E-administracja
Wyzwania dla cyfrowych usług publicznych w Unii Europejskiej

E-Government
Challenges for Digital Public Services in the EU

REDAKCJA / EDITED BY
Sławomir Dudzik · Inga Kawka · Renata Śliwa

Krakow Jean Monnet Research Papers

E-administracja
Wyzwania dla cyfrowych usług publicznych w Unii Europejskiej

E-Government
Challenges for Digital Public Services in the EU

Krakow Jean Monnet Research Papers

3

E-administracja
Wyzwania dla cyfrowych usług publicznych w Unii Europejskiej

E-Government
Challenges for Digital Public Services in the EU

REDAKCJA / EDITED BY

Sławomir Dudzik · Inga Kawka · Renata Śliwa

WYDAWNICTWO KSIĘGARNIA AKADEMICKA

Kraków 2024

Sławomir Dudzik
Uniwersytet Jagielloński, Kraków
s.dudzik@uj.edu.pl

Inga Kawka
Uniwersytet Jagielloński, Kraków
inga.kawka@uj.edu.pl

Renata Śliwa
Uniwersytet Komisji Edukacji Narodowej, Kraków
renata.sliwa@up.krakow.pl

Recenzja: dr hab. Grzegorz Krawiec, prof. UKEN

Opracowanie redakcyjne: Artur Foryt (j. francuski), Dorota Ilnicka (j. polski), Christopher Thornton (j. angielski)

Projekt okładki: Marta Jaszczuk

ISBN 978-83-8368-025-5
https://doi.org/10.12797/9788383680255

Publikacja dofinansowana przez Wydział Prawa i Administracji Uniwersytetu Jagiellońskiego oraz Uniwersytet Komisji Edukacji Narodowej w Krakowie

With the support of Jean Monnet Activities within ERASMUS+ Programme of the European Union

Wsparcie Komisji Europejskiej dla produkcji tej publikacji nie stanowi poparcia dla treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie może zostać pociągnięta do odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

WYDAWNICTWO KSIĘGARNIA AKADEMICKA
ul. św. Anny 6, 31-008 Kraków
tel.: 12 421-13-87; 12 431-27-43
e-mail: publishing@akademicka.pl

Księgarnia internetowa: akademicka.pl

Spis treści | Table of contents

E-administracja. Wyzwania dla cyfrowych usług publicznych w Unii Europejskiej
E-Government: Challenges for Digital Public Services in the EU | s. 45-64
https://doi.org/10.12797/9788383680255.03

Kinga Sabina Zielińska[1]

E-administracja działająca w granicach prawa i godna zaufania

Prawo do prywatności i ochrona danych osobowych jako wyzwanie dla rozwoju e-administracji

Abstrakt: Dynamiczny rozwój e-administracji, a także postęp w dziedzinie nowych technologii, które mogą być w niej wykorzystywane, niezmiennie budzi zainteresowanie. Generowane w ramach administracji dane o obywatelach mogą stawać się w przyszłości przedmiotem ataków podmiotów chcących wejść w posiadanie określonych informacji. Organy władzy również nie zawsze wykorzystują przetwarzane dane w taki sposób, w jaki winny być one wykorzystywane. Pogodzenie działań e-administracji i prawa do prywatności oraz ochrony danych osobowych jest z założenia trudne, choć – jak wynika z ugruntowanego już orzecznictwa – nie jest niemożliwe.

Niniejszy artykuł poświęcony jest refleksji na temat możliwych zagrożeń dla prawa do prywatności i ochrony danych osobowych. Autorka identyfikuje najistotniejsze w jej ocenie zagrożenia dla tych praw wynikające z działalności państwa oraz możliwości wykorzystania pozycji dominującej w stosunkach obywatel–państwo. Słabsza pozycja obywatela w tej relacji wymusza konieczność zapewnienia właściwych gwarancji ochrony jego praw i wolności.

Ponadto autorka wskazuje na potrzebę tworzenia systemów obsługujących e-administrację w sposób budujący zaufanie obywateli do państwa. Gwarantem tego zaufania oraz sprawnie działającej e-administracji jest bezwzględne

[1] Mgr Kinga Sabina Zielińska, Zespół Prawa Konstytucyjnego, Międzynarodowego i Europejskiego w Biurze Rzecznika Praw Obywatelskich, Akademia Leona Koźmińskiego, https://orcid.org/ 0000-0002-3146-6319.

przestrzeganie zasady legalizmu, a więc działania organów państwa jedynie na podstawie i w granicach prawa. Każde inne działanie nie tylko burzy zaufanie do państwa, ale także otwiera możliwość kwestionowania przed sądami międzynarodowymi sposobu działania państwa.

Otwierające nowe możliwości nowoczesne technologie mogą stanowić także pokusę dla państwa, by nadużywać władzy względem obywateli, dlatego tak ważną rolę – w ocenie autorki coraz ważniejszą – odgrywa organ właściwy w sprawach ochrony danych osobowych, który być może w niedalekiej przyszłości posiadać będzie również kompetencje związane z działaniem sztucznej inteligencji. Tylko niezależny organ nadzoru może stanowić gwarancję ochrony praw i wolności obywateli w bardzo wrażliwym obszarze, jakim jest prywatność i możliwość ingerowania w nią ze strony państwa.

Słowa kluczowe: e-administracja, prawo do prywatności, ochrona danych osobowych, nowe technologie w usługach publicznych, zaufanie do państwa, zasada legalizmu

E-Government Acting within the Limits of the Law and with Trust: The Right to Privacy and Protection of Personal Data as a Challenge for the Development of e-Government

Abstract: The dynamic development of e-government, as well as the development of new technologies that can be used in e-government, invariably arouses interest. Citizen data generated within the administration may in future become the object of attacks by entities wishing to gain possession of specific information. Authorities also use processed data not always in the way it should be used. The need to reconcile e-government activities and the right to privacy and the protection of personal data is intrinsically difficult, although – as is clear from already well-established case law – not impossible.

This article reflects on possible threats to the right to privacy and the protection of personal data. The author identifies the most significant, in her opinion, threats to these rights arising from the activities of the state and the possibilities of exploiting the dominant position in the citizen-state relationship. The weaker position of the citizen in this relationship enforces the necessity of ensuring appropriate guarantees for the protection of his/her rights and freedoms.

Furthermore, the author points out the need to create systems that support e-government in a way that builds citizens' trust in the state. The guarantor of this trust and efficient e-government, however, is the absolute observance of the principle of legalism, i.e. state authorities acting only on the basis and within the limits of the law. Any other action not only shatters trust in the state, but also opens up the possibility of challenging before international courts the way the state acts.

New technologies, which open up new possibilities, may also constitute a temptation for the state to abuse its power in relation to citizens, which is

why, in the author's opinion, the authority competent in matters of personal data protection, which may in the near future also have competences related to the operation of artificial intelligence, plays such an increasingly important role. Only an independent supervisory authority can provide a guarantee for the protection of citizens' rights and freedoms in a very sensitive area, such as privacy and the possibility of state interference with it.

Keywords: e-government, right to privacy, personal data, protection of personal data, new technologies in public services, confidence in the state, principle of legalism

1. Wstęp

Sposób zdefiniowania, a także określenia zakresu e-administracji, zwłaszcza w ostatnich latach, jest przedmiotem wielu opracowań i analiz[2]. Na wstępie zaznaczyć należy, że w literaturze dokonuje się zasadniczego rozróżnienia na e-government (e-administrację) oraz e-governance. E-administracja dotyczy przede wszystkim wykorzystywania przez administrację publiczną narzędzi informatycznych i komunikacyjnych mających na celu usprawnienie obiegu korespondencji i komunikacji z obywatelem. Pojęciem znacznie szerszym, zapewniającym o wiele bardziej zaawansowane relacje i działania między obywatelem a państwem, jest e-governance. Obejmuje ono swoim zakresem e-government, ale znacząco wykracza poza jego ramy i rozumiane jest jako e-nadzór[3].

Nie ulega wątpliwości, że sprawna e-administracja jest bardzo pomocna dla obywatela. Zapewnia możliwość realizacji zobowiązań względem państwa, jednocześnie oszczędzając czas, a także niwelując potrzebę przemieszczania się. W dyskusji dotyczącej e-administracji często zwraca się także uwagę na to, że z jednej strony zwiększa ona dostęp obywateli do usług, z drugiej zaś sposób ich świadczenia ogranicza koszty samej administracji, co stanowi ważny argument ekonomiczny[4]. Ponadto okoliczności zewnętrzne, jak np. okres pandemii COVID-19, pokazują, jak ważna jest potrzeba zapewnienia takiej formy kontaktu z państwem. Obywatel dzięki sprawnie działającej

---

[2] Zob. m.in. T. Gajowniczek, *E-gov w Ukrainie – zarys problemu*, „Środkowoeuropejskie Studia Polityczne" 2022, nr 4, s. 169-191; A. Haręża, *Wprowadzenie do problematyki elektronicznej administracji publicznej*, „Prawo Mediów Elektronicznych" 2011, nr 1, s. 26-31.

[3] Zob. K. Śledziewska, D. Zięba, *E-administracja w Polsce na tle Unii Europejskiej. Jak z niej (nie) korzystamy*, Warszawa 2016, s. 2.

[4] A. Al-Besher, K. Kumar, *Use of Artificial Intelligence to Enhance e-Government Services*, „Measurement: Sensors" 2022, vol. 24, 100484; P. Viechnicki, W.D. Eggers, *How Much Time and Money Can AI Save Government? Cognitive Technologies Could Free up Hundreds of Millions of Public Sector Worker Hours*, https://www2.deloitte.com/content/dam/insights/us/articles/3834_How-much-time-and-money-can-AI-save-government/DUP_How-much-time-and-money-can-AI-save-government.pdf (8.07.2023).

e-administracji może realizować obowiązki – w szczególności podatkowe – względem państwa, co niewątpliwie stanowi bardzo poważny argument na rzecz konieczności rozwoju e-administracji we współczesnych, dosyć niespokojnych czasach[5].

Nie można jednak zapominać o zagrożeniach dla obywateli płynących z bardzo szerokiego zakresu danych dostępnych dzięki funkcjonowaniu e-administracji, a także o szeregu innych niebezpieczeństw związanych ze specyfiką jej działania, a więc możliwością innego dostępu do danych niż tylko do wersji papierowych dokumentów przechowywanych w siedzibach urzędów.

Zagrożenia związane z generowaniem dużych zasobów danych o obywatelach mogą mieć dwojaki charakter. Po pierwsze, są to zagrożenia wynikające z niewłaściwych działań samej administracji, co niewątpliwie wymaga wprowadzenia odpowiednich bezpieczników, a także gwarancji, że władza korzysta z danych obywateli w taki sposób, w jaki powinna, a więc w granicach prawa. Niejednokrotnie bowiem sam Trybunał Konstytucyjny (dalej: TK, Trybunał) podkreślał, że władza lubi wiedzieć dużo o obywatelach i niekoniecznie są to informacje niezbędne do jej sprawowania, lecz zbierane są one w sposób nadmiarowy w celu potwierdzenia nadrzędnej pozycji wobec jednostki. Przywołać można jeden z wyroków[6], w którym TK wskazał, że

> […] istnienie w art. 51 ust. 2 Konstytucji RP odrębnej regulacji dotyczącej proporcjonalności wkraczania w prywatność jednostki należy tłumaczyć tym, że naruszenie autonomii informacyjnej poprzez żądanie niekoniecznych, lecz wygodnych dla władzy publicznej informacji o jednostce, jest typowym dla czasów współczesnych instrumentem, po który władza publiczna chętnie sięga i dzięki któremu uzyskuje potwierdzenie swej pozycji wobec jednostki. Autonomia informacyjna, której wyodrębnienie normatywne z całości ochrony prawa do prywatności przewiduje art. 51, jest uzasadniona częstotliwością, uporczywością i typowością wkraczania w prywatność przez władzę publiczną. Normatywne wyodrębnienie, ustanowione w art. 51 ust. 2 Konstytucji RP odrębnego zakazu – ułatwia dostrzeżenie takiego wkroczenia i upraszcza przedmiot dowodu, iż takie wkroczenie nastąpiło. Przedmiotem dowodu staje się wtedy bowiem tylko to, czy pozyskiwanie informacji było konieczne, czy tylko „wygodne" lub „użyteczne" dla władzy. Dowodu wymaga, że złamanie autonomii informacyjnej było konieczne (niezbędne) w demokratycznym państwie prawnym. Analiza relacji przepisów art. 31 ust. 3 i art. 51 ust. 2 Konstytucji RP uzasadnia stwierdzenie, że naruszenie autonomii informacyjnej przez niedozwolone

[5] „Jednym z kluczowych czynników, który wpłynął na ciągłość państwa, jest proces digitalizacji Ukrainy, który rozpoczął się w 2015 roku" – K. Przyborska, *e-Ukraina – państwo w smartfonie*, https://krytykapolityczna.pl/swiat/ukraina-cyfryzacja-digitalizacja/ (3.07.2023).

[6] Wyrok TK z 20.11.2002 r., K 41/02, OTK ZU 2002/6/A, poz. 83.

pozyskiwanie informacji o obywatelach powinno odpowiadać wymaganiom określonym w art. 31 ust. 3 Konstytucji RP.

Po drugie, są to zagrożenia, które można uznać za typowo zewnętrzne, tj. związane z dostaniem się osób niepowołanych do generowanych przez administrację zestawów danych poprzez naruszenie zapór bezpieczeństwa systemów, w których te dane są przetwarzane[7]. Coraz bardziej rozbudowane systemy informatyczne, bazy danych i rejestry wymagają coraz bardziej złożonych zabezpieczeń[8], przy czym za bezpieczeństwo informacji uznaje się pewność ochrony dostępu do informacji zgromadzonej, a także pewność ochrony informacji przesłanej. Znaczenie tej cechy zależy od tego, jak cenne są przechowywane dane oraz jak istotna jest operatywność systemów prezentujących te dane i oferujących różne funkcje na tych danych wykonywane[9]. Nie tylko systemy informatyczne narażone są na ataki – także narzędzia przeznaczone do ochrony systemu mogą zawierać wady i stanowić samodzielny obiekt ataku[10].

2. Zasada legalności i zaufanie obywateli jako gwarancje dobrej e-administracji

Odnosząc się do pierwszego z przywołanych zagrożeń, a więc związanego z samą administracją i sposobem jej działania, w ocenie autorki wskazać można dwa filary, na których oprzeć należy dobrze funkcjonującą i sprawną e-administrację. Przede wszystkim są to działanie państwa na podstawie i w granicach prawa, a także zaufanie obywateli. Zaufanie budowane jest poprzez rzetelne i legalne działanie organów państwa, na które składają się zarówno bezpieczne systemy, gwarancje prawne, jak również sankcje związane z ich naruszeniem. Każdy nieuprawniony dostęp do da-

---

[7] Przechowywanie to też przetwarzanie – zob. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.Urz. UE 2016, L 119, s. 1 ze sprost., art. 4 pkt 2 [dalej: rozporządzenie 2016/679].

[8] H. Wyrębek, *Bezpieczeństwo w zarządzaniu informacją na poziomie systemów informatycznych*, „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Seria Administracja i Zarządzanie" 2012, nr 95, s. 464.

[9] J. Gruber, J. Wasylów, *Bezpieczne aplikacje .NET w technologii Web serwisów*, [w:] *Bezpieczeństwo systemów informatycznych*, A. Niemiec, J.S. Nowak, J.K. Grabara (red.), Katowice 2006, s. 81.

[10] Z. Mazur, T. Mendyk-Krajewska, *Złożoność i kompleksowość narzędzi ochrony systemów komputerowych*, [w:] *Bezpieczeństwo systemów…*, s. 15.

nych gromadzonych przez państwo, a takie incydenty niestety mają miejsce[11], osłabia zaufanie obywateli do państwa.

Sprawnie działająca e-administracja to z jednej strony coraz większe zestawy danych, które generuje oraz przetwarza wewnątrz dedykowanych rejestrów czy systemów, z drugiej zaś – potrzeba zapewnienia odpowiednich gwarancji związanych z prawem do prywatności oraz ochroną danych osobowych obywateli. Standard wyznaczający prawo do prywatności oraz ochronę danych osobowych, zarówno konstytucyjny, Rady Europy, jak i Unii Europejskiej, był już przedmiotem wielu prac i analiz[12], wobec czego omawianie poszczególnych przepisów regulujących wspomnianą kwestię pozostaje poza zakresem niniejszego artykułu.

Warto jednak przypomnieć, że szczególna pozycja prawa do prywatności, o którym mowa w art. 47 Konstytucji RP, oraz jego doniosłość w systemie konstytucyjnej ochrony praw i wolności człowieka i obywatela wynika z faktu, że jest ono nienaruszalne nawet w ustawach ograniczających inne prawa, wydawanych w stanach wojennym i wyjątkowym (art. 233 ust. 1 Konstytucji RP). Warunki zatem, nawet tak wyjątkowe i ekstremalne, nie zezwalają ustawodawcy na złagodzenie przesłanek, przy spełnieniu których można wkroczyć w sferę życia prywatnego, nie narażając się na zarzut niekonstytucyjnej arbitralności[13].

---

[11] Przykład nieuprawnionego dostępu do danych dotyczących projektów realizowanych za unijne pieniądze przez polskie firmy oraz danych beneficjentów, w posiadaniu których było Centrum Projektów Polska Cyfrowa – zob. M. Maj, *Tajemnicze włamanie do rządowej instytucji zarządzającej miliardami złotych oraz tragiczny obraz polskiego cyberbezpieczeństwa w sektorze publicznym*, https://niebezpiecznik.pl/post/tajemnicze-wlamanie-do-rzadowej-instytucji-zarzadzajacej-miliardami-zlotych-oraz-tragiczny-obraz-polskiego-cyberbezpieczenstwa-w-sektorze-publicznym/ (10.06.2023). Ponadto inne informacje o incydentach: *Dziwny atak na serwery rządowej instytucji CUW obsługującej Kancelarię Prezesa Rady Ministrów*, https://niebezpiecznik.pl/post/dziwny-atak-na-serwery-rzadowej-instytucji-cuw-obslugujacej-kancelarie-prezesa-rady-ministrow/ (10.07.2023); *Kancelaria Premiera, MSZ, MON i Kancelaria Prezydenta zhackowane. Wiemy kto stoi za tymi włamaniami*, https://niebezpiecznik.pl/post/kancelaria-premiera-msz-mon-i-kancelaria-prezydenta-zhackowane-wiemy-kto-stoi-za-tymi-wlamaniami/ (10.07.2023); *Włamanie do sieci Kancelarii Premiera? Atakujący miał uzyskać dostęp do poczty pracowników KPRM*, https://niebezpiecznik.pl/post/wlamanie-do-sieci-kancelarii-premiera-atakujacy-mial-uzyskac-dostep-do-poczty-pracownikow-kprm/ (10.07.2023); *[AKTUALIZACJA] Rządowy serwis eFaktura.gov[.]pl zhackowany. Dwa razy :D*, https://niebezpiecznik.pl/post/rzadowy-serwis-efaktura-gov-pl-zhackowany/https://niebezpiecznik.pl/post/rzadowy-serwis-efaktura-gov-pl-zhackowany/ (10.07.2023).

[12] S. Dudzik, *Podstawy prawne działania e-administracji a ochrona danych osobowych*, [w:] *E-administracja. Skuteczna, odpowiedzialna i otwarta administracja publiczna w Unii Europejskiej*, S. Dudzik, I. Kawka, R. Śliwa (red.), Kraków 2022, s. 13-28, *Krakow Jean Monnet Research Papers*, 1.

[13] Zob. wyroki TK: z 20.06.2005 r., K 4/04, OTK ZU 2005/6/A, poz. 64; oraz z 20.11.2002 r., K 41/02, OTK ZU nr 2002/6/A, poz. 83.

3. Zagrożenia dla prawa do prywatności i ochrony danych osobowych

3.1. Pokusa łączenia baz danych

Pokusa łączenia baz danych i pozyskiwania nowych, często nadmiarowych informacji, wykraczających poza upoważnienie danego organu, jest problemem, który pojawia się na styku relacji obywatel – państwo. Z taką sytuacją mieliśmy do czynienia chociażby w czasie pandemii COVID-19, kiedy to organ państwa wszedł w posiadanie danych, do przetwarzania których nie miał upoważnienia, by sprawdzić poziom zaszczepienia osób znajdujących się w trzech grupach: nauczycieli akademickich, studentów i doktorantów. Powyższe informacje zostały pozyskane na podstawie porozumienia[14]. Żaden z aktów prawa powszechnie obowiązującego nie daje ministrowi właściwemu do spraw szkolnictwa wyższego i nauki podstaw do dostępu do danych o charakterze zdrowotnym osób znajdujących się w grupach, o których mowa powyżej: ani Ustawa z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce[15], ani Ustawa z dnia 4 września 1997 r. o działach administracji rządowej[16], ani także Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia[17], na co uwagę zwrócił Rzecznik Praw Obywatelskich w wystąpieniu do Ministra Edukacji i Nauki[18], szeroko omawiając zarówno zakres podmiotowy, jak i przedmiotowy przepisów upoważniających Ministra Edukacji i Nauki do wykazów osób znajdujących się w trzech grupach, których dotyczyła ingerencja. Dużym rozczarowaniem wydaje się fakt, że sprawa ta – jak dotychczas – nie została zakończona przez organ właściwy w zakresie ochrony danych osobowych.

3.2. Zbyt szeroki zakres podmiotów uprawnionych do dostępu do danych obywateli

Kolejnym zagrożeniem dla prawa do prywatności i ochrony danych osobowych w związku z działaniem oraz dalszym rozwijaniem e-administracji jest problem polegający na

---

[14] Komunikat z dnia 13 stycznia 2022 r. na ten temat wciąż znajduje się na stronie internetowej Ministerstwa Edukacji i Nauki. Zob. Ministerstwo Edukacji i Nauki, *Podsumowanie akcji szczepień na polskich uczelniach*, https://www.gov.pl/web/edukacja-i-nauka/podsumowanie-akcji-szczepien-na-polskich-uczelniach (28.06.2023).

[15] Ustawa z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce, Dz.U. 2023, poz. 742.

[16] Ustawa z dnia 4 września 1997 r. o działach administracji rządowej, Dz.U. 2022, poz. 2512.

[17] Ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, Dz.U. 2022, poz. 1555 ze zm.

[18] Pismo Rzecznika Praw Obywatelskich do Ministra Edukacji i Nauki z dnia 26.01.2022 r., https://bip.brpo.gov.pl/sites/default/files/2022-01/RPO_do_MEN_26.1.2022.pdf (28.06.2022).

zbyt szerokim udostępnianiu danych osobowych obywateli w ramach administracji publicznej – podmiotom publicznym.

Regulacją, która weszła w życie także w czasie pandemii COVID-19 i którą zaliczyć można do tych, których zasadność w zakresie udostępniania danych obywateli podawana była w wątpliwość, jest Rozporządzenie Rady Ministrów z dnia 6 maja 2021 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z występowaniem stanu epidemii[19]. Przepisy zawarte w przywołanym rozporządzeniu kwestionował także Rzecznik Praw Obywatelskich[20].

Zbyt szeroki katalog podmiotów mających dostęp do tak wielu danych o charakterze sensytywnym nie jest bowiem uzasadniony i niezbędny w demokratycznym państwie. Wielokrotnie już TK wypowiadał się w tej kwestii. Każdorazowo w ocenie Trybunału wymóg „konieczności ograniczenia w demokratycznym państwie" nakazuje badać ustawodawcy, czy za pomocą danego ograniczenia jest możliwe osiągnięcie zamierzonych skutków, czy projektowane unormowanie jest niezbędne dla ochrony interesu publicznego, któremu ma służyć, oraz czy efekty projektowanego ograniczenia pozostają w proporcji do ciężaru nałożonego na obywatela[21]. Przesłanka wskazana powyżej, o której mowa w art. 31 ust. 3 Konstytucji RP, stanowi w pewnym sensie odpowiednik wypowiadanych w orzecznictwie TK postulatów kształtujących treść zasady proporcjonalności. Z jednej strony konieczne jest każdorazowe stwierdzenie przez prawodawcę rzeczywistej potrzeby dokonania w danym stanie faktycznym ingerencji w zakres prawa bądź wolności jednostki. Z drugiej zaś konieczne jest stosowanie takich tylko środków prawnych, które będą skuteczne, a więc rzeczywiście będą służyły realizacji zamierzonych przez prawodawcę celów. Środki, o których mowa powyżej, mają być także niezbędne, a więc muszą chronić określone wartości w sposób bądź w stopniu, który nie mógłby być osiągnięty przy zastosowaniu innych środków. Należy także podkreślić, że niezbędność to również skorzystanie tylko z takich środków, które są jak najmniej uciążliwe dla podmiotów, których prawa lub wolności ulegną ograniczeniu. Nieodzowne jest zatem, aby ingerencja w sferę statusu jednostki pozostawała w racjonalnej i odpowiedniej proporcji do celów, których ochrona uzasadnia dokonane ograniczenie[22].

---

[19] Rozporządzenie Rady Ministrów z dnia 6 maja 2021 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z występowaniem stanu epidemii, Dz.U. 2021, poz. 861 ze zm.

[20] Pismo Rzecznika Praw Obywatelskich do Prezesa Urzędu Ochrony Danych Osobowych z dnia 18.02.2022 r., https://bip.brpo.gov.pl/sites/default/files/2022-02/RPO_do_PUODO_18.02.2022.pdf (22.01.2024).

[21] Wyrok TK z 29.06.2001 r., K 23/00, OTK ZU 2001/5, poz. 124.

[22] Wyrok TK z 22.05.2007 r., SK 36/06, OTK ZU 2007/6/A, poz. 50.

Niewątpliwie ta kwestia wciąż pozostaje dużym wyzwaniem dla polskiego ustawodawcy, a rozwój e-administracji winien wymusić podejmowanie takich działań, które z jednej strony usprawniać będą kontakt obywatela z urzędem, z drugiej zaś – gwarantować dostęp do danych obywateli tylko tym podmiotom, które w przeciwnym razie nie mogą zrealizować zadania publicznego, a więc osiągnąć celu, dla którego konieczne jest przetwarzanie tych danych. Udostępnianie danych w szerszym zakresie narusza bowiem standardy ochrony danych osobowych.

3.3. Rejestry publiczne i zakres udostępnianych danych

Jednym z elementów e-administracji wykonywanym z zastosowaniem ICT (ang. *Information and Communications Technologies*) są rejestry publiczne[23]. Problemem nierozwiązanym od lat jest kwestia udostępniania w tych rejestrach przez organy państwa różnych zestawów danych w zależności od rejestru i jego celu. Jednym z rejestrów publicznych jest Centralny Rejestr Beneficjentów Rzeczywistych. Jawność powyższego rejestru wynika z art. 67 Ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[24]. Rejestr ma formę elektroniczną, a wszystkie zawarte w nim informacje są udostępniane bezpłatnie. W rejestrze tym przetwarzany jest m.in. numer PESEL. Mimo że zgodnie z rozporządzeniem 2016/679 identyfikator ten nie należy do katalogu danych wrażliwych, to jednak od lat zwraca się uwagę na potrzebę jego zabezpieczenia. Jest bowiem numerem identyfikacyjnym i jako taki winien podlegać szczególnej ochronie zgodnie z art. 87 tego rozporządzenia.

Najnowsze orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (dalej: TSUE) także odnosi się do tej kwestii, co powinno stanowić dla polskiego ustawodawcy istotny bodziec do zmiany aktualnego prawodawstwa. TSUE w wyroku w połączonych sprawach C-37/20 i C-601/20[25] orzekł, że art. 1 pkt 15 lit. c Dyrektywy Parlamentu Europejskiego i Rady UE 2018/843 z dnia 30 maja 2018 r. zmieniającej dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu oraz zmieniającej dyrektywy 2009/138/WE i 2013/36/UE jest nieważny w zakresie, w jakim przepis ten zmienił art. 30 ust. 5 akapit pierwszy lit. c dyrektywy Parlamentu Europejskiego i Rady UE 2015/849

---

[23] M. Błażewski, *Elektroniczne rejestry publiczne jako środki komunikacji elektronicznej*, „Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy" 2018, nr 26(1), s. 171.

[24] Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Dz.U. 2023, poz. 1124.

[25] Wyrok TS z 22.11.2022 r., WM i Sovim SA przeciwko Luxembourg Business Registers, C-37/20 i C-601/20, ECLI:EU:C:2022:912.

z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniającej rozporządzenie Parlamentu Europejskiego i Rady UE nr 648/2012 i uchylającej dyrektywę 2005/60/WE Parlamentu Europejskiego i Rady oraz dyrektywę Komisji 2006/70/WE, w taki sposób, że ów art. 30 ust. 5 akapit pierwszy lit. c w zmienionej wersji przewiduje, iż państwa członkowskie zapewniają, aby informacje o beneficjentach rzeczywistych podmiotów o charakterze korporacyjnym i innych podmiotów prawnych utworzonych na ich terytorium były we wszystkich przypadkach udostępniane każdej osobie.

TSUE wskazał[26], że skoro dane, o których mowa w art. 30 ust. 5 zmienionej dyrektywy, zawierają informacje o konkretnych osobach fizycznych, a mianowicie o beneficjentach rzeczywistych podmiotów o charakterze korporacyjnym i innych podmiotów prawnych utworzonych na terytorium państw członkowskich, dostęp do nich każdej osoby ma wpływ na podstawowe prawo do poszanowania życia prywatnego zagwarantowane w art. 7 Karty Praw Podstawowych UE (dalej: KPP)[27]. Publiczne zaś udostępnienie tych danych stanowi przetwarzanie danych objętych zakresem art. 8 KPP[28]. TSUE przypomniał także, że udostępnianie danych osobowych osobom trzecim stanowi ingerencję w prawa podstawowe ustanowione w art. 7 i art. 8 KPP, niezależnie od tego, w jaki sposób te dane zostaną później wykorzystane. W tym względzie nie ma znaczenia, czy rozpatrywane informacje dotyczące życia prywatnego są danymi szczególnie chronionymi, czy nie, ani czy osoby, których dane dotyczą, ucierpiały z powodu ewentualnych niedogodności wynikających z tej ingerencji[29]. Publiczny zatem dostęp do informacji dotyczących beneficjentów rzeczywistych, przewidziany w art. 30 ust. 5 zmienionej dyrektywy 2015/849, stanowi – w ocenie TSUE – ingerencję w prawa zagwarantowane w art. 7 i art. 8 KPP[30].

Wskazany powyżej wyrok TSUE winien także zostać uwzględniony przez polskiego ustawodawcę, do którego należy nowelizacja obowiązującej ustawy w trybie naprawczym. Wyrok TSUE z pewnością także będzie wytyczną dla budowania dalszych narzędzi e-administracji i tworzonych rejestrów publicznych, które muszą – jak wynika z jego orzecznictwa – respektować w szerszym stopniu prawo do prywatności osób, których dane umieszczane są w takim rejestrze.

---

26 *Ibidem*, pkt 38.

27 Zob. także wyrok TS z 21.06.2022 r., Ligue des droits humains przeciwko Conseil des ministres, C817/19, EU:C:2022:491, pkt 94.

28 Zob. także wyrok TS z 9.11.2010 r., Volker und Markus Schecke i Hartmut Eifert przeciwko Land Hessen, C92/09 i C93/09, EU:C:2010:662, pkt 52, 60.

29 Wyrok TS z 22.11.2022 r., WM i Sovim SA…, pkt 39.

30 *Ibidem*, pkt 40.

3.4. Bezpieczeństwo baz danych, systemów i rejestrów

W wyroku Trybunału Konstytucyjnego[31] w sprawie o sygn. K 23/11 Trybunał wskazał, że gromadzenie i przetwarzanie danych w rozmaitych zautomatyzowanych bazach rodzi jeszcze inne zagrożenie konstytucyjnych wolności oraz praw człowieka i obywatela. Jakkolwiek przywołany wyrok dotyczy niejawnej inwigilacji obywateli, co z jednej strony wykracza poza klasyczny sposób rozumienia e-administracji, a z drugiej strony wchodzi bardziej w zakres e-nadzoru, o którym była mowa na wstępie, to jednak część wniosków TK może mieć zastosowanie także do dalszych rozważań. W ocenie TK istnieje bowiem niebezpieczeństwo wycieku informacji spowodowanego zachowaniami podmiotów odpowiedzialnych za ich gromadzenie, jak też ograniczonymi możliwościami zabezpieczeń technicznych. Także w przypadku e-administracji należy pamiętać o tym, jak ważna jest kwestia bezpieczeństwa danych obywateli, które z uwagi na świadczone usługi, zakres danych, a także ich wrażliwy charakter mogą być przedmiotem ataków ze strony podmiotów niepowołanych.

Niestety zdarzają się przykłady braku zabezpieczeń bądź niewłaściwych zabezpieczeń systemu i to w dużej mierze takie incydenty, a także sposób, w jaki państwo radzi sobie z nimi, decydują o poziomie zaufania obywateli do państwa oraz do e--administracji. Kwestia bezpieczeństwa danych jest przedmiotem zainteresowania wszystkich organów nadzorczych. Naruszenia danych osobowych związane z brakiem odpowiednich zabezpieczeń technicznych i podatnościami systemów są trudne do zaakceptowania w podmiotach publicznych, których działania winny koncentrować się na tym, aby strzec danych obywateli ze szczególną starannością. Przywołać można w tym miejscu przykład holenderskiego organu właściwego ds. ochrony danych osobowych (Autoriteit Persoonsgegevens), który nałożył wysoką karę pieniężną na organ podatkowy (The Tax and Customs Administration) w związku z wykorzystywaniem przez ów organ systemu FSV (*Fraud Signaling Facility*)[32]. Wśród motywów nałożenia kary organ wskazał niezastosowanie odpowiednich zabezpieczeń oraz brak wdrożenia odpowiednich środków technicznych i organizacyjnych dotyczących bezpieczeństwa dostępu i danych osobowych w systemie FSV. Należy także zaznaczyć, że w tej sprawie organ nadzorczy dopatrzył się szeregu innych naruszeń ze strony organu podatkowego – m.in. naruszenia polegającego na tym, że dane osobowe przetwarzane były

---

31 Wyrok TK z 30.07.2014 r., K 23/11, OTK ZU 7A/2014, poz. 80.

32 Informacje na ten temat m.in. w: *GDPR Fine: Dutch DPA Fined Tax and Customs Administration €3.7 Million,* https://dataprivacymanager.net/gdpr-fine-dutch-dpa-fined-tax-and-customs--administration-e3-7-million/?fbclid=IwAR31lPJRFjlTEbxErzNpyUsWDcbYhjDJj94I7jkw8k4PPrhY1Io0E_XhUcA (28.06.2023).

bez podstawy prawnej, nie były aktualizowane, a więc w systemie przetwarzane były dane nieprawdziwe. Powyższe okoliczności kumulatywnie uzasadniały wysoką karę nałożoną na organ publiczny.

Innym przykładem może być także dostęp do danych innego użytkownika po zalogowaniu się na swój profil użytkownika na publicznej stronie internetowej www.podatki.gov.pl. W tej sprawie osoba, która weszła w posiadanie cudzych danych osobowych, skierowała wniosek do Rzecznika Praw Obywatelskich, który był przedmiotem postępowania wyjaśniającego[33]. W wyniku przedmiotowego postępowania Minister Finansów wykazał, że ów przypadek miał charakter jednostkowy i wynikał z błędu operatora, nie zaś wadliwego działania serwisu e-Urząd Skarbowy[34], jednak o tym naruszeniu musiał zostać poinformowany podmiot danych.

4. Rozwój nowych technologii oraz perspektywy dla prawa do prywatności i ochrony danych osobowych

Postęp w dziedzinie nowych technologii bez wątpienia sprzyja wykorzystaniu ich w e-administracji. Ogromną szansą dla dalszego rozwoju usług e-administracji jest sztuczna inteligencja, o której jest mowa w strategiach 36 państw, w tym również tych wchodzących w skład Unii Europejskiej, jako potencjale dla sektora publicznego[35]. Dostrzegalne jest ponadto zapotrzebowanie na usługi publiczne, które lepiej (w coraz większym stopniu) odpowiadają na zmieniające się oczekiwania użytkowników – nie tylko w zakresie szybkości reakcji, ale także personalizacji świadczonych usług[36]. Automatyzacja wielu prostych procesów może doprowadzić do oszczędności nie tylko czasowych, ale i finansowych. Z badań przeprowadzonych w 2017 r. wynika, że z 4,3 mld godzin przepracowanych rocznie w rządzie Stanów Zjednoczonych od 96,7 mln do 1,2 mld godzin może zostać zastąpionych pełną automatyzacją z potencjalnymi oszczędnościami wahającymi się od 3,3 mld dolarów na najniższym poziomie do 41,1

[33] Pismo Rzecznika Praw Obywatelskich do Ministra Finansów z dnia 13.03.2022 r., https://bip.brpo.gov.pl/sites/default/files/2023-03/Do_MF_podatki_dane_ujawnienie_13.03.2023.pdf (1.07.2023).

[34] Wyjaśnienia Ministra Finansów z dnia 19 kwietnia 2023 r. zob. Odpowiedź na pismo z 13 marca 2023 r., uzupełnione 27 marca 2023 r. w sprawie nieuprawnionego dostępu do danych, https://bip.brpo.gov.pl/sites/default/files/2023-05/Odpowiedz_MF_podatki_dane_ujawnienie_19.04.2023_wymazany.pdf (1.07.2023).

[35] J. Berryhill et al., *Hello, World: Artificial Intelligence and Its Use in the Public Sector*, Paris 2019, s. 73, *OECD Working Papers on Public Governance*, 36.

[36] B. Ubaldi et al., *State of the Art in the Use of Emerging Technologies in the Public Sector*, Paris 2019, s. 12, *OECD Working Papers on Public Governance*, 31.

mld dolarów w wariancie najbardziej optymistycznym[37]. W warunkach polskich analizowane są zaś kwestie związane z optymalizacją procesów zakupowych w sektorze publicznym z wykorzystaniem sztucznej inteligencji[38].

Mimo pierwotnych założeń dotyczących chęci przede wszystkim zautomatyzowania prostych i powtarzalnych czynności, które przynieść mogą ogromne oszczędności, pojawiają się coraz częściej plany na zdecydowanie szersze zastosowanie sztucznej inteligencji, w szczególności w celach predykcyjnych[39]. O ile jednak zastępowanie prostych czynności ich automatyzacją stanowi znikome zagrożenie dla praw człowieka, w tym prawa do prywatności, to jednak plany dotyczące budowania systemów predykcyjnych opartych o uczenie maszynowe i inne techniki kognitywne budzą szereg zastrzeżeń związanych z możliwymi naruszeniami prawa do prywatności i ochrony danych osobowych, zwłaszcza wobec konieczności budowania wzorców prognoz na ogromnych zestawach danych obywateli.

W strategiach poszczególnych państw unijnych dotyczących rozwoju sztucznej inteligencji, ale również wykorzystania jej w sektorze publicznym, dużo miejsca poświęca się poprawie jakości danych. Wiele państw chcących w perspektywie rozwijać narzędzia sztucznej inteligencji w sektorze publicznym stawia także na poprawę dostępności danych sektora publicznego[40]. Ponadto w obliczu planowanego zwiększenia wykorzystania systemów sztucznej inteligencji w sektorze publicznym podkreślana jest potrzeba zapewnienia przejrzystości sposobu ich działania[41].

Nową technologią, która także jest i może być w przyszłości wykorzystywana przez państwa, jest *blockchain*[42]. Powstawanie i rozwój tej technologii uznaje się za

---

37 *Ibidem*, s. 38.

38 Zob. Raport Fundacji Moje Państwo: M. Siwanowicz-Suska et al., *Sztuczna inteligencja i automatyczne podejmowanie decyzji w zamówieniach publicznych – wytyczne dla sektora publicznego*, https://mojepanstwo.pl/aktualnosci/787 (28.06.2023).

39 B. Ubaldi et al., *State of the Art…*, s. 38.

40 G. Misuraca, C. Van Noordt, *AI Watch – Artificial Intelligence in Public Services. Overview of the Use and Impact of AI in Public Services in the EU*, Joint Research Centre Science for Policy, European Commission, 2020, https://op.europa.eu/en/publication-detail/-/publication/4c72dd88--bcda-11ea-811c-01aa75ed71a1/language-en (3.07.2023).

41 Raport Fundacji Moje Państwo: M. Siwanowicz-Suska, M. Kajalidis, D. Macyszyn, *Dobre standardy w zarządzaniu systemami sztucznej inteligencji i automatycznego podejmowania decyzji w sektorze publicznym*, https://mojepanstwo.pl/pliki/zarzadzanie-ai-adm-sektor-publiczny.pdf (1.07.2023).

42 D. Allessie, M. Sobolewski, L. Vaccari, *Blockchain for Digital Government. An Assessment of Pioneering Implementations in Public Services*, Joint Research Centre Science for Policy, European Commission, 2019, https://joinup.ec.europa.eu/sites/default/files/document/2019-04/JRC115049%20blockchain%20for%20digital%20government.pdf (6.07.2023).

nową erę w sieciowym przetwarzaniu informacji[43]. W literaturze wskazuje się na to, że *blockchain* może znaleźć zastosowanie tam, gdzie właściwe zarządzanie informacją elektroniczną obniża koszty transakcyjne i przyśpiesza rozliczenia. Ponadto technologia ta – jak wynika z analiz – jest bardziej transparentna i ogranicza możliwość duplikowania dokumentów, przez co zyskuje opinię bezpiecznej metody weryfikacyjnej dla szeregu transakcji[44]. Wobec zagrożeń związanych z kradzieżą tożsamości i naruszeniami danych osobowych wskazuje się, z uwagi na wspomniane powyżej bezpieczeństwo tej technologii, na możliwość ustanowienia cyfrowej tożsamości działającej na podstawie *blockchain*. Technologia ta może być także wykorzystywana w celu potwierdzenia prawa własności oraz w elektronicznym głosowaniu[45], jak również do dystrybucji oraz kontroli środków z pomocy publicznej, w szczególności świadczeń socjalnych[46]. Jakkolwiek *blockchain* określa się w literaturze jako technologię wspierającą prywatność[47], to jednak – jak wskazują sami eksperci[48] – bariery prywatności w niej stosowane (głównie kryptografia) nie są całkowite ani niemożliwe do przełamania. Należy ponadto zaznaczyć, że specyfika tej technologii generuje trudności na styku z rozporządzeniem 2016/679, polegające na tym, że realnym problemem – z uwagi na rozproszoną konstrukcję rejestru bloków – jest ustalenie administratora danych oraz realizacja praw osób, których dane dotyczą[49]. Rekomendowanym rozwiązaniem jest w tej sytuacji indywidualizacja każdego jednostkowego procesu, gdyż – jak wskazują eksperci – nie da się jednoznacznie stwierdzić, czy *blockchain* to rozwiązanie niepodlegające przepisom rozporządzenia 2016/679. Jednak – co warto w tym miejscu podkreślić – technologia ta mimo różnych opinii w zakresie stosowania do niej przepisów rozporządzenia 2016/679 będzie w najbliższym czasie przedmiotem zainteresowania i analizy ze strony Europejskiej Rady Ochrony Danych, mającej na celu wypracowanie wytycznych dla tej technologii[50].

---

[43] W. Mincewicz, *Potencjał wykorzystania technologii blockchain na szczeblu samorządu terytorialnego*, „Studia Politologiczne" 2023, vol. 67, s. 128.

[44] D. Dudek, *Możliwości wykorzystania technologii blockchain w obszarze edukacji*, „Informatyka Ekonomiczna" 2017, nr 3(45), s. 59.

[45] W. Mincewicz, *Potencjał wykorzystania…*, s. 136.

[46] M. Kowalczyk, D. Wilga, *Blockchain – perspektywy wdrożeń w sektorze publicznym*, „Roczniki Kolegium Analiz Ekonomicznych SGH" 2019, nr 56, s. 128.

[47] D. Mider, E.A. Ziemak, *Technologie wspierające prywatność – ideologia, prawo, wdrożenia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2021, vol. 13, nr 24, s. 132-172.

[48] *Ibidem*, s. 160.

[49] M. Dymiński, D. Ferenc, *RODO w „łańcuchu bloków"*, „Przegląd Prawa Publicznego" 2020, nr 6, s. 7-23.

[50] European Data Protection Board, *EDPB Work Programme 2023/2024*, https://edpb.europa.eu/system/files/2023-02/edpb_work_programme_2023-2024_en.pdf (10.07.2023).

5. Rola organu nadzorczego

Rola organu nadzorczego w zakresie ochrony prawa do prywatności i ochrony danych osobowych w dobie cyfryzacji i e-administracji zdecydowanie nabiera na ważności. Stosowanie nowych narzędzi do dostarczania usług publicznych wymaga z jednej strony nowych zabezpieczeń i gwarancji, z drugiej zaś – szczególnej czujności organu właściwego w sprawach ochrony danych osobowych. Bez względu bowiem na to, jak zaawansowane będą zabezpieczenia, istotne jest, by nad bezpieczeństwem kontaktu cyfrowego obywatela z państwem czuwał niezależny organ, mogący w razie potrzeby w sposób bezkompromisowy i skuteczny działać na rzecz praw i wolności obywateli.

Relacja obywatel – państwo jest relacją nierówną z wyraźnym wskazaniem na możliwości państwa, co w sposób oczywisty wymusza wprowadzenie niezależnego bezpiecznika stojącego na straży prawa do prywatności i ochrony danych osobowych. Rolę tę w warunkach polskich pełni Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).

Normatywne gwarancje niezależności każdego europejskiego organu nadzorczego zawarte zostały w art. 52 rozporządzenia 2016/679, zgodnie z którym każdy organ nadzorczy podczas wypełniania swoich zadań i wykonywania swoich uprawnień działa w sposób w pełni niezależny (ust. 1), a członek lub członkowie każdego organu nadzorczego podczas wypełniania swoich zadań i wykonywania swoich uprawnień wolni są od bezpośrednich i pośrednich wpływów zewnętrznych, nie zwracają się do nikogo o instrukcje ani ich od nikogo nie przyjmują (ust. 2)[51]. Polskie przepisy o ochronie danych osobowych w ramach wskazanych powyżej gwarancji przewidują angażujący obie izby parlamentu sposób powołania Prezesa UODO na stanowisko, określają wymogi kwalifikacyjne dla kandydata na urząd, a także przewidują możliwość podlegania Prezesa UODO w zakresie wykonywania zadań jedynie ustawie.

Nie wdając się w szerszą dyskusję związaną z kryzysem praworządności w Polsce, gdyż nie temu poświęcony jest niniejszy artykuł, wskazać należy, iż kwestia powołania w 2019 r. Prezesa UODO budziła duże kontrowersje. Organizacje pozarządowe podnosiły brak kompetencji zgłoszonego kandydata, a więc niespełnienie jednego z ustawowych wymogów, a także podawały w wątpliwość jego niezależność[52]. W działalności

[51] Szerzej na temat niezależności organu nadzorczego w kontekście prywatności w łączności elektronicznej zob. M. Rojszczak, *Reforma krajowych przepisów o ochronie danych a kwestia niezależności organów nadzorczych na tle rozporządzenia 2016/679 i dyrektywy 2002/58 – uwagi krytyczne*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2018, vol. 7, nr 4, s. 70-85.

[52] Informacje o działaniach Fundacji Panoptykon oraz Helsińskiej Fundacji Praw Człowieka dostępne m.in. na stronach internetowych – zob. W. Klicki, *Apelujemy o spokojny wybór nowego Prezesa UODO!*, https://panoptykon.org/wiadomosc/apelujemy-o-spokojny-wybor-nowego-prezesa-uodo

Prezesa UODO wskazać można dwie kontrowersyjne i szeroko dyskutowane sprawy, które ostatecznie stały się przedmiotem postępowania sądowo-administracyjnego, a także krytyki działalności organu nadzorczego.

Pierwszą ze spraw poddawanych krytyce w związku z brakiem reakcji ze strony organu nadzorczego była kwestia tzw. wyborów kopertowych, a także jego stanowisko, zgodnie z którym Poczta Polska SA mogła pozyskiwać dane osobowe obywateli, co skutkowało nieuwzględnianiem skarg obywateli[53]. Wojewódzki Sąd Administracyjny w Warszawie w jednej ze spraw[54] stwierdził, że stanowisko organu dotyczące braku podstaw do prowadzenia postępowania odnośnie do naruszenia przez Pocztę Polską SA obowiązku informacyjnego było co najmniej przedwczesne, a zawarte w skardze zarzuty naruszenia art. 15 ust. 1 w zw. z art. 12 ust. 3 rozporządzenia 2016/679 oraz art. 7, art. 77, art. 80, art. 107 § 3 Ustawy z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego[55] w zw. z art. 7 ust. 1 Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[56] uznał za uzasadnione. Należy także zaznaczyć, że przywołane powyżej rozstrzygnięcie nie było jedynym w tej sprawie[57].

Kolejną kwestią mogącą budzić wątpliwości w zakresie niezależności organu nadzorczego była także szeroko komentowana sprawa poparcia dla list do Krajowej Rady Sądownictwa (KRS). Mimo prawomocnego wyroku sądu Prezes UODO nie dopuścił do ujawnienia opinii publicznej list poparcia dla kandydatów na sędziów. W głośnym rozstrzygnięciu Naczelny Sąd Administracyjny[58] wskazał, że Prezes UODO – podejmując działania w tej sprawie – w istocie polemizował z wyrokami sądów administracyjnych, stawiając się w roli swego rodzaju „superrecenzenta" wyroków sądowych i naruszając zawartą w art. 10 ust. 1 Konstytucji RP zasadę podziału władzy. W ocenie NSA działanie Prezesa UODO jako bezprawne łamało także zasadę wyrażoną w art. 2 Konstytucji RP, a więc zasadę demokratycznego państwa prawnego. NSA, wskazując na powyższe naruszenia, zarzucił także Prezesowi UODO sprze-

(1.07.2023); Pismo Prezes Fundacji Panoptykon do Marszałka Sejmu RP z dnia 1.04.2019 r., https://panoptykon.org/sites/default/files/panoptykon_i_hfpc_marszalek_tryb_wyboru_prezesa_uodo_1.04.2019.pdf (1.07.2023); Fundacja Panoptykon, *Monitorujemy wybory nowego Prezesa Urzędu Ochrony Danych Osobowych*, https://panoptykon.org/wyboryuodo (1.07.2023).

53 Wyrok WSA w Warszawie z 25.02.2022 r., II SA/Wa 2286/21.

54 *Ibidem*.

55 Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego, Dz.U. 2023, poz. 775.

56 Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. 2019, poz. 1781.

57 Zob. także wyrok WSA w Warszawie z 15.03.2021 r., II SA/Wa 1743/20, w którym sąd uchylił zaskarżone postanowienie Prezesa Urzędu Ochrony Danych Osobowych w przedmiocie odmowy wszczęcia postępowania.

58 Wyrok NSA z 6.04.2023 r., III OSK 2991/21.

niewierzenie się określonemu w art. 35 ust. 1 ustawy o ochronie danych osobowych ślubowaniu, w którego rocie wprost zapisano, iż zobowiązuje się on do dochowania wierności Konstytucji RP oraz stania na straży prawa ochrony danych osobowych.

Powyżej przywołane przykłady odnieść należy do rozstrzygnięcia TSUE[59], jakkolwiek wydanego pod rządami poprzedzającej rozporządzenie 2016/679 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[60], to jednak utrzymującego swoją aktualność z uwagi na to, że w ocenie TSUE wystarczającą przeszkodą w niezależnym wykonywaniu zadań organu jest samo zagrożenie możliwością wpływu politycznego. Z orzecznictwa TSUE wynika bowiem, że całkowita niezależność, o której mowa była w art. 28 ust. 1 dyrektywy 95/46, oznacza pełną niezależność od bezpośrednich lub pośrednich wpływów, zapewniając danemu organowi nadzorczemu możliwość w pełni swobodnego działania, z wyłączeniem jakichkolwiek instrukcji czy nacisków, bez wpływu z zewnątrz i bez ryzyka, że tego rodzaju wpływ mógłby być wywierany[61].

Mając powyższe na uwadze, należy zauważyć, że krytykowana i podważana działalność Prezesa UODO jako organu właściwego w sprawie ochrony danych osobowych nie wpływa budująco na sposób realizacji i respektowania prawa do prywatności przez organy państwa. Powyższa kwestia jest jeszcze bardziej niepokojąca w obliczu możliwego rozszerzenia kompetencji Prezesa UODO o sprawy wynikające z unijnej regulacji dotyczącej sztucznej inteligencji. Aktywność organu nadzorczego w naturalny sposób winna koncentrować się na analizie i śledzeniu rozwijających się nowych technologii, jednak działania te i sposób reagowania na zagrożenia są dalece niewystarczające.

6. Wnioski

Zarówno obecny, jak i planowany sposób działania e-administracji jest trudny czy wręcz niemożliwy do pogodzenia z gwarancjami wynikającymi z prawa do prywatności i ochrony danych osobowych. Zagrożeniami dla ochrony danych osobowych gromadzonych w systemach i rejestrach państwowych są: ich nadmiarowość, udostępnianie nieupoważnionym podmiotom (także w ramach sektora publicznego)

---

[59] Wyrok TSUE z 8.04.2014 r., Komisja Europejska przeciwko Węgrom, ECLI:EU:C:2014:237.

[60] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.Urz. UE, L 281/31.

[61] *Ibidem*, pkt 37.

oraz – jak pokazano w niniejszym artykule – udostępnianie części danych w ramach publicznych rejestrów. Dobro obrotu gospodarczego i transparentność prowadzonych transakcji nie uzasadniają wkraczania w sferę prywatną osób prowadzących działalność gospodarczą. Polski ustawodawca zmuszony będzie w najbliższym czasie zmierzyć się z powyższym zagadnieniem i dokonać zmian w prawie powszechnie obowiązującym, które – jak niedawno orzekł TSUE w jednej ze spraw – niezgodne jest ze standardami europejskimi i narusza KPP.

Zarówno w kwestiach związanych z dostosowywaniem przepisów prawa do standardów europejskich, jak również w zakresie stania na straży prawa do prywatności i ochrony danych osobowych w kontekście nowych technologii, dynamicznie wchodzących w obszar e-administracji, przed organem nadzorczym z pewnością stoi wiele wyzwań merytorycznych i technologicznych. Ważną, także poruszoną w niniejszym artykule kwestią jest potrzeba – w związku z rozwojem nowych technologii większa nawet niż dotychczas – niezależnego działania organu nadzorczego, który da poczucie pewności, stabilności i bezpieczeństwa obywatelom poruszającym się w coraz bardziej zdigitalizowanym państwie. Każda zatem próba łamania zasady legalności ze strony władzy, naruszająca prawo do prywatności i zasadę ochrony danych osobowych, winna się spotykać z bezwzględną reakcją ze strony Prezesa UODO, do którego kompetencji należy piętnowanie takich zachowań.

Nowe technologie w e-administracji to zdecydowanie nowe wyzwania dla organu nadzorczego i to jego działania, a przede wszystkim sposób reakcji na naruszenia ze strony władzy, w dużej mierze będą miały wpływ na poziom zaufania obywateli do państwa i stosowane nowoczesne kanały komunikacji i świadczone nowe usługi.

Bibliografia

[AKTUALIZACJA] Rządowy serwis eFaktura.gov[.]pl zhackowany. Dwa razy :D, https://niebezpiecznik.pl/post/rzadowy-serwis-efaktura-gov-pl-zhackowany/.

Al-Besher A., Kumar K., *Use of Artificial Intelligence to Enhance e-Government Services*, „Measurement: Sensors" 2022, vol. 24, 100484, https://doi.org/10.1016/j.measen.2022.100484.

Allessie D., Sobolewski M., Vaccari L., *Blockchain for Digital Government. An Assessment of Pioneering Implementations in Public Services*, Joint Research Centre Science for Policy, European Commission, 2019, https://joinup.ec.europa.eu/sites/default/files/document/2019-04/JRC115049%20blockchain%20for%20digital%20government.pdf.

Berryhill J. et al., *Hello, World: Artificial Intelligence and Its Use in the Public Sector*, Paris 2019, *OECD Working Papers on Public Governance*, 36.

Błażewski M., *Elektroniczne rejestry publiczne jako środki komunikacji elektronicznej*, „Zeszyty Naukowe Państwowej Wyższej Szkoły Zawodowej im. Witelona w Legnicy" 2018, nr 26(1), s. 171-181.

Dudek D., *Możliwości wykorzystania technologii blockchain w obszarze edukacji*, „Informatyka Ekonomiczna" 2017, nr 3(45), s. 55-65.

Dudzik S., *Podstawy prawne działania e-administracji a ochrona danych osobowych*, [w:] *E-administracja. Skuteczna, odpowiedzialna i otwarta administracja publiczna w Unii Europejskiej*, S. Dudzik, I. Kawka, R. Śliwa (red.), Kraków 2022, s. 13-28, *Krakow Jean Monnet Research Papers*, 1, https://doi.org/10.12797/9788381386739.01.

Dymiński M., Ferenc D., *RODO w „łańcuchu bloków"*, „Przegląd Prawa Publicznego" 2020, nr 6, s. 7-23.

Dziwny atak na serwery rządowej instytucji CUW obsługującej Kancelarię Prezesa Rady Ministrów, https://niebezpiecznik.pl/post/dziwny-atak-na-serwery-rzadowej-instytucji-cuw-obslugujacej-kancelarie-prezesa-rady-ministrow/.

European Data Protection Board, *EDPB Work Programme 2023/2024*, https://edpb.europa.eu/system/files/2023-02/edpb_work_programme_2023-2024_en.pdf.

Fundacja Panoptykon, *Monitorujemy wybory nowego Prezesa Urzędu Ochrony Danych Osobowych*, https://panoptykon.org/wyboryuodo.

Gajowniczek T., *E-gov w Ukrainie – zarys problemu*, „Środkowoeuropejskie Studia Polityczne" 2022, nr 4, s. 169-191, https://doi.org/10.14746/ssp.2022.4.9.

GDPR Fine: Dutch DPA Fined Tax and Customs Administration €3.7 Million, https://dataprivacymanager.net/gdpr-fine-dutch-dpa-fined-tax-and-customs-administration-e3-7-million/?fbclid=IwAR31lPJRFjlTEbxErzNpyUsWDcbYhjDJj94I7jkw8k4PPrhY1Io0E_XhUcA.

Gruber J., Wasylów J., *Bezpieczne aplikacje .NET w technologii Web serwisów*, [w:] *Bezpieczeństwo systemów informatycznych*, A. Niemiec, J.S. Nowak, J.K. Grabara (red.), Katowice 2006, s. 75-100.

Haręża A., *Wprowadzenie do problematyki elektronicznej administracji publicznej*, „Prawo Mediów Elektronicznych" 2011, nr 1, s. 26-31.

Kancelaria Premiera, MSZ, MON i Kancelaria Prezydenta zhackowane. Wiemy kto stoi za tymi włamaniami, https://niebezpiecznik.pl/post/kancelaria-premiera-msz-mon-i-kancelaria-prezydenta-zhackowane-wiemy-kto-stoi-za-tymi-wlamaniami/.

Klicki W., *Apelujemy o spokojny wybór nowego Prezesa UODO!*, https://panoptykon.org/wiadomosc/apelujemy-o-spokojny-wybor-nowego-prezesa-uodo.

Kowalczyk M., Wilga D., *Blockchain – perspektywy wdrożeń w sektorze publicznym*, „Roczniki Kolegium Analiz Ekonomicznych SGH" 2019, nr 56, s. 121-131.

Maj M., *Tajemnicze włamanie do rządowej instytucji zarządzającej miliardami złotych oraz tragiczny obraz polskiego cyberbezpieczeństwa w sektorze publicznym*, https://niebezpiecznik.pl/post/tajemnicze-wlamanie-do-rzadowej-instytucji-zarzadzajacej-miliardami-zlotych-oraz-tragiczny-obraz-polskiego-cyberbezpieczenstwa-w-sektorze-publicznym/.

Mazur Z., Mendyk-Krajewska T., *Złożoność i kompleksowość narzędzi ochrony systemów komputerowych*, [w:] *Bezpieczeństwo systemów informatycznych*, A. Niemiec, J.S. Nowak, J.K. Grabara (red.), Katowice 2006, s. 11-36.

Mider D., Ziemak E.A., *Technologie wspierające prywatność – ideologia, prawo, wdrożenia*, „Przegląd Bezpieczeństwa Wewnętrznego" 2021, vol. 13, nr 24, s. 132-172, https://doi.org/10.4467/20801335PBW.21.003.13560.

Mincewicz W., *Potencjał wykorzystania technologii blockchain na szczeblu samorządu terytorialnego*, „Studia Politologiczne" 2023, vol. 67, s. 127-150, http://dx.doi.org/10.33896/SPolit.2023.67.8.

Ministerstwo Edukacji i Nauki, *Podsumowanie akcji szczepień na polskich uczelniach*, https://www.gov.pl/web/edukacja-i-nauka/podsumowanie-akcji-szczepien-na-polskich-uczelniach.

Misuraca G., Noordt C. Van, *AI Watch: Artificial Intelligence in Public Services. Overview of the Use and Impact of AI in Public Services in the EU*, Joint Research Centre Science for Policy, European Commission, 2020, https://op.europa.eu/en/publication-detail/-/publication/4c72dd88-bcda-11ea-811c-01aa75ed71a1/language-en.

Odpowiedź [Ministra Finansów] na pismo z 13 marca 2023 r., uzupełnione 27 marca 2023 r. w sprawie nieuprawnionego dostępu do danych, https://bip.brpo.gov.pl/sites/default/files/2023-05/Odpowiedz_MF_podatki_dane_ujawnienie_19.04.2023_wymazany.pdf.

Pismo Prezes Fundacji Panoptykon do Marszałka Sejmu RP z dnia 1.04.2019 r., https://panoptykon.org/sites/default/files/panoptykon_i_hfpc_marszalek_tryb_wyboru_prezesa_uodo_1.04.2019.pdf.

Pismo Rzecznika Praw Obywatelskich do Ministra Edukacji i Nauki z dnia 26.01.2022 r., https://bip.brpo.gov.pl/sites/default/files/2022-01/RPO_do_MEN_26.1.2022.pdf.

Pismo Rzecznika Praw Obywatelskich do Prezesa Urzędu Ochrony Danych Osobowych z dnia 18.02.2022 r., https://bip.brpo.gov.pl/sites/default/files/2022-02/RPO_do_PUODO_18.02.2022.pdf.

Pismo Rzecznika Praw Obywatelskich do Ministra Finansów z dnia 13.03.2022 r., https://bip.brpo.gov.pl/sites/default/files/2023-03/Do_MF_podatki_dane_ujawnienie_13.03.2023.pdf.

Przyborska K., *e-Ukraina – państwo w smartfonie*, https://krytykapolityczna.pl/swiat/ukraina-cyfryzacja-digitalizacja/.

Rojszczak M., *Reforma krajowych przepisów o ochronie danych a kwestia niezależności organów nadzorczych na tle rozporządzenia 2016/679 i dyrektywy 2002/58 – uwagi krytyczne*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny" 2018, vol. 7, nr 4, s. 70-85.

Siwanowicz-Suska M. et al., *Sztuczna inteligencja i automatyczne podejmowanie decyzji w zamówieniach publicznych – wytyczne dla sektora publicznego*, https://mojepanstwo.pl/aktualnosci/787.

Siwanowicz-Suska M., Kajalidis M.,Macyszyn D., *Dobre standardy w zarządzaniu systemami sztucznej inteligencji i automatycznego podejmowania decyzji w sektorze publicznym*, https://mojepanstwo.pl/pliki/zarzadzanie-ai-adm-sektor-publiczny.pdf.

Śledziewska K., Zięba D., *E-administracja w Polsce na tle Unii Europejskiej. Jak z niej (nie) korzystamy*, Warszawa 2016.

Ubaldi B. et al., *State of the Art in the Use of Emerging Technologies in the Public Sector*, Paris 2019, *OECD Working Papers on Public Governance*, 31, https://doi.org/10.1787/932780bc-en.

Włamanie do sieci Kancelarii Premiera? Atakujący miał uzyskać dostęp do poczty pracowników KPRM, https://niebezpiecznik.pl/post/wlamanie-do-sieci-kancelarii-premiera-atakujacy-mial-uzyskac-dostep-do-poczty-pracownikow-kprm/.

Wyrębek H., *Bezpieczeństwo w zarządzaniu informacją na poziomie systemów informatycznych*, „Zeszyty Naukowe Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach. Seria Administracja i Zarządzanie" 2012, nr 95, s. 463-470.

Viechnicki P., Eggers W.D., *How Much Time and Money Can AI Save Government? Cognitive Technologies Could Free up Hundreds of Millions of Public Sector Worker Hours*, https://www2.deloitte.com/content/dam/insights/us/articles/3834_How-much-time-and-money-can-AI-save-government/DUP_How-much-time-and-money-can-AI-save-government.pdf.

Niniejsza monografia powstała jako trzecia w serii Krakow Jean Monnet Research Papers w ramach realizowanego przez Katedrę Prawa Europejskiego Uniwersytetu Jagiellońskiego projektu Jean Monnet Module pt. „E-administracja – europejskie wyzwania dla administracji publicznej w państwach członkowskich UE i krajach partnerskich/ eGovEU+".

Przedstawia ona analizę wdrożenia i funkcjonowania cyfrowych usług publicznych w Polsce i w Europie ze szczególnym uwzględnieniem związanych z tym wyzwań. Dotyczą one m.in. rozwoju infrastruktury teleinformatycznej, zapobiegania wykluczeniu cyfrowemu oraz zapewniania ochrony prywatności i bezpieczeństwa obywatelom.

Książka adresowana jest do badaczy zajmujących się administracją, prawem administracyjnym i europejskim oraz do praktyków w wymienionych dziedzinach. Mamy nadzieję, że publikacja poszerzy wiedzę czytelników na temat cyfryzacji usług publicznych oraz zachęci środowisko naukowe do dalszych badań w tym zakresie.

This monograph is the third in the Krakow series of Jean Monnet Research Papers and was written as part of the Jean Monnet Module project, carried out by the Chair of European Law at the Jagiellonian University, "E-government – European Challenges for Public Administration in EU Member States and Partner Countries/eGovEU+."

The book presents an analysis of the implementation and functioning of digital public services in Poland and Europe with a particular focus on the challenges involved. These include the development of ICT infrastructure, preventing digital exclusion and ensuring privacy and security of citizens.

The monograph is addressed to researchers in administration, administrative and European law as well as to practitioners in the mentioned fields. We hope the publication will broaden the readers' knowledge of the digitization of public services and encourage the scientific community to further research in this area.

WYDAWNICTWO KSIĘGARNIA AKADEMICKA

https://akademicka.pl

ISBN 978-83-8368-025-5