹⁷⁹ Dz. U. z 2020 r., poz. 491.

z wystąpieniem stanu epidemii¹⁸⁰ ograniczające ilość potencjalnych uczestników spotkania niesłużbowego. Przyjąć zaś należało, iż przetarg nie będzie miał charakteru spotkania służbowego, skoro uczestniczyć w nim będą przede wszystkim osoby niezatrudnione w urzędach administracji publicznej. Podejmując zaś decyzję o organizacji przetargu trudno było przewidzieć ilość osób, które mogły stawić się jako uczestnicy licytacji w siedzibie urzędu. Ewentualne zakażenie osób wirusem COVID-19 na skutek działań organów gminy, niewątpliwie groziło odpowiedzialnością odszkodowawczą jednostki samorządu terytorialnego na podstawie art. 417 czy też nawet art. 417 (2) KC¹⁸¹. Należy również wspomnieć o możliwej odpowiedzialności karnej osób, które by do zakażenia doprowadziły na podstawie poszczególnych paragrafów art. 165 KK¹⁸².

Żadnych istotnych regulacji w zakresie opisywanego zagadnienia nie wprowadziła ustawa z 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, zwana popularnie tarczą antycovidową¹⁸³, ani też jej szybkie liczne nowelizacje. Wręcz przeciwnie nakładały one na jednostki samorządu terytorialnego kolejne obowiązki poprzez np. odroczenie terminu zapłaty opłaty rocznej za użytkowanie wieczyste za rok 2020 do 31 stycznia 2021 r., czy też wprowadzając możliwość przymusowego obniżenia opłaty rocznej albo związanej z przekształceniem prawa użytkowania wieczystego w prawo odrębnej własności. Warto jednak zauważyć, iż a contrario wprowadzała ona pewne regulacje w zakresie prowadzenia postępowań w przedmiocie zamówień publicznych.

Należało zatem na bieżąco rozwiązywać liczne problemy prawne związane z wykonywaniem przez jednostki samorządu terytorialnego zadań z zakresu gospodarki nieruchomości na podstawie przepisów przyjętych przed rozpoczęciem stanu epidemii. W szczególności należało kontynuować działania w celu zgodnego z prawem i sprawnego przeprowadzenia postępowań przetargowych. Nie bez znaczenia była również presja na pozyskanie środków finansowych potrzebnych gminom, powiatom i województwom aby móc realizować inne zadania związane z epidemią o charakterze priorytetowym- mających na celu ratowanie ludzkiego życia i zdrowia.

Wspomnieć należy o kilku wątpliwościach natury prawnej, które należało w owym czasie rozstrzygnąć i które pozostają nadal aktualne, gdyby zagrożenie epidemiologiczne pojawiło się ponownie.

¹⁸⁰ Dz. U. z 2020 r., poz. 86.

¹⁸¹ Tj.: Dz. U. z 2022 r., poz. 1360 ze zm.

¹⁸² Tj.: Dz. U. z 2022 r., poz. 1138 ze zm.

¹⁸³ Tj.: Dz. U. z 2024 r. poz. 374.

Problemy prawne z czasów pandemii

Jedną z pierwszych wątpliwości jakie pojawiły się wiosną i latem 2020 roku była odmowa przez administratorów nieruchomości należących do podmiotów publicznonprawnych fizycznego, bezpośredniego pokazywania nieruchomości w szczególności nieruchomości lokalowych osobom zainteresowanym ich nabyciem. Zwyczajowo nieruchomości te były udostępniane do wglądu dla osób zainteresowanych nabyciem ich własności. Administratorzy zaproponowali, iż będą udostępniać wyłącznie opis, fotografie czy też nagrania filmów obrazujących stan nieruchomości, bez bezpośredniego kontaktu z potencjalnymi nabywcami. Pojawił się pomysł, by przyszli uczestnicy przetargów na nabycie nieruchomości, składali oświadczenia o rezygnacji ze swojego prawa przewidzianego w art. 546 KC z uwagi na stan epidemii. Przedstawioną propozycję należało jednak uznać za sprzeczną z prawem. Proponowane oświadczenie o rezygnacji z uprawnienia przez przyszłego kupującego jako naruszające p rzepis raczej o charakterze *ius cogens* byłoby nieważne. Choć część autorów uznaje, że art. 546 § 1 KC ma charakter dyspozytywny, tzn. strony mogą wyłączyć odpowiedzialność sprzedawcy za brak wykonania przewidzianego w nim obowiązku zarówno w umowie sprzedaży, jak i w poprzedzającej ją umowie przedwstępnej¹⁸⁴, w stosunkach prawnych pomiędzy podmiotem publicznonprawnym a innymi podmiotami prawa tego rodzaju działania nie powinny mieć miejsca. W relacjach z władzą publiczną obywatel jest słabszym partnerem i ma prawo pozostawać w przekonaniu, że działanie jej organów nie narazi go na konflikt z prawem i nie spowoduje dla niego negatywnych konsekwencji finansowych¹⁸⁵. Warto zwrócić uwagę, iż w momencie przygotowywania przetargu na zbycie nieruchomości absolutnie nie powinno się spekulować czy w jego wyniku jako nabywca zostanie wyłoniiony przedsiębiorca, czy też konsument. Zakładając tą drugą możliwość pracownicy urzędów jednostek samorządu terytorialnego, winni są działać z wyższą starannością. Należało zatem zwrócić uwagę, iż praktykowany w czasach przedpandemicznych obowiązek fizycznego udostępniania lokali stanowił tylko jedną z możliwych form realizacji powinności przyszłego sprzedawcy, o którym stanowi art. 546 § 1 k.c. Opracowano zatem inny sposób realizacji tego obowiązku. Ostatecznie przyjęto przesyłanie osobom zainteresowanym dość szczegółowego filmu obrazującego oferowaną nieruchomość, najczęściej lokalu mieszkalnego wraz z informacją, iż stan techniczny i prawny potencjalnego przedmiotu sprzedaży od czasu sporządzenia filmu nie uległ istotnym zmianom.

Kolejną propozycją zmniejszenia ilości kontaktów międzyludzkich mogących skutkować zakażeniem kolejnych osób niebezpiecznym patogenem w działaniach

¹⁸⁴ R. Trzaskowski, Komentarz do art 546 KC [w:] Komentarz do kodeksu cywilnego, Tom IV Zobowiązania Część Szczegółowa, wyd. II (red.) nauk. J. Gudowski, Warszawa 2017, s. 225.

¹⁸⁵ Wyrok Sądu Apelacyjnego w Łodzi z dnia 9 maja 2014 r., I ACa 1460/13, LEX nr 1474372.

jednostek samorządu terytorialnego w zakresie zbywania nieruchomości było planowane dopuszczanie do akceptacji ofert wysłanych drogą mailową- pocztą elektroniczną czy też za pośrednictwem ePUAPU. Jednakże § 17 ust. 1 rozporządzenia Rady Ministrów z 14.09.2004 r. w sprawie sposobu i trybu przeprowadzania przetargów oraz rokowań na zbycie nieruchomości wykluczał w owym czasie w zasadzie wykorzystanie innych środków dostarczenia oferty niż przekazanie jej pocztą, albo w kopercie w skrzynce wystawionej na zewnątrz urzędu i późniejszym potwierdzeniem mailowym wpływu korespondencji. Celem wspomnianego przepisu jest przecież brak dostępu kogokolwiek do treści oferty nabycia nieruchomości przed otwarciem jej na części jawnej przetargu. Przy dostarczeniu oferty przez ePUAP treść ofert byłaby znana urzędnikom wcześniej, co mogłoby mieć istotne znaczenie przy wyborze potencjalnego nabywcy.

Innym pomysłem mającym w zamyśle również prowadzić do zmniejszenia kontaktów międzyludzkich było wykorzystanie w większym niż dotychczas zakresie przetargów pisemnych. Dotychczas ta forma przetargu pojawiała się rzadko, najczęściej w sytuacjach, gdy interes jednostki samorządu terytorialnego nie polegał wyłącznie na uzyskaniu jak najwyższej ceny za nieruchomość. Miał on zastosowanie w wypadku, gdy sprzedaży podlegała nieruchomość położona w miejscu będącym przedmiotem szczególnego zainteresowania lokalnej społeczności. Kryterium wyboru w opisanej sytuacji była nie tylko cena ale przede wszystkim pomysł na wykorzystanie nieruchomości. Mógł on polegać na przedstawieniu oferty świadczenia usług dotychczas nieobecnych w sąsiedztwie, czy też na ciekawym założeniu architektonicznym zabudowy, nie tylko zgodnym z planem zagospodarowania przestrzennego, ale też ładnie komponujący się z sąsiednią historyczną zabudową. W prawie polskim brak jest bowiem instytucji, którą można by określić „wywłaszczeniem estetycznym” i samorząd może tylko rozsądnie gospodarując nieruchomościami zapobiegać obniżeniu poziomu ogólnego wyglądu miejscowości, poprzez realizację nieszablonowych pomysłów jej przyszłego właściciela. Przetarg pisemny nie cieszy się również zainteresowaniem urzędników, gdyż jako odwołujący się do kryteriów nieostrych, uznawany jest przez kontrolujące ich instytucje za potencjalnie bardziej korupcjogenny. W czasie pandemii okazał się być jednak interesującym rozwiązaniem bieżących problemów z organizacją przetargów.

Od razu powstała wątpliwość, czy po pierwszym przetargu ustnym, który nie wyłonił nabywcy nieruchomości, drugi przetarg może zostać zorganizowany jako pisemny. Przyjąć jednak należało, iż stanowiąc w art. 40 ust. 3 u.g.n. o wyborze przez organizatora jednej z form przetargu ustawodawca nie nakazał dokonania jednego wyboru co do wszystkich przetargów dotyczących jednej nieruchomości, ale pozwolił na dokonanie swobodnego wyboru przy każdym przetargu. Nie sposób jednak zaprzeczyć, iż przetarg pisemny planowano zorganizować w sytuacji, gdy konkurencja pomiędzy oferentami miała ograniczać się do wyboru najkorzystniejszej

ceny. Przyjmując zgodnie z art. 40 ust. 3 u.g.n. o nakazie wyboru rodzaju przetargu przez organizatora, ustawodawca nie nakazał dokonania jednego wyboru co do wszystkich przetargów dotyczących jednej nieruchomości. Pozwolił natomiast na dokonanie swobodnego wyboru przy każdym kolejnym przetargu. Tego ostatniego sformułowania ustawodawca w art. 3 u.g.n. jednak nie zdefiniował.

Zakładając racjonalność ustawodawcy należy zatem skorzystać z dorobku powstałego w innych dziedzinach prawa prywatnego stosowanego przez podmioty publiczno-prawne. Pojęciem najkorzystniejszej oferty posługuje się bowiem ustawa z 11 września 2019 r. Prawo Zamówień Publicznych¹⁸⁶ art. 239 ust. 2 stanowi, że jest to oferta przedstawiająca najkorzystniejszy stosunek jakości do ceny lub kosztu lub oferta z najniższą ceną lub kosztem. Wspomniany przepis przyznaje zatem prawo dla zamawiającego samodzielnego ukształtowania kryteriów dla niego najważniejszych w każdym, konkretnym postępowaniu¹⁸⁷. Analogia pozwala tu zatem na przyjęcie, że w art. 40 ust. 2 u.g.n. ustawodawca związał organizatora przetargu ustnego obowiązkiem stosowania wyłącznie kryterium najniższej ceny, zaś organizatorowi przetargu pisemnego zezwolił stosować zarówno kryterium najniższej ceny, jak i inne kryteria. Jeśli zatem za wyborem przetargu pisemnego przemawiały kryteria bezpieczeństwa zdrowotnego, stanowiło one dostateczne uzasadnienie, aby również w przetargu pisemnym zastosować kryterium najniższej ceny.

Inną wątpliwością, która powstała również wiosną i latem 2020r. była prawna możliwość organizowania części jawnej przetargu, o której wspomina § 19 ust. 1 rozporządzenia z 14 września 2004 r. w sprawie sposobu i trybu przeprowadzania przetargów oraz rokowań na zbycie nieruchomości bez fizycznego udziału zainteresowanych osób, ale w postaci ogólnodostępnej transmisji internetowej. Wśród oferentów zainteresowanych nabyciem nieruchomości mogła pojawić się przecież osoba nie mająca dostępu do Internetu. Pomysł nie wzbudził kontrowersji, niewątpliwie działania dotyczące gospodarki nieruchomościami stanowią informacje o mieniu publicznym podlegają ujawnieniu na podstawie ustawy z 6 września 2001 r. o dostępie do informacji publicznej¹⁸⁸. Jedną zaś z form udostępniania informacji publicznej stanowi, zgodnie z art. 7 ust. 1 pkt. 3 *in fine* wspomnianej ustawy, również transmisja audiowizualna i teleinformatyczna. Wobec braku obecności osób niezatrudnionych w urzędzie nie wystąpił problem publikacji ich wizerunku. Rozważano również zagadnienie możliwości ujawnienia tajemnicy przedsiębiorstwa w rozumieniu art. 11 ust.1 ustawy z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji¹⁸⁹, w szczególności ceny oferowanej za nieruchomość. Obawiano się potencjalnej odpowiedzialności karnej

¹⁸⁶ Tj. Dz. U. z 2024.r. poz. 1320.

¹⁸⁷ Ł. Jaźwiński, J. Jerzykowski, M. Kittel, M. Stachowiak, W. Dzierżanowski, Prawo zamówień publicznych. Komentarz, (red.) nauk., W. Dzierżanowski, Warszawa 2021. s. 656

¹⁸⁸ Tj.: Dz.U. z 2022 r., poz. 902.

¹⁸⁹ Tj. Dz.U. z 2022 r., poz. 1233.

na podstawie art. 23 ust. 1 wspomnianej ustawy. Ceny oferowane w przetargach stanowią jednak element informacji publicznej, gdyż osoba zainteresowana mogłaby je uzyskać w zwykłej i dozwolonej drodze wniosku o jej udostępnienie¹⁹⁰. Podobnie same dane potencjalnego nabywcy można było również ujawnić, na tych samych zasadach jak ujawnia się dane podmiotów ubiegających się o udzielenie zamówienia publicznego. Należy również zauważyć, iż uchyla bezprawność ujawnienie, wykorzystanie lub pozyskanie cudzych informacji poufnych, jeśli zmierza ono do ochrony „uzasadnionego interesu chronionego prawem”¹⁹¹, którym w opisywanej sytuacji była ochrona zdrowia i życia ludzkiego.

Rada Ministrów reaguje...

Pewne doświadczenia, które zbierały jednostki samorządu terytorialnego zostały wykorzystane przy zmianie rozporządzenia w sprawie organizacji przetargów i rokowań na zbycie nieruchomości. Rozporządzenie Rady Ministrów z 24 września 2020 r.¹⁹² zmieniające podstawowy akt prawny w zakresie zbywania nieruchomości przez podmioty publicznoprawne weszło w życie dopiero 6 października 2020 r. Wprowadziło ono m.in. rozdział 6a o *Sposobie i trybie przeprowadzania przetargu ustnego nieograniczonego oraz przetargu ustnego ograniczonego w okresie obowiązywania stanu zagrożenia epidemicznego albo stanu epidemii*. Przetargi na zbycie nieruchomości publicznych mogły wreszcie odbywać się na precyzyjnie określonej podstawie prawnej, bez potrzeby bezpośredniego kontaktu pomiędzy komisją przetargową a oferentami. Przepisy te w tej chwili z uwagi na zniesienie stanu zagrożenia epidemiologicznego z dniem 1 lipca 2023 r. nie mogą być już jednak obecnie stosowane.

Podsumowanie

Czas pandemii spowodował powstanie dorobku prawnego w postaci nieszablonych rozwiązań prawnych powstałych w nietypowych warunkach. W pewnej części winien on stanowić materiał dla ustawodawcy pozwalający na podjęcie zmian w obowiązujących przepisach. Jego jednak istotna część pozostaje tylko pewnymi przemyśleniami prawnymi, które nawet nie zawsze zostały zweryfikowane na drodze sądowej. Mimo to warto o powstałych rozwiązaniach pamiętać, jeśli nadal rozwiązania prawne w zakresie gospodarowania nieruchomościami przez podmioty publiczne zostaną utrzymane, na wypadek gdyby sytuacja zagrożenia pandemicznego wystąpiła ponownie, co jak można przypuszczać wcześniej czy później nastąpi.

¹⁹⁰ Wyrok SN z dnia 5 września 2001 r., I CKN 1159/00 OSNC 2002 nr 5 poz. 67.

¹⁹¹ K. Szczepanowska-Kozłowska, E. Nowińska, Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz, wyd. II, (red.) nauk. E. Nowińska Warszawa 2022., s. 277.

¹⁹² Dz.U. z 2020 r., poz. 1698.

Bibliografia:

Akty prawne

1. Ustawa z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego, tj.: Dz. U. z 2024 r. poz. 168.
2. Ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny, tj.: Dz. U. z 2024 r. poz. 1061.
3. Ustawa z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, tj.: Dz.U. z 2022 r., poz. 1233 ze zm.
4. Ustawa z dnia 21 sierpnia 1997 r., o gospodarce nieruchomościami, tj. Dz. U. z 2024r. , poz. 1145.
5. Ustawa z dnia 6 dnia września 2001 r. o dostępie do informacji publicznej, tj.: Dz. U. z 2022 r., poz. 902 ze zm.
6. Ustawa z dnia 11 września 2019 r. - Prawo zamówień publicznych, tj.: Dz. U. z 2024.r., poz. 1320.
7. Ustawa z dnia 2 marca 2020r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych, tj.: Dz. U. z 2024 r., poz. 340 ze zm.
8. Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych, tj.: Dz.U. z 2024 r. poz. 374.
9. Rozporządzenie Rady Ministrów z dnia 2 maja 2020 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii, tj.: Dz. U. z 2020 r., poz. 792.
10. Rozporządzenie Ministra Zdrowia z 20 marca 2020 r. w sprawie ogłoszenia na obszarze RP stanu epidemii, tj.: Dz. U. z 2020 r., poz. 491 ze zm.
11. Rozporządzenia Rady Ministrów z dnia 6 maja 2020 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii, tj.: Dz. U. z 2020 r., poz. 861 ze zm.
12. Rozporządzenie Rady Ministrów z 24 września 2020 r. zmieniające Rozporządzenie w sprawie sposobu i trybu przeprowadzenia przetargów i rokowań na zbycie nieruchomości, Dz.U. z 2020 r. poz. 1698.

Orzecznictwo

1. Postanowienie NSA z dnia 31 marca 2011 r., I OSK 492/11, LEX nr 1079780.
2. Wyrok Sądu Apelacyjnego w Łodzi z dnia 9 maja 2014 r., I ACA 1460/13, LEX nr 1474372.
3. Wyrok Sądu Okręgowego w Poznaniu z dnia 20 września 2016r. XVIII C 845/15, LEX nr 2213100.

Literatura

1. Jaźwiński Ł., Jerzykowski J., Kittel M., Stachowiak M., Dzierżanowski W., Prawo zamówień publicznych. Komentarz, (red.) nauk., W. Dzierżanowski, Warszawa 2021
2. Kalus S., Marmaj Z., Mzyk E., Bieniek G., Ustawa o gospodarce nieruchomościami. Komentarz, wyd. IV, red. nauk. G. Bieniek, Warszawa 2010.
3. Kociński C., Zbycie nieruchomości gruntowej przez Ośrodek Sportu i Rekreacji Spółkę z o.o., „Nowe Zeszyty Samorządowe” 2014, nr 3.
4. Kosikowski C., Działalność gospodarcza gmin, Białystok 1992.
5. Kościuk D., Informatyzacja współdziałania organów administracji po nowelizacji kodeksu postępowania administracyjnego związanej z wejściem w życie ustawy o doręczeniach elektronicznych, „Acta Universitatis Resoviensis Folia Juridica” 2021, nr 3.
6. Kotlińska J., Niekomercyjna działalność gospodarcza gminy - zrozumieć zmysły ustawodawcy, „Finanse Komunalne” 2010, nr 6.
7. Szczepanowska-Kozłowska K., Nowińska E., Ustawa o zwalczaniu nieuczciwej konkurencji. Komentarz, wyd. II, (red.) nauk. E. Nowińska Warszawa 202
8. Rogala E., Czy oszacowana przez rzeczoznawcę majątkowego wartość rynkowa gminnego gruntu budowlanego to wartość z podatkiem VAT?, „Finanse Komunalne” 2008, nr 7-8.
9. Stefaniuk K., Wybór formy przetargu i jego ogłoszenie oraz wniesienie wadium w świetle ustawy o gospodarce nieruchomościami, „Rejent” 1999, nr 10.
10. Śwital P., Wykorzystanie środków komunikacji elektronicznej w procesach partycypacji społecznej, „Acta Universitatis Resoviensis Folia Juridica” 2021, nr 3.
11. Trzaskowski R. [w:] Kodeks cywilny. Komentarz. Tom IV. Zobowiązania. Część szczegółowa, wyd. II, (red.) J. Gudowski, Warszawa 2017

dr Marcin Jan Stępień

Uniwersytet Szczeciński

ORCID: 0000-0002-0762-548X

Adres email: marcin.stepien@usz.edu.pl

Sztuczna inteligencja a cyberbezpieczeństwo – wybrane aspekty regulacji cyberbezpieczeństwa w projekcie Aktu ws. Sztucznej Inteligencji w wersji zaproponowanej przez Parlament Europejski

Artificial intelligence and cybersecurity – selected aspects of cybersecurity in the proposal for an Artificial Intelligence Act in the version proposed by the European Parliament

Streszczenie

Dnia 21 kwietnia 2021 r. Komisja Europejska przedstawiła wniosek zawierający projekt rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii. W niedługim czasie projekt rozporządzenia doczekał się kolejnych wersji. Ostatnia, przyjęta przez Parlament Europejski w czerwcu 2023 r., wprowadza daleko idące zmiany w projektowanym akcie, w tym dotyczące tzw. „modelu generatywnego” systemów sztucznej inteligencji. Istotnym dla problematyki regulacyjnej sztucznej inteligencji na gruncie ww. projekt jest zagadnienie cyberbezpieczeństwa. Zauważa się bowiem, że systemy sztucznej inteligencji powinny być odporne na zagrożenia cybernetyczne. Niniejsze opracowanie poświęcone jest problematyce cyberbezpieczeństwa na tle tekstu projektowanej regulacji dotyczącej sztucznej inteligencji po zmianach zaproponowanych przez Parlament Europejski. Zostało ono przygotowane w oparciu o stan prawny obowiązujący na dzień 21 listopada 2023 r.

Wprowadzenie

Zagadnienie cyberbezpieczeństwa jest jednym z istotnych aspektów projektowanej, unijnej regulacji poświęconej sztucznej inteligencji. Już w pierwotnej wersji projektu rozporządzenia Parlamentu Europejskiego i Rady *ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii*¹⁹³ zagadnieniu temu

¹⁹³ Wniosek Komisji Europejskiej z dnia 21 kwietnia 2021 r. Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej

poświęcono szczególną regulację w art. 15, jakkolwiek pojawia się ono zarówno w motywach, jak i w wielu innych przepisach projektu rozporządzenia. Wydaje się, że na gruncie aktualnej wersji projektu, zaproponowanej w czerwcu 2023 r. przez Parlament Europejski, problematyka cyberbezpieczeństwa zyskała jeszcze bardziej na znaczeniu. W szczególności w kontekście wyróżnienia tzw. generatywnych systemów sztucznej inteligencji. Wymaga zatem przesłedzenia na przeddzień przyjęcia regulacji sztucznej inteligencji, w jakich aspektach ustawodawca unijny odnosi się do problematyki cyberbezpieczeństwa tych systemów.

Cyberbezpieczeństwo w wybranych aktach prawnych Unii Europejskiej do przyjęcia poprawek Parlamentu Europejskiego w sprawie wniosku dotyczącego Aktu ws. Sztucznej Inteligencji

Cyberbezpieczeństwo stanowi jedno z wymagań względem systemów sztucznej inteligencji¹⁹⁴, od początku towarzyszących postulatom regulacyjnym dotyczącym tej technologii w ramach Unii Europejskiej.

Do cyberbezpieczeństwa, jako istotnej materii przyszłej regulacji prawnej systemów sztucznej inteligencji, odnoszono się w Komunikacie Komisji z dnia 7 grudnia 2018 r. do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów *Skoordynowany plan w sprawie sztucznej inteligencji* (COM/2018/795 final)¹⁹⁵. I tak, m.in. w załączniku do powyższego komunikatu podnoszono „zapewnienie „cyberbezpieczeństwa” rozumianego jako zapobieganie nadużyciom (hakovaniu lub manipulacji algorytmami SI, lub też manipulacji danymi przetwarzanymi przez algorytm SI), jak również włączenie mechanizmów zapewniających bezpieczeństwo konsumentów oraz skuteczne dochodzenie roszczeń poszkodowanych w przypadku szkody, a także ułatwiających prowadzenie dochodzeń w przypadku naruszenia integralności systemu SI. Konieczne będzie określenie

inteligencji) i zmieniające niektóre akty ustawodawcze Unii (COM/2021/206 final), <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52021PC0206> [data dostępu: 21.11.2023].

¹⁹⁴ Por. uwagi K. Biczysko-Pudelfko, D. Szostek, *Koncepcje dotyczące osobowości prawnej robotów – zagadnienia wybrane*, „Prawo Mediów Elektronicznych” 2019, nr 2, s. 14-15. W literaturze przedmiotu wskazuje się również na okoliczności, iż to technologia sztucznej inteligencji może sprzyjać rozwijaniu cyberbezpieczeństwa. Jak zauważają J. Worona i Z. Zawadzka „Zastosowanie algorytmów sztucznej inteligencji do przewidywania ataków może w przyszłości znacząco wpłynąć na wzrost cyberbezpieczeństwa” (J. Worona, Z. Zawadzka, 7. Wybrane problemy własności intelektualnej w aspekcie cyberbezpieczeństwa [w:] Cyberbezpieczeństwo. Zarys wykładu, (red.) C. Banasiński, Warszawa 2018, s. 377.). Por. P. Stawicka, Twórca utworu stworzonego przez sztuczną inteligencję, „Prawo Mediów Elektronicznych” 2022, nr 3, s. 29.

¹⁹⁵ Komunikat Komisji Europejskiej z dnia 7 grudnia 2018 r. do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów *Skoordynowany plan w sprawie sztucznej inteligencji* (COM/2018/795 final), <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52018DC0795> [data dostępu: 21.11.2023].

wymogów w zakresie cyberbezpieczeństwa SI, które powinny być oparte na systemie certyfikacji przewidzianym w proponowanych europejskich ramach certyfikacji cyberbezpieczeństwa¹⁹⁶.

Na problematykę cyberbezpieczeństwa uwagę zwróciła również Niezależna Grupa Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji w swoich *Wytycznych w zakresie etyki dotyczącej godnej zaufania sztucznej inteligencji*, opublikowanych 8 kwietnia 2019 r.¹⁹⁷ W szczególności - odnośnie do odporności na cyberataki systemów sztucznej inteligencji, w kontekście stawianego jej wymogu „technologicznej solidności i bezpieczeństwa” (ang. *technical robustness and safety*). Otóż techniczną solidności i bezpieczeństwo zaliczono do kluczowych siedmiu wymogów jakie spełniać powinna godna zaufania sztuczna inteligencja i to w całym cyklu życia tego systemu¹⁹⁸.

Siedem wymagań dotyczących godnej zaufania sztucznej inteligencji zostało następnie powtórzonych w wydanym również 8 kwietnia 2019 r. Komunikacie Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów *Budowanie zaufania do sztucznej inteligencji ukierunkowanej na człowieka*¹⁹⁹. W kontekście cyberbezpieczeństwa, w komunikacie tym, zwrócono uwagę na możliwości zafałszowania wyników działania sztucznej inteligencji za pomocą cyberataków²⁰⁰. Jednocześnie dostrzeżono, iż technologia sztucznej inteligencji może okazać się pomocna przy wykrywaniu zagrożeń związanych z cyberbezpieczeństwem²⁰¹.

Dnia 19 lutego 2020 r. została opublikowana przez Komisję *Biała Księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania*²⁰². W Białej Księdze stwierdzono, że pojawienia się technologii sztucznej inteligencji w ramach produktów lub usług może generować ryzyka, które dotychczas nie były przedmiotem

¹⁹⁶ Załącznik do Komunikatu Komisji Europejskiej z dnia 7 grudnia 2018 r. do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Skoordinowany plan w sprawie sztucznej inteligencji (COM/2018/795 final) s. 7, https://eur-lex.europa.eu/resource.html?uri=cellar:22ee84bb-fa04-11e8-a96d-01aa75ed71a1.0016.02/DOC_2&format=PDF [data dostępu: 21.11.2023].

¹⁹⁷ Wytyczne w zakresie etyki dotyczącej godnej zaufania sztucznej inteligencji z dnia 8 kwietnia 2019 r. Niezależnej Grupy Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji, https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/JURI/DV/2019/11-06/Ethics-guidelines-AI_PL.pdf [data dostępu: 21.11.2023].

¹⁹⁸ Ibidem, s. 29.

¹⁹⁹ Komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 8 kwietnia 2019 r. Budowanie zaufania do sztucznej inteligencji ukierunkowanej na człowieka (COM(2019) 168 final), s. 1, <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52019DC0168&from=GA> [data dostępu: 21.11.2023].

²⁰⁰ Ibidem, s. 2.

²⁰¹ Ibidem, s. 1.

²⁰² Biała księga w sprawie sztucznej inteligencji Europejskie podejście do doskonałości i zaufania z dnia 19 lutego 2020 r. (COM(2020) 65 final), s. 17, <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020DC0065> [data dostępu: 21.11.2023].

materii regulacyjnej Unii Europejskiej. Do ryzyk takich zaliczono w pierwszej kolejności właśnie cyberbezpieczeństwo, a do przeciwdziałania im oraz oceny stopnia ryzyka w kontekście technologii sztucznej inteligencji, postulowano sięgnięcie do doświadczeń Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA)²⁰³.

Następnie, dnia 20 października 2020 r. zostały wydane trzy rezolucje Parlamentu Europejskiego, zawierające zalecenia dla Komisji:

- w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii²⁰⁴,
- w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję²⁰⁵,
- w sprawie praw własności intelektualnej w dziedzinie rozwoju technologii sztucznej inteligencji²⁰⁶.

Szczególnie w rezolucji poświęconej aspektom etycznym w pkt. 100 zaapelowano do Komisji by „zawarła budowanie zdolności w zakresie cyberbezpieczeństwa w swojej polityce przemysłowej w celu zapewnienia, by rozwijano i realizowano bezpieczne, odporne i niezawodne systemy wykorzystujące AI i systemy robotyczne”²⁰⁷.

Wreszcie, dnia 21 kwietnia 2021 r. Komisja przedstawiła wniosek zawierający projekt Rozporządzenia Parlamentu Europejskiego i Rady *ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii*²⁰⁸. Już w motywie 51. projektowanego rozporządzenia uznano, że „cyberbezpieczeństwo odgrywa kluczową rolę w zapewnianiu odporności systemów sztucznej inteligencji na próby modyfikacji ich zastosowania, zachowania, skuteczności działania lub obejścia ich zabezpieczeń przez działające w złej wierze osoby trzecie wykorzystujące podatności systemu”²⁰⁹. Zaś wymaganiami w zakresie cyberbezpieczeństwa w kontekście systemów sztucznej inteligencji wysokiego ryzyka poświęcono regulację zawartą w art. 15 („Dokładność, solidność i cyberbezpieczeństwo”)²¹⁰. W krótkim

²⁰³ Ibidem, s. 17.

²⁰⁴ 2020/2012(INL).

²⁰⁵ 2020/2014(INL).

²⁰⁶ 2020/2015(INI).

²⁰⁷ <https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52020IP0275> [data dostępu: 21.11.2023]. Por. również uwagi R. Stefanicki, Sztuczna inteligencja tworzona przez człowieka, ukierunkowana na osobę ludzką i przez nią kontrolowana, „Przegląd Prawa Handlowego” 2023, nr 1, s. 7).

²⁰⁸ Wniosek Komisji Europejskiej z dnia 21 kwietnia 2021 r. Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii (COM/2021/206 final), <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52021PC0206> [data dostępu: 21.11.2023].

²⁰⁹ Ibidem.

²¹⁰ Por. A. Auleytner, M.J. Stępień, Wymagania względem produktów maszynowych zawierających systemy sztucznej inteligencji. Analiza na tle proponowanych rozwiązań prawnych w prawie Unii Europejskiej, „Prawo Nowych Technologii” 2022, Nr 1, s. 36. M. Nowakowski, Ostatnie zmiany w ramach prawnych dla sztucznej inteligencji w Unii Europejskiej – krytyczna analiza, „Prawo Nowych Technologii” 2021, Nr 2, s. 28.

okresie przedstawiono kolejne wersje projektu rozporządzenia. Wpierw, w listopadzie 2022 r., przedstawiono wersję zaproponowaną przez Radę, zwaną „wersją kompromisową”, czy też „tekstem kompromisowym”²¹¹. Następnie, dnia 14 czerwca 2023 r. przedstawiono wersję projektu, zawierającą poprawki przyjęte przez Parlament Europejski²¹² (dalej jako „Akt ws. Sztucznej Inteligencji”).

Cyberbezpieczeństwo w projekcie Aktu ws. Sztucznej Inteligencji po przyjęciu poprawek Parlamentu Europejskiego

W Akcie ws. Sztucznej Inteligencji zapewnienie cyberbezpieczeństwa systemów sztucznej inteligencji upatruje się jako jeden z elementów gwarantujących, że technologia ta będzie rozwijana zgodnie z wartościami unijnymi. Zaś stosowny poziom cyberbezpieczeństwa powinien charakteryzować system sztucznej inteligencji wysokiego ryzyka w całym cyklu życia tych systemów. Zapewnienie systemów sztucznej inteligencji bezpiecznych i godnych zaufania wymusza, aby systemy takie podlegały pewnym wymogom. W motywie czterdziestym trzecim Aktu ws. Sztucznej Inteligencji wskazuje się na takie wymogi, jak jakość istotność wykorzystywanych danych, rejestrowanie zdarzeń, przejrzystość, nadzór ze strony człowieka, solidność oraz cyberbezpieczeństwo.

Jak wskazano powyżej, już w wersji Komisji Aktu ws. Sztucznej Inteligencji w motywach tego projektu podkreślono „kluczową rolę” cyberbezpieczeństwa systemów sztucznej inteligencji. Odnosi się ona do takich aspektów tych systemów, jak odporność na próby modyfikacji czy obchodzenia ich zabezpieczeń. W motywie pięćdziesiątym pierwszym Aktu ws. Sztucznej Inteligencji wskazuje się na takie przypadki, gdy „cyberataki na systemy sztucznej inteligencji mogą polegać na wykorzystaniu konkretnych zasobów, takich jak zbiory danych treningowych (np. „data poisoning”) lub trenowane modele (np. ataki polegające na wprowadzeniu do modelu złośliwych danych w celu spowodowania niezamierzonego działania systemu lub ataki na poufność)”²¹³. Wskazuje się przy tym - w kontekście zapewnienia pewnego poziomu cyberbezpieczeństwa przez dostawców takich systemów - na ryzyka związane z podatnością systemów sztucznej inteligencji w zakresie m.in. infrastruktury technologii informacyjno-komunikacyjnej (ICT, ang. *information and communication technologies*).

²¹¹ Por. <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/pl/pdf> [data dostępu: 21.11.2023].

²¹² Poprawki przyjęte przez Parlament Europejski w dniu 14 czerwca 2023 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)), https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_PL.html [data dostępu: 21.11.2023].

²¹³ Por. https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_PL.html [data dostępu: 21.11.2023].

Problematyka cyberbezpieczeństwa odgrywa istotną rolę w kontekście wymogu przejrzystości systemów sztucznej inteligencji. Zagadnieniu przejrzystości poświęcono w szczególności art. 13 Aktu ws. Sztucznej Inteligencji („Przejrzystość i udostępnianie informacji”). Na skutek poprawek zaproponowanych przez Parlament Europejski przejrzystość systemów sztucznej inteligencji została doprecyzowana w ustępie pierwszym²¹⁴. Zaś wedle ustępu drugiego art. 13. Aktu ws. Sztucznej Inteligencji do systemów sztucznej inteligencji dołącza się instrukcje obsługi. Powinny być one dołączone w odpowiednim formacie cyfrowym lub udostępnione w innym formacie na trwałym nośniku. Przy tym powinny zawierać informacje zrozumiałe dla użytkowników, przede wszystkim zwięzłe oraz poprawne. Tak, aby były one pomocne użytkownikom takiej technologii przy korzystaniu z systemu sztucznej inteligencji, a także przy podejmowaniu świadomych decyzji związanych z korzystaniem z takiego systemu. W kontekście wymogów w zakresie cyberbezpieczeństwa należy zwrócić uwagę na art. 13 ust. 3 lit. b) ppkt (ii). Aktu ws. Sztucznej Inteligencji. Otóż w świetle tego przepisu informacje zawarte w ww. instrukcjach obsługi powinny zawierać również postanowienia o możliwościach, cechach czy ograniczeniach przy działaniu systemów sztucznej inteligencji wysokiego ryzyka, w tym - w stosownych przypadkach - również dotyczących poziomu cyberbezpieczeństwa, o których mowa w art. 15 Aktu ws. Sztucznej Inteligencji.

Wspominany art. 15 Aktu ws. Sztucznej Inteligencji jest przepisem szczególnie odnoszącym się m.in. do problematyki cyberbezpieczeństwa tych systemów. Wedle ustępu pierwszego tego przepisu systemy sztucznej inteligencji projektuje się z uwzględnieniem zasad bezpieczeństwa na każdym etapie, tj. na etapie projektowania, jak i tzw. „bezpieczeństwa domyślnego”. W efekcie powinny one - systemy sztucznej inteligencji - posiadać odpowiedni poziom cyberbezpieczeństwa oraz z uwzględnieniem tego poziomu działać przez cały cykl życia tych systemów. Obok cyberbezpieczeństwa wskazują się również na osiągnięcie odpowiedniego poziomu dokładności, solidności oraz bezpieczeństwa tych systemów. Wedle zmian zaproponowanych przez Parlament Europejskiego do analizowanego przepisu Aktu ws. Sztucznej Inteligencji, osiągnięcie tych wymogów, tj. w zakresie odpowiedniego poziomu cyberbezpieczeństwa i jego przestrzegania, zakłada wdrożenie stosownych środków odpowiadających aktualnemu stanowi wiedzy, jak również adekwatnych do określonej dziedziny rynku lub obszaru zastosowania.

²¹⁴ Zgodnie z dodanym do projektu akapitem drugim: „Przejrzystość oznacza zatem, że w momencie wprowadzania do obrotu systemu sztucznej inteligencji wysokiego ryzyka wykorzystuje się wszystkie dostępne środki techniczne zgodnie z powszechnie uznanym aktualnym stanem wiedzy, aby zapewnić dostawcy i użytkownikowi możliwość interpretacji wyników systemu sztucznej inteligencji. Użytkownik musi być w stanie zrozumieć system sztucznej inteligencji oraz korzystać z niego na podstawie ogólnej wiedzy na temat sposobu funkcjonowania systemu sztucznej inteligencji i przetwarzanych przez niego danych, dzięki czemu będzie on mógł wyjaśnić decyzje podjęte przez system sztucznej inteligencji osobom, których decyzje te będą dotyczyć zgodnie z art. 68 lit. c).” (https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_PL.html [data dostępu: 21.11.2023]).

W wersji Parlamentu Europejskiego Aktu ws. Sztucznej Inteligencji do art. 29, dotyczącego obowiązków ciążących na operatorach systemów sztucznej inteligencji wysokiego ryzyka, zasugerowano dodanie ust. 1a pkt (iii). Wedle zaproponowanego przez Parlament Europejski przepisu, operatorzy systemów sztucznej inteligencji - w zakresie w jakim sprawują kontrolę nad tymi systemami wysokiego ryzyka - mają obowiązek zapewnienia adekwatnych i aktualnych środków w zakresie cyberbezpieczeństwa. Ponadto, wymaga się od nich, aby regularnie monitorowali skuteczność tych środków.

Pewne zmiany Parlamentu Europejskiego zaproponowane zostały również do regulacji z art. 33 ust. 2 Aktu ws. Sztucznej Inteligencji, która odnosi się do tzw. „jednostek notyfikowanych” i nakłada na nie pewne wymagania w zakresie cyberbezpieczeństwa. W świetle definicji zawartych w projektowanym Akcie ws. Sztucznej Inteligencji jednostki notyfikowane dokonują oceny zgodności, zmierzającej do wykazania, czy spełnione zostały wymagania dla systemów sztucznej inteligencji wysokiego ryzyka (por. tytuł III rozdział 2 aktu), co następnie przekazują na zasadach przewidzianych w tym akcie lub w innych przepisach unijnych (art. 3 akapit 1 pkt 20 i 22 Aktu ws. Sztucznej Inteligencji). I tak, w świetle zmienionego art. 33 ust. 2 Aktu ws. Sztucznej Inteligencji wymaga się aby jednostki notyfikowane spełniały minimalne wymagania w zakresie cyberbezpieczeństwa określone dla jednostek administracji publicznej uznanych za operatorów usług kluczowych na podstawie Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 *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*²¹⁵.

Projektowane przez Parlament Europejski zmiany dotyczą również tzw. „piaskownic regulacyjnych” w zakresie sztucznej inteligencji. W świetle dodanego do art. 3 Aktu ws. Sztucznej Inteligencji pkt. 44g) piaskownica regulacyjna to „ustanowione przez organ publiczny kontrolowane środowisko, które ułatwia bezpieczne opracowywanie, testowanie i walidację innowacyjnych systemów sztucznej inteligencji przez ograniczony czas przed ich wprowadzeniem do obrotu lub oddaniem do użytku zgodnie z określonym planem pod nadzorem regulacyjnym”²¹⁶. I tak, proponuje się przyjęcie w ramach Aktu ws. Sztucznej Inteligencji art. 53a określającego zasady tworzenia i wdrażania oraz funkcjonowania takich piaskownic regulacyjnych. Zasady te mają być sformułowane w akcie delego-

²¹⁵ 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).

²¹⁶ Por. https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_PL.html [data dostępu: 21.11.2023].

wanym, przyjmowanym przez Komisję w porozumieniu z Urzędem ds. Sztucznej Inteligencji. Akt ten ma również określać tryb uczestnictwa i wycofania się z piaskownic regulacyjnych. W świetle ustępu drugiego lit h) powyższego artykułu wskazuje się na kwestie dotyczące systemów sztucznej inteligencji „istotne” dla piaskownic regulacyjnych - w tym cyberbezpieczeństwo. Ustanawia się przy tym aby piaskownice sprzyjały tworzeniu narzędzi i infrastruktury do testowania, analizy i wyjaśnienia również ww. aspektu sztucznej inteligencji jakim jest cyberbezpieczeństwo²¹⁷.

Rola Agencji Unii Europejskiej ds. Cyberbezpieczeństwa w świetle zmienionego projektu Aktu ws. Sztucznej Inteligencji

Parlament Europejski zaproponowała uzupełnienie art. 15 Aktu ws. Sztucznej Inteligencji o dwa kolejne ustępy (1a-1b), z których ważnym w kontekście cyberbezpieczeństwa jest nowy ust. 1b. Zgodnie z proponowanym brzmieniem: „aby sprostać wszelkim pojawiającym się na rynku wewnętrznym problemom związanym z cyberbezpieczeństwem, Agencja Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) współpracuje z Europejską Radą ds. Sztucznej Inteligencji zgodnie z art. 56 ust. 2 lit. b)”²¹⁸. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa w świetle Aktu o cyberbezpieczeństwie²¹⁹ jest następcą utworzonej w 2004 r. Europejskiej Agencji ds. Bezpieczeństwa Sieci i Informacji (ENISA, ang. *European Network and Information Security Agency*)²²⁰. W świetle Aktu o cyberbezpieczeństwie ENISA ma stanowić instytucję wspierającą cyberbezpieczeństwo w Unii Europejskiej, dysponującą profesjonalną wiedzą w zakresie cyberbezpieczeństwa. Jej celem w świetle art. 4 ww. aktu jest m.in. wspieranie państw członkowskich oraz instytucji i organów Unii Europejskiej w realizacji polityki unijnej w sektorze cyberbezpieczeństwa. Zaś w świetle art. 11 tego aktu - również doradzanie tymże instytucjom oraz państwom członkowskim w zakresie innowacji i badań nad cyberbezpieczeństwem. Stąd art. 15 ust. 1b Aktu ws. Sztucznej Inteligencji wskazujący na współpracę z Agencją Unii Europejskiej ds. Cyberbezpieczeństwa należy uznać jako realiza-

²¹⁷ Por. uwagi K. Wyderka, Piaskownica regulacyjna jako instrument wspierania innowacji w zakresie sztucznej inteligencji, „Prawo Mediów Elektronicznych” 2023, nr 2, s. 10.

²¹⁸ Por. https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_PL.html [data dostępu: 21.11.2023].

²¹⁹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. U. UE. L. z 2019 r. Nr 151, str. 15), dalej jako: „Akt o cyberbezpieczeństwie”.

²²⁰ ENISA została utworzona na mocy rozporządzenia (WE) nr 460/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiającego Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (Dz. U. UE. L. z 2004 r. Nr 77, str. 1 ze zm.). Por. K. Chałubińska-Jentkiewicz, 9. Zagrożenia związane z nowymi technologiami. Cyberprzestępczość a bezpieczeństwo w sieci [w:] Prawo nowych technologii. Wybrane zagadnienia, red. K. Chałubińska-Jentkiewicz, M. Karpiuk, Warszawa 2015, s. 410.

cję postanowień art. 4 ust. 1 Aktu o cyberbezpieczeństwie. Na skutek zmian zaproponowanych przez Parlament Europejski ulec zmianie ma również Europejska Rada ds. Sztucznej Inteligencji przemianowana na Europejski Urząd ds. Sztucznej Inteligencji (por. art. 56 ust 1 Aktu ws. Sztucznej). Akt ws. Sztucznej Inteligencji określa strukturę i zadania Europejskiego Urzędu ds. Sztucznej Inteligencji. Warto nadmienić, że w świetle zmian zaproponowanych przez Parlament Europejski, dodany do projektu Aktu ws. Sztucznej Inteligencji art. 57 a ust. 1 lit d, zakłada, że w skład zarządu Europejskiego Urzędu ds. Sztucznej Inteligencji wchodzi jeden przedstawiciel Agencji Unii Europejskiej ds. Cyberbezpieczeństwa, bez prawa głosu. W skład zarządu ponadto wchodzić będą po jednym przedstawicielu Komisji, Europejskiego Inspektora Ochrony Danych (EIOD) oraz Agencji Praw Podstawowych Unii Europejskiej (FRA), również bez prawa głosu. Przy tym, w skład zarządu wchodzić mają ponadto przedstawiciele krajowych organów nadzorczych ds. sztucznej inteligencji z każdego państwa członkowskiego, dysponujący prawem głosu. Powyższe wskazuje na doradczą funkcję przedstawiciela Agencji Unii Europejskiej ds. Cyberbezpieczeństwa w składzie tego centralnego organu Europejskiego Urzędu ds. Sztucznej Inteligencji. Należy bowiem zauważyć, że zarząd w świetle art. 57b ust. 1 lit. a) Aktu ws. Sztucznej Inteligencji jest organem, który ma podejmować „strategiczne decyzje dotyczące działalności Urzędu ds. Sztucznej Inteligencji”.

Na marginesie niniejszych uwag można dodać, że w czerwcu 2023 r. Agencja Unii Europejskiej ds. Cyberbezpieczeństwa przedstawiła analizę zatytułowaną *Badania nad sztuczną inteligencją i cyberbezpieczeństwem* (ang. *Artificial intelligence and cybersecurity research*)²²¹. Na s. 5 przedmiotowej analizy czytamy, że badania nad sztuczną inteligencją na potrzeby cyberbezpieczeństwa oraz zapewnienie bezpiecznej sztucznej inteligencji, stanowią realizację obowiązków agencji wynikających z ww. art. 11 Aktu ws. Cyberbezpieczeństwa. Analiza zawiera pewne wskazania w zakresie wpływu sztucznej inteligencji na cyberbezpieczeństwo skierowane przede wszystkim do Komisji oraz Europejskiego Centrum Kompetencji w dziedzinie Cyberbezpieczeństwa (ECCC, ang. *European Cybersecurity Competence Centre*). Poddanie głębszej uwadze przedmiotowej analizy wykracza poza temat niniejszego opracowania, niemniej jednak warto zwrócić uwagę na jej konkluzje. I tak, zauważa się w analizie, że rozwój technologii sztucznej inteligencji stanowi ważny czynnik umożliwiający innowację w dziedzinie cyberbezpieczeństwa, m.in. z uwagi na to, że daje ona duże, nieznane dotychczas możliwości w zakresie wykrywania cyberzagrożeń oraz reagowania na nie.

²²¹ S. Ntalampiras, G. Misuraca, P. Rossel, Artificial intelligence and cybersecurity research - ENISA Research and Innovation Brief, European Union Agency for Cybersecurity 2023.

Cyberbezpieczeństwo a generatywne systemy sztucznej inteligencji

Novum na tle proponowanych zmian Parlamentu Europejskiego dotyczy modelu generatywnego (ang. *foundation model*) systemów sztucznej inteligencji. Generatywne systemy sztucznej inteligencji, jak zauważa się w literaturze, zdolne są do zaawansowanych działań zbliżonych do działalności twórczej człowieka²²². Jak wskazują M. Kubiak i M. Kudła, wyodrębnienie tej szczególnej kategorii systemów sztucznej inteligencji przez Parlament Europejski „wynika z licznych problemów, które ujawniły się na tle korzystania z rozwiązań takich jak ChatGPT. Projekt wprowadza szereg obowiązków nakładanych na dostawców modeli generatywnych jeszcze przed wprowadzeniem takiego modelu do obrotu lub oddaniem go do użytku”²²³. I tak, zaproponowany art. 28b Aktu ws. Sztucznej Inteligencji określa obowiązki dostawcy modelu generatywnego.

Artykuł 28b określa wymogi, które powinny być spełnione dla modelu generatywnego przed wprowadzeniem go do obrotu lub oddaniem do użytku przez dostawcę. Przy tym, nie jest istotne w jaki sposób eksploatowany ma być model generatywny sztucznej inteligencji, tj. jako samodzielny produkt, element systemu sztucznej inteligencji, czy jako wmontowany w produkt. Projektodawca unijny przykładowo wskazuje również na taką eksploatację jak ta, że może być on dostarczany na podstawie nieodpłatnych lub publicznych licencji. I tak, jeden z wymogów, określonych w ust. 2 lit c) powyższego artykułu, przewiduje, że model generatywny powinien być tak projektowany i rozwijany, aby przez cały cykl jego życia spełniał on odpowiedni poziom cyberbezpieczeństwa. Cyberbezpieczeństwo na odpowiednim poziomie wymagane jest również obok takich cech, które powinien spełniać model generatywny, jak skuteczności działania, przewidywalności, interpretowalności, korygowalność czy bezpieczeństwo. Osiągnięcie odpowiedniego poziomu, w tym cyberbezpieczeństwa, modelu generatywnego może być oceniane za pomocą wszelkich „adekwatnych metod”, w tym takich jak niezależne opinie ekspertów, dokumentacja, analizy przeprowadzane na różnych etapach, testy modelu, np. na etapie opracowywania, projektowania czy realizacji.

²²² I tak, „do systemów AI zaliczamy też narzędzia Generative AI pozwalające na generowanie dzieł postrzeganych jako „utwory” podobne do tych tworzonych przez człowieka. Generatywna sztuczna inteligencja to rodzaj sztucznej inteligencji, który pozwala na tworzenie nowych treści (takich jak obrazy, tekst, audio czy wideo), wzorców lub rozwiązań na podstawie dostępnych systemowi, wytrenowanych uprzednio danych. Do tworzenia tych danych system oparty na Generative AI wykorzystuje m.in. algorytmy uczenia maszynowego, głównie sieci neuronowe, naśladując w ten sposób ludzki proces twórczy.” (A. Auleytner, T. Zalewski, Sprawozdanie z debaty Stowarzyszenia Prawa Nowych Technologii na temat zagadnień prawnoautorskich dotyczących generatywnej sztucznej inteligencji, „Prawo Nowych Technologii” 2023, nr 1, s. 36). Por. A. Bar, Prawo autorskie w erze sztucznej inteligencji. Uwagi na tle historii „Portretu Edmonda de Belamy”, „Prawo Mediów Elektronicznych” 2022, nr 1, s. 24.

²²³ M. Kubiak, M. Kudła, Stronniczość i uprzedzenia sztucznej inteligencji (AI Bias) - ryzyko i sposoby jego mitygacji, „Prawo Nowych Technologii” 2023, Nr 2, Legalis.pl, <https://sip.legalis.pl/document-full.seam?documentId=mjxw62zogi3danbugaydsmy&refSource=search#tabs-metrical-info> [data dostępu: 21.11.2023].

Podsumowanie

Cyberbezpieczeństwo stanowi jedno z zagadnień, które od początku upatrywano jako istotny element przyszłej, unijnej regulacji systemów sztucznej inteligencji. Mianowicie regulacji, która będzie sprzyjała tworzeniu technologii godnej zaufania, co możliwe będzie do osiągnięcia przy określeniu wymagań dotyczących opracowywania i eksploataowania systemów również odpornych na cyberzagrożenia.

W kolejnych aktach organów Unii Europejskiej, poświęconych sztucznej inteligencji, nawiązywano do cyberbezpieczeństwa, w ślad za czym – przedstawiano propozycje regulacyjne. W efekcie, już w pierwszej wersji projektu Aktu ws. Sztucznej Inteligencji, przedstawionej przez Komisję w 2021 r., zagadnienie cyberbezpieczeństwa stało się jednym z kluczowych wymogów odniesionych do systemów sztucznej inteligencji, mających swoje uregulowanie w wielu postanowieniach tego aktu. Tym samym, pomimo, że zagadnienie to od początku stanowiło ważki aspekt projektowanej w ramach Unii Europejskiej regulacji systemów sztucznej inteligencji, nie da się nie odnieść wrażenia, że cyberbezpieczeństwo nabrało jeszcze większego znaczenia na tle regulacji projektowanego Aktu ws. Sztucznej Inteligencji po poprawkach zaproponowanych przez Parlament Europejski.

Na powyższe wskazuje m.in. uwzględnienie roli Agencji ds. Cyberbezpieczeństwa w ramach Zarządu Urzędu ds. Sztucznej Inteligencji, który to organ – jak czytamy z proponowanych zmian – będzie podejmować strategiczne decyzje dotyczące działalności Urzędu. Również świadczy o tym uwzględnienie ryzyk związanych z cyberbezpieczeństwem tzw. modeli generatywnych systemów sztucznej inteligencji. Wzrost zainteresowania problematyką cyberbezpieczeństwa należy przyjąć z aprobatą, bowiem sprostanie temu problemowi jest warunkiem bezpiecznego użytkowania technologii sztucznej inteligencji. W szczególności, w kontekście wyróżnienia generatywnej kategorii systemów sztucznej inteligencji. Otóż działające w wyższym stopniu zaawansowane generatywne systemy sztucznej inteligencji, stanowią większe wyzwanie odnośnie do ustalenia zachodzących w nich procesów działania. Przez to ich zachowania okazują się mniej przewidywalne, a nadzór człowiek nad działaniem takich systemów staje się coraz bardziej utrudniony. Tym samym, w kontekście potrzeby zapewnienia również bezpiecznych modeli generatywnych zagadnienie cyberbezpieczeństwa znowu zyskuje na znaczeniu dla regulacji systemów sztucznej inteligencji.

Bibliografia

Akty prawne

1. Komunikat Komisji Europejskiej z dnia 7 grudnia 2018 r. do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Skoordinowany plan w sprawie sztucznej inteligencji (COM/2018/795 final).
2. Komunikat Komisji Europejskiej do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 8 kwietnia 2019 r. Budowanie zaufania do sztucznej inteligencji ukierunkowanej na człowieka (COM(2019) 168 final).
3. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) (Dz. U. UE. L. z 2019 r. Nr 151, str. 15).
4. Biała księga w sprawie sztucznej inteligencji Europejskie podejście do doskonałości i zaufania z dnia 19 lutego 2020 r. (COM(2020) 65 final).
5. Rezolucja Parlamentu Europejskiego, zawierająca zalecenia dla Komisji z dnia 20 października 2020 r. w sprawie ram aspektów etycznych sztucznej inteligencji, robotyki i powiązanych z nimi technologii (2020/2012(INL)).
6. Rezolucja Parlamentu Europejskiego, zawierająca zalecenia dla Komisji z dnia 20 października 2020 r. w sprawie systemu odpowiedzialności cywilnej za sztuczną inteligencję (2020/2014(INL)).
7. Rezolucja Parlamentu Europejskiego, zawierająca zalecenia dla Komisji z dnia 20 października 2020 r. w sprawie praw własności intelektualnej w dziedzinie rozwoju technologii sztucznej inteligencji (2020/2015(INI)).
8. Wniosek Komisji Europejskiej z dnia 21 kwietnia 2021 r. Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniające niektóre akty ustawodawcze Unii (COM/2021/206 final).
9. Poprawki przyjęte przez Parlament Europejski w dniu 14 czerwca 2023 r. w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej inteligencji (akt w sprawie sztucznej inteligencji) i zmieniającego niektóre akty ustawodawcze Unii (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)).
10. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. U. UE. L. z 2022 r. Nr 333, str. 80).

Literatura

1. Auleytner A., Stępień M. J., Wymagania względem produktów maszynowych zawierających systemy sztucznej inteligencji. Analiza na tle proponowanych rozwiązań prawnych w prawie Unii Europejskiej, „Prawo Nowych Technologii” 2022, nr 1.
2. Auleytner A., Zalewski T., Sprawozdanie z debaty Stowarzyszenia Prawa Nowych Technologii na temat zagadnień prawnoautorskich dotyczących generatywnej sztucznej inteligencji, „Prawo Nowych Technologii” 2023, nr 1.
3. Banasiński C. (red.), Cyberbezpieczeństwo, Warszawa 2018.
4. Bar A., Prawo autorskie w erze sztucznej inteligencji. Uwagi na tle historii „Portretu Edmonda de Belamy”, „Prawo Mediów Elektronicznych” 2022, nr 1.
5. Biczysko-Pudełko K., Szostek D., Koncepcje dotyczące osobowości prawnej robotów – zagadnienia wybrane, „Prawo Mediów Elektronicznych” 2019, nr 2.
6. Chałubińska-Jentkiewicz K., Karpiuk M. (red.), Prawo nowych technologii. Wybrane zagadnienia, Warszawa 2015.
7. Kubiak M., Kudła M., Stronniczość i uprzedzenia sztucznej inteligencji (AI Bias) - ryzyko i sposoby jego mitygacji, „Prawo Nowych Technologii” 2023, nr 2.
8. Nowakowski M., Ostatnie zmiany w ramach prawnych dla sztucznej inteligencji w Unii Europejskiej – krytyczna analiza, „Prawo Nowych Technologii” 2021, nr 2.
9. Stawicka P., Twórca utworu stworzonego przez sztuczną inteligencję, „Prawo Mediów Elektronicznych” 2022, nr 3.
10. Stefanicki R., Sztuczna inteligencja tworzona przez człowieka, ukierunkowana na osobę ludzką i przez nią kontrolowana, „Przegląd Prawa Handlowego” 2023, nr 1.
11. Wyderka K., Piaskownica regulacyjna jako instrument wspierania innowacji w zakresie sztucznej inteligencji, „Prawo Mediów Elektronicznych” 2023, nr 2.

Netografia

1. <https://data.consilium.europa.eu/doc/document/ST-14954-2022-INIT/pl/pdf> [data dostępu: 21.11.2023].

Inne

1. Wytyczne w zakresie etyki dotyczącej godnej zaufania sztucznej inteligencji z dnia 8 kwietnia 2019 r. Niezależnej Grupy Ekspertów Wysokiego Szczebla ds. Sztucznej Inteligencji;
2. S. Ntalampiras, G. Misuraca, P. Rossel, Artificial intelligence and cybersecurity research - ENISA Research and Innovation Brief, European Union Agency for Cybersecurity 2023.

Elektroniczne konsultacje społeczne

Electronic public consultations

Streszczenie

Demokracja jako ustrój państwa daje możliwość sprawowania władzy przez obywateli. Powszechne staje się zaangażowanie obywateli w sprawy publiczne. Akcentowany jest udział obywateli w formach partycypacji społecznej. Gwarancje prawne wprowadzane są jako wymóg w wielu procedurach w administracji publicznej. Z reguły mają one charakter fakultatywny. Pomimo gwarancji prawnych dla obywateli zauważalny jest niski udział obywateli w procesach decyzyjnych. Odpowiedzią na ten problem może stać się zastosowanie form elektronicznych. Są one stosowane alternatywnie do tradycyjnej formy prowadzenia konsultacji. Mają one wiele zalet w zakresie pozyskiwania informacji. Wśród form znaleźć można ankiety elektroniczne, geoankiety, geodyskusje. Celem rozdziału na gruncie nauk prawnych jest przedstawienie elektronicznych konsultacji społecznych. W pracy zostaną przeanalizowane założenia konsultacji społecznych, elektroniczna partycypacja społeczna, a następnie omówione elektroniczne formy partycypacji społecznej.

Wprowadzenie

Konsultacje społeczne są instytucją demokracji bezpośredniej, polegającą na wyrażaniu przez członków zbiorowości opinii na temat przedstawionego jej zagadnienia, oraz jedną z metod dialogu obywatelskiego. Jest to proces informowania i zasięgania opinii obywateli podczas podejmowania najważniejszych decyzji dotyczących aktów prawnych, planowanych inwestycji oraz innych istotnych przedsięwzięć. Konsultacje inicjowane są zarówno przez przedstawicieli władz rządowych bądź samorządowych, jak i przez podmioty społeczne, a uczestniczyć w nich mogą pojedynczy obywatele, reprezentujące ich instytucje i organizacje pozarządowe oraz specjaliści i eksperci zewnętrzni²²⁴. Magdalena Tabernacka zauważa, że

²²⁴ A. Ferens, R. Kondas, I. Matysiak, G. Rzeźnik, M. Szyrski, Jak skutecznie prowadzić konsultacje społeczne w samorządach. Zasady i najlepsze praktyki współpracy samorządów z przedstawicielami społeczności lokalnych. Przewodnik dla samorządowców, Warszawa 2010, s. 13.

podstawowym warunkiem istnienia społeczeństwa obywatelskiego jest istnienie powszechnej i niezagrożonej represyjnymi działaniami ze strony państwa komunikacji obywateli z władzą²²⁵.

Wyrazem idei demokracji jest uznanie, że danej społeczności (grupie, społeczeństwu) przysługuje naturalne prawo decydowania o swoich sprawach w sposób bezpośredni (demokracja bezpośrednia) bądź za pośrednictwem przedstawicieli. Rozróżnienie na demokrację bezpośrednią i demokrację przedstawicielską (pośrednią) jest właściwie we współczesnej demokratycznej formie państwa²²⁶. Demokracja to ideał społeczeństwa wolnego od dominacji, którego podstawę stanowi racjonalna, niezakłócona komunikacja społeczna. Jest formą wspólnoty życia zbiorowego i uczestnictwa w życiu społecznym, a więc typem kultury, a nie tylko formą rządów, choć niewątpliwie ten aspekt stanowi najczęstszy przedmiot analiz przedstawicieli doktryny²²⁷. Demokracja bezpośrednia zakłada zatem sprawowanie władzy wprost przez samych obywateli – bez elementów pośredniczących. Jest to najbardziej samorządny sposób decydowania społeczności o własnym losie²²⁸. Demokracja bezpośrednia jest to zatem forma wyrażania woli przez suwerenne społeczeństwo, która polega – ogólnie rzecz ujmując – na bezpośrednim uczestnictwie²²⁹.

Uczestnictwo obywateli związane jest z pojęciem partycypacji społecznej. Z punktu widzenia nauki prawa administracyjnego i nauki administracji pojęcie partycypacji ma różne zasadnicze znaczenia. Związane są one nieodłącznie z pojęciem demokracji jako formy ustroju państwa. Partycypacja polega na posiadaniu przez wszystkich obywateli praw i wolności zapewniających każdemu udział w sprawowaniu władzy. To uczestniczenie w sprawowaniu władzy przybiera formy bezpośredniej lub pośredniej formy sprawowania władzy²³⁰. Paweł Starosta uważa natomiast, że partycypacja polega na braniu udziału mieszkańców w zbiorowych czynach, akcjach i przedsięwzięciach wyrastających z faktu użytkowania zasobów

²²⁵ M. Tabernacka, Komunikacja obywateli z władzą – warunek funkcjonowania demokracji i społeczeństwa obywatelskiego, [w:] *Public relations w sferze publicznej. Wizerunek i komunikacja*, (red.) M. Tabernacka, A. Szadok-Bratuń, Warszawa 2012, s. 408.

²²⁶ M. Chmaj (red.), *Ustrój samorządu terytorialnego w Polsce*, Warszawa 2005, s. 82.

²²⁷ E. Prokop-Perzyńska, *Formy współczesnej demokracji – pomiędzy demokracją pośrednią a bezpośrednią. Rozważania teoretyczno-prawne*, [w:] *Instytucje demokracji bezpośredniej na tle rozwiązań konstytucyjnych i ustawowych. Stan obecny i postulaty de lege ferenda*, (red.) M. Bożek, P. Świtał, K. Walczuk, Radom 2012, s. 21.

²²⁸ A. Konopelko, *Instrumenty demokracji bezpośredniej w Polsce jako jeden z elementów procesu demokratyzacji systemu*, [w:] *Sistemnaâ transformaciâ obšestva: istoričeskij opyt, sovremennost' i perspektivy. Sbornik naučnyh trudov kafedr social'no-gumanitarnyh nauk*, (red.) Â. S. Âskevič, Brześć 2009, s. 126.

²²⁹ M. Sidor, *Referendum lokalne jako forma demokracji bezpośredniej*, [w:] *Samorząd lokalny w Polsce*, (red.) S. Michałowski, A. Pawłowska, Lublin 2004, s. 186–188.

²³⁰ I. Niżnik-Dobosz, *Partycypacja jako pojęcie i instytucja demokratycznego państwa prawnego i prawa administracyjnego*, [w:] *Partycypacja społeczna w samorządzie terytorialnym*, (red.) B. Dolnicki, Warszawa 2014, s. 21 i n.

danego terenu, zorientowanych na zaspokojenie potrzeb ludzi tam zamieszkujących²³¹. Partycypacja ma prowadzić do zwiększenia skuteczności działań władz lokalnych, dzięki lepszemu rozpoznaniu przez nie potrzeb społeczności, oraz umocnić pozycję władz lokalnych²³². Partycypacja obywatelska związana jest z ideą społeczeństwa obywatelskiego, konsensusu, dialogu społecznego. Może być rozumiana szeroko – jako wszelkie przejawy organizowania się (zrzeszania) ludzi zmierzających do osiągnięcia wspólnych celów (w tym także do zaspokojenia swoich potrzeb materialnych i niematerialnych) – bądź wąsko – jako włączanie się ludności oraz stworzonych przez nią organizacji w proces realizacji zadań publicznych przez władze rządowe lub samorządowe²³³.

Stwarzanie obywatelom podstaw do aktywnego uczestnictwa w zarządzaniu swoją wspólnotą samorządową jest jednym z instrumentów budowy społeczeństwa obywatelskiego, zaangażowanego nie tylko w indywidualne, własne sprawy²³⁴. Społeczna aktywność obywatelska polega na wspólnej i świadomej artykulacji, realizacji i obronie interesów (potrzeb, aspiracji) jakiejś grupy społecznej przez jej członków²³⁵. Zaangażowanie publiczne może przybrać formę konsultacji społecznych.

Konsultacje społeczne

Konsultacje społeczne to pojęcie dość młode, niemające ugruntowanej pozycji w świecie nauki. Wywodzi się ono od łacińskiego *consulto* (pytać o radę, radzić się) i *consultatio* (pytanie o radę)²³⁶. Potrzeba konsultacji społecznych przy współtworzeniu prawa wynika z zasady demokratycznego państwa prawnego. Stanowią one formę bezpośredniego udziału w samorządzie terytorialnym. Dzięki konsultacjom uzyskuje się opinię wspólnoty samorządowej na dotyczące ja tematy²³⁷. Jak twierdzi Roman Marchaj, konsultacje te umożliwiają prowadzenie stałego dialogu pomiędzy społeczeństwem a organami władzy publicznej. Cechą wspólną wszystkich procedur konsultacyjnych w Polsce jest ich opiniodawczy charakter. Oznacza to, że nie stanowią one formy rozstrzygania o sprawach publicznych, lecz mają dostarczyć

²³¹ P. Starosta, Poza metropolią. Wiejskie i małomiasteczkowe zbiorowości lokalne a wzory porządku makrospołecznego, Łódź 1995, s. 198.

²³² R. Skrzypiec, Badanie lokalnej aktywności obywatelskiej – problematyka, metody i techniki badań, [w:] Lokalne społeczeństwo obywatelskie, (red.) P. Frączak, Warszawa 2002, s. 49–50.

²³³ D. R. Kijowski, Partycypacja obywatelska w samorządowych procesach decyzyjnych – zagadnienia ogólne, „Samorząd Terytorialny” 2010, nr 1–2, s. 9.

²³⁴ P. Śwital, Gwarancje prawne udziału obywateli we współzarządzaniu gminą, Radom 2019, s. 75.

²³⁵ P. Gliński, H. Palska, Cztery wymiary społecznej aktywności obywatelskiej, [w:] Elementy nowego ładu, (red.) H. Domański, A. Rychard, Warszawa 1997, s. 365–366.

²³⁶ J. Sondel, Słownik łacińsko-polski dla prawników i historyków, Kraków 2009, s. 214.

²³⁷ M. Pytlewska-Smółka, Rola konsultacji jako partycypacji społecznej w samorządzie terytorialnym – aspekty prawne, [w:] Partycypacja społeczna w samorządzie terytorialnym – aspekty prawne, ekonomiczne i społeczne, (red.) K. Głębicka, P. Śwital, Radom 2016, s. 83–84.

decydentowi opinii osób bezpośrednio dotkniętych planowanym rozstrzygnięciem. Dzięki temu organy władzy publicznej mogą stanowić lepsze prawo lub podejmować decyzje uwzględniające kontekst społeczny²³⁸. Marta Banat wskazuje, że konsultacje odgrywają one istotną rolę w demokratycznym ustroju, umożliwiając partycypację obywateli w zarządzaniu sprawami publicznymi. Można je również uznać za formę komunikowania się organów władzy publicznej ze społeczeństwem. Instytucja ta nabiera szczególnego znaczenia zwłaszcza w samorządzie terytorialnym, którego istota opiera się na przekazaniu władzy członkom wspólnoty samorządowej²³⁹. Istotę konsultacji definiuje także Ewa Olejniczak-Szałowska, dowodząc, że z konsultacją mamy do czynienia wówczas, gdy podmiot konsultujący podejmuje działanie podstawowe, na jakimś jego etapie (ale zawsze przed podjęciem decyzji) uruchamia działanie konsultacyjne w społeczności lokalnej, przy czym działanie konsultacyjne nie ma bytu samoistnego, lecz jest subsydiarne w stosunku do działu podstawowego²⁴⁰.

W orzecnictwie podkreśla się, że konsultacje społeczne mają charakter opiniodawczy i są niewiążące, nie kreują prawa. Ich wyniki nie wiążą organów gminy w odróżnieniu od instytucji referendum gminnego. Powinny być one prowadzone z uwzględnieniem specyfiki warunków lokalnych. Konsultacje służą organizowaniu podejmowania decyzji w taki sposób, aby w jego trakcie umożliwić decydentowi zapoznanie się z opiniami osób trzecich. Proces konsultacji ma charakter subsydiarny w stosunku do podstawowego działania organów wypracowujących rozstrzygnięcia²⁴¹. Konsultacje przeprowadza się zgodnie z postanowieniami uchwały rady gminy ustalającej zasady i tryb przeprowadzania konsultacji. Wymagane jest bowiem najpierw podjęcie uchwały w przedmiocie konsultacji z mieszkańcami, a następnie faktyczne przeprowadzenie takich konsultacji²⁴².

Uczestnikami procesu konsultacji są zawsze dwa podmioty. pierwszym jest organ konsultujący (decydent) uprawniony do rozstrzygania o sposobie wykonywania zadań publicznych. Jego rolą jest rozstrzygnięcie sprawy, która była przedmiotem konsultacji, a także zorganizowanie konsultacji społecznych pod względem prawnym oraz technicznym. Podmiotem konsultującym są organy gminy, gdyż tylko one posiadają kompetencje do rozstrzygania o sprawach publicznych ważnych dla lokalnej wspólnoty samorządowej. Drugim uczestnikiem konsultacji społecznych jest zbiorowy podmiot konsultowany, czyli mieszkańcy jednostki samorządu terytorialnego przeprowadzającej konsultacje²⁴³.

²³⁸ R. Marchaj, *Samorządowe konsultacje społeczne*, Warszawa 2016, s. 17.

²³⁹ M. Banat, *Konsultacje społeczne w samorządzie terytorialnym*, „Samorząd Terytorialny” 2014, nr 1-2, s. 13.

²⁴⁰ E. Olejniczak-Szałowska, *Konsultacje we wspólnocie samorządowej*, „Samorząd Terytorialny” 1997, nr 1-2, s. 108.

²⁴¹ Wyrok NSA z dnia 13 grudnia 2017 r., II OSK 564/17, LEX nr 2441376.

²⁴² Wyrok NSA z dnia 29 lipca 2020 r., II OSK 852/20, LEX nr 3058767.

²⁴³ Wyrok WSA w Krakowie z dnia 5 lipca 2022 r., III SA/Kr 517/22, LEX nr 3362847.

Elektroniczna partycypacja społeczna

Istotnym aspektem kształtowania partycypacji społecznej jest przebieg procesu informatyzacji oraz cyfryzacji usług publicznych w Polsce²⁴⁴. Idea e-administracji zakłada informatyzację administracji publicznej poprzez zapewnienie elektronicznej obsługi obywateli i innych zainteresowanych podmiotów przez organy administracyjne. Jej realizacja jest procesem mającym prowadzić do powstania systemu e-administracji (e-government)²⁴⁵. E-administracja wykonuje swoje zadania oraz świadczy usługi publiczne, uwzględniając interes obywateli, którzy są traktowani jako jej klienci²⁴⁶.

Partycypacja elektroniczna oparta jest na wykorzystaniu komunikacji elektronicznej. Elektroniczna partycypacja jest przy tym rozumiana jako angażowanie obywateli w proces podejmowania i realizowania decyzji politycznych za pośrednictwem narzędzi elektronicznych. Odnosi się ona do działań administracji publicznej, dostarczania usług publicznych, podejmowania decyzji czy przygotowania oraz wdrażania polityki publicznej. Są to więc relacje, jakie zachodzą pomiędzy sferą polityki i administracji a sferą społeczeństwa obywatelskiego²⁴⁷. Jak zauważa Maciej Błażewski „Elektroniczna partycypacja społeczna obejmuje dwa rodzaje działań: pozyskanie oraz udostępnienie informacji z zastosowaniem środków komunikacji elektronicznej. Organ administracji publicznej pozyskuje informacje, zwracając się bezpośrednio do podmiotu konsultowanego lub odbierając od niego informacje za pośrednictwem m.in. elektronicznej skrzynki podawczej, poczty elektronicznej lub forum internetowego. Udostępnienie informacji dotyczy dwóch etapów konsultacji: zbierania stanowisk i opinii oraz ogłoszenia wyników partycypacji”²⁴⁸.

Pojęcie „środek komunikacji elektronicznej” jest definicją legalną, którą zawiera ustawa o świadczeniu usług drogą elektroniczną. Zgodnie z art. 2 pkt 5 u.s.u.d.e.²⁴⁹ środki komunikacji elektronicznej są to rozwiązania techniczne, w tym urządzenia teleinformatyczne i współpracujące z nimi narzędzia programowe, umożliwiające indywidualne porozumiewanie się na odległość przy wykorzystaniu

²⁴⁴ M. Stasz, Elektroniczne formy partycypacji społecznej w polskim samorządzie terytorialnym na przykładzie gminy, [w:] *Ewolucja elektronicznej administracji publicznej*, (red.) R. Kusiak-Winter, J. Korczak, Wrocław 2021, s. 123.

²⁴⁵ M. Kotulska, Zakres stosowania środków komunikacji elektronicznej w postępowaniu administracyjnym, „Samorząd Terytorialny” 2015, nr 7-8, s. 74.

²⁴⁶ A. Sytek, Rozwój elektronicznej administracji ze szczególnym uwzględnieniem ePUAP i profili zaufanych - wybrane zagadnienia, „Samorząd Terytorialny” 2016, nr 6, s. 71.

²⁴⁷ N. Lubik-Reczek, I. Kapsa, M. Musiał-Karg, Elektroniczna partycypacja obywatelska w Polsce. Deklaracje i opinie Polaków na temat e-administracji i e-głosowania, Poznań 2020, s. 24.

²⁴⁸ M. Błażewski, Elektroniczna partycypacja społeczna na przykładzie Polski i Niemiec, [w:] *Współczesne polityczno-prawne systemy państw Europy, Azji i Ameryki Łacińskiej*, (red.) K. Complak, P. Gutierrez, J. Rosiak, Wrocław 2017, s. 154.

²⁴⁹ Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, t.j. Dz. U. z 2020 r. poz. 344.

transmisji danych między systemami teleinformatycznymi, a w szczególności poczta elektroniczna. Dane rozwiązanie techniczne musi łącznie spełniać wszystkie przesłanki, aby mogło być uznane za środek komunikacji elektronicznej. Jak zauważa Aleksandra Monarcha-Matlak, „komunikacja elektroniczna to przede wszystkim komunikacja za pośrednictwem komputerów. Elektroniczne postacie przekazu informacji przewyższają dotychczasowe sposoby komunikowania się w obrocie prawnym. Komputerowy przekaz danych i informacji następuje szybciej, z wykorzystaniem różnorodnych narzędzi komunikacyjnych, w każdym czasie i z każdego miejsca”²⁵⁰.

Aby wykształcić w pełni społeczeństwo informatyczne, należy techniki elektronicznej partycypacji stosować uzupełniając do już znanych form tradycyjnych celem osiągania lepszych efektów pozyskiwania informacji i włączania kolejnych grup społecznych, a także aby nie powodować wykluczenia społecznego osób, które nie mają zagwarantowanego dostępu do internetu²⁵¹. Celem informatyzacji administracji publicznej jest stworzenie zrozumiałych i przejrzystych dla mieszkańców procesów poprzez wykorzystanie narzędzi teleinformatycznych wraz z ich szerokim zastosowaniem, usprawnienie działań samej administracji, a także zapewnienie nieustannie rozwijających się technologii informacyjnych i informatycznych²⁵².

Elektroniczne formy konsultacji społecznych

Powstanie i gwałtowny rozwój technologii informacyjno-komunikacyjnych (ICT) zmieniły społeczeństwo, musi więc nastąpić także zmiana sposobu działania administracji publicznej, również na szczeblu samorządu terytorialnego²⁵³. Pomimo stwarzania szeregu warunków prawnych do udziału obywateli w sprawach wspólnoty samorządowej udział obywateli w proces decyzyjny nie jest zjawiskiem powszechnym. Jak zauważa Roman Marchaj powodów niewielkiego zaangażowania mieszkańców w procesie przeprowadzania konsultacji społecznych jest sporo. Przede wszystkim należy wskazać ogólny niski poziom kapitału społecznego, przejawiający się niewielkim zaangażowaniem obywateli w życie państwa – na poziomie czy to wspólnoty ogólnonarodowej, czy wspólnoty lokalnej. Jest to problem systemowy, który z całą pewnością nie zostanie szybko wyeliminowany²⁵⁴.

²⁵⁰ A. Monarcha-Matlak, Pojęcie komunikacji elektronicznej w doktrynie i aktach prawnych, „Lingwistyka Stosowana” 2017, nr 24(4), s. 142.

²⁵¹ P. Śwital, Wykorzystanie środków komunikacji elektronicznej w procesach partycypacji społecznej, „Acta Iuridica Resoviensia” 2021, 34(116), s. 353.

²⁵² P. Romaniuk, Szanse i zagrożenia dla administracji publicznej w świadczeniu usług drogą elektroniczną, „Studia Prawnoustrojowe” 2022, nr 58, s. 439.

²⁵³ S. Kańduła, W stronę elektronicznej administracji w gminach, „Finanse Komunalne” 2023, nr 2, s. 7.

²⁵⁴ R. Marchaj, Samorządowe konsultacje społeczne. Propozycje de lege ferenda, „Samorząd Terytorialny” 2020,

Wśród form elektronicznych konsultacji w aktach prawnych możemy znaleźć również te, które prowadzone są z wykorzystaniem narzędzi ICT. Przykładowo wskazać można ustawę o rewitalizacji²⁵⁵ gdzie wskazano, że formami konsultacji są: zbieranie uwag w postaci papierowej lub elektronicznej, w tym za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej lub formularzy zamieszczonych na stronie podmiotowej gminy w Biuletynie Informacji Publicznej. Ustawodawca wskazuje także, że spotkania i debaty mogą być przeprowadzane również za pomocą środków porozumiewania się na odległość, zapewniających jednoczesną transmisję wizji i dźwięku. Również w odniesieniu do ankiet i wywiadów wskazano, że mogą być przeprowadzane również za pomocą środków porozumiewania się na odległość. W ustawie o planowaniu i zagospodarowaniu przestrzennym²⁵⁶ wskazano, że konsultacje prowadzi się w formie zbierania uwag, spotkań otwartych, paneli eksperckich lub warsztatów, które poprzedzone są prezentacją projektu aktu planowania przestrzennego, spotkania plenerowe lub spacer studyjne, zorganizowane na obszarze objętym aktem planowania przestrzennego, ankiety lub geoankiety, wywiady, prowadzenie punktu konsultacyjnego lub dyżury projektanta. Konsultacje społeczne w zakresie form, wyżej wskazanych prowadzi się w postaci papierowej lub elektronicznej, w tym za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej. Konsultacje te można prowadzić w szczególności za pomocą formularzy udostępnionych przez organ sporządzający projekt aktu planowania przestrzennego w Biuletynie Informacji Publicznej na stronie podmiotowej obsługującego go urzędu, a także w innej formie, jeżeli zostanie ona określona przez ten organ w ogłoszeniu o rozpoczęciu konsultacji społecznych.

Wprowadzenie formy elektronicznej ma pobudzić obywateli do aktywności w zakresie brania udziału w konsultacjach społecznych. Może stać się to odpowiedzią na niską aktywność obywateli w procesach konsultacji. Konsultacje te niosą również szereg korzyści dla administracji. Wśród nich wyróżnić możemy: bezpłatne otrzymywanie informacji zwrotnych, jest to prosty sposób na zdobycie podstawowych informacji na temat przedmiotu konsultacji oraz stosunku obywateli do proponowanego przedsięwzięcia, a także oszczędność czasu i środków przy zastosowaniu form elektronicznych. Wadami form elektronicznych są: niewielka reprezentatywność otrzymanych opinii, skupienie się przez interesariuszy najczęściej na krytyce obecnych rozwiązań, a nie na proponowanych zmianach. Dyskusja bywa powierzchowna, ponieważ uczestnicy nie uzyskują wcześniej szczegółowych informacji na temat danej kwestii, natomiast opierają się na swoich opiniach.

nr 7-8, s. 67.

²⁵⁵ Ustawa z dnia 9 października 2015 r. o rewitalizacji, t.j. Dz. U. z 2024 r. poz. 278.

²⁵⁶ Ustawa z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym, t.j. Dz. U. z 2023 r. poz. 977 z późn. zm.

Warto pochylić się nad dwoma formami konsultacji są to geoankiety oraz geodyskusje. Partycypacyjne systemy informacji geograficznej to idea wraz z metodami i technikami należącymi do systemów informacji geograficznej. Ich podstawową zaletą jest szeroka możliwość zbierania i konsultowania informacji przestrzennych. W metodach tych elementy systemów informacji geograficznej mogą być wykorzystywane do charakterystyki przestrzeni lokalnej w oparciu o wiedzę i opinie mieszkańców, promując komunikację wśród lokalnej społeczności w postaci szerszej niż tradycyjne formy partycypacji społecznej²⁵⁷. Do narzędzi wspierających partycypację społeczną opartych na systemach informacji geograficznej należy geoankieta. Oparta jest ona na tradycyjnej ankiecie, która uzupełniona została o pytania związane z aspektami możliwymi do identyfikacji w przestrzeni. Geoankieta pozwala respondentom na wskazywanie, charakterystykę, a także, w zależności od potrzeb, ocenę elementów przestrzeni. Za pośrednictwem zastosowanej w geoankiecie interaktywnej mapy respondent może korzystać z trzech rodzajów obiektów: punktów, linii oraz obszarów, stosowanych w oprogramowaniu GIS²⁵⁸. W opisie techniki wskazuje się, że wypełnienie Geoankiety powinno być anonimowe i trwać optymalnie około 10 minut. Należy pamiętać, żeby podać informacje o zaangażowanych partnerach np. o urzędzie lub biurach projektowych. Ważne jest dokładne scharakteryzowanie obszaru stanowiącego podmiot konsultacji (opisanie np. jego lokalizacji w przestrzeni miasta oraz linii wyznaczających jego granice)²⁵⁹. Metoda ta może być przydatna na dwóch etapach procesu planistycznego: składania wniosków do planu jak i wyłożenia planu do wglądu publicznego.

Geodyskusja jest internetową aplikacją mającą zastosowanie w przypadku potrzeby dialogu w kontekście zagospodarowania przestrzeni. Z powodzeniem jest wykorzystywana w konsultacjach społecznych, kiedy gotowa jest np. koncepcja zagospodarowania obszaru. W przypadku miejscowych planów zagospodarowania przestrzennego może być utożsamiana z etapem wyłożenia projektu planu do publicznego wglądu. W ramach geodyskusji uczestnicy konsultacji społecznych mogą wypowiadać się i oceniać prezentowane propozycje planistyczne. Geodyskusja w odróżnieniu od geoankiety umożliwia interakcję pomiędzy uczestnikami (respondentami, decydentami, planistami itd.), przez co możliwe jest uzyskanie opinii dotyczących proponowanych rozwiązań i rozstrzyganie wątpliwych kwestii (związanych np. z uregulowaniami prawnymi) na etapie konsultacji społecznych²⁶⁰. Geodyskusja umożliwia dodawanie komentarzy i reakcji na komentarze innych osób,

²⁵⁷ T. Kaczmarek (red.), *Zastosowanie aplikacji geoankiety i geodyskusji w partycypacyjnym planowaniu przestrzennym – dobre praktyki*, Poznań 2018, s. 11.

²⁵⁸ E. Bąkowska, T. Kaczmarek, Ł. Mikula, Wykorzystanie geoankiety jako narzędzia konsultacji społecznych w procesie planowania przestrzennego w aglomeracji poznańskiej, „Roczniki Geomatyki” 2017, tom XV, zeszyt 2(77), s. 151.

²⁵⁹ Geoankeita, <https://www.partycypacjaobywatelska.pl/strefa-wiedzy/techniki/geoankieta/> [data dostępu: 15.01.2024].

²⁶⁰ T. Kaczmarek (red.), *Zastosowanie aplikacji geoankiety i geodyskusji..* op.cit, s. 33.

a jednocześnie zawiera mapy, plany, prognozy, wyniki badań. W ramach narzędzia umieszczone są na mapach punkty, linie albo obszary, które wskazują na wątki w dyskusji. Zebrane dane są analizowane i sortowane. Na ich podstawie są formułowane wnioski na temat projektu.

Podsumowanie

Elementem kluczowym świadomości demokratycznej w odniesieniu do wspólnot lokalnych jest sposób definiowania roli obywatela i roli władz lokalnych. Konieczne staje się poszukiwanie alternatywnych form dla zaangażowania obywateli. Wykorzystanie form elektronicznych może przyczynić się do zwiększenia udziału obywateli w proces podejmowania decyzji w jednostkach samorządu terytorialnego. Partycypacja elektroniczna staje się aktualnie zjawiskiem powszechnym. Stanowi coś więcej niż elektroniczny wymiar procedur – jest głębszym zaangażowaniem obywatelskim pośredniczonym przez nowe technologie komunikacyjne. Konieczne staje się promowanie nowych form i zapoznavanie obywateli z zaletami ich stosowania. Pozytywnie ocenić należy wprowadzenie partycypacji społecznej do ustawy o rewitalizacji oraz planowania przestrzennego. Takie działania powinny być promowane również na gruncie ustaw samorządowych. Mogą stać się one również nie tyle alternatywą, co powinny mieć pierwszeństwo zastosowania.

Bibliografia

Akty prawne

1. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, t.j. Dz. U. z 2020 r. poz. 344.
2. Ustawa z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym, t.j. Dz. U. z 2023 r. poz. 977 z późn. zm.
3. Ustawa z dnia 9 października 2015 r. o rewitalizacji, t.j. Dz. U. z 2024 r. poz. 278.

Orzecznictwo

1. Wyrok NSA z dnia 13 grudnia 2017 r., II OSK 564/17, LEX nr 2441376.
2. Wyrok NSA z dnia 29 lipca 2020 r., II OSK 852/20, LEX nr 3058767.
3. Wyrok WSA w Krakowie z dnia 5 lipca 2022 r., III SA/Kr 517/22, LEX nr 3362847.

Literatura

1. Banat M., *Konsultacje społeczne w samorządzie terytorialnym*, „Samorząd Terytorialny” 2014, nr 1-2.
2. Bąkowska E., Kaczmarek T., Mikuła Ł., Wykorzystanie geoankiety jako

- narzędzia konsultacji społecznych w procesie planowania przestrzennego w aglomeracji poznańskiej, „Roczniki Geomatyki” 2017, tom XV, zeszyt 2(77).
3. Błazewski M., Elektroniczna partycypacja społeczna na przykładzie Polski i Niemiec, (w:) Współczesne polityczno-prawne systemy państw Europy, Azji i Ameryki Łacińskiej, (red.) K. Complak, P. Gutierrez, J. Rosiak, Wrocław 2017.
 4. Chmaj M. (red.), Ustrój samorządu terytorialnego w Polsce, Warszawa 2005.
 5. Ferens A., Kondas R., Matysiak I., Rzeźnik G., Szyrski M., Jak skutecznie prowadzić konsultacje społeczne w samorządach. Zasady i najlepsze praktyki współpracy samorządów z przedstawicielami społeczności lokalnych. Przewodnik dla samorządowców, Warszawa 2010.
 6. Gliński P., Palska H., Cztery wymiary społecznej aktywności obywatelskiej, [w:] Elementy nowego ładu, (red.) H. Domański, Warszawa 1997.
 7. Kaczmarek T. (red.), Zastosowanie aplikacji geoankiety i geodyskusji w partycypacyjnym planowaniu przestrzennym – dobre praktyki, Poznań 2018.
 8. Kańduła S., W stronę *elektronicznej administracji w gminach*, „Finanse Komunalne” 2023, nr 2.
 9. Kijowski D. R., Partycypacja obywatelska w samorządowych procesach decyzyjnych – zagadnienia ogólne, „Samorząd Terytorialny” 2010, nr 1–2.
 10. Konopelko A., Instrumenty demokracji bezpośredniej w Polsce jako jeden z elementów procesu demokratyzacji systemu, [w:] Â. S. Âskevič (red.), Sistemnaâ transformaciâ obšestva: istoričeskij opyt, sovremennost' i perspektivy. Sbornik naučnyh trudov kafedr social'no-gumanitarnyh nauk, Brześć 2009.
 11. Kotulska M., Zakres stosowania środków komunikacji *elektronicznej w postępowaniu administracyjnym*, „Samorząd Terytorialny” 2015, nr 7-8.
 12. Lubik-Reczek N., Kapsa I., Musiał-Karg M., Elektroniczna partycypacja obywatelska w Polsce. Deklaracje i opinie Polaków na temat e-administracji i e-głosowania, Poznań 2020.
 13. Marchaj R., Samorządowe *konsultacje społeczne*. Propozycje de lege ferenda, „Samorząd Terytorialny” 2020, nr 7-8.
 14. Marchaj R., Samorządowe konsultacje społeczne, Warszawa 2016.
 15. Monarcha-Matlak A., *Pojęcie komunikacji elektronicznej w doktrynie i aktach prawnych*, „Lingwistyka Stosowana” 2017, nr 24(4).
 16. Niżnik-Dobosz I., Partycypacja jako pojęcie i instytucja demokratycznego państwa prawnego i prawa administracyjnego, [w:] Partycypacja społeczna w samorządzie terytorialnym, (red.) B. Dolnicki, Warszawa 2014.
 17. Olejniczak-Szałowska E., Konsultacje we wspólnocie samorządowej, „Samorząd Terytorialny” 1997, nr 1-2.
 18. Prokop-Perzyńska E., Formy współczesnej demokracji – pomiędzy demokracją pośrednią a bezpośrednią. Rozważania teoretyczno-prawne, [w:] M. Bożek, P. Śwital, K. Walczuk (red.), Instytucje demokracji bezpośredniej na tle

- rozwiązań konstytucyjnych i ustawowych. Stan obecny i postulaty de lege ferenda, Radom 2012.
19. Pytlewska-Smółka M., Rola konsultacji jako partycypacji społecznej w samorządzie terytorialnym – aspekty prawne, [w:] Partycypacja społeczna w samorządzie terytorialnym – aspekty prawne, ekonomiczne i społeczne, (red.) K. Głębicka, P. Śwital, Radom 2016.
 20. Romaniuk P., Szanse i zagrożenia dla administracji publicznej w świadczeniu usług drogą elektroniczną, „Studia Prawnoustrojowe” 2022, nr 58.
 21. Sidor M., Referendum lokalne jako forma demokracji bezpośredniej, [w:] S. Michałowski, A. Pawłowska (red.), Samorząd lokalny w Polsce, Lublin 2004.
 22. Skrzypiec R., Badanie lokalnej aktywności obywatelskiej – problematyka, metody i techniki badań, [w:] Lokalne społeczeństwo obywatelskie, (red.) P. Frączyk, Warszawa 2002.
 23. Sondel J., Słownik łacińsko-polski dla prawników i historyków, Kraków 2009.
 24. Starosta P., Poza metropolią. Wiejskie i małomiasteczkowe zbiorowości lokalne a wzory porządku makrospołecznego, Łódź 1995.
 25. Stasz M., Elektroniczne formy partycypacji społecznej w polskim samorządzie terytorialnym na przykładzie gminy, [w:] Ewolucja elektronicznej administracji publicznej, (red.) R. Kusiak-Winter, J. Korczak, Wrocław 2021.
 26. Sytek A., *Rozwój elektronicznej administracji ze szczególnym uwzględnieniem ePUAP i profili zaufanych - wybrane zagadnienia*, „Samorząd Terytorialny” 2016, nr 6.
 27. Śwital P., Gwarancje prawne udziału obywateli we współzarządzaniu gminą, Radom 2019.
 28. Śwital P., Wykorzystanie środków komunikacji elektronicznej w procesach partycypacji społecznej, „Acta Iuridica Resoviensia” 2021, 34(116).
 29. Tabernacka M., Komunikacja obywateli z władzą – warunek funkcjonowania demokracji i społeczeństwa obywatelskiego, [w:] Public relations w sferze publicznej. Wizerunek i komunikacja, (red.) M. Tabernacka, A. Szadok-Bratuń Warszawa 2012.

Netografia

1. Geoankeita, <https://www.partycypacjaobywatelska.pl/strefa-wiedzy/techniki-geoankieta/> [data dostępu: 15.01.2024].

Redaktorzy naukowí

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 Śwital – 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 wydawniczych

Przedstawiona do zaopiniowania monografia – ponad wszelką wątpliwość – dotyczy niezwykle istotnych, zarówno z teoretycznego jak i praktycznego punktu widzenia zagadnień. Pozytywnie należy ocenić całość opracowania, które podejmuje problemy współczesnej administracji, a w którym wyeksponowano problematykę cyfryzacji administracji. Podsumowując, opiniowaną publikację uważam za niezmiernie interesującą. [...] Opiniowane dzieło ujawnia wielką erudycję Autorów, można się spodziewać, że odbije się zauważalnym echem nie tylko w środowisku prawniczym.

dr hab. prof. US Aleksandra Monarcha-Matlak

Umieszczone w monografii opracowania obejmują bardzo różnorodne aspekty cyfryzacji, informatyzacji i cyberbezpieczeństwa w administracji publicznej. Autorzy rozdziałów w interdyscyplinarny sposób odnieśli się do aktualnych perspektyw, szans i wyzwań w obszarze e-modernizacji sektora usług publicznych. Głównym założeniem monografii jest podjęcie debaty na temat pełnej cyfryzacji sektora publicznego oraz dyskusji w zakresie wprowadzenia zmian natury organizacyjno-prawnej, społecznej i technologicznej w celu rozwoju administracji publicznej.

dr hab. prof. URad. Joanna Smarż