

Prawo publiczne i prywatne w dobie informatyzacji – ocena dotychczasowych rozwiązań i perspektywy na przyszłość



Redakcja naukowa

Bartosz Kotowicz, Angelika Kurzawa, Łukasz Nosarzewski

Prawo publiczne i prywatne w dobie informatyzacji – ocena dotychczasowych rozwiązań i perspektywy na przyszłość

*Redakcja naukowa
Bartosz Kotowicz, Angelika Kurzawa,
Łukasz Nosarzewski*



Warszawa 2023

Prawo publiczne i prywatne w dobie informatyzacji – ocena dotychczasowych rozwiązań i perspektywy na przyszłość

Redakcja naukowa:

Bartosz Kotowicz (Uczelnia Łazarskiego, ORCID 0000-0003-1560-9938)

Angelika Kurzawa (Uczelnia Łazarskiego, ORCID 0000-0003-3338-3848)

Łukasz Nosarzewski (Uczelnia Łazarskiego, ORCID 0000-0001-8769-6757)

Recenzenci: dr hab. Joanna Smarż, prof. UTH Rad.

dr hab. Jan Chmielewski, prof. ALK

Redaktor prowadząca: Aleksandra Szudrowicz

Redakcja językowa i korekta: PanDawer

Projekt okładki: Paweł Pietrzyk (image: Pixabay.com)

Autorzy:

Dominik Borek

(Ministerstwo Sportu i Turystyki, ORCID 0000-0002-4359-9426)

Justyna Dudzińska

(Uczelnia Łazarskiego, ORCID 0000-0001-7258-9182)

Beata Gocko

(Państwowa Akademia Nauk Stosowanych w Przemysłu, ORCID 0000-0001-6202-6423)

Olga Józefczyk

(Uczelnia Łazarskiego, ORCID 0000-0003-2156-7711)

Paweł Śwital

(Uniwersytet Technologiczno-Humanistyczny im. Kazimierza Pułaskiego w Radomiu,
ORCID 0000-0002-7404-5143)

Renata Kuśpiel

(Uczelnia Łazarskiego, ORCID 0000-0002-5887-4451)

Mirosława Pytlewska

(Instytut de Republica, ORCID 0000-0002-0299-055X)

Katarzyna Tomiło-Nawrocka

(Uczelnia Łazarskiego, ORCID 0000-0001-6477-293X)

Beata Zając-Dutkiewicz

(Uczelnia Łazarskiego, ORCID 0009-0005-8193-5341)

Bożena Dąbkowska-Mastalerek

(Uczelnia Łazarskiego, ORCID 0000-0001-6034-3839)

Magdalena Zawisza

(Okręgowa Izba Adwokacka w Warszawie; Uczelnia Łazarskiego, ORCID 0000-0002-6883-5050)

DOI 10.26399/978-83-66723-59-7

ISBN 978-83-66723-59-7

e-ISBN 978-83-66723-60-3

© Copyright by Uczelnia Łazarskiego 2022



Wydanie 1

Oficyna Wydawnicza Uczelni Łazarskiego, Warszawa 2023

SPIS TREŚCI

Wykaz ważniejszych skrótów	7
Wstęp	10
Część I	
Jednostka i państwo wobec informatyzacji	13
System rejestrów publicznych w turystyce jako narzędzie służące zarządzaniu i informatyzacji branży turystycznej – aspekty organizacyjno-prawne	
<i>Dominik Borek</i>	<i>15</i>
Głosa krytyczna do wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 7 sierpnia 2020 r. (II SA/Wa 809/20)	
<i>Justyna Dudzińska</i>	<i>41</i>
Unijne systemy informacyjne na potrzeby zarządzania granicami i bezpieczeństwa wewnętrznego	
<i>Beata Gocko</i>	<i>63</i>
Przetwarzanie danych biometrycznych a prawo do prywatności	
<i>Olga Józefczyk</i>	<i>91</i>

Informatyzacja administracji publicznej w Polsce – wyzwania i problemy	
<i>Paweł Śwital</i>	111
Część II	
Sądownictwo w dobie informatyzacji	131
Informatyzacja postępowania karnego a prawo do obrony	
<i>Renata Kuśpiel</i>	133
Elektroniczne postępowanie wieczystoksięgowe w kontekście informatyzacji postępowań sądowych	
<i>Mirosława Pytlewska</i>	159
Wnoszenie oraz doręczanie pism procesowych za pośrednictwem środków komunikacji elektronicznej w postępowaniu sądowoadministracyjnym	
<i>Katarzyna Tomiło-Nawrocka</i>	177
Sądownictwo administracyjne w dobie informatyzacji – ocena wybranych rozwiązań i perspektywy na przyszłość	
<i>Beata Zając-Dutkiewicz, Bożena Dąbkowska-Mastalerek</i>	193
Elektroniczne postępowanie upominawcze jako wzorzec informatyzacji postępowania cywilnego	
<i>Magdalena Zawisza</i>	209
Nota o redaktorach naukowych	223

WYKAZ WAŻNIEJSZYCH SKRÓTÓW

Akty normatywne

Konstytucja RP	Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. Nr 78 poz. 483 z późn. zm.)
Konwencja	Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z dnia 4 listopada 1950 r. (Dz.U. z 1993 r. Nr 61 poz. 284)
kpc	ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (t.j. Dz.U. z 2021 r. poz. 1805 z późn. zm.)
kpk	ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. Dz.U. z 2022 r. poz. 1375)
pps	ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz.U. z 2022 r. poz. 329 z późn. zm.)
rde	rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (Dz.U. z 2018 r. poz. 180)
RODO	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 119/1)
rozporządzenie eIDAS	rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz.Urz. UE L 257/73)

uidp	ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2021 r. poz. 2070)
ukwh	ustawa z dnia 6 lipca 1982 r. o księgach wieczystych i hipotece (t.j. Dz.U. z 2022 r. poz. 1728)
ustawa o COVID-19	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 2020 r. poz. 1842 z późn. zm.)

Organy i sądy

ETPCz	Europejski Trybunał Praw Człowieka
MSiT	Ministerstwo Sportu i Turystyki
NSA	Naczelny Sąd Administracyjny
PUODO	Prezes Urzędu Ochrony Danych Osobowych
RPO	Rzecznik Praw Obywatelskich
TK	Trybunał Konstytucyjny
TSUE	Trybunał Sprawiedliwości Unii Europejskiej
WSA	wojewódzki sąd administracyjny

Czasopisma

IAP	Informacja w Administracji Publicznej
OSNKW	Orzecznictwo Sądu Najwyższego Izba Karna i Wojskowa
OTK	Orzecznictwo Trybunału Konstytucyjnego
OTK-A	Orzecznictwo Trybunału Konstytucyjnego Seria A
MoP	Monitor Prawniczy
MoPH	Monitor Prawa Handlowego
NPN	Nowy Przegląd Notarialny
PBW	Przegląd Bezpieczeństwa Wewnętrznego

PiP	Państwo i Prawo
PME	Prawo Mediów Elektronicznych
PPA	Przegląd Prawa i Administracji
PPP	Przegląd Prawa Publicznego
Prok. i Pr.	Prokuratura i Prawo
PUG	Przegląd Ustawodawstwa Gospodarczego
ST	Samorząd Terytorialny
ZNSA	Zeszyty Naukowe Sądownictwa Administracyjnego
ZNUJ	Zeszyty Naukowe Uniwersytetu Jagiellońskiego

Inne

CBOSA	Centralna Baza Orzeczeń Sądów Administracyjnych
Dz.U.	Dziennik Ustaw Rzeczypospolitej Polskiej
Dz.Urz. MSiT	Dziennik Urzędowy Ministra Sportu i Turystyki
Dz.Urz. UE	Dziennik Urzędowy Unii Europejskiej
ePUAP	Elektroniczna Platforma Usług Administracji Publicznej
późn. zm.	późniejsze zmiany
t.j.	tekst jednolity

WSTĘP

Ewolucja społeczeństwa informacyjnego, skutkująca zintensyfikowaniem roli oraz użycia nowoczesnych technologii komunikacyjnych i informacyjnych, wywołała wiele społeczno-gospodarczych zmian. Szybki rozwój technologii ułatwiający komunikację oraz przyspieszający transmisję danych spowodował, że zaczęto postrzegać przesyłanie informacji za pomocą Internetu za kluczowy czynnik komunikacji międzyludzkiej. Na przestrzeni ostatnich lat zauważa się rosnące wykorzystanie sieci wirtualnych w przeróżnych obszarach, związanych zarówno z prowadzeniem gospodarstw domowych, jak i działalnością przedsiębiorstw, ale również funkcjonowaniem instytucji, takich jak wymiar sprawiedliwości czy administracja publiczna.

Informatyzacja społeczeństwa stała się równoznaczna z informatyzacją państwa.

W ciągu ostatnich kilkunastu lat doszło do wielu zmian w funkcjonowaniu administracji publicznej, polegających na wdrożeniu systemów teleinformatycznych umożliwiających oferowanie obywatelom oczekiwanych przez nich szeroko pojętych usług elektro-nicznych. Informatyzacja państwa nadal jest procesem dynamicznym. Część regulacji wprowadzonych przez ustawodawcę można uznać za bezpośredni skutek pandemii COVID-19, która niewątpliwie spowodowała przyspieszenie niektórych zmian w obszarze procedur sądowych, chociażby wprowadzenie rozpraw zdalnych. Zmiany te dotyczyły również procedur administracyjnych. Współcześnie trudno wyobrazić sobie funkcjonowanie organów administracyjnych i sądowych, kiedy to ręcznie sporządzano skowidze, wyroki, decyzje, postanowienia, zarządzenia czy wezwania. Wynika to z wdrażania od wielu lat zarówno w administracji

publicznej, jak i sądownictwie nowych technologii, których celem jest w szczególności usprawnienie postępowań, zastąpienie tradycyjnej formy utrwalania czynności procesowych wykorzystaniem nowoczesnych rozwiązań technologicznych, podniesienie przejrzystości postępowań sądowych, odstąpienie od tradycyjnego protokolowania rozpraw, a w konsekwencji obniżenie kosztów postępowania sądowego.

Zarówno informatyzacja procedur administracyjnych, jak i sądowych przyczynia się nie tylko do usprawnienia postępowania, w tym obsługi spraw przez kadre urzędniczą, ale również zwiększa przejrzystość prowadzenia spraw i skraca czas trwania rozpraw. Informatyzacja postępowań administracyjnych i sądowych oprócz korzyści niesie także zagrożenia.

Jednym z najistotniejszych elementów elektronizacji postępowań jest konieczność dostosowania systemów informatycznych do istniejących zasad procesowych, w tym zasady bezpośredniości. Ponadto konieczne jest zbudowanie zabezpieczeń, które uchronią strony postępowań administracyjnych i sądowych przed ujawnieniem treści akt postępowania. Dla zapewnienia sprawności przebiegu postępowań niezbędne jest również zintegrowanie funkcjonujących już systemów teleinformatycznych.

Uzasadnione jest zatem podjęcie w ramach rozważań o informatyzacji państwa tematu procedur administracyjnych i sądowych, w których można w sposób najbardziej efektywny skorzystać z nowych technologii, przy jednoczesnym uwzględnieniu uwarunkowań wynikających ze szczególnej roli administracji publicznej oraz wymiaru sprawiedliwości dla funkcjonowania współczesnego państwa. Organizacja działania sądów powszechnych i administracyjnych będzie zatem pochodną ustaleń poczynionych w tych dwóch sferach.

W opracowaniu zostaną wykorzystane informacje na temat funkcjonujących już systemów teleinformatycznych, publicznych rejestrów, elektronicznych procedur administracyjnych i sądowych,

a także postulaty formułowane zarówno przez przedstawicieli nauki, jak i praktyki prawa.

Niniejsza monografia składa się z dwóch części. W pierwszej zatytułowanej *Jednostka i państwo wobec informatyzacji* omówiono zagadnienia związane z informatyzacją państwa na szczeblu krajowym i unijnym. Autorzy podjęli rozważania na temat: ochrony danych osobowych, w szczególności przetwarzania danych biometrycznych, informatyzacji administracji publicznej, w tym aspektów prawnych systemów rejestrów publicznych w turystyce, a także unijnych systemów informacyjnych dotyczących zarządzania granicami i bezpieczeństwa wewnętrznego.

W części drugiej zatytułowanej *Sądownictwo w dobie informatyzacji* dokonano syntetycznej prezentacji istniejących procedur sądowych poddanych elektronizacji, a także oceny zmian wprowadzonych przez ustawodawcę w związku z koniecznością dostosowania przepisów proceduralnych do wymogów współczesności. Autorzy podjęli rozważania na temat: informatyzacji procesu karnego, elektronicznego postępowania wieczystoksięgowego, elektronicznego postępowania upominawczego, a także wnoszenia oraz doręczania pism procesowych za pośrednictwem środków komunikacji elektronicznej w postępowaniu sądowoadministracyjnym, systemu informacyjnego sądów administracyjnych oraz rozpraw zdalnych.

Niewątpliwym walorem niniejszej monografii jest to, że Autorami poszczególnych tekstów są zarówno doświadczeni naukowcy i praktycy, jak również osoby, które ukończyły studia i dopiero rozpoczynają swoją karierę naukową. Publikacja ta powstała dzięki wysiłkowi przedstawicieli Uczelni Łazarskiego w Warszawie.

Redaktorom naukowym pozostaje zatem życzyć Czytelnikom owocnej i jednocześnie przyjemnej lektury.

Bartosz Kotowicz
Angelika Kurzawa
Łukasz Nosarzewski

CZĘŚĆ I

**JEDNOSTKA I PAŃSTWO
WOBEC INFORMATYZACJI**

SYSTEM REJSTRÓW PUBLICZNYCH W TURYSTYCE JAKO NARZĘDZIE SŁUŻĄCE ZARZĄDZANIU I INFORMATYZACJI BRANŻY TURYSTYCZNEJ – ASPEKTY ORGANIZACYJNO-PRAWNE

DOMINIK BOREK¹

MINISTERSTWO SPORTU I TURYSTYKI



0000-0002-4359-9426

Wstęp

Prace nad omawianym tu narzędziem zostały wszczęte w stanie prawnym, gdy dział administracji rządowej turystyka był częścią Ministerstwa Sportu i Turystyki. Taki stan rzeczy utrzymywał się w latach 2007–2019², aż do czasu wydania rozporządzenia Rady Ministrów z dnia 19 listopada 2019 r. w sprawie utworzenia Ministerstwa Rozwoju³, które powstało w wyniku przekształcenia ówczesnego Ministerstwa Przedsiębiorczości i Technologii. Zmiany w roku 2019 polegały na połączeniu wskazanego resortu z komórkami obsługującymi sprawy działu administracji rządowej: budownictwo, planowanie i zagospodarowanie przestrzenne oraz mieszkalnictwo, jak również z komórką organizacyjną dotychczasowego Ministerstwa Sportu i Turystyki zajmującą się prowadzeniem spraw działu administracji

¹ Niniejsze opracowanie prezentuje osobiste poglądy autora i nie może być interpretowane jako stanowisko jakiegokolwiek organu, podmiotu czy instytucji. Opracowanie odnosi się do stanu prawnego na dzień 25 czerwca 2022 r.

² D. Borek [w:] *Prawo turystyki. Podręcznik*, red. D. Borek, H. Zawistowska, Gdańsk 2021, s. 11–19.

³ Rozporządzenie Rady Ministrów z dnia 19 listopada 2019 r. w sprawie utworzenia Ministerstwa Rozwoju (Dz.U. z 2019 r. poz. 2291).

rządowej turystyka⁴. Taki stan prawny trwał krótko, bo tylko do dnia 26 października 2021 r. Aby zrozumieć zmiany, które wówczas nastąpiły, należy dokładnie przedstawić sekwencję zdarzeń w zakresie zmieniającego się stanu faktycznego i prawnego.

Zgodnie z postanowieniami ustawy z dnia 4 września 1997 r. o działach administracji rządowej⁵ wyróżniamy 37 działów administracji rządowej; każdy z nich zawiera wyszczególnienie spraw, które wchodzi w jego zakres. Działem kieruje określony minister na zasadach zawartych w przepisach ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów⁶. W pierwszej kolejności na podstawie rozporządzenia Rady Ministrów tworzy się jednak urząd, który będzie zapewniał obsługę danego ministra⁷. Dopiero następnie (również w formie rozporządzenia Rady Ministrów) ustala się szczegółowy zakres działania ministra poprzez określenie jego nazwy, a także działów (działu), jakimi kieruje, i części budżetu, którymi dysponuje⁸; na tym etapie jest już znana osoba, która będzie sprawować funkcję ministra⁹. W praktyce oba rozporządzenia są wydawane w jednym czasie, choć zdarzają się odstępstwa od tej reguły – tak było w przypadku obecnie działającego Ministerstwa Sportu i Turystyki. Dnia 25 października 2021 r.

⁴ Por. D. Borek, K. Świtaj, H. Zawistowska, *O zgodności z prawem UE regulacji art. 15k ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw* [w:] *Prawo – narzędzie sprawiedliwości czy władzy?*, red. I. Barwicka-Tylek, P. Dziewałtowski-Gintowt, K. Zyzik, Ł. Łyżwa, Kraków 2020, s. 51–81.

⁵ Dz.U. z 2021 r. poz. 1893 z późn. zm.

⁶ Dz.U. z 2021 r. poz. 178 z późn. zm.

⁷ Zob. [online:] <https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/utworzenie-ministerstwa-sportu-i-turystyki-19157851> [dostęp: 10.08.2022].

⁸ Zob. [online:] <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20210001946/O/D20211946.pdf> [dostęp: 10.08.2022].

⁹ Zob. [online:] <https://www.gov.pl/web/sport/kamil-bortniczuk-powolany-na-stanowisko-ministra-sportu-i-turystyki> [dostęp: 10.08.2022].

opublikowano rozporządzenie tworzące Ministerstwo Sportu¹⁰, ale nie powołano jeszcze Ministra Sportu. Dwa dni później wydano rozporządzenie tworzące Ministerstwo Sportu i Turystyki oraz w drodze aktu wykonawczego określono zakres działania ministra¹¹. Co ciekawe, oba akty prawne wchodziły w życie z dniem ogłoszenia (dnia 27 października 2021 r.), jednak z mocą od dnia 26 października 2021 r., czyli z tą samą datą, z którą w życie wchodziło rozporządzenie z dnia 25 października 2021 r. w sprawie utworzenia Ministerstwa Sportu; dnia 26 października był też już powołany Minister Sportu i Turystyki przez Prezydenta RP¹².

Utrata mocy rozporządzenia Rady Ministrów z dnia 25 października 2021 r. w sprawie utworzenia Ministerstwa Sportu nastąpiła na podstawie rozporządzenia Rady Ministrów z dnia 27 października 2021 r. w sprawie utworzenia Ministerstwa Sportu i Turystyki. Formalnie można zatem wskazać, że rozporządzenie z dnia 25 października 2021 r. w sprawie utworzenia Ministerstwa Sportu weszło w życie, jednak zostało uchylone z mocą wsteczną tego samego dnia, w którym miało wejść w życie. Jest to dosyć skomplikowana konstrukcja, dopuszczalna jednak przez Zasady Techniki Prawodawczej¹³. W praktyce trudno byłoby także odmówić ważności podjętych działań w związku z wejściem w życie dnia 26 października 2021 r. rozporządzenia Rady Ministrów z dnia 25 października 2021 r. w sprawie utworzenia Ministerstwa Sportu, polegających np. na wyrobieniu pieczętek urzędowych tego dnia, ponieważ rozporządzenie uchylające jego moc zostało opublikowane dopiero dnia 27 października 2021 r.,

¹⁰ Rozporządzenie Rady Ministrów z dnia 25 października 2021 r. w sprawie utworzenia Ministerstwa Sportu (Dz.U. z 2021 r. poz. 1932).

¹¹ Powołanie K. Bortniczuka przez Prezydenta RP na stanowisko Ministra Sportu i Turystyki miało miejsce dnia 26 października 2022 r.

¹² Zob. [online:] <https://turystyka.rp.pl/nowe-trendy/art19050251-powrot-ministerstwa-sportu-i-turystyki-na-czele-kamil-bortniczuk> [dostęp: 10.08.2022].

¹³ Rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej” (Dz.U. z 2016 r. poz. 283).

stąd niemożliwe byłoby np. powstrzymanie się w dniu 26 października 2021 r. od niektórych działań. Należy jednak pamiętać, że ta niezwykle skomplikowana sytuacja organizacyjno-prawna ogranicza się tylko do jednego dnia – 26 października 2021 r., kiedy formalnie nie było jeszcze Ministra Sportu i Turystyki jako organu.

Przewrotnie można zadać pytanie, czy działania podjęte w zakresie funkcjonowania działu administracji rządowej turystyka, który w dniu 26 października 2021 r. znajdował się w strukturach Ministerstwa Rozwoju i Technologii, są ważne jako podjęte w ramach tegoż urzędu? Z całą pewnością tak, bowiem ze względu na zasadę kontynuacji i ciągłości działania te zachowują moc i nie wymagają dodatkowej konwalidacji. Przytoczony przeze mnie niezwykle skomplikowany stan prawny i faktyczny wskazuje, że kwestia trwałości infrastruktury informatycznej – w obliczu zmian w administracji rządowej – jest zagadnieniem niezwykle istotnym. Projekt Systemów Rejestrów Publicznych w Turystyce rozpoczęto w roku 2019 w Ministerstwie Sportu i Turystyki, przez dwa lata był realizowany w Ministerstwie Rozwoju, by w roku 2022 w trakcie jego rozliczenia ponownie znaleźć się w urzędzie obsługującym Ministra Sportu i Turystyki. Najistotniejszą kwestią w tej sprawie jest jednak przydatność zaplanowanego programu dla branży turystycznej w całej Polsce.

Projekt „Otwarte dane plus”

Po wprowadzeniu i omówieniu niezwykle skomplikowanego stanu prawnego należy przedstawić genezę projektu Systemu Rejestrów Publicznych w Turystyce. Został on zrealizowany w ramach programu Projekt „Otwarte dane plus”, który jest kontynuacją podjętego już w roku 2017 projektu „Otwarte dane – dostęp, standard, edukacja” (OD-DSE), którego podstawowym założeniem było zwiększenie otwartości i dostępności do danych cyfrowych gromadzonych przez

administrację publiczną¹⁴. Projekt „Otwarte dane plus” jest finansowany z Funduszy Europejskich w ramach II osi Program Operacyjny Polska Cyfrowa E-administracja i otwarty rząd, poddziałanie 2.3.1 „Cyfrowe udostępnienie informacji sektora publicznego ze źródeł administracyjnych i zasobów nauki”¹⁵. Założeniem podstawowym projektu „Otwarte dane plus” jest udostępnienie przez strony uczestniczące w projekcie tzw. API (ang. *application programming interface*) interfejsu programowania aplikacji¹⁶. Najprościej rzecz ujmując, chodzi o otwarcie baz danych, ale również udostępnienie kodu źródłowego w celu korzystania z API przez podmioty trzecie. Na bazie tak zbudowanego narzędzia każdy zainteresowany przedsiębiorca może np. stworzyć własną aplikację wykorzystującą źródło programistyczne stworzone przez partnera projektu. Założenie to pozwala na wdrożenie narzędzi ułatwiających zarządzanie procesem otwierania danych, a także stworzenie tzw. Laboratorium Otwartych Danych, co w przyszłości ma stanowić swego rodzaju instrumentarium zapewniające wsparcie w zakresie analitycznym, prawnym, technicznym oraz bezpieczeństwa udostępniania danych, jak również badań, które bazują na otwieranych danych¹⁷.

Projekt Systemu Rejestrów Publicznych w Turystyce był jednym z kluczowych założeń dokumentu zatytułowanego Biała Księga Regulacji Systemu Promocji Turystycznej w Polsce, który stanowił materiał analityczny oddany do konsultacji w lipcu 2018 r.¹⁸ Ustalenia dotyczące wskazanego dokumentu objęły przede wszystkim system promocji

¹⁴ Zob. [online:] <https://www.gov.pl/web/cyfryzacja/otwarte-dane-plus> [dostęp: 10.08.2022].

¹⁵ *Ibidem*.

¹⁶ Zob. [online:] <https://www.techtarget.com/searchapparchitecture/definition/application-program-interface-API> [dostęp: 10.08.2022].

¹⁷ Zob. [online:] <https://dane.gov.pl/pl/knowledgebase/useful-materials/raporty-laboratorium-otwartych-danych> [dostęp: 10.08.2022].

¹⁸ A. Staszewska, *Biała Księga Systemu Promocji Turystycznej w Polsce jako przykład wytyczenia prawnych ram w działaniach promocyjnych* [w:] *Prawne i praktyczne*

turystycznej oraz ewentualne możliwości jego finansowania, ale również problematykę tzw. ekonomii współdzielenia, wynikającej z analizy sposobu finansowania promocji turystycznej¹⁹. Powyższe spowodowało objęcie tymi pracami także zagadnienia dotyczącego usług hotelarskich, w tym zwłaszcza kwestii krótkoterminowego wynajmu mieszkań turystom, a co za tym idzie – rejestracji tego rodzaju przedsięwzięć²⁰. Z dokładnej analizy materiału, jakim był raport z prekonsultacji projektu Białej Księgi Regulacji Systemu Promocji Turystycznej w Polsce²¹ wynika, że największym zainteresowaniem cieszyły się postulaty zmiany uregulowań dotyczących funkcjonowania rynku usług hotelarskich w Polsce. Ministerstwo Sportu i Turystyki planowało w tamtym okresie m.in. pomoc w realizacji zadań własnych jednostek samorządu terytorialnego związanych z ewidencjonowaniem obiektów zakwaterowania. Wsparcie miało polegać na zapewnieniu bezpłatnego narzędzia opartego na systemie teleinformatycznym „Rejestrów publicznych w turystyce” utworzonym w ramach realizacji projektu „Otwarte dane plus”²².

Stworzenie systemu, według pierwotnych założeń, miało stać się sposobem na wyeliminowanie negatywnych zjawisk tzw. szarej strefy poprzez zewidencjonowanie w centralnym miejscu wszystkich podmiotów działających na rynku usług turystycznych w Polsce²³. Powstanie jednej bazy dla wszystkich obiektów świadczących usługi hotelarskie, w tym obiektów hotelarskich i innych obiektów, w których są świadczone usługi hotelarskie, miało pozwolić na stałe śledzenie i kontrolowanie całego rynku usług zakwaterowania w celach turystycznych

aspekty turystyki i rekreacji, red. K. Płonka-Bielenin, D. Wolski, Katowice 2021, s. 149–165.

¹⁹ Biała Księga Regulacji Systemu Promocji Turystycznej w Polsce, Warszawa 2018.

²⁰ Zob. też w tym obszarze Założenia do projektu ustawy o rodzajach usług turystycznych oraz o zmianie niektórych innych ustaw (roboczy tytuł), Warszawa 2021.

²¹ Biała Księga Regulacji Systemu Promocji Turystycznej w Polsce, Warszawa 2018.

²² Zob. [online:] <https://www.gov.pl/web/sport/otwarte-dane-plus> [dostęp: 10.08.2022].

²³ D. Borek, E. Wyrwicz, *Turystyczna działalność gospodarstw rolnych w świetle regulacji sektorowych*, „Zagadnienia Doradztwa Rolniczego” 2019, nr 3, s. 12–23.

w Polsce – w tym usług oferowanych za pośrednictwem platform rezerwacyjnych (tzw. OTA – Online Travel Agencies)²⁴. Czy udało się osiągnąć zamierzony cel? Jakie jeszcze założenia zrealizowano w ramach Systemu Rejestrów Publicznych w Turystyce i z jakich regulacji one wynikają?

Podstawy organizacyjno-prawne

Decyzja o utworzeniu projektu Systemu Rejestrów Publicznych w Turystyce została podjęta dnia 9 lipca 2018 r. po podpisaniu porozumienia między Ministerstwem Sportu i Turystyki, Głównym Urzędem Statystycznym, Ministerstwem Finansów a Ministerstwem Cyfryzacji w ramach projektu „Otwarte dane plus”, realizowanego z Programu Operacyjnego Polska Cyfrowa²⁵. Na poziomie intencji zawarcia umowy między partnerami ustalono jako podstawowe cele:

- dostosowanie rejestrów do obecnie obowiązujących przepisów prawa, w tym głównie do wymogów Krajowych Ram Interoperacyjności²⁶;
- udostępnienie e-usług w celu ułatwienia składania wniosków i komunikacji z systemem;
- stworzenie nowoczesnego instrumentu służącego promocji i pozyskiwaniu sprawdzonych informacji na temat bazy noclegowej w Polsce²⁷.

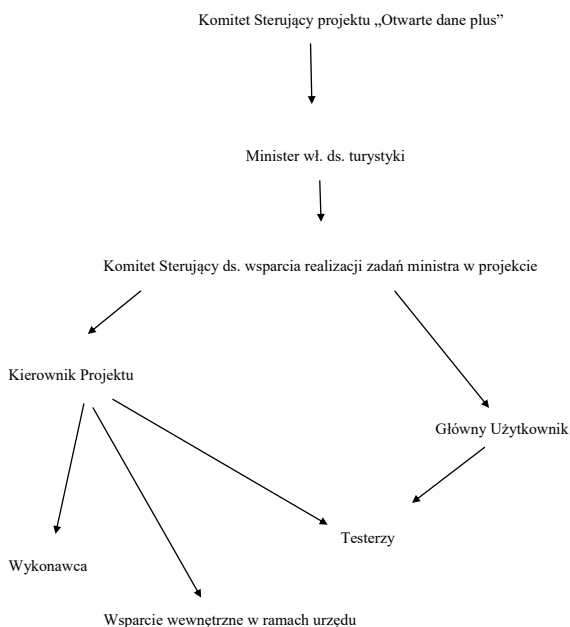
²⁴ *Ibidem*.

²⁵ Zob. [online:] <https://cyberdefence24.pl/polityka-i-prawo/nowy-projekt-ministerstwa-cyfryzacji-otwarte-dane-dostep-standard-edukacja> [dostęp: 10.08.2022].

²⁶ Por. cele w innych obszarach na przykładzie J. Petzel, *Komputerowe systemy wyszukiwania informacji prawnej a potrzeby ich użytkowników* [w:] *Prawo wobec nowych technologii*, red. P. Girdwoyń, Warszawa 2008, s. 189–203.

²⁷ Opis funkcjonalności systemu Rejestry publiczne w turystyce, Warszawa 2019 [online:] https://bip.msit.gov.pl/download/2/9704/Zalacznik_nr_2_do_SIWZ_-_Dokumentacja_projektowa.pdf&cd=2&hl=pl&ct=clnk&gl=pl&client=firefox-b-d [dostęp: 10.08.2022].

Następstwem podpisanego porozumienia było ogłoszenie przez Ministra Sportu i Turystyki zarządzenia nr 30 z dnia 17 grudnia 2018 r. w sprawie powołania Komitetu Sterującego do spraw realizacji przez Ministra Sportu i Turystyki zadań określonych w Porozumieniu o partnerstwie na rzecz wspólnego przygotowania i realizacji projektu „Otwarte dane plus”²⁸. Schemat organizacyjny w zarządzaniu projektem prawidłowo obrazuje poniższa grafika (rys.1).



Rysunek 1. Schemat organizacyjny w zarządzaniu projektem „Otwarte dane plus”

Źródło: opracowanie własne.

²⁸ Zarządzenie nr 30 z dnia 17 grudnia 2018 r. w sprawie powołania Komitetu Sterującego do spraw realizacji przez Ministra Sportu i Turystyki zadań określonych w Porozumieniu o partnerstwie na rzecz wspólnego przygotowania i realizacji projektu „Otwarte dane plus” (Dz.Urz. MSiT 2018 poz. 96).

Na czele omawianego projektu stoi Komitet Sterujący projektu „Otwarte dane plus” (KS POD+), którego przewodniczącym (tzw. Liderem Projektu) jest Minister Cyfryzacji. Poprzez cykliczne spotkania KS POD+ monitoruje stan realizacji składowych projektu. Jednym z elementów całego produktu jest System Rejestrów Publicznych w Turystyce. Do podstawowych zadań KS POD+ należą również monitoring terminowości i prawidłowości prowadzenia, przechowywania i archiwizowania dokumentacji projektowej, a także przygotowywanie sprawozdań rzeczowo-finansowych oraz sprawozdań z kontroli zarządczej w projekcie²⁹. Podczas spotkań KS POD+ każdy z partnerów zapewnia udział reprezentacji na odpowiednim poziomie w osobie ministra lub osoby upoważnionej. W Ministerstwie Sportu i Turystyki sprawy podnoszone na posiedzeniach KS POD+ były najpierw omawiane podczas spotkań Komitetu Sterującego ds. wsparcia realizacji zadań ministra w projekcie. Ten z kolei sprawował nadzór nad Kierownikiem Projektu, którego podstawową funkcją jest czuwanie nad prawidłowością i terminowością programu oraz osiągnięciem zakładanych celów. Kluczowym partnerem dla Kierownika Projektu jest Główny Użytkownik, który odpowiada za merytoryczne aspekty projektu, m.in. w zakresie zgodności z prawem, ale również funkcjonalności. Główny Użytkownik sprawuje nadzór osobowy wyłącznie nad testerami oprogramowania, od których zbiera sugestie co do poprawności i celowości testowanych narzędzi. Kierownik Projektu jest z kolei w bieżącym kontakcie z Wykonawcą, poprzez udzielanie wskazówek co do ewentualnych modyfikacji przygotowywanych instrumentów. Kierownik Projektu ma też dostarczyć produkt w uzgodnionych z KS MSiT ramach³⁰. Projekt Systemu Rejestrów Publicznych w Turystyce, jako osadzony w pewnych realiach urzędu

²⁹ Zob. [online:] <https://nabory.kprm.gov.pl/mazowieckie/warszawa/specjalista,64148> [dostęp: 10.08.2022].

³⁰ *Prince 2 – Skuteczne zarządzanie projektami*, Wielka Brytania 2018, s. 374.

obsługującego ministra właściwego ds. turystyki, wymaga także wsparcia wewnętrznego zapewnianego przez pracowników MSiT (np. obsługa prawna, księgowość); jednostki wspierające mają za zadanie angażować się w projekt w zależności od potrzeb i wskazanego czasu³¹.

Warto w tym miejscu omówić zadania i samą strukturę Komitetu Sterującego ds. wsparcia realizacji zadań ministra w projekcie (KS MSiT). Podmiot ten, bez osobowości prawnej, był organem pomocniczym Ministra Sportu i Turystyki. Do zadań Komitetu Sterującego należało wspieranie Ministra w wykonywaniu zadań określonych w Porozumieniu o partnerstwie na rzecz wspólnego przygotowania i realizacji projektu „Otwarte dane plus”, a w szczególności:

- 1) zarządzanie przebiegiem realizacji projektu oraz niezwłoczne informowanie Ministra w przypadku dostrzeżenia nieprawidłowości lub zagrożeń;
- 2) współpraca w realizacji zadań przedstawiciela Ministerstwa Sportu i Turystyki w KS POD+;
- 3) formułowanie wniosków i sugestii dotyczących realizacji projektu oraz przedstawianie ich Ministrowi;
- 4) wsparcie w rzetelnym przygotowywaniu dla Lidera Projektu dokumentów niezbędnych do prawidłowej sprawozdawczości i rozliczania projektu, w tym sprawozdania i rozliczenia finansowego;
- 5) opiniowanie projektów odpowiedzi i wyjaśnień kierowanych do Lidera Projektu w zakresie kontroli prowadzonych w związku z realizacją projektu.

Rozstrzygnięcia Komitetu Sterującego zapadały zwykłą większością głosów, a w razie równej liczby głosów „za” i „przeciw” przeważał głos przewodniczącego. Skład osobowy to przewodniczący i 6 dodatkowych osób, które reprezentowały urząd oraz

³¹ PM Agile Project Management Handbook v. 2 (wydanie polskie), Wielka Brytania 2019, s. 78.

organizacje branżowe. W ten sposób udział w zarządzaniu projektem miał również samorząd gospodarczy. Komitet faktycznie uległ samorozwiązaniu; zakończenie prac było spowodowane wydaniem rozporządzenia Rady Ministrów z dnia 19 listopada 2019 r. w sprawie utworzenia Ministerstwa Rozwoju³², które powstało w wyniku przekształcenia ówczesnego Ministerstwa Przedsiębiorczości i Technologii³³. Zespół nie mógł więc kontynuować pracy w formule określonej w Ministerstwie Sportu i Turystyki, ponieważ nowym organem, któremu przypisano właściwość w sprawach turystyki, stał się Minister Rozwoju. Niemniej zespół w ramach swojej krótkiej, ale intensywnej pracy wsparł Kierownika Projektu w kluczowych decyzjach na etapie pierwotnych ustaleń mających na celu wytyczenie ścieżki potwierdzającej zasadność biznesową projektu³⁴.

Podstawy prawne funkcjonalności Systemu Rejestrów Publicznych w Turystyce

Lektura Białej Księgi Systemu Promocji Turystycznej w Polsce³⁵ oraz raportu z prekonsultacji³⁶ tego dokumentu wskazuje, że System Rejestrów Turystycznych w Polsce był jednym z kluczowych elementów zakładanej reformy. Warto przytoczyć jedną z ważnych opinii przedłożoną przez Europejskie Centrum Konsumenckie

³² Rozporządzenie Rady Ministrów z dnia 19 listopada 2019 r. w sprawie utworzenia Ministerstwa Rozwoju (Dz.U. z 2019 r. poz. 2291).

³³ Por. D. Borek, K. Świtaj, H. Zawistowska, *O zgodności z prawem UE...*, *op. cit.*, s. 51–81.

³⁴ *Prince 2...*, *op. cit.*, s. 62–64.

³⁵ Biała Księga Systemu Promocji Turystycznej w Polsce, Warszawa 2018.

³⁶ Raport z prekonsultacji projektu Białej Księgi Regulacji Systemu Promocji Turystycznej w Polsce, Warszawa 2020 [online:] <https://www.gov.pl/web/rozwoj-technologie/raport-z-prekonsultacji-projektu-bialej-ksiegi-regulacji-systemu-promocji-turystycznej-w-polsce> [dostęp: 10.08.2022].

Polska (ECK Polska), wedle którego bardzo pozytywnie należy oceniać działania zmierzające do realizacji projektu „Otwarte dane plus” przez MSiT: „Możliwość zapoznania (się) i weryfikacji (w ramach) rejestru publicznego online danych podmiotów świadczących usługi będzie z pewnością dużym ułatwieniem dla turystów i zwiększy komfort wyboru i bezpieczeństwo. W opinii ECK Polska wraz z rosnącym stale zainteresowaniem turystów z zagranicy ofertą noclegową dostępną w Polsce celowym byłaby również publikacja w języku angielskim. Taka dwujęzyczność z pewnością będzie się korzystnie przyczyniała do promocji polskiej turystyki”³⁷. Twórcy narzędzia poszli o krok dalej i udostępnili aż trzy wersje obcojęzyczne: angielską, niemiecką i rosyjską. Przechodząc zatem do podstaw prawnych funkcjonalności narzędzia, poniżej dokonano omówienia poszczególnych zakładerek zawartych na portalu turystyka.gov.pl.

A. Centralny Wykaz Obiektów Hotelarskich (Rejestr CWOH)

Na podstawie przekazywanych w formie elektronicznej przez marszałków województw danych dotyczących skategoryzowanych w województwie obiektów hotelarskich zamieszcza się Centralny Wykaz Obiektów Hotelarskich³⁸. Wykaz ten jest jawny i zawiera następujące informacje:

- 1) określenie przedsiębiorcy świadczącego usługi hotelarskie wraz z adresem jego siedziby, a w przypadku gdy przedsiębiorcą jest osoba fizyczna – wraz z adresem miejsca zamieszkania;
- 2) nazwę i adres obiektu;
- 3) określenie rodzaju i kategorii obiektu;

³⁷ *Ibidem*.

³⁸ Zob. [online:] <https://dane.gov.pl/en/dataset/1083,centralny-wykaz-obiektow-hotelarskich> [dostęp: 10.08.2022].

- 4) informację o stałym lub sezonowym charakterze świadczonych usług wraz z podaniem czasu trwania sezonu;
- 5) opis obiektu zawierający informacje o liczbie miejsc noclegowych, liczbie jednostek mieszkalnych oraz ich strukturze, zakresie świadczonych usług, położeniu obiektu oraz numer telefonu, a także – o ile obiekt posiada – numer faksu, adres poczty elektronicznej oraz adres strony internetowej;
- 6) informacje o promesach, decyzjach dotyczących rodzaju i kategorii obiektu oraz o dopuszczonych odstępstwach od wymagań co do wyposażenia i zakresu świadczonych usług³⁹.

Ponadto w zakładce dotyczącej obiektów hotelarskich można znaleźć tzw. tagi, wśród których jest m.in. informacja o przyjmowaniu płatności Polskim Bonem Turystycznym. Prawo do przyjmowania płatności dokonywanych za pomocą bonu przysługuje przedsiębiorcy turystycznemu oraz organizacji pożytku publicznego znajdującym się na liście przedsiębiorców turystycznych oraz organizacji pożytku publicznego mających prawo do przyjmowania takich płatności. Listę, o której mowa powyżej, udostępnia na swojej stronie internetowej Polska Organizacja Turystyczna⁴⁰, nie ma jednak przeszkód, aby informacja ta, ze względu na jej wartość, była szeroko prezentowana. Dodatkowym kanałem dystrybucji listy uprawnionych do pobierania płatności bonem turystycznych obiektów hotelarskich jest portal turystyka.gov.pl. Na podobnych zasadach działa zakładka na portalu ewidencja.ufg.pl. Ubezpieczeniowy Fundusz Gwarancyjny, w ramach Turystycznego Funduszu Gwarancyjnego, tworzy i prowadzi system teleinformatyczny obsługujący Centralną Ewidencję Organizatorów Turystyki i Przedsiębiorców Ułatwiających Nabywanie Powiązanych Usług Turystycznych.

³⁹ Rozporządzenie Ministra Gospodarki i Pracy z dnia 19 sierpnia 2004 r. w sprawie obiektów hotelarskich i innych obiektów, w których są świadczone usługi hotelarskie (Dz.U. z 2017 r. poz. 2166).

⁴⁰ Por. inne zadania POT – zob. D. Borek, *Ustawa z dnia 25 czerwca 1999 r. o Polskiej Organizacji Turystycznej. Komentarz*, Radom 2019, s. 9–11.

W ramach wskazanego narzędzia również udostępniono informacje o organizatorach turystyki, którzy są uprawnieni do przyjmowania płatności Polskim Bonem Turystycznym.

Wracając do Centralnego Wykazu Obiektów Hotelarskich, należy zwrócić uwagę, że jest on wzbogacony o moduł mapowy. Rejestr został skonstruowany z myślą o wykorzystaniu funkcjonalności w postaci prawa do uzupełniania go i aktualizowania o dodatkowe atrakcyjne informacje, istotne z punktu widzenia turysty. Wśród danych tych znajduje się m.in. informacja o istniejących w okolicy pomnikach przyrody, instytucjach kultury, zabytkach, parkach narodowych, parkach krajobrazowych. *De lege ferenda* analogiczny obowiązek jak dla marszałków województw powinien być nałożony na wójtów/burmistrzów/prezydentów miast. Na podstawie przekazywanych w formie elektronicznej przez wójtów/burmistrzów/prezydentów miast danych dotyczących wpisanych do ewidencji innych obiektów świadczących usługi hotelarskie powinno zamieszczać się Centralny Wykaz Innych Obiektów Świadczących Usługi Hotelarskie. W ten sposób konsument miałby dostęp w jednym, centralnym miejscu do wszystkich obiektów, które oferują zakwaterowanie w celach turystycznych⁴¹.

B. Centralny Wykaz Organizatorów Szkoleń dla Kandydatów na Przewodników Górskich

Na podstawie informacji o dokonanych wpisach do rejestru organizatorów szkoleń przekazywanych w postaci elektronicznej przez marszałków województw⁴², na stronie internetowej ministra właściwego do spraw turystyki zamieszcza się Centralny

⁴¹ M. Rafał, D. Borek, *Digitalizacja edukacji jako szansa na postpandemicznym rynku pracy gospodarki czasu wolnego*, „Rynek Pracy” 2022, nr 2, s. 46–60.

⁴² Por. P. Waszkiewicz, *Rozwój systemów monitoringu wizyjnego w miastach i stosunek do nich mieszkańców europejskich miast* [w:] *Prawo wobec nowych technologii*, red. P. Girdwoyń, Warszawa 2008, s. 237–245.

Wykaz Organizatorów Szkoleń dla Kandydatów na Przewodników Górskich⁴³.

Wykaz ten jest jawny i zawiera następujące dane:

- 1) nazwa podmiotu, jego siedziba i adres;
- 2) wskazanie, czy działalność szkoleniowa jest prowadzona w ramach działalności gospodarczej;
- 3) określenie zakresu szkolenia, które ma być prowadzone, w tym wskazanie:
 - a) czy szkolenie ma mieć charakter podstawowy czy uzupełniający,
 - b) obszaru górskiego, którego ma dotyczyć szkolenie przewodników górskich;
- 4) wskazanie, czy działalność organizatora szkoleń ma dotyczyć: zorganizowania jednego szkolenia czy organizowania szkoleń na stałe (tzw. szkolenia stałe);
- 5) wskazanie kierownika szkolenia lub innej osoby upoważnionej do występowania wobec marszałka województwa w sprawach związanych ze szkoleniem;
- 6) informacje o dotychczasowych szkoleniach prowadzonych przez podmiot;
- 7) opis warunków szkolenia, w tym wskazanie miejsca odbywania wykładów i zajęć praktycznych, a także określenie miejsca przechowywania dokumentacji szkolenia i archiwum wydanych dokumentów⁴⁴.

Podobnie jak Centralny Wykaz Obiektów Hotelarskich, także i Centralny Wykaz Organizatorów Szkoleń dla Kandydatów na Przewodników Górskich jest wyposażony w moduł mapowy, gdzie można wyszukać poszczególne podmioty. Ponadto w obu

⁴³ Ustawa z dnia 29 sierpnia 1997 r. o usługach hotelarskich oraz usługach pilotów wycieczek i przewodników turystycznych (Dz.U. z 2020 r. poz. 2211).

⁴⁴ W zakresie odpowiedniego przechowywania dokumentacji – por. B. Makowicz, *Compliance w przedsiębiorstwie*, Warszawa 2011, s. 146–150.

przypadkach możemy wygenerować statystyki zawierające zarówno podstawowe zestawienia, jak np. liczba podmiotów z podziałem na formę prawną, po bardziej zaawansowane, jak np. liczba zgłoszonych szkoleń z podziałem na ich zakres, czy też lista obiektów hotelarskich posiadających basen⁴⁵.

C. Centralny Wykaz Przewodników Górskich

Na podstawie danych o nadanych uprawnieniach przewodnika górskiego przekazywanych w postaci elektronicznej przez marszałków województw na stronie internetowej ministra właściwego do spraw turystyki są udostępniane dane liczbowe dotyczące uprawnień nadanych przez poszczególnych marszałków województw⁴⁶. Dane te są jawne, jednocześnie informacje o nadanych uprawnieniach przewodnika górskiego wpisywane i przekazywane w postaci elektronicznej przez marszałków województw ministrowi właściwemu do spraw turystyki są udostępniane w postaci elektronicznej wszystkim marszałkom województw. W zakresie przewodnictwa górskiego jesteśmy zatem jako użytkownicy uprawnieni do zapoznania się ze statystykami, które są najbogatsze ze wszystkich dotychczas zaprezentowanych. W pracach roboczych Ministerstwa Sportu i Turystyki przewijała się propozycja stworzenia odpowiedniej podstawy prawnej do utworzenia rejestru przewodników górskich, wzorowanego na rejestrach zawodów zaufania publicznego⁴⁷. W ramach systemu miałyby funkcjonować moduły służące do udostępniania danych dotyczących organizatorów szkoleń dla

⁴⁵ Zob. [online:] turystyka.gov.pl [dostęp: 10.08.2022].

⁴⁶ Por. D. Borek, E. Wyrwicz, *Rola systemu IMI w uznawaniu kwalifikacji przewodników górskich* [w:] *Rynek pracy przewodników turystycznych, pilotów wycieczek i animatorów czasu wolnego*, red. Z. Kruczek, Kraków 2020, s. 112–127.

⁴⁷ Zob. [online:] <https://www.gov.pl/web/rozwoj-technologia/bezpieczne-wakacje-z-portalem-turystykagovpl--tutaj-znajdziesz-najwazniejsze-informacje-o-uslugach-turystycznych> [dostęp: 10.08.2022].

kandydatów na przewodników górskich oraz osób, którym zostały nadane uprawnienia przewodników górskich⁴⁸. Wydaje się, że jest to jeden z wniosków *de lege ferenda*, który ma duże szanse na realizację w najbliższych latach.

Informatyzacja branży turystycznej

Cyfryzacja, dążenie do z informatyzowania działalności turystycznej, jest zjawiskiem nieuniknionym. Społeczeństwo żyjące w świecie usług cyfrowych oczekuje ich szerokiego dostępu. Dziś nie stanowi bariery możliwość zakupu imprezy turystycznej o każdej porze dnia i nocy, podobnie jak wynajęcie pokoju hotelowego, włącznie z dokonaniem płatności. Z drugiej strony mamy grupę konsumentów, która oczekuje kontaktu z drugim człowiekiem, co jest podstawą turystyki jako zjawiska społecznego. Stąd duża popularność agentów turystycznych, którzy prezentując oferty od wielu organizatorów turystyki⁴⁹, są w stanie pomóc klientowi w wyborze tej najkorzystniejszej i najatrakcyjniejszej dla niego. W gąszczu informacji, które często są trudno weryfikowalne, agent turystyczny zaczyna pełnić rolę podmiotu, który poprowadzi klienta przez cały proces rezerwacyjny i wskaże najważniejsze prawa i obowiązki wynikające z zawartej umowy. Informatyzacja branży turystycznej powinna ten proces bezpośredniego kontaktu tylko ułatwić, nie zaś go zastępować, np. przez wykorzystanie botów czy sztucznej inteligencji. Turystyka nie może być odhumanizowana, bowiem to właśnie kontakt z drugą osobą jest kluczowym elementem tego gospodarczego i społecznego zjawiska.

⁴⁸ D. Borek, E. Wyrwicz, *Rola systemu IMI...*, op. cit., s. 112–127.

⁴⁹ P. Kociszewski, *Kształtowanie oferty na rynku turystyki kulturowej przez organizatorów turystyki (na przykładzie turystów seniorów)*, „Turystyka Kulturowa” 2017, nr 1, s. 80–105.

Warto wskazać za M. Rafałem i D. Borkiem, że procesy informatyzacyjne „są fundamentalne wobec wyzwań, jakie stają przed *leisure market* lub *leisure economy* – i to na niespotykaną dotąd skalę. Rynek sektorów składających się na gospodarkę czasu wolnego w najbliższym czasie będzie potrzebował ogromnej liczby specjalistów z zakresu IT i dziedzin pokrewnych, aby móc w pełni wykorzystywać swój potencjał, a także sprostać wyzwaniom, jakie przynosi ciągle obecne na świecie zagrożenie epidemiologiczne. W związku z tym najistotniejszą rekomendacją pozostaje możliwie jak najszerzy nacisk na edukację cyfrową w kształceniu specjalistów dla branży sportowej, turystycznej i eventowej”⁵⁰.

Turystyka jako taka jest immanentnym elementem tzw. przemysłu czasu wolnego, przez co zmiany następujące w tym obszarze dotyczą jej w każdym wymiarze. Turystyka jest bowiem związana z podróżą do innej miejscowości poza stałym miejscem pobytu na okres nieprzekraczający 12 miesięcy, dla której celem nie jest podjęcie stałej pracy w odwiedzanej miejscowości, a jest nim skorzystanie z noclegu przynajmniej przez jedną noc⁵¹. Świadczy to dobitnie, że każda dodatkowa usługa związana z powyższym zjawiskiem będzie elementem turystyki, w tym przemysłu czasu wolnego.

Podsumowanie

Na potrzeby promocji Systemu Rejestrów Publicznych w Turystyce stworzono także aplikację mobilną prezentującą w niezwykle nowoczesny sposób dane pochodzące z ewidencji obiektów hotelarskich poprzez tzw. rzeczywistość rozszerzoną. Użytkownik po skierowaniu

⁵⁰ M. Rafał, D. Borek, *Digitalizacja edukacji...*, op. cit., s. 46–60.

⁵¹ Por. D. Borek, *Konsekwencje niewypłacalności Thomasa Cooka dla angielskiej Premiership* [w:] *Prawne i praktyczne aspekty turystyki i rekreacji*, red. K. Płonka-Bielenin, D. Wolski, Katowice 2021, s. 11–31.

swojego telefonu na dany obiekt może uzyskać podstawowe dane o tym obiekcie i ustawić nawigację GPS⁵². Ta pilotażowa aplikacja ma na celu zachęcać do tworzenia przez wszystkich zainteresowanych swoich własnych produktów, ponieważ System Rejestrów Publicznych w Turystyce powstał w ramach projektu „Otwarte dane plus”, którego ideą jest otwartość danych, możliwość korzystania z nich poprzez używanie bezpłatnego API i prawo opracowywania własnych produktów.

W niniejszym opracowaniu zastosowanie znalazły: metoda empiryczna, wynikająca z pracy autora na rzecz organu administracji rządowej odpowiadającego za omawianą problematykę, oraz metoda historyczno-prawna i dogmatyczna. System Rejestrów Publicznych w Turystyce ma być jednym z takich programów, które przyczynią się do informatyzacji branży turystycznej, o czym świadczy popularność aplikacji tworzonych na bazie tego produktu⁵³. W ramach prowadzonych tu rozważań przedstawiono w pierwszej kolejności kwestie obszaru organizacyjno-prawnego, bez którego nie można mówić o wyzwaniach merytorycznych dotyczących informatyzacji⁵⁴ branży turystycznej. Odniesiono się także do Białej Księgi Systemu Promocji Turystycznej w Polsce, wstępnych założeń regulacji usług hotelarskich, pilotażu i przewodnictwa, a także regulacji wewnętrznych dotyczących samego rejestru.

Pozostaje mieć nadzieję, że omówione postulaty *de lege ferenda*, jeśli zostaną wprowadzone, spotęgują informatyzację branży turystycznej. Tak jak wykazano w niniejszym opracowaniu,

⁵² Opis funkcjonalności systemu Rejestry publiczne w turystyce, Warszawa 2019 [online:] https://bip.msit.gov.pl/download/2/9704/Zalacznik_nr_2_do_SIWZ_Dokumentacja_projektowa.pdf&cd=2&hl=pl&ct=clnk&gl=pl&client=firefox-b-d [dostęp: 10.08.2022].

⁵³ Zob. [online:] <https://dane.gov.pl/pl/knowledgebase/useful-materials/api-dla-rejestrow-centralnej-ewidencji-i-wykazow-w-turystyce?lang=pl> [dostęp: 10.08.2022].

⁵⁴ Por. M. Zubik, *Nowe technologie jako wyzwanie i zagrożenie dla prawa, statusu jednostek i państwa* [w:] *Prawo wobec nowych technologii*, red. P. Girdwoyń, Warszawa 2008, s. 37–51.

branża turystyczna w obliczu informatyzacji powinna zmierzać nie w kierunku odhumanizowania relacji międzyludzkich i zastępowania ich botami lub sztuczną inteligencją, a raczej w stronę wykorzystania nowych technologii do podtrzymywania relacji z klientem⁵⁵. Tylko w ten sposób wskresimy ogromny potencjał osób pasjonujących się turystyką i znających uwarunkowania konkretnych usług turystycznych.

Bibliografia

Akty normatywne

1. Ustawa z dnia 8 sierpnia 1996 r. o Radzie Ministrów (Dz.U. z 2021 r. poz. 178 z późn. zm.).
2. Ustawa z dnia 29 sierpnia 1997 r. o usługach hotelarskich oraz usługach pilotów wycieczek i przewodników turystycznych (Dz.U. z 2020 r. poz. 2211).
3. Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (Dz.U. z 2021 r. poz. 1893 z późn. zm.).
4. Rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej” (Dz.U. z 2016 r. poz. 283).
5. Rozporządzenie Ministra Gospodarki i Pracy z dnia 19 sierpnia 2004 r. w sprawie obiektów hotelarskich i innych obiektów, w których są świadczone usługi hotelarskie (Dz.U. z 2017 r. poz. 2166).
6. Rozporządzenie Rady Ministrów z dnia 19 listopada 2019 r. w sprawie utworzenia Ministerstwa Rozwoju (Dz.U. z 2019 r. poz. 2291).
7. Rozporządzenie Rady Ministrów z dnia 25 października 2021 r. w sprawie utworzenia Ministerstwa Sportu (Dz.U. z 2021 r. poz. 1932).

⁵⁵ Por. H. Izdebski, *Działalność gospodarcza z zastosowaniem nowych technologii a „granice prawa” – na przykładzie prawa telekomunikacyjnego* [w:] *Prawo wobec nowych technologii*, red. P. Girdwoyń, Warszawa 2008, s. 51–61.

8. Rozporządzenie Rady Ministrów z dnia 27 października 2021 r. w sprawie utworzenia Ministerstwa Sportu i Turystyki (Dz.U. z 2021 r. poz. 1953).
9. Zarządzenie nr 30 z dnia 17 grudnia 2018 r. w sprawie powołania Komitetu Sterującego do spraw realizacji przez Ministra Sportu i Turystyki zadań określonych w Porozumieniu o partnerstwie na rzecz wspólnego przygotowania i realizacji Projektu „Otwarte Dane Plus” (Dz.Urz. MSiT z 2018 r. poz. 96).

Literatura przedmiotu

1. Borek D., *Ustawa z dnia 25 czerwca 1999 r. o Polskiej Organizacji Turystycznej – Komentarz*, Radom 2019.
2. Borek D., Wyrwicz E., *Turystyczna działalność gospodarstw rolnych w świetle regulacji sektorowych*, „Zagadnienia Doradztwa Rolniczego” 2019, nr 3.
3. Borek D., Świtaj K., Zawistowska H., *O zgodności z prawem UE regulacji art. 15k ustawy o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych oraz niektórych innych ustaw [w:] Prawo – narzędzie sprawiedliwości czy władzy?*, red. I. Barwicka-Tylek, P. Dziewałtowski-Gintowt, K. Zyzik, Ł. Łyżwa, Kraków 2020.
4. Borek D., Wyrwicz E., *Rola systemu IMI w uznawaniu kwalifikacji przewodników górskich [w:] Rynek pracy przewodników turystycznych, pilotów wycieczek i animatorów czasu wolnego*, red. A. Krucek, Kraków 2020.
5. Borek D., *Konsekwencje niewypłacalności Thomasa Cooka dla angielskiej Premiership [w:] Prawne i praktyczne aspekty turystyki i rekreacji*, red. K. Płonka-Bielenin, D. Wolski, Katowice 2021.
6. Borek D., *Od redakcji: turystyczny rynek pracy po pandemii Covid-19 – analiza stanu obecnego oraz perspektywy na przyszłość*, „Rynek Pracy” 2022, nr 2.

7. Borek D., Zawistowska H., *Prawo turystyki. Podręcznik*, Gdańsk 2021.
8. Kociszewski P., *Kształtowanie oferty na rynku turystyki kulturowej przez organizatorów turystyki (na przykładzie turystów seniorów)*, „Turystyka Kulturowa” 2017, nr 1.
9. Makowicz B., *Compliance w przedsiębiorstwie*, Warszawa 2011.
10. Petzel J., *Komputerowe systemy wyszukiwania informacji prawnej a potrzeby ich użytkowników* [w:] *Prawo wobec nowych technologii*, red. P. Girdwoyń, Warszawa 2008.
11. *Prince 2 – Skuteczne zarządzanie projektami*, Wielka Brytania 2018.
12. *PM Agile Project Management Handbook v. 2* (wydanie polskie), Wielka Brytania 2019.
13. Rafał M., Borek D., *Digitalizacja edukacji jako szansa na postpandemicznym rynku pracy gospodarki czasu wolnego*, „Rynek Pracy” 2022, nr 2.
14. Staszewska A., *Biała Księga Systemu Promocji Turystycznej w Polsce jako przykład wytyczenia prawnych ram w działaniach promocyjnych* [w:] *Prawne i praktyczne aspekty turystyki i rekreacji*, red. K. Płonka-Bielenin, D. Wolski, Katowice 2021.
15. Waszkiewicz P., *Rozwój systemów monitoringu wizyjnego w miastach i stosunek do nich mieszkańców europejskich miast* [w:] *Prawo wobec nowych technologii*, red. P. Girdwoyń, Warszawa 2008.
16. Zubik M., *Nowe technologie jako wyzwanie i zagrożenie dla prawa, statusu jednostek i państwa* [w:] *Prawo wobec nowych technologii*, red. P. Girdwoyń, Warszawa 2008.

Źródła internetowe

1. https://bip.msit.gov.pl/download/2/9704/Zalacznik_nr_2_do_SIWZ [dostęp: 10.08.2022]
2. <https://cyberdefence24.pl/polityka-i-prawo/nowy-projekt-ministerstwa-cyfryzacji-otwarte-dane-dostep-standard-edukacja> [dostęp: 10.08.2022]
3. <https://dane.gov.pl/pl/knowledgebase/useful-materials/raporty-laboratorium-otwartych-danych> [dostęp: 10.08.2022]

4. <https://dane.gov.pl/en/dataset/1083,centralny-wykaz-objektow-hotelarskich> [dostęp: 10.08.2022]
5. <https://dane.gov.pl/pl/knowledgebase/useful-materials/api-dla-rejestrow-centralnej-ewidencji-i-wykazow-w-turystyce?lang=pl> [dostęp: 10.08.2022]
6. <https://www.gov.pl/web/rozwoj-technologia/bezpieczne-wakacje-z-portalem-turystykagovpl--tutaj-znajdziesz-najwazniejsze-informacje-o-uslugach-turystycznych> [dostęp: 10.08.2022]
7. <https://www.gov.pl/web/sport/kamil-bortniczuk-powolany-na-stanowisko-ministra-sportu-i-turystyki> [dostęp: 10.08.2022]
8. <https://www.gov.pl/web/rozwoj-technologia/raport-z-prekonsultacji-projektu-bialej-ksiegi-regulacji-systemu-promocji-turystycznej-w-polsce> [dostęp: 10.08.2022]
9. <https://www.gov.pl/web/cyfryzacja/otwarte-dane-plus> [dostęp: 10.08.2022]
10. <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20210001946/O/D20211946.pdf> [dostęp: 10.08.2022]
11. <https://nabory.kprm.gov.pl/mazowieckie/warszawa/specjalista,64148> [dostęp: 10.08.2022]
12. <https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/utworzenie-ministerstwa-sportu-i-turystyki-19157851> [dostęp: 10.08.2022]
13. <https://www.techtarget.com/searchapparchitecture/definition/application-program-interface-API> [dostęp: 10.08.2022]
14. <https://turystyka.rp.pl/nowe-trendy/art19050251-powrot-ministerstwa-sportu-i-turystyki-na-czele-kamil-bortniczuk> [dostęp: 10.08.2022]

Dokumenty rządowe

1. Biała Księga Regulacji Systemu Promocji Turystycznej w Polsce, Warszawa 2018.
2. Opis funkcjonalności systemu Rejestry publiczne w turystyce, Warszawa 2019.

3. Raport z prekonsultacji projektu Białej Księgi Regulacji Systemu Promocji Turystycznej, Warszawa 2020.
4. Założenia do projektu ustawy o rodzajach usług turystycznych oraz o zmianie niektórych innych ustaw (roboczy tytuł), Warszawa 2021.

Streszczenie

System rejestrów publicznych w turystyce jest instrumentem mającym służyć realizacji zadań ministra właściwego ds. turystyki w zakresie publicznego udostępniania danych, o których mowa w ustawie z dnia 29 sierpnia 1997 r. o usługach hotelarskich oraz usługach pilotów wycieczek i przewodników turystycznych. W ramach tego systemu można odnaleźć informacje dotyczące skategoryzowanej bazy noclegowej, organizatorów szkoleń dla przewodników górskich oraz wiadomości o nadanych uprawnieniach przewodnickich. Niniejsze opracowanie ma na celu zaprezentowanie narzędzia teleinformatycznego, jakim jest portal turystyka.gov.pl. Przedstawiono funkcjonalności systemu rejestrów publicznych w turystyce, a także atuty tego instrumentu dla branży turystycznej. Informatyzacja i cyfryzacja tej ostatniej jest dziś kluczowa dla rozwoju i wyjścia z postpandemicznego impasu⁵⁶. W pracy wykorzystano metodę dogmatyczno-egzegetyczną, a także empiryczną, związaną z doświadczeniami własnymi autora, w zakresie wdrażania systemu rejestrów publicznych w turystyce. W opracowaniu nie zabrakło odniesienia do dokumentu źródłowego, jakim jest *Opis funkcjonalności systemu Rejestry publiczne w turystyce*. Niejednokrotnie omówienie elementów składowych systemu następuje wprost słowami organu administracji rządowej – ministra właściwego ds. turystyki. W ten sposób, w nawiązaniu do właściwych dokumentów, najważniejsze kwestie przedstawiono w skróconej formie, przystępnej dla czytelników. W celu poszerzenia ewentualnej wiedzy w tym zakresie

⁵⁶ M. Rafał, D. Borek, *Digitalizacja edukacji...*, op. cit.; D. Borek, *Od redakcji: turystyczny rynek pracy po pandemii Covid-19 – analiza stanu obecnego oraz perspektywy na przyszłość*, „Rynek Pracy” 2022, nr 2, s. 46–60.

autor opracowania odsyła bezpośrednio do wskazanego uprzednio dokumentu, na podstawie którego dokonano kompilacji skróconej i klarownej informacji.

Słowa kluczowe

rejstry publiczne, turystyka, obiekty hotelarskie, przewodnicy górscy

**GŁOSA KRYTYCZNA DO WYROKU
WOJEWÓDZKIEGO SĄDU ADMINISTRACYJNEGO
W WARSZAWIE Z DNIA 7 SIERPNIA 2020 R.
(II SA/Wa 809/20)**

JUSTYNA DUDZIŃSKA

UCZELNIA ŁAZARSKIEGO



0000-0001-7258-9182

Wprowadzenie

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 (ogólnego rozporządzenia o ochronie danych)¹ stosowane jest w krajach Unii Europejskiej, począwszy od dnia 25 maja 2018 r. Relatywnie krótki okres stosowania tego aktu prawnego, niejednoznaczność jego przepisów, a także pozostawienie przez prawodawcę administratorom swobody w zakresie realizacji pewnych wymogów nakładanych przez RODO powoduje, że obecnie każdy wyrok sądu administracyjnego wydany w przedmiocie przetwarzania danych osobowych spotyka się z ogromnym zainteresowaniem przedstawicieli doktryny oraz ma istotny wpływ na kształtowanie praktyki.

W komentowanym orzeczeniu z dnia 7 sierpnia 2020 r. (II SA/Wa 809/20) Wojewódzki Sąd Administracyjny w Warszawie

¹ Dz.Urz. UE. 2016 L 119/2.

wypowiedział się na temat przetwarzania przez szkołę publiczną danych osobowych dzieci (ich danych biometrycznych), uznając, że dane te mogą być przez szkołę – jako administratora – przetwarzane na podstawie wyraźnej zgody, udzielonej przez rodziców lub opiekunów prawnych (tj. w oparciu o podstawę prawną określoną w art. 9 ust. 2 lit. a RODO²). Dodatkowo WSA przedstawił odmienną od przyjętej przez Prezesa Urzędu Ochrony Danych Osobowych (dalej: Prezesa UODO) interpretację zasady minimalizacji danych (art. 5 ust. 1 lit. c RODO³), stwierdzając, że nie powinna być ona rozumiana jako nakaz przetwarzania jedynie takich danych osobowych, bez których nie da się osiągnąć celu przetwarzania.

Ze względu na swoją doniosłość dla praktyki wyrok WSA zasługuje na szerszy komentarz, tym bardziej że trudno zgodzić się ze wszystkimi wnioskami z niego płynącymi.

Należy ocenić, że Sąd nietrafnie przyjął, iż wyraźna zgoda na przetwarzanie danych biometrycznych dzieci stanowi właściwą podstawę prawną przetwarzania danych osobowych w celu weryfikacji ich prawa do korzystania ze stołówki szkolnej. W tym kontekście za mankament rozważań Sądu należy uznać brak całościowej oceny warunków wyrażenia ważnej zgody na tego rodzaju przetwarzanie danych, w szczególności przesłanki „dobrowolności”.

² Art. 9 ust. 1: Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. Ust. 2: Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków: a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1.

³ Art. 5 ust. 1: Dane osobowe muszą być: c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”).

Opis sprawy

Komentowany wyrok WSA zapadł w następstwie skargi złożonej przez Szkołę Podstawową nr (...) z oddziałami (...) im. (...) w Gdańsku na decyzję Prezesa UODO z dnia 18 lutego 2020 r. (sygn. akt. ZSZS.440.768.2018), stwierdzającą naruszenie przez Szkołę Podstawową nr (...) z oddziałami (...) im. (...) w Gdańsku (dalej: Szkoła), dla której organem prowadzącym jest Miasto Gdańsk, przepisów art. 5 ust. 1 lit. c oraz art. 9 ust. 1 RODO „polegające na przetwarzaniu danych biometrycznych dzieci podczas korzystania przez nie z usług stołówki szkolnej”, a w konsekwencji:

1. nakazującą Szkole usunięcie danych osobowych w zakresie przetworzonych do postaci cyfrowej informacji o charakterystycznych punktach linii papilarnych palców dzieci korzystających z usług stołówki szkolnej;
2. nakazującą Szkole zaprzestanie zbierania danych osobowych w zakresie przetworzonych do postaci cyfrowej informacji o charakterystycznych punktach linii papilarnych palców dzieci korzystających z usług stołówki szkolnej;
3. nakładającą na Szkołę karę pieniężną w wysokości 20 000,00 zł (słownie: dwadzieścia tysięcy złotych).

W wyniku rozpoznania sprawy WSA uchylił zaskarżoną decyzję oraz zasądził zwrot kosztów postępowania sądowego na rzecz Skarżącej.

Stan faktyczny oraz prawny

Decyzja Prezesa UODO (dalej także: organ nadzorczy) oraz wyrok WSA zostały wydane w oparciu o poniżej opisany stan faktyczny.

Szkoła wdrożyła system pozwalający na weryfikację uprawnienia danego ucznia do korzystania przez niego ze świadczeń stołówki szkolnej przez identyfikację jego odcisku palca. Szkoła pozyskiwała

dane biometryczne⁴ dzieci na podstawie pisemnej zgody rodziców (opiekunów prawnych), wyrażanej w umowie o korzystanie z posiłków w stołówce szkolnej (w umowie zapewniono możliwość wyrażenia zgody na korzystanie z czytnika palca lub niewyrażenia takiej zgody). Uczniowie posiadający identyfikację biometryczną byli wpuszczani do stołówki jako pierwsi (pozostali uczniowie niekorzystający z tego rodzaju uwierzytelnienia oczekiwali na końcu kolejki).

Organ nadzorczy w uzasadnieniu skarżonej decyzji przypominał, że istnieje generalny zakaz prawny przetwarzania tzw. danych osobowych szczególnej kategorii⁵, do której zaliczane są dane biometryczne. Zakaz ten wyartykułowany w art. 9 ust. 1 RODO może zostać uchylony w przypadku wystąpienia którejś z przesłanek wymienionych w art. 9 ust. 2 RODO.

Prezes UODO przyjął, że zgoda rodziców (opiekunów prawnych) uczniów nie mogła być podstawą prawną przetwarzania danych osobowych. Zdaniem organu nadzorczego takiej zgodzie brak jest przymiotu „dobrowolności”, co spowodowane jest brakiem równowagi pomiędzy osobą, której dane dotyczą (dziećmi), a administratorem (Szkołą). Organ nadzorczy wyraził pogląd, że w celu realizacji zadania Szkoły, którym jest prowadzenie stołówki, właściwą podstawę prawną przetwarzania „jakichkolwiek” danych osobowych dzieci stanowić będzie niezbędność w celu wykonania zadania publicznego (art. 6 ust. 1 lit. e RODO). Podkreślił on dalej,

⁴ Dane biometryczne oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne (art. 4 pkt 14 RODO).

⁵ Tj. danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz danych genetycznych, biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.

że przepisy prawa powszechnie obowiązującego wskazują rodzaj danych, jakie skarżąca Szkoła może pozyskiwać od swoich uczniów i żaden z nich nie zezwala na pobieranie i przetwarzanie danych biometrycznych uczniów.

W konsekwencji powyższego Prezes UODO uznał, że Szkoła nie legitymuje się podstawą prawną przetwarzania danych określonych w art. 9 ust. 2 RODO, a zatem jako administrator naruszyła art. 9 ust. 1 RODO, a także zasadę minimalizacji danych (art. 5 ust. 1 lit. c RODO).

Od decyzji Prezesa UODO Szkoła wniosła skargę do WSA. W treści skargi Szkoła wyjaśniła, że zgoda rodziców (opiekunów prawnych) była dobrowolna, konkretna, świadoma i jednoznaczna, bowiem wprowadzenie czytnika linii papilarnych zostało dokonane z inicjatywy Rady Rodziców w związku z brakiem skuteczności poprzedniego sposobu weryfikacji płatności za posiłek, polegającego na korzystaniu z kart magnetycznych (dzieci gubiły karty lub zapominały je przynosić do szkoły). Tym samym Szkoła stwierdziła, że zastosowała się do zasady minimalizacji danych, bowiem czytnik odcisku palca wprowadziła dopiero na skutek powstałych problemów.

W odpowiedzi na skargę organ nadzorczy podtrzymał swoje stanowisko, w tym w szczególności co do braku posiadania przez Szkołę podstawy prawnej do przetwarzania danych osobowych w postaci zgody.

WSA uchylił decyzję Prezesa UODO, stwierdzając, że narusza ona zarówno wiążące Polskę przepisy prawa europejskiego, jak i regulacje prawa krajowego w stopniu mającym istotny wpływ na końcowy wynik sprawy, w szczególności zaś, że narusza ona art. 5 ust. 1 lit. c RODO oraz art. 9 ust. 1 i ust. 2 lit. a RODO przez ich niewłaściwą wykładnię i zastosowanie, a w konsekwencji wadliwe uznanie, że Szkoła, przetwarzając dane biometryczne swoich uczniów podczas korzystania przez nich z usług stołówki szkolnej, dopuściła się zarówno naruszenia zasady minimalizacji danych, o której mowa

w art. 5 ust. 1 lit. c RODO, jak również naruszenia polegającego na przetwarzaniu wspomnianych wyżej danych szczególnych kategorii, ze złamaniem zakazu przetwarzania takich danych.

Uwagi

Należy stwierdzić, że WSA zbyt powierzchownie ocenił prawidłowość zastosowania przez administratora podstawy prawnej przetwarzania danych w postaci wyraźnej zgody jako przesłanki legalizującej przetwarzanie danych biometrycznych, w związku z czym błędnie przyjął, iż Szkoła miała prawo przetwarzać te dane. Warto podkreślić, że bez ustalenia, czy zachodzą warunki dla ważnego wyrażenia zgody, nie można dokonać oceny legalności posługiwania się tą podstawą prawną.

Sąd wprawdzie zauważył, że warunkiem odebrania ważnej zgody na przetwarzanie danych osobowych wymaganej przez art. 9 ust. 2 lit. a RODO jest spełnienie generalnych warunków wyrażenia zgody wskazanych w art. 4 pkt 11 RODO (zgodnie z wymienionym przepisem zgoda na przetwarzanie danych osobowych powinna być dobrowolna, konkretna, świadoma i jednoznaczna⁶), jednakże nie zajął się dogłębną analizą spełnienia przez Szkołę wspomnianych warunków.

Na potrzeby niniejszej glosy irrelevantne będzie odniesienie się do przesłanek „konkretności, świadomości i jednoznaczności”, albowiem zapewnienie tych aspektów ważności zgody nie było kwestionowane przez organ nadzorczy.

Należy natomiast podkreślić, że najbardziej istotna w przedmiotowej sprawie ocena spełnienia warunku „dobrowolności” zgody nie została przez Sąd przeprowadzona. W kontekście tym

⁶ Por. P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, s. 205.

konieczne było dokonanie szczegółowej analizy statusu prawnego uczestników biorących udział w procesie przetwarzania danych biometrycznych oraz innych okoliczności świadczących o zapewnieniu podmiotowi danych pełnej swobody podczas podejmowania decyzji w przedmiocie wyrażenia zgody.

W swoich rozważaniach WSA poprzestał jedynie na ustaleniu, że zgoda wyrażana przez rodziców (opiekunów prawnych) na piśmie spełniała kryterium „wyraźności”, wymagane przez art. 9 ust. 2 lit. a RODO, co nie było kwestionowane przez Prezesa UODO.

W ramach niniejszej glosy poza komentarzem pozostawiona zostanie zaprezentowana przez Sąd w uzasadnieniu orzeczenia, a odmienna od przyjętej dotychczas przez organ nadzorczy, interpretacja zasady minimalizacji danych.

Ocena warunków ważności zgody stanowi bowiem priorytet.

Przesłanka „dobrowolności” jako warunek ważności zgody na przetwarzanie danych osobowych

WSA stwierdził, że każda z przesłanek uchylających zakaz przetwarzania danych osobowych wskazana w art. 9 ust. 2 RODO ma charakter autonomiczny i niezależny, przy czym „podstawową przesłanką, uchylającą zakaz przetwarzania danych wrażliwych, jest zgoda osoby, której dane dotyczą”. Sąd wywiódł zatem prosty wniosek, że skoro podstawy przetwarzania danych przewidziane prawem są co do zasady równoprawne, spełnienie jednej z nich – w tym przypadku wyrażnej zgody – uzasadnia legalność przetwarzania danych osobowych.

Jak stwierdziła Grupa Robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych (dalej: Grupa Robocza Art. 29; obecnie Europejska Rada Ochrony Danych)⁷ w opinii

⁷ Grupa Robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, która została powołana na mocy art. 29 Dyrektywy 95/46/WE

dotyczącej uzasadnionych interesów⁸: „Główne ustalenia poczynione w opinii dotyczą tego, że zgoda jest jedną z kilku podstaw prawnych przetwarzania danych osobowych, a nie główną podstawą”.

Sklaniałabym się wręcz do wniosku, że podstawa ta znajduje ewentualne zastosowanie jako „ostatnia” w takim przypadku, w którym brak jest ewentualnych innych podstaw prawnych przetwarzania danych osobowych. Zgody nie można bowiem stosować w jakimkolwiek przypadku, w którym inna podstawa prawna znajduje zastosowanie. „Zastąpienie” innej właściwej podstawy prawnej przetwarzania danych osobowych zgodą prowadziłoby do wprowadzenia podmiotu danych w błąd. Podmiot danych, udzielając zgody na przetwarzanie danych osobowych, nabywa bowiem przekonania (administrator ma obowiązek o tym poinformować), że może zgodę wycofać w każdym czasie. Tymczasem jeżeli uznać, że inna podstawa prawna przetwarzania jest właściwa, w przypadku wycofania zgody administrator nadal miałby prawo przetwarzać dane na tej innej podstawie prawnej. Zgadzam się zatem z przedstawicielami doktryny twierzącymi, że „zgoda jest jedną z częściej wykorzystywanych w Polsce podstaw przetwarzania danych. Jest to jednak podstawa nadużywana”⁹.

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 1995 L 281/31). Z dniem 25 maja 2018 r. uległa ona automatycznemu przekształceniu w Europejską Radę Ochrony Danych, która jest niezależnym organem europejskim działającym na rzecz spójnego stosowania zasad ochrony danych w całej Unii Europejskiej. Na potrzeby niniejszej glosy używana będzie nazwa „Grupa Robocza Art. 29” w związku z faktem odwoływania się do opinii bądź wytycznych wydanych pierwotnie przez ten organ.

⁸ Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE, przyjęta w dniu 9 kwietnia 2014 r., WP 217, s. 18.

⁹ Zob. M. Gawroński, M. Sztąberek [w:] *Ochrona Danych Osobowych. Przewodnik po ustawie i RODO z wzorami*, red. M. Gawroński, Warszawa 2018, s. 109.

Niezależnie od powyższego, w przypadku woli skorzystania z przesłanki zgody należy zapewnić warunki ważnego jej wyrażenia. Grupa Robocza Art. 29 w wytycznych dotyczących zgody na mocy rozporządzenia 2016/679¹⁰ podkreśliła, że w przypadku zastosowania zgody jako podstawy prawnej przetwarzania danych osobowych administrator powinien zapewnić spełnienie warunków dla ważnego jej wyrażenia, w tym warunku „dobrowolności”¹¹.

Zgoda może stanowić ważną podstawę prawną przetwarzania danych wyłącznie w sytuacji, gdy osoba, której dane dotyczą, ma możliwość dokonania rzeczywistego wyboru. Podnosi się, że możliwość dokonania takiego rzeczywistego wyboru nie zachodzi w przypadku ryzyka wprowadzenia w błąd, zastraszenia, przymusu lub znaczących negatywnych konsekwencji dla podmiotu, jeżeli nie wyrazi on zgody na przetwarzanie danych w określonym celu¹².

Na decyzję osoby, której dane dotyczą, mogą wpłynąć czynniki związane z kontekstem przetwarzania. Grupa Robocza Art. 29 wyjaśniła, że czynniki te mogą mieć wymiar finansowy, ale mogą

¹⁰ Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 przyjęte dnia 28 listopada 2017 r. (ostatnio zmienione i przyjęte dnia 10 kwietnia 2018 r.), WP 259 rev.01, s. 3.

¹¹ Grupa Robocza Art. 29 stwierdziła, że: „Zwracając się o zgodę, administrator ma obowiązek oceny, czy spełni wszystkie wymogi uzyskania ważnej zgody. Zgoda uzyskana w pełnej zgodności z RODO jest narzędziem zapewniającym osobom, których dane dotyczą, kontrolę nad tym, czy dotyczące ich dane osobowe będą przetwarzane. W braku zgodności zgody z RODO kontrola ze strony osoby, której dane dotyczą, staje się złudna, a zgoda będzie nieważną podstawą przetwarzania, co spowoduje niezgodność z prawem czynności przetwarzania”.

¹² Zob. Opinia nr 15/2011 w sprawie definicji zgody przyjęta dnia 13 lipca 2011 r., WP187, s. 37–38; podobnie A. Nerka [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, red. M. Sakowska-Baryła, Warszawa 2018, s. 117.

też (i tak będzie w przypadku Szkoły) mieć wymiar społeczny lub psychologiczny¹³.

Uważam, że sytuacja, gdy podczas przerwy na posiłek uczniowie korzystający z czytnika odcisku palca wchodzi na stołówkę jako pierwsi, a inni uczniowie oczekują w tym czasie na końcu kolejki, może powodować u dzieci pojawienie się negatywnych odczuć. Co za tym idzie, okoliczności takie sprzyjać będą wywieraniu na uczniów przymusu o charakterze społecznym i psychologicznym. Jest oczywiste, że dzieci, zwłaszcza te młodsze, odczuwać mogą w takich warunkach dyskomfort, ale mogą także czuć się niesprawiedliwie traktowane, nie rozumiejąc przyczyn, dla których zmuszone są przepuścić w kolejce innych kolegów czy koleżanki z klasy. To z kolei może powodować w nich poczucie, że są gorsze, lub wzbudzać pretensje do rodziców o to, że nie zgodzili się na podobny do tego, z którego korzystają koledzy, sposób weryfikacji uprawnienia do korzystania z usług stołówki¹⁴. Warto jeszcze raz podkreślić, że ten istotny aspekt różnicowania sytuacji uczniów, a wręcz „promowania” uczniów, których rodzice wyrazili zgodę na przetwarzanie danych biometrycznych, pozostał poza zainteresowaniem WSA, mimo iż Prezes UODO posunął się do daleko idącego stwierdzenia, że opisane konsekwencje należy traktować jak dyskryminację¹⁵.

Możliwość cofnięcia zgody bez uszczerbku dla podmiotów danych stanowi kolejny aspekt, na jaki należy zwrócić uwagę, oceniając przesłankę jej „dobrowolności”. Zachowanie przymiotu

¹³ Zob. D. Lubasz [w:] *RODO Ogólne Rozporządzenie o Ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 247.

¹⁴ Zob. Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679 wersja 1.1. przyjęta dnia 4 maja 2020 r., s. 10, gdzie Europejska Rada Ochrony Danych stwierdziła, że nie można mówić o dobrowolności zgody w przypadku, „gdy pojawi się jakikolwiek element przymusu, presji lub braku możliwości swobodnego okazania woli”.

¹⁵ Zob. [online:] <https://uodo.gov.pl/pl/138/1943> [dostęp: 15.01.2022].

dobrowolności zgody wymaga, aby w przypadku jej cofnięcia podmiot danych nie odczuł negatywnych konsekwencji tej decyzji, w szczególności aby odmowa wyrażenia zgody nie miała wpływu na inne uprawnienia podmiotu danych¹⁶.

Jak wynika z opisanego stanu faktycznego, w przypadku cofnięcia zgody na przetwarzanie danych osobowych przez rodzica (opiekuna prawnego) sytuacja dziecka zmieniałaby się o tyle, że nie miałoby już ono prawa skorzystać z „pierwszeństwa” wejścia na stołówkę. Tym samym, w praktyce, odczułoby ono negatywne skutki podjęcia przez rodzica (opiekuna prawnego) decyzji w przedmiocie cofnięcia zgody na przetwarzanie danych biometrycznych. Konsekwentnie, także z tej przyczyny, zgody na przetwarzanie danych biometrycznych nie można uznać za „dobrowolną”.

W analizowanej sprawie Szkoła wyjaśniła, że czytnik biometryczny został przez nią zainstalowany celem weryfikacji uprawnień uczniów, bowiem poprzedni system weryfikacji (karty) nie spełnił swojej roli (dzieci gubiły karty lub ich zapominały). Pomijając, że trudno uznać, iż gubienie kart dotyczyło wszystkich dzieci lub większości z nich, w takiej sytuacji można było podjąć kroki w celu poprawy tego zjawiska (przykładowo poprosić rodziców o przypilnowanie, aby dziecko zabrało kartę do szkoły). Wymaganą alternatywność rozwiązania dla uczniów, których rodzice (opiekunowie prawni) nie wyrazili zgody, Szkoła upatrywała w „ręcznej” weryfikacji uprawnień (sprawdzanie danych osobowych w postaci numeru umowy i nazwiska), która dokonywana była jednak dopiero po weryfikacji biometrycznej wszystkich uczniów, których wzorzec biometryczny Szkoła posiadała. Tego typu okoliczności zostały uznane przez Grupę Roboczą Art. 29 za niestwarzające warunków wyrażenia ważnej zgody¹⁷.

¹⁶ Zob. P. Litwiński [w:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych*. Komentarz, red. P. Litwiński, Warszawa 2018, s. 231.

¹⁷ Opinia 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych przyjęta dnia 27 kwietnia 2012 r., WP 193, s. 11. Grupa Robocza Art. 29

Status uczestników procesu przetwarzania danych osobowych a „dobrowolność” zgody

Brak dobrowolności zgody ma miejsce wówczas, gdy administrator wywiera taki wpływ na osobę, której dane dotyczą, że istnieje brak równowagi stron ze względu na stosunek zależności, np. podrzędności, gdy ze względu na szczególny charakter łączącej strony relacji, podmiot danych może się obawiać odmiennego traktowania, jeżeli nie wyrazi zgody na przetwarzanie danych.

W rozpoznawanej sprawie należało zatem ocenić, jaka zależność zachodzi między Szkołą i uczniami oraz udzielić odpowiedzi na pytanie, czy w związku z zachodzącą między nimi relacją możliwe jest zapewnienie dobrowolności wyrażenia zgody (w ramach przetwarzania danych w celu weryfikacji prawa do korzystania z usług stołówki szkolnej). Odpowiedź na to pytanie powinna być negatywna.

Administratorem w analizowanym przypadku jest szkoła publiczna, której organem prowadzącym jest Miasto Gdańsk, a zatem podmiot o określonym, szczególnym charakterze.

Szkoła publiczna zaliczana jest do podmiotów pełniących funkcje publiczne¹⁸. Szkoły publiczne powoływane są dla realizacji określonych

stwierdza, że w wielu przypadkach, w których dane biometryczne przetwarza się bez zapewnienia dopuszczalnego rozwiązania alternatywnego, takiego jak stosowanie hasła lub karty magnetycznej, nie można uznać, że zgoda została udzielona dobrowolnie. „Przykładowo systemu zniechęcającego osoby, których dane dotyczą, do jego stosowania (np. poprzez nadmierny czas marnowany przez użytkownika lub złożoność systemu) nie można uznać za dopuszczalne rozwiązanie alternatywne, a zatem jego zastosowanie nie prowadzi do udzielenia ważnej zgody”.

¹⁸ Zob. więcej R. Raszewska-Skałeczka, *Szkoła publiczna jako zdecentralizowany podmiot administracji publicznej. Studium administracyjnoprawne*, Wrocław 2019, s. 16.

„Na gruncie doktryny podkreślić należy, że szkoła publiczna jako zakład administracyjny i podmiot administracji publicznej jest jednym z najważniejszych instrumentów i sposobów wykonywania zadań publicznych tzw. administracji świadczącej (oświatowej). (...) Co ważne, szkoła publiczna z istoty rzeczy jest tą kategorią

zadań publicznych polegających na bezpośrednim świadczeniu usług socjalno-kulturalnych oraz o wyjątkowym społecznym znaczeniu, w obszarze oświaty. Szkoła dba także o potrzeby socjalne, np. przez świadczenie usług stołówki szkolnej. Cele i zadania oraz funkcje szkół publicznych precyzują przepisy prawa oświatowego. Zakładanie i prowadzenie szkół publicznych jest obowiązkowym zadaniem gmin¹⁹.

Pewnych wskazówek w zakresie przetwarzania danych przez podmioty publiczne mogą dostarczyć, w drodze analogii, wspomniane już wytyczne Grupy Roboczej Art. 29 dotyczące zgody na mocy Rozporządzenia 2016/679. Grupa Robocza Art. 29 stwierdziła, iż „jest mało prawdopodobne, że organy publiczne mogą bazować na zgodzie jako przesłance legalizującej przetwarzanie danych, ponieważ gdy administratorem jest organ publiczny, często istnieje wyraźny brak równowagi sił w relacji między administratorem a osobą, której dane dotyczą. Jest również oczywiste w większości przypadków, że osoba, której dane dotyczą, nie będzie miała rzeczywistych alternatywnych możliwości akceptacji (warunków) przetwarzania danych przez tego administratora. Grupa Robocza Art. 29 uważa, że istnieją inne legalne podstawy, które są, co do zasady, bardziej odpowiednie dla działalności organów publicznych”²⁰.

jednostek organizacyjnych, która powołana jest do służenia określonej grupie użytkowników, ponadto kwalifikuje się ją w kategorii dobra publicznego jako «wspólne dobro całego społeczeństwa», które wypełnia swe cele, funkcje i zadania oświatowe w interesie publicznym. Co znamienne, zadania publiczne statuowane w państwie w sferze edukacji publicznej wynikają z podmiotowych praw podstawowych obywateli, w przypadku szkół i placówek oświatowych – z prawa do nauki”.

¹⁹ Zob. wyrok NSA z dnia 5 grudnia 2006 r., I OSK 1377/06, LEX nr 320481; wyrok NSA z dnia 9 lutego 2006 r., I OSK 1372/05, LEX nr 194880; wyrok WSA w Warszawie z dnia 16 maja 2006 r., I SA/Wa 1818/05, LEX nr 227701; wyrok WSA w Olsztynie z dnia 20 września 2011 r., II SA/OI 453/11, LEX nr 1101379; wyrok WSA w Poznaniu z dnia 24 stycznia 2013 r., II SA/Po 745/12, LEX nr 1343187.

²⁰ Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 przyjęte dnia 28 listopada 2017 r. (ostatnio zmienione i przyjęte dnia 10 kwietnia 2018 r.), WP 259 rev. 01., s. 8.

Z powyższego wynika, że z samego faktu, iż administrator posiada status „podmiotu publicznego”, wynikają określone „preferencje” w zakresie korzystania przez taki podmiot z konkretnych podstaw prawnych przetwarzania danych osobowych²¹.

Szczególne konsekwencje dla oceny możliwości skorzystania z przesłanki zgody na przetwarzanie danych osobowych jako podstawy prawnej przetwarzania ma ustalenie, w jakiej sferze (dominium czy imperium) działa administrator.

W doktrynie istnieje zgoda co do tego, że podstawa prawna w postaci zgody nie może być podstawą prawną przetwarzania danych osobowych w przypadku, gdy podmiot realizuje władztwo państwowe. Ewentualna jej dopuszczalność dotyczyłaby sfery dominium²².

Z uzasadnienia wyroku Wojewódzkiego Sądu Administracyjnego w Łodzi z dnia 27 września 2017 r.²³ płynie wniosek, że działalność szkół publicznych w zakresie świadczenia usług stołówki szkolnej stanowi działalność w sferze imperium.

²¹ Należy zgodzić się z M. Jabłońskim oraz K. Wygodą, że: „W przypadku gdy administrator ze sfery publicznej nie działa według wzorów wynikających wprost z przepisów (np. nie używa w procesie pozyskiwania danych normatywnie określonego formularza), wkroczenie w sferę prywatności osoby fizycznej powinno pozostawać w odpowiedniej proporcji do celów, których ochrona uzasadnia dokonane ograniczenie”. Zob. M. Jabłoński, K. Wygoda, *Legalność pozyskiwania i przetwarzania danych osobowych w sferze publicznej. Aspekty praktyczne*, Warszawa 2021, s. 47.

²² Jasne stanowisko w tej kwestii, w zakresie przesłanki zgody na tle brzmienia art. 9 ust. 2 lit a. RODO, wyraziła M. Baryła oraz K. Wygoda, którzy stwierdzili, że „należy wyrazić daleko idące zastrzeżenia i uznać, że bez wyartykułowanego *expressis verbis* wymogu uzyskania owej zgody przez podmioty zaliczane do szeroko pojętej administracji publicznej, nie należy jej traktować jako dopuszczalnej przesłanki legalizującej proces przetwarzania tej kategorii danych w sferze imperium państwa”. Zob. M. Sakowska-Baryła, K. Wygoda [w:] M. Jabłoński, M. Sakowska-Baryła, K. Wygoda, *Czy jesteśmy gotowi na stosowanie RODO? Wybrane zagadnienia z zakresu funkcjonowania administracji publicznej*, Wrocław 2018, s. 76.

²³ Wyrok WSA w Łodzi z dnia 27 września 2017 r., I SA/Łd 581/17, LEX nr 2377734.

Mając powyższe na uwadze, zgodzić się należy z Prezesem UODO, że rodzaj danych osobowych uczniów, jakie może pozyskiwać Szkoła, wskazany jest przepisami prawa, a skoro żaden z tych przepisów nie dopuszcza możliwości przetwarzania danych biometrycznych dzieci w celu wykonania świadczenia usług stołówki szkolnej, należy uznać, iż głównymi podstawami przetwarzania danych osobowych uczniów będą niezbędność do wypełnienia obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c RODO) oraz niezbędność do wykonania zadania realizowanego w interesie publicznym (art. 6 ust. 1 lit. e RODO). W tym zakresie Szkoła nie powinna zatem przetwarzać danych biometrycznych uczniów (w tym celu powinny być przetwarzane zwykłe dane osobowe).

Dobrowolność wyrażenia zgody a status dziecka jako uczestnika procesu przetwarzania

Przy ocenie dobrowolności wyrażenia zgody oraz ocenie zachowania równorzędności stron istotny jest także status osoby, której dane dotyczą. W analizowanej sprawie przetwarzanie danych osobowych dotyczyło dzieci. Zgodnie z definicjami przyjętymi w aktach prawa międzynarodowego dziecko jest osobą poniżej 18. roku życia, chyba że do tego wieku osiągnie pełnoletność prawną²⁴. Ze względu na swoje właściwości oraz potrzeby psychiczne i emocjonalne wymaga ono szczególnej ochrony.

Na temat danych osobowych dzieci wypowiedziała się też Grupa Robocza Art. 29 w opinii 2/2009²⁵, która pozostaje aktualna w zakresie zasad i intencji dotyczących ochrony danych osobowych

²⁴ Art. 1 Konwencji o prawach dziecka ONZ z dnia 20 listopada 1989 r. (Dz.U. z 1991 r. Nr 120 poz. 526).

²⁵ Opinia 2/2009 w sprawie ochrony danych osobowych dzieci (ogólne wytyczne i szczególny przypadek szkół) przyjęta dnia 11 lutego 2009 r., WP 160, s. 4.

dzieci. Grupa Robocza Art. 29 stwierdza, że: „Główną zasadą prawną jest najlepsze zabezpieczenie interesów dziecka (...). Zasady tej muszą przestrzegać wszystkie podmioty, publiczne lub prywatne, które podejmują decyzje dotyczące dzieci. Ma ona zastosowanie również w odniesieniu do rodziców i innych przedstawicieli prawnych dzieci, jeżeli interesy każdej ze stron są sprzeczne lub gdy w imieniu dziecka występuje przedstawiciel. Zazwyczaj zasadę tę powinien stosować przedstawiciel dziecka, jednak jeżeli zaistnieje konflikt interesów między dziećmi a ich przedstawicielami prawnymi, decyzję powinien podjąć sąd lub w stosownych przypadkach organ ochrony danych”.

Grupa Robocza Art. 29 przypomniła także, że prawo do ochrony danych osobowych przysługuje dziecku, a nie jego przedstawicielom prawnym, bowiem oni jedynie te prawa wykonują. W przypadku gdy rodzice lub opiekunowie wyrażają zgodę na przetwarzanie danych osobowych dziecka, powinni oni podchodzić do tej kwestii ze szczególną troską i podejmować decyzje z uwzględnieniem zabezpieczenia jego interesów, w szczególności uwzględniać sytuacje, w których ujawnienie danych może stanowić zagrożenie dla prywatności lub istotnych interesów dziecka. Grupa Robocza Art. 29 do sytuacji, które mogą w „wyjątkowo inwazyjny” sposób naruszać prywatność dzieci, zaliczyła gromadzenie danych biometrycznych, telewizję przemysłową (monitoring) oraz identyfikację radiową, stwierdzając, że środki te mogą być niewspółmierne do celu.

Zgodnie z Motywem 30 RODO: „Dzieci wymagają szczególnej ochrony, albowiem mogą być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych”.

Tym samym, ważąc status Szkoły publicznej oraz ucznia – dziecka jako podmiotu wymagającego szczególnej troski i ochrony interesów, wydaje się oczywiste, że w ramach procesu weryfikacji uprawnień do korzystania z usług stołówki szkolnej podmioty te nie występują względem siebie w równorzędnej pozycji.

Co więcej, decyzja w przedmiocie wyrażenia zgody na przetwarzanie danych w postaci linii papilarnych, w kontekście środowiska „szkolnego”, może zostać podyktowana przymusem społecznym, a zatem w sposób wykluczający warunek „dobrowolności” zgody.

Warto dodać, że przetwarzanie danych biometrycznych dzieci jest kwestionowane nie tylko przez polski organ nadzoru. Szwedzki organ nadzorczy nałożył karę na szkołę za przetwarzanie danych biometrycznych uczniów, w postaci rysów ich twarzy, w celu automatycznego potwierdzenia ich obecności w klasie. Organ ten stwierdził, że zgoda nie może być podstawą prawną legalizującą przetwarzanie danych, w przypadku gdy nie spełnia ona podstawowych warunków zgody, takich jak dobrowolność.

Brak dobrowolności zgody spowodowany stosunkiem zwierzchnictwa szkoły w stosunku do uczniów potwierdził także Sąd Administracyjny w Marsylii, który zakwestionował tę przesłankę prawną przetwarzania danych przez dwie szkoły wykorzystujące technologie biometryczne w postaci rozpoznawania twarzy do kontrolowania wejścia uczniów do budynku i wyjścia z niego²⁶.

Podsumowanie

Powyżej przytoczone argumenty prowadzą do wniosku, że podstawą prawną przetwarzania przez Szkołę danych biometrycznych uczniów w postaci odcisków palców nie może być wyraźna zgoda ich rodziców (opiekunów prawnych).

Okoliczność, że artykuł 9 ust. 2 lit. a RODO przewiduje przesłankę uchylającą zakaz przetwarzania danych szczególnych kategorii w postaci „wyraźnej zgody” oraz że przesłanka ta jest autonomiczna (równoprawna z innymi podstawami przetwarzania danych

²⁶ Zob. [online:] <https://uodo.gov.pl/pl/138/1943> [dostęp: 10.01.2022].

osobowych), nie gwarantuje legalności przetwarzania danych osobowych na jej podstawie.

W każdym przypadku administrator zamierzający skorzystać z podstawy prawnej w postaci zgody (także wyraźnej przewidzianej w art. 9 ust. 2 lit. a RODO) zobowiązany jest w pierwszej kolejności ocenić spełnienie warunków dla jej ważności, przewidzianych w art. 4 pkt 11 RODO, w tym m.in. warunku „dobrowolności”.

W komentowanym wyroku WSA nie przeanalizował, czy wyrażenie przez rodziców / opiekunów prawnych uczniów zgody na przetwarzanie danych osobowych spełniało warunek „dobrowolności”.

Biorąc pod uwagę status prawny administratora oraz podmiotów danych, których dane były przetwarzane, a także pozostałe okoliczności składające się na kontekst przetwarzania danych osobowych, przesłanka „dobrowolności” nie została spełniona. Nie można bowiem uznać, że Szkoła jako podmiot publiczny oraz uczniowie – dzieci znajdują się względem siebie na „równorzędnej” pozycji w przypadku procesu polegającego na weryfikacji uprawnienia do korzystania z usług stołówki szkolnej.

O braku dobrowolności wyrażenia zgody świadczy też istnienie/powstanie negatywnych skutków dla uczniów w postaci konieczności oczekiwania na końcu kolejki (przepuszczenia wszystkich dzieci podlegających weryfikacji biometrycznej) w przypadku braku wyrażenia zgody na przetwarzanie danych biometrycznych w postaci linii papilarnych lub też cofnięcia zgody na takie przetwarzanie.

Tym samym zgodzić się trzeba z organem nadzorczym, że w związku z brakiem ważności pobieranej zgody na przetwarzanie danych osobowych Szkoła w istocie nie legitymowała się podstawą prawną przetwarzania danych szczególnej kategorii wskazaną w art. 9 ust. 2 lit. a RODO, a w konsekwencji przetwarzając te dane, naruszyła zakaz określony w art. 9 ust. 1 lit. a RODO. W związku z tym WSA niesłusznie przyjął, że skarżona decyzja organu nadzorczego naruszała prawo w tym zakresie.

Bibliografia

Akty prawne

1. Konwencja o prawach dziecka przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 20 listopada 1989 r. (Dz.U. z 1991 r. Nr 120 poz. 526).
2. 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 (ogólnego rozporządzenia o ochronie danych, Dz.Urz. UE 2016 L 119/2).

Literatura przedmiotu

1. Barta P., Kawecki M. (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018.
2. Bielak-Jomaa E., Lubasz D. (red.), *RODO Ogólne Rozporządzenie o Ochronie danych. Komentarz*, Warszawa 2018.
3. Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.
4. Gawroński M. (red.), *Ochrona Danych Osobowych. Przewodnik po ustawie i RODO z wzorami*, Warszawa 2018.
5. Jabłoński M., Wygoda K., *Legalność pozyskiwania i przetwarzania danych osobowych w sferze publicznej. Aspekty praktyczne*, Warszawa 2021.
6. Jabłoński M., Sakowska-Baryła M., Wygoda K., *Czy jesteśmy gotowi na stosowanie RODO? Wybrane zagadnienia z zakresu funkcjonowania administracji publicznej*, Wrocław 2018.
7. Raszevska-SkałECKa R., *Szkoła publiczna jako zdecentralizowany podmiot administracji publicznej. Studium administracyjnoprawne*, Wrocław 2019.

8. Sakowska-Baryła M. (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018.

Orzecznictwo

1. Wyrok NSA z dnia 9 lutego 2006 r., I OSK 1372/05, LEX nr 194880.
2. Wyrok WSA w Warszawie z dnia 16 maja 2006 r., I SA/Wa 1818/05, LEX nr 227701.
3. Wyrok NSA z dnia 5 grudnia 2006 r., I OSK 1377/06, LEX nr 320481.
4. Wyrok WSA w Olsztynie z dnia 20 września 2011 r., II SA/OI 453/11, LEX nr 1101379.
5. Wyrok WSA w Poznaniu z dnia 24 stycznia 2013 r., II SA/Po 745/12, LEX nr 1343187.
6. Wyrok WSA w Łodzi z dnia 27 września 2017 r., I SA/Łd 581/17, LEX nr 2377734.

Inne

1. Opinia 2/2009 w sprawie ochrony danych osobowych dzieci (ogólne wytyczne i szczególny przypadek szkół) przyjęta dnia 11 lutego 2009 r., WP 160.
2. Opinia 15/2011 w sprawie definicji zgody przyjęta dnia 13 lipca 2011 r., WP 187.
3. Opinia 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych przyjęta dnia 27 kwietnia 2012 r., WP 193.
4. Opinia 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE przyjęta dnia 9 kwietnia 2014 r., WP 217.
5. Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 przyjęte dnia 28 listopada 2017 r. (ostatnio zmienione i przyjęte dnia 10 kwietnia 2018 r.), WP 259 rev. 01.
6. Wytyczne 05/2020 dotyczące zgody na mocy rozporządzenia 2016/679 wersja 1.1 przyjęta dnia 4 maja 2020 r.

Streszczenie

Prezentowana glosa dotyczy Wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 7 sierpnia 2020 r. (III SA/Wa 809/20). WSA, analizując podstawy prawne przetwarzania danych biometrycznych dzieci w celu weryfikacji uprawnienia danego ucznia do korzystania przez niego ze świadczeń stołówki szkolnej, uznał wyraźną zgodę ich rodziców (opiekunów prawnych) za właściwą podstawę prawną przetwarzania danych. Niniejsza glosa przedstawia uwagi krytyczne względem tego stanowiska, zarzucając sądowi brak oceny wszystkich warunków ważności zgody, a w szczególności brak przeprowadzenia rzetelnej analizy „dobrowolności” zgody.

Słowa kluczowe

zgoda na przetwarzanie danych osobowych, dane biometryczne, dane osobowe dzieci, podstawy prawne przetwarzania danych biometrycznych, zasada minimalizacji danych osobowych, dane szczególnej kategorii

UNIJNE SYSTEMY INFORMACYJNE NA POTRZEBY ZARZĄDZANIA GRANICAMI I BEZPIECZEŃSTWA WEWNĘTRZNEGO

BEATA GOCKO

PAŃSTWOWA AKADEMIA NAUK STOSOWANYCH W PRZEMYSŁU



0000-0001-6202-6423

Wstęp

Strefa Schengen¹ jest to obszar, na którym zniesione są kontrole graniczne na granicach wewnętrznych między państwami członkowskimi oraz stosowane są ściśle określone jednolite zasady dotyczące: kontroli na granicach zewnętrznych, wzajemnej współpracy pomiędzy służbami państw sygnatariuszy, w szczególności w zakresie współpracy policyjnej i sądowej w sprawach karnych, wzoru wiz wydawanych cudzoziemcom, jak również działania Systemu Informacyjnego Schengen. Strefa Schengen w ostatnich latach była wielokrotnie wystawiana na próbę ze względu na występujące kryzysy (np. kryzys uchodźczy, zagrożenia terrorystyczne, pandemia COVID-19) i łączące się z tym wyzwania. W konsekwencji po roku 2015 Niemcy, Austria, Francja, Szwecja i Dania wprowadziły niemal stałe kontrole na granicach wewnętrznych, obchodząc układ z Schengen² dotyczący swobodnego przepływu osób i wbrew

¹ Strefa Schengen powstała na mocy układu z Schengen z dnia 14 czerwca 1985 r. (O. J.L. 2000.239.19) zawartego między Belgią, Francją, Holandią, Luksemburgiem i Niemcami.

² Państwa korzystały przy tym z art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu

orzeczeniu Trybunału Sprawiedliwości Unii Europejskiej³. Rząd Czech dnia 29 września 2022 r. zdecydował o czasowym przywróceniu kontroli na granicy ze Słowacją w związku ze wzrostem nielegalnej migracji.

W 2021 r. liczba przekroczeń granicy Polski wyniosła 193,3 mln osób⁴. W stosunku do poprzedniego roku odnotowano wzrost ruchu granicznego cudzoziemców o 3,2%, a Polaków o 8,0%. Z danych Straży Granicznej wynika, że w 2021 r. było 39 697 prób nielegalnego przekroczenia granicy z Białorusią do Polski⁵. Rozpoczęta dnia 24 lutego 2022 r. agresja wojsk Federacji Rosyjskiej na Ukrainę jest przyczyną potencjalnie największego przemieszczenia uchodźczego w Europie od II wojny światowej. Według raportu ONZ z dnia 20 września 2022 r. liczba uchodźców z Ukrainy odnotowanych w całej Europie to 7,4 mln⁶. Od początku agresji Rosji granicę polsko-ukraińską przekroczyło ponad 6,54 mln uchodźców z Ukrainy. Polska, posiadając zewnętrzną granicę strefy Schengen,

zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen) (Dz.Urz. UE 2016 L 77/1), który umożliwia przywrócenie kontroli granicznych na granicach wewnętrznych „w wyjątkowych okolicznościach, gdy ogólne funkcjonowanie obszaru bez wewnętrznej kontroli granicznej jest zagrożone w wyniku utrzymujących się poważnych niedociągnięć związanych z kontrolą na granicach zewnętrznych”.

³ Wyrok TSUE z dnia 26 kwietnia 2022 r. w sprawie dotyczącej możliwości tymczasowego przywrócenia przez państwo UE kontroli granicznej na granicach wewnętrznych, sprawy połączone C-368/20 i C-369/20 (Landespolizeidirektion Steiermark) (Dz.Urz. UE 2022 C 237/08).

⁴ Dane GUS, *Ruch graniczny oraz wydatki cudzoziemców w Polsce i Polaków za granicą w 2021 roku* [online:] <https://stat.gov.pl/obszary-tematyczne/ceny-handel/handel/ruch-graniczny-oraz-wydatki-cudzoziemcow-w-polsce-i-polakow-za-granica-w-4-kwartale-2021-roku,13,34.html> [dostęp: 20.09.2022].

⁵ E. Szczepańska, *Nielegalne przekroczenia granicy z Białorusią w 2021 roku* [online:] <https://www.strazgraniczna.pl/pl/aktualnosci/9689,Nielegalne-przekroczenia-granicy-z-Bialorusia-w-2021-r.html> [dostęp: 21.09.2022].

⁶ Zob. [online:] *Refugees from Ukraine recorded across Europe*, <https://data.unhcr.org/en/situations/ukraine> [dostęp: 25.09.2022].

ponosi podwójną odpowiedzialność, tj. wobec wszystkich osób korzystających z możliwości podróżowania bez konieczności poddawania się kontrolom na granicach wewnętrznych oraz wobec własnych obywateli i przedsiębiorstw. Wzmocnienie w sposób kompleksowy unijnych ram zarządzania granicami, migracji i współpracy w zakresie bezpieczeństwa oraz narzędzi informacyjnych jest w sytuacji konfliktu bardzo ważne. Brak granic wewnętrznych w strefie Schengen wymaga więc silnego i niezawodnego zarządzania przepływem osób przez granice zewnętrzne. Istniejące realne zagrożenie dla bezpieczeństwa wewnętrznego Europy wpływa na to, że obywatele Unii Europejskiej oczekują, iż kontrole osób na granicach zewnętrznych będą skuteczne, umożliwią prawidłową kontrolę migracją, a tym samym przyczynią się do bezpieczeństwa wewnętrznego. Straży granicznej, organom celnym, funkcjonariuszom policji oraz organom sądowym systemy informacyjne powinny zapewnić do ich dyspozycji niezbędne informacje. Istnieje szereg systemów informacyjnych i baz danych na poziomie Unii Europejskiej, które dostarczają tym formacjom odpowiednich informacji o osobach, zgodnie z wymaganymi celami.

Fundamentalnym, traktatowym zadaniem Unii Europejskiej jest wspomaganie funkcjonowania przestrzeni wolności, bezpieczeństwa i sprawiedliwości w poszanowaniu praw podstawowych oraz różnych systemów i tradycji prawnych państw członkowskich. Na podstawie ust. 3 art. 67 Traktatu o funkcjonowaniu Unii Europejskiej⁷ dążeniem Unii jest zapewnienie wysokiego poziomu bezpieczeństwa za pomocą środków zapobiegających przestępczości, rasizmowi i ksenofobii oraz zwalczających te zjawiska, a także za pomocą środków służących koordynacji i współpracy organów policyjnych, sądowych oraz innych właściwych organów, również przez wzajemne uznawanie orzeczeń sądowych w sprawach karnych i w miarę potrzeby przez zbliżanie przepisów karnych.

⁷ Traktat o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE 2012 C 326/47).

Zapewnianie bezpieczeństwa obywatelom Unii Europejskiej zmienia się wraz z postępem technologicznym, co znajduje odzwierciedlenie w reakcjach na nowe zagrożenia, jakie niosą ze sobą migracje ludności w skali globalnej. Digitalizacja danych oraz cały czas rozwijane systemy kontroli i monitorowania wpływają na tworzenie nowych rodzajów interakcji między polityką, prawem, administracją i technologią, a to prowadzi do innowacji w sektorze bezpieczeństwa.

Dla osiągnięcia wzrostu skuteczności i efektywności kontroli, które podejmowane są przez instytucje bezpieczeństwa, konieczne jest zastosowanie technologii cyfrowych. Do dyspozycji jest więc sprzęt monitorujący granice, np. kamery, radary (umieszczane np. na dronach, helikopterach, satelitach), sensory wykrywające ruch, czy też roboty mobilne. Z technologii rentgenowskiej, automatycznych rejestracji i identyfikacji radiowej, promieniowania cieplnego i podczerwieni korzysta się do skanowania bagaży, ludzi i pojazdów. Informacje biometryczne, takie jak np. cechy charakterystyczne tęczyówki i siatkówki, kolor tęczyówki, linie papilarne, układ naczyń krwionośnych palców, geometria dłoni, odcisk palców, czy też obraz twarzy, gromadzone i wprowadzane są do baz danych. Zaawansowane programy analityczne pozwalają skoordynować drogi przemieszczania się migrantów oraz wzajemne powiązania między nimi. Systemy informacyjne, które wspomagają pracę służb dla potrzeb kontroli granic, pozwalają lepiej zarządzać procesami migracyjnymi, przyczyniając się tym samym do zwiększenia bezpieczeństwa wewnętrznego.

Dobrze zaprojektowana i prawidłowo wykorzystywana technologia i systemy informatyczne mogą pomóc władzom publicznym w przestrzeganiu praw podstawowych. Każdy z istniejących systemów informacyjnych w Unii Europejskiej, który służy do zarządzania granicami i bezpieczeństwa wewnętrznego, ma swoje własne cele, podstawy prawne, grupy użytkowników i kontekst instytucjonalny. Wspólnie tworzą one złożony wzorzec odpowiednich baz danych.

Trzy główne scentralizowane systemy informatyczne opracowane przez Unię Europejską to: (1) System Informacyjny Schengen (SIS)⁸ z szerokim zakresem wpisów dotyczących osób i przedmiotów, (2) Wizowy System Informacyjny (VIS) zawierający dane dotyczące wiz krótkoterminowych oraz (3) EURODAC, system zawierający dane daktyloskopijne osób ubiegających się o azyl i obywateli państw trzecich, którzy nielegalnie przekroczyli granice zewnętrzne. Te trzy systemy uzupełniają się, a także wspierają władze krajowe w zwalczaniu przestępczości i terroryzmu. Czwartym scentralizowanym systemem zarządzania granicami jest system wjazdu/wyjazdu (EES) oraz Europejski System Informacji o Podróży oraz Zezwoleń na podróż (ETIAS).

Elektroniczne systemy, które wspomagają zarządzanie migracjami w UE

Wspólną, elektroniczną bazą danych o poszukiwanych przez służby państw członkowskich osobach i przedmiotach jest System Informacyjny Schengen (SIS). System ten zapewnia wymianę informacji pomiędzy służbą graniczną, służbami wydającymi wizy i innymi organami odpowiedzialnymi za bezpieczeństwo. Zaczął on obowiązywać od dnia 26 marca 1995 r. SIS zapewnia organom wyznaczonym przez kraje – strony porozumienia – dostęp do baz danych gromadzących wpisy dzięki zautomatyzowanej procedurze wyszukiwania⁹.

System Informacyjny Schengen drugiej generacji (SIS II) zaczął działać dnia 9 kwietnia 2013 r. Dostarcza on informacji o osobach

⁸ W 2013 r. wprowadzono drugą generację systemu SIS (SIS II) oferującą nowe opcje, takie jak możliwość dodania do wpisów odcisków palców i fotografii.

⁹ A. Dragan, *System Informacyjny Schengen drugiej generacji jako nowoczesne rozwiązanie informatyczne*, „Annales Universitatis Mariae Curie-Skłodowska” 2015, vol. 62, nr 1, s. 35.

nieuprawnionych do wjazdu lub pobytu na terytorium Schengen lub pobytu w niej oraz poszukiwanych w związku z działalnością przestępczą. SIS II ma być podłączony do Wizowego Systemu Informacyjnego (VIS). System Informacyjny Schengen to największa w Europie baza danych, która ułatwia wymianę informacji pomiędzy instytucjami państw w obszarze Schengen, kompensująca zniesienie kontroli na jej wewnętrznych granicach. Dostęp do systemu mają organy ścigania i wymiaru sprawiedliwości, w tym służby graniczne, celne i policyjne. Zawarte są tu też informacje o osobach poszukiwanych, zwłaszcza o dzieciach lub innych szczególnie zagrożonych osobach, które wymagają ochrony. Rejestrowane są w nim również dane na temat niektórych przedmiotów, np. samochodów, broni palnej, jednostek pływających i dokumentów tożsamości, które mogły zostać utracone lub skradzione bądź wykorzystane do popełnienia przestępstwa. Dnia 28 listopada 2018 r. przyjęto pakiet reform Systemu Informacyjnego Schengen, tak zwany SIS recast¹⁰. Reforma systemu rozszerza zakres jego funkcji, głównie przez dodanie nowych kategorii wpisów i regulowanie dostępu do bazy danych przez unijne agencje Frontex i Europol.

¹⁰ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1860 z dnia 28 listopada 2018 r. w sprawie użytkowania Systemu Informacyjnego Schengen do celów powrotu nielegalnie przebywających obywateli państw trzecich (Dz.Urz. UE 2018 L 312/1); Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1861 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmiany konwencji wykonawczej do układu z Schengen oraz zmiany i uchylecia rozporządzenia (WE) nr 1987/2006 (Dz.Urz. UE 2018 L 312/14); Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylecia decyzji Rady 2007/533/WSiSW oraz uchylecia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE (Dz.Urz. UE 2018 L 312/56).

Z kolei Wizowy System Informacyjny (VIS) służy wymianie danych wizowych między państwami członkowskimi oraz umożliwia upoważnionym do tego celu organom krajowym wprowadzanie i uaktualnianie danych wizowych, a także elektroniczną konsultację tych danych. System VIS¹¹ został operacyjnie uruchomiony dnia 11 października 2011 r. Kluczowym celem Wizowego Systemu Informacyjnego jest skuteczniejsza realizacja wspólnej polityki wizowej, zwiększenie bezpieczeństwa wewnętrznego i zwalczanie terroryzmu w jasno określonych i kontrolowanych warunkach. Założeniem VIS jest sprawdzanie, czy osoba ubiegająca się o wizę w konsulacie jest tą samą osobą, która przekracza granicę. W tym celu wykorzystuje się dane biometryczne, które zbierane są w konsulacie, a następnie porównywane na granicy. System ten stanowi istotne uzupełnienie Systemu Informacyjnego Schengen. Zapewnia skuteczną współpracę pomiędzy państwami członkowskimi m.in. w zakresie: zapobiegania handlu wizami, wspólnej polityki wizowej, identyfikacji osób, które mogą nie spełniać warunków wjazdu, pobytu lub zamieszkania na terytorium Unii Europejskiej. W maju 2018 r. Komisja Europejska zaproponowała reformę Wizowego Systemu Informacyjnego (VIS), służącego do wymiany danych na temat wiz krótkoterminowych. Zgodnie z propozycjami Komisji Europejskiej do systemu mają zostać włączone informacje o osobach wnioskujących o wizy długoterminowe. Zmianie ma też ulec katalog gromadzonych informacji poprzez dodanie do niego kopii dokumentów podróży osób ubiegających się o wizę¹².

System informatyczny do porównywania odcisków palców osób ubiegających się o azyl oraz osób należących do niektórych kategorii nielegalnych imigrantów to Europejski Zautomatyzowany

¹¹ Nowy system VIS ma zacząć działać jeszcze przed końcem 2023 r.

¹² J. Szymańska, *Scentralizowane systemy informacyjne w zarządzaniu procesami migracyjnymi w UE*, PISM 2018 [online:] https://pism.pl/publikacje/Scentralizowane_systemy_informacyjne_w_zarz_dzaniu_procesami_migracyjnymi_w_UE [dostęp: 04.10.2022].

System Rozpoznawania Odcisków Palców (Eurodac). Został on pierwotnie utworzony na podstawie rozporządzenia Rady (WE) z dnia 11 grudnia 2000 r. dotyczącego ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania Konwencji Dublińskiej¹³. System Eurodac pozwala państwom członkowskim UE zidentyfikować osoby występujące o azyl oraz osoby zatrzymane przy próbie nielegalnego przekroczenia zewnętrznej granicy Unii. Dzięki porównaniu danych daktyloskopijnych państwa członkowskie mogą stwierdzić, czy ubiegający się o azyl lub cudzoziemiec, którego pobyt w państwie

¹³ Rozporządzenie Rady (WE) nr 2725/2000 z dnia 11 grudnia 2000 r. dotyczące ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania Konwencji Dublińskiej (Dz.Urz. UE 2000 L 316/1), które zostało zmienione rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (rozporządzenie o Eurodac). Zob. więcej [online:] <https://uodo.gov.pl/pl/118/186> [dostęp: 02.10.2022]. Konwencja Dublińska została zastąpiona przez rozporządzenie Rady (WE) nr 343/2003 z dnia 18 lutego 2003 r. ustanawiające kryteria i mechanizmy określania Państwa Członkowskiego właściwego dla rozpatrywania wniosku o azyl, wniesionego w jednym z Państw Członkowskich przez obywatela państwa trzeciego (Dz.Urz. UE 2003 L 50/1), które zostało zmienione rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 604/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia kryteriów i mechanizmów ustalania Państwa Członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z Państw Członkowskich przez obywatela państwa trzeciego lub bezpaństwowca.

członkowskim okazał się nielegalny, nie ubiegał się poprzednio o azyl w innym państwie członkowskim albo też czy ubiegający się o azyl nie przedostał się na terytorium Unii nielegalnie. System rozpoczął działanie dnia 15 stycznia 2003 r. Obecnie planowana jest jego aktualizacja.

Wspólne ramy wymiany informacji i współpracy między państwami członkowskimi a Agencją Frontex, które służą poprawie znajomości sytuacji i zwiększeniu zdolności reagowania na zewnętrznych granicach do celów wykrywania i zwalczania nielegalnej imigracji i przestępczości transgranicznej oraz zapobiegania im, a w związku z tym do celów zapewnienia ochrony i ratowania życia migrantów, stanowi System EUROSUR¹⁴. Stosuje się go do ochrony granic zewnętrznych lądowych i morskich (a na zasadzie dobrowolności także do granic powietrznych), w tym monitorowania, wykrywania, identyfikowania, śledzenia, przechwytywania osób nielegalnie przekraczających granice oraz zapobiegania temu zjawisku. EUROSUR łączy krajowe systemy nadzoru granic w sieć europejską zarządzaną przez Agencję Frontex. W Polsce organem odpowiedzialnym za pełnienie funkcji Krajowego Ośrodka Koordynacji EUROSUR jest Komendant Główny Straży Granicznej. Organy państw członkowskich odpowiedzialne za nadzór granic, w tym straż graniczna, straż przybrzeżna, policja, służba celna i marynarka wojenna, mogą w ramach systemu i mechanizmu EUROSUR wymieniać informacje operacyjne i prowadzić współpracę za pośrednictwem Europejskiej Agencji Straży Granicznej i Przybrzeżnej Frontex. Wymiana informacji odbywa się przy użyciu „obrazów sytuacyjnych”, które można opisać jako graficzne interfejsy prezentowania informacji i danych wywiadowczych. Obrazy sytuacyjne,

¹⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1052/2013 z dnia 22 października 2013 r. ustanawiające europejski system nadzorowania granic (EUROSUR) (Dz.Urz. UE 2013 L 295/11).

dzięki zastosowaniu podobnej struktury na poziomie krajowym i europejskim, ułatwiają wymianę informacji¹⁵.

We wrześniu 2018 r. przyjęto rozporządzenie ustanawiające Europejski System Informacji o Podróżach oraz Zezwoleń na Podróż (ETIAS)¹⁶. Oczekuje się, że ETIAS zacznie działać w listopadzie 2023 r. Będzie on w dużej mierze zautomatyzowanym systemem informatycznym powstałym w celu identyfikacji zagrożeń dla bezpieczeństwa, nielegalnej migracji lub wysokich zagrożeń epidemicznych stwarzanych przez osoby podróżujące do państw Schengen zwolnionych z obowiązku wizowego, a jednocześnie ułatwi przekraczanie granic zdecydowanej większości podróżnych, którzy nie stanowią takiego ryzyka. Obywatele państw trzecich, którzy nie potrzebują wizy, aby podróżować do strefy Schengen, będą musieli złożyć wniosek o zezwolenie na podróż za pośrednictwem systemu ETIAS przed podróżą. Informacje zgromadzone dzięki ETIAS umożliwią, przy pełnym poszanowaniu praw podstawowych i zasad ochrony danych, na wcześniejszą weryfikację potencjalnego niebezpieczeństwa, nielegalnej migracji o wysokim ryzyku epidemicznym. Po wypełnieniu internetowego formularza wniosku system przeprowadzi kontrole w unijnych systemach informacyjnych dotyczących granic i bezpieczeństwa oraz w zdecydowanej większości przypadków wyda zezwolenie na podróż w ciągu kilku minut. W wyjątkowych przypadkach, gdy konieczna będzie dalsza kontrola podróżnego, wydanie zezwolenia na podróż może potrwać do 30 dni. Zezwolenie na podróż ETIAS będzie obowiązkowym warunkiem wstępnym wjazdu do państw Schengen.

¹⁵ Projekt: Rozwój systemu Eurosur [online:] <https://piap.lukasiewicz.gov.pl/badanie/projekt-rozwoj-systemu-eurosur/> [dostęp: 03.10.2022].

¹⁶ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1240 z dnia 12 września 2018 r. ustanawiające europejski system informacji o podróżach oraz zezwoleń na podróż (ETIAS) i zmieniające rozporządzenia (UE) nr 1077/2011, (UE) nr 515/2014, (UE) 2016/399, (UE) 2016/1624 i (UE) 2017/2226 (Dz.Urz. UE 2018 L 236/1).

Będzie ono sprawdzane wraz z dokumentami podróży przez straż graniczną podczas przekraczania granicy Unii Europejskiej. Ta uprzednia weryfikacja obywateli spoza Unii Europejskiej zwolnionych z obowiązku wizowego ułatwi odprawę graniczną, zapewni skoordynowaną i zharmonizowaną ocenę ryzyka obywateli państw trzecich, pozwoli na uniknięcie biurokracji i opóźnień dla podróżnych przy stawianiu się na granicach oraz znacznie zmniejszy liczbę odmów wjazdu na przejściach granicznych. ETIAS umożliwi przekazanie istotnych informacji niezbędnych do oceny potencjalnego ryzyka związanego z osobami podróżującymi do Unii Europejskiej i w razie konieczności będzie można odmówić wydania zezwolenia na podróż. Państwa uczestniczące w strefie Schengen będą mogły więc skuteczniej zarządzać swoimi granicami zewnętrznymi i poprawiać bezpieczeństwo wewnętrzne.

W 2012 r. w celu ułatwienia wymiany informacji o wyrokach skazujących pomiędzy państwami członkowskimi Unii Europejskiej powstał Europejski system przekazywania informacji z rejestrów karnych (ECRIS)¹⁷. Obecnie większość wymienianych informacji dotyczy obywateli państw członkowskich UE, ponieważ system nie dysponuje środkami umożliwiającymi skuteczne przetwarzanie danych dotyczących obywateli państw trzecich. W czerwcu 2017 r. Komisja Europejska zaprezentowała wniosek w sprawie rozporządzenia ustanawiającego nowy elektroniczny system ECRIS-TCN, który ma uzupełniać funkcjonujący od 2012 r. system ECRIS, służący wymianie danych o wyrokach skazujących wydanych wobec obywateli Unii Europejskiej. ECRIS-TCN umożliwi analogiczne działania wobec cudzoziemców spoza Unii. Zawierać będzie zarówno dane osobowe, jak i odciski palców wszystkich obywateli państw trzecich i bezpaństwowców skazanych w państwach Unii. W kwietniu

¹⁷ Decyzja ramowa Rady 2009/315/WSiSW z dnia 26 lutego 2009 r. w sprawie organizacji wymiany informacji pochodzących z rejestru karnego pomiędzy państwami członkowskimi oraz treści tych informacji (Dz.Urz. UE 2009 L 93/23).

2019 r.¹⁸ Unia Europejska przyjęła nowe przepisy mające na celu usprawnienie ECRIS. Zreformowany system będzie obejmował scentralizowaną bazę informacji o wyrokach skazujących obywateli państw trzecich i bezpieczeństwa. ECRIS zacznie działać od połowy listopada 2023 r.

Komisja Europejska w 2013 r. rozpoczęła prace w ramach projektu inteligentnych granic UE nad systemem wjazdu/wyjazdu (EES). Prace te wznowiono w kwietniu 2016 r., by w listopadzie 2017 r. przyjąć rozporządzenie¹⁹ w sprawie EES. Nowy system ma służyć rejestracji danych biometrycznych oraz informacji o czasie i miejscu wjazdu oraz wyjazdu cudzoziemców dopuszczonych do pobytu krótkoterminowego na terytorium Unii Europejskiej. Za pomocą automatycznego kalkulatora system EES ma obliczać okres dozwolonego pobytu podróżnych w państwach członkowskich. Jego zastosowanie powinno zmniejszyć opóźnienia w odprawie granicznej i podnieść jej jakość poprzez automatyczne obliczanie dozwolonego pobytu każdego podróżnego. System ten ma ułatwić systematyczną i rzetelną identyfikację osób przekraczających dozwolony czas pobytu, jak również wspomóc walkę

¹⁸ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/816 z dnia 17 kwietnia 2019 r. ustanawiające scentralizowany system służący do ustalania państw członkowskich posiadających informacje o wyrokach skazujących wydanych wobec obywateli państw trzecich i bezpieczeństwa (ECRIS-TCN) na potrzeby uzupełnienia europejskiego systemu przekazywania informacji z rejestrów karnych oraz zmieniające rozporządzenie (UE) 2018/1726 (Dz.Urz. UE 2019 L 135/1).

¹⁹ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2226 z dnia 30 listopada 2017 r. ustanawiające system wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich i danych dotyczących odmowy wjazdu w odniesieniu do takich obywateli oraz określające warunki dostępu do EES na potrzeby ochrony porządku publicznego i zmieniające konwencję wykonawczą do układu z Schengen i rozporządzenia (WE) nr 767/2008 i (UE) nr 1077/2011 (Dz.Urz. UE 2017 L 327/20).

z przestępczością i terroryzmem (dzięki udostępnieniu historii podróży organom ścigania). Budową nowego systemu zajmie się eu-LISA wraz z państwami członkowskimi. EES ma być gotowy do użytku do połowy maja 2023 r.

Instrumentami zarządzania granicami, które wspomagają wyżej wymienione systemy, jest baza danych skradzionych i zagubionych dokumentów podróży (SLTD) Interpolu oraz informacje o pasażerach przekazywane z wyprzedzeniem (API), które zbierają dane o pasażerach przed lotami wykonywanymi do Unii Europejskiej. Szczególnie do celów egzekwowania prawa, prowadzenia dochodzeń w sprawach karnych i współpracy sądowej Unia Europejska wprowadziła zdecentralizowane narzędzia wymiany informacji, a mianowicie: (1) Prüm, który służy do wymiany DNA, odcisków palców i danych rejestracyjnych pojazdów oraz (2) europejski system przekazywania informacji z rejestrów karnych (ECRIS) służący do wymiany informacji z krajowych rejestrów karnych. ECRIS umożliwia wymianę informacji, za pośrednictwem zabezpieczonej sieci o wcześniejszych wyrokach skazujących, które wydane zostały przeciwko konkretnej osobie przez sąd karny w Unii Europejskiej.

Z kolei Europol wspiera wymianę informacji między krajowymi organami policji jako centrum informacji kryminalnych Unii Europejskiej. System Informacyjny Europolu (EIS) stanowi scentralizowaną bazę danych informacji kryminalnych, w której państwa członkowskie mogą przechowywać i przeszukiwać dane dotyczące poważnej przestępczości i terroryzmu. Punkty kontaktowe w Europolu dostarczają pliki robocze do analiz tematycznych z informacjami o operacjach trwających w państwach członkowskich. Aplikacja sieci bezpiecznej wymiany informacji (SIENA) Europolu umożliwia państwom członkowskim szybką, bezpieczną i przyjazną dla użytkownika wymianę informacji między sobą, z Europolem lub ze stronami trzecimi, które zawarły umowę o współpracy z Europolem.

Dodatkowym zestawem systemów przetwarzania danych osobowych są dane dotyczące nazwisk pasażerów (PNR). Dane PNR

to dane osobowe podawane przez pasażerów, które gromadzone i przechowywane są przez przewoźników lotniczych. Obejmują m.in. imię i nazwisko, datę i trasę podróży, numer miejsca w samolocie, informacje o bagażu, dane kontaktowe oraz sposób płatności. System PNR uzupełnia dotychczasowe narzędzia zwalczania przestępczości transgranicznej. Przetwarzanie danych PNR pozwala organom ścigania identyfikować osoby, które wcześniej nie były podejrzewane o związki z przestępczością lub terroryzmem, zanim szczegółowa analiza danych wykaże, że osoby te posiadają takie związki. Dane PNR można wykorzystywać na kilka sposobów, tj.: do oceny pasażerów przed przylotem lub wylotem według określonych kryteriów ryzyka lub do identyfikacji konkretnych osób; do opracowywania takich kryteriów ryzyka; w konkretnych dochodzeniach lub postępowaniach sądowych. W celu ochrony praw podstawowych (prawa do ochrony danych osobowych, prawa do prywatności i prawa do niedyskryminacji), dyrektywa Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r.²⁰ do pewnego stopnia ogranicza przekazywanie, przetwarzanie i zatrzymywanie danych PNR, a mianowicie:

- nie wolno gromadzić ani wykorzystywać danych szczególnie chronionych;
- dane można przechowywać tylko przez 5 lat, a po 6 miesiącach należy je zanonimizować, tak by uniemożliwić identyfikację osoby, której dotyczą;
- państwa członkowskie muszą ustanowić jednostkę ds. informacji o pasażerach odpowiedzialną za dane i ich ochronę, a w skład takiej jednostki musi wchodzić inspektor ochrony danych;

²⁰ Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz.Urz. UE 2016 L 119/132).

- państwa członkowskie muszą dopilnować, by pasażerowie byli jasno informowani o gromadzeniu ich danych i o przysługujących im prawach;
- zautomatyzowane przetwarzanie danych PNR nie może być jedyną podstawą decyzji wywołujących niekorzystne skutki prawne lub mających poważne skutki dla danej osoby;
- dane pasażera można przekazywać państwom trzecim tylko w rzadkich i indywidualnych przypadkach.

Dyrektywa o PNR reguluje przekazywanie informacji o rezerwacji podanej w momencie dokonywania rezerwacji i odprawy organom ścigania w państwach członkowskich oraz przetwarzanie tych danych do celów zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie oraz ich ścigania.

Organy celne również odgrywają kluczową rolę we współpracy na granicach zewnętrznych. Mają różne systemy²¹ oraz bazy danych zawierające dane o przepływach towarów, identyfikację podmiotów gospodarczych i informacje dotyczące ryzyka, które można wykorzystać do wzmocnienia bezpieczeństwa wewnętrznego. Systemy te mają również własną kontrolowaną, ograniczoną i bezpieczną infrastrukturę (*Common Communication Network*). Do innych elektronicznych systemów, które wspomagają zarządzanie migracjami w UE, zaliczyć należy m.in.:

- PRADO – publiczny rejestr *online* autentycznych dokumentów tożsamości i dokumentów podróży (system niekompletny);

²¹ Systemy informacji celnej obejmują wszystkie systemy stworzone na mocy Wspólnotowego Kodeksu Celnego (rozporządzenie 2913/92) i unijnego kodeksu celnego (rozporządzenie 952/2013), decyzji w sprawie eliminowania papierowej formy dokumentów w sektorach cel i handlu (decyzja 70/2008/WE) oraz Systemu Informacji Celnej powstałego na mocy Konwencji CIS z 1995 r. Jego celem jest pomoc w zwalczaniu przestępczości celnej poprzez ułatwienie współpracy między europejskimi organami celnymi.

- baza danych Interpolu SLTD²² – zawiera informacje o dokumentach podróży i dokumentach tożsamości, które zostały zgłoszone jako skradzione, utracone, cofnięte, nieważne lub skradzione puste miejsce;
- SIENA – aplikacja sieciowa bezpiecznej wymiany informacji²³. Celem jej jest zapewnienie bezpiecznej wymiany informacji wrażliwych i zastrzeżonych²⁴;
- EIXM – europejski model wymiany informacji – baza DNA²⁵;
- ANPR – system automatycznego rozpoznawania tablic rejestracyjnych w czasie rzeczywistym bez udziału człowieka;
- EPRIS – transgraniczny dostęp do danych z akt policyjnych;
- CISE – dane związane z bezpieczeństwem na wodach morskich²⁶.

Wielkoskalowymi systemami informatycznymi na potrzeby polityki Unii Europejskiej w zakresie ochrony granic, migracji

²² *SLTD database (travel and identity documents)* [online:] <https://www.interpol.int/How-we-work/Databases/SLTD-database-travel-and-identity-documents> [dostęp: 03.10.2022].

²³ *Secure Information Exchange Network Application (SIENA)* [online:] <https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena> [dostęp: 03.10.2022].

²⁴ Wymiana informacji za pośrednictwem SIENA w 2021 r. (dane ze strony internetowej: <https://www.europol.europa.eu/>):

- wszczęto 123 tys. nowych spraw (wzrost o 38% w stosunku do 2020 r.);
- wymieniono 1,54 mln komunikatów operacyjnych (wzrost o 22% w porównaniu z 2020 r.);
- 2400 właściwych organów krajowych z 51 krajów i 14 organizacji/agencji międzynarodowych;
- ponad 19 000 użytkowników końcowych połączyło się.

²⁵ Za: H. Wyligła, *Cyfryzacja zarządzania migracjami w Unii Europejskiej*, „Rocznik Bezpieczeństwa Międzynarodowego” 2019, vol. 13, nr 2, s. 105.

²⁶ *Common information sharing environment (CISE)* [online:] https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/common-information-sharing-environment-cise_en [dostęp: 02.10.2022].

i egzekwowania prawa operacyjnie zarządza unijna agencja eu-LISA, to jest Agencja Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości²⁷. Nowa agencja zastąpiła dotychczasową agencję eu-LISA z 2011 r.²⁸ Agencja eu-LISA odpowiada za rozwój wielkoskalowych systemów informatycznych z wykorzystaniem odpowiedniej struktury zarządzania projektami. Zapewnia skuteczne, bezpieczne i nieprzerwane działanie wielkoskalowych systemów informatycznych, a także sprawne zarządzanie wielkoskalowymi systemami informatycznymi i ich rozliczanie. Agencja odpowiada za wysoki poziom ochrony danych zgodnie z przepisami Unii Europejskiej o ochronie danych, w tym warunkami szczególnymi odnoszącymi się do każdego z wielkoskalowych systemów informatycznych. Agencja jest odpowiedzialna za wykonywanie następujących zadań:

- za zarządzanie operacyjne systemem informacyjnym Schengen, wizowym systemem informacyjnym oraz europejskim systemem do porównywania danych o odciskach palców osób ubiegających się o azyl; systemy te w skuteczny sposób przyczyniają się do zapewnienia bezpieczeństwa strefy Schengen;
- przygotowywanie i rozwijanie lub zarządzanie operacyjne w odniesieniu do systemu wjazdu/wyjazdu, DubliNet, europejskiego systemu informacji o podróży oraz zezwoleń na podróż,

²⁷ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1726 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA), zmiany rozporządzenia (WE) nr 1987/2006 i decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia (UE) nr 1077/2011 (Dz.Urz. UE 2018 L 295/99).

²⁸ Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1077/2011 z dnia 25 października 2011 r. ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (Dz.Urz. UE 2011 L 286/1).

- europejskiego systemu przekazywania informacji z rejestrów karnych – informacje o wyrokach skazujących wydanych wobec obywateli państw trzecich (ECRIS-TCN) oraz oprogramowania wzorcowego ECRIS, a od dnia 21 czerwca 2022 r. – systemu e-CODEX, informatycznego systemu transgranicznej wymiany danych w obszarze współpracy sądowej w sprawach cywilnych i współpracy wymiarów sprawiedliwości w sprawach karnych, jak określono w rozporządzeniu zmieniającym (UE) 2022/850;
- przygotowywanie i rozwijanie innych wielkoskalowych systemów informatycznych w przestrzeni wolności, bezpieczeństwa i sprawiedliwości lub zarządzanie operacyjne takimi systemami, włącznie z istniejącymi systemami, jeśli przewidują to stosowne przepisy Unii Europejskiej regulujące owe systemy, które przyjęto na podstawie art. 67–89 Traktatu o funkcjonowaniu Unii Europejskiej;
 - za zapewnianie jakości danych zgodnie ze stosownymi przepisami Unii Europejskiej regulującymi systemy;
 - opracowywanie środków niezbędnych w celu zapewnienia interoperacyjności zgodnie ze stosownymi przepisami UE regulującymi systemy lub ich interoperacyjność;
 - prowadzenie badań;
 - prowadzenie projektów pilotażowych, weryfikacji poprawności projektów oraz ich testowanie;
 - udzielanie wsparcia państwom członkowskim Unii Europejskiej i Komisji Europejskiej²⁹.

Agencja eu-LISA aktualnie zarządza następującymi systemami IT: Wizowym Systemem Informacyjnym, Systemem Informacyjnym

²⁹ Agencja Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA) [online:] <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=LE-GISSUM:4374366> [dostęp: 05.10.2022].

Schengen oraz Eurodac. Ponadto rozwija następujące systemy IT: system wjazdu/wyjazdu, ETIAS oraz system ECRIS-TCN³⁰.

Podsumowanie

Każdego dnia granice wewnętrzne i zewnętrzne przekraczają miliony obywateli Unii Europejskiej i obywateli państw trzecich. Wobec braku granic wewnętrznych w strefie Schengen silnie chroniona i wytrzymała granica zewnętrzna jest niezbędna do zapewnienia wysokiego poziomu bezpieczeństwa wewnętrznego i swobodnego przepływu osób. Utworzenie strefy Schengen bez granic wewnętrznych przyniosło znaczne korzyści zarówno obywatelom, jak i przedsiębiorstwom Unii Europejskiej. Istniejące systemy informacyjne na potrzeby kontroli granicznej i bezpieczeństwa wewnętrznego w Unii Europejskiej obejmują szeroki zakres funkcji, nadal jednak istnieją niedociągnięcia w systemach, którymi należy się zająć w celu optymalizacji wydajności i ułatwienia pracy organom krajowym. Funkcjonariusze straży granicznej i organy ścigania, urzędnicy imigracyjni i organy wymiaru sprawiedliwości muszą w razie konieczności dysponować odpowiednim dostępem do wszystkich istniejących baz danych, aby uzyskać wsparcie w wykonywaniu swoich konkretnych zadań.

Unia Europejska nieustannie podejmuje kroki w celu zapewnienia lepszej ochrony granic Unii Europejskiej. Aby zapobiegać przestępczości i terroryzmowi oraz aby kontrolować migrację, należy skutecznie sprawdzać i nadzorować granice zewnętrzne. Zważywszy na rosnącą presję na granicach zewnętrznych UE spowodowaną sytuacją w zakresie bezpieczeństwa i migracji, Europejski Trybunał

³⁰ Rada UE, *Polityka* [online:] <https://www.consilium.europa.eu/pl/policies/it-systems-security-justice/> [dostęp: 05.10.2022].

Obrachunkowy³¹ przeprowadził w 2019 r. kontrolę, która miała na celu wskazanie tych aspektów w założeniach koncepcyjnych systemów i w ich użytkowaniu, które mogą pomóc funkcjonariuszom straży granicznej skuteczniej wykonywać ich obowiązki. Europejski Trybunał Obrachunkowy stwierdził, że funkcjonariusze straży granicznej w coraz większym stopniu korzystają z tych systemów i polegają na nich przy przeprowadzaniu odpraw granicznych. W systemach brakuje jednak pewnych danych, a inne dane są niekompletne bądź nie są wprowadzane w przewidzianych na to terminach, co negatywnie wpływa na efektywność niektórych odpraw granicznych.

Każde państwo należące do strefy Schengen jest odpowiedzialne za zabezpieczenie swoich własnych granic, ale by zapewnić ochronę całej strefy, należy skutecznie współpracować, a to wymaga koordynacji odpraw granicznych. Omawiane w niniejszym opracowaniu systemy informacyjne zapewniają funkcjonariuszom straży granicznej i funkcjonariuszom policji dostęp do istotnych informacji na temat osób przekraczających granice wewnętrzne i zewnętrzne UE. W razie konieczności i w miarę możliwości należy zapewnić wzajemne połączenie tych systemów i ich interoperacyjność. Należy ponadto ułatwić jednoczesne przeszukiwanie tych systemów. W 2019 r. Rada Unii Europejskiej przyjęła dwa rozporządzenia ustanawiające ramy interoperacyjności unijnych systemów informacyjnych w dziedzinie zarządzania granicami, bezpieczeństwa i migracji. Interoperacyjność oznacza zdolność różnych systemów informacyjnych do komunikowania się, wymiany danych i wykorzystywania wymienianych informacji, z poszanowaniem uprawnień dostępu do systemów³².

³¹ Sprawozdanie specjalne nr 20 Europejskiego Trybunału Obrachunkowego przedstawiono na mocy art. 287 ust. 4 akapit drugi TFUE z 2019 r. pt. *Unijne systemy informacyjne wspierające kontrole graniczne – narzędzie efektywne, lecz wymagające bardziej aktualnych i kompletnych danych* [online:] https://www.eca.europa.eu/Lists/ECADocuments/SR19_20/SR_Border_control_PL.pdf [dostęp: 05.10.2022].

³² A. Gajda, *Interoperacyjność unijnych systemów operacyjnych w zakresie bezpieczeństwa, ochrony granic i zarządzania migracjami*, Kwartalnik Kolegium

Architektura systemu zarządzania danymi powinna być modułowa, wykorzystująca najnowsze technologie i uwzględniająca ochronę prywatności już w fazie projektowania. Zgodnie z Kartą Praw Podstawowych³³ pełne poszanowanie wszystkich praw podstawowych obywateli UE i państw trzecich powinno być od początku zasadniczym elementem całego procesu. Wykorzystanie wielkoskalowych baz komputerowych stanowi więc wyzwanie dla zapewniania bezpieczeństwa w Unii Europejskiej. Zgodnie z nowymi przepisami mają powstać: 1) europejski portal wyszukiwania, który pozwoli właściwym organom dokonywać kwerend w kilku systemach informacyjnych jednocześnie; 2) wspólny serwis kojarzenia danych biometrycznych pozwalający je wyszukiwać i porównywać; 3) moduł wykrywający multiplikację tożsamości, który ostrzeże władze o możliwym oszustwie dotyczącym tożsamości; 4) wspólne repozytorium tożsamości zawierające dane identyfikacyjne obywateli państw trzecich³⁴. Ta nowa interoperacyjność powinna zacząć funkcjonować do końca czerwca 2024 r. Ma ona zapewniać pojedynczy interfejs wyszukiwania, a także usługę kojarzenia danych biometrycznych ułatwiającą identyfikację. Modernizacja i integracja systemów baz danych w celu bardziej efektywnego skutecznego wykrywania zagrożeń dla bezpieczeństwa z pewnością przyczyni się do ochrony obywateli Unii Europejskiej i zwiększy skuteczność kontroli granic zewnętrznych. Przyczyni się to do lepszego zarządzania procesami migracyjnymi w Unii Europejskiej, a tym samym do zwiększania bezpieczeństwa wewnętrznego.

Ekonomiczno-Społecznego „Studia i Prace” 2019, nr 1(37), s. 159.

³³ Karta Praw Podstawowych Unii Europejskiej z dnia 7 grudnia 2000 r. (Dz.Urz. UE 2012 C 326/391).

³⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/818 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności systemów informacyjnych UE w obszarze współpracy policyjnej i sądowej, azylu i migracji oraz zmieniające rozporządzenia (UE) 2018/1726, (UE) 2018/1862 i (UE) 2019/816.

Bibliografia

Akty prawne

1. Karta Praw Podstawowych Unii Europejskiej z dnia 7 grudnia 2000 r. (Dz.Urz. UE 2012 C 326/391).
2. Traktat o funkcjonowaniu Unii Europejskiej (Dz.Urz. UE 2012 C 326/47).
3. Rozporządzenie Rady (WE) nr 2725/2000 z dnia 11 grudnia 2000 r. dotyczące ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania Konwencji Dublińskiej (Dz.Urz. UE 2000 L 316/1).
4. Rozporządzenie Rady (WE) nr 343/2003 z dnia 18 lutego 2003 r. ustanawiające kryteria i mechanizmy określania Państwa Członkowskiego właściwego dla rozpatrywania wniosku o azyl, wniesionego w jednym z Państw Członkowskich przez obywatela państwa trzeciego (Dz.Urz. UE 2003 L 50/1).
5. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1077/2011 z dnia 25 października 2011 r. ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (Dz.Urz. UE 2011 L 286/1).
6. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen) (Dz.Urz. UE 2016 L 77/1).
7. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2226 z dnia 30 listopada 2017 r. ustanawiające system wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich i danych dotyczących odmowy wjazdu w odniesieniu do takich obywateli oraz określające warunki dostępu do EES na potrzeby ochrony porządku publicznego i zmieniające

- konwencję wykonawczą do układu z Schengen i rozporządzenia (WE) nr 767/2008 i (UE) nr 1077/2011 (Dz.Urz. UE 2017 L 327/20).
8. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1726 z dnia 14 listopada 2018 r. w sprawie Agencji Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA), zmiany rozporządzenia (WE) nr 1987/2006 i decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia (UE) nr 1077/2011 (Dz.Urz. UE 2018 L 295/99).
 9. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1860 z dnia 28 listopada 2018 r. w sprawie użytkowania Systemu Informacyjnego Schengen do celów powrotu nielegalnie przebywających obywateli państw trzecich (Dz.Urz. UE 2018 L 312/1).
 10. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1861 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie odpraw granicznych, zmiany konwencji wykonawczej do układu z Schengen oraz zmiany i uchylenia rozporządzenia (WE) nr 1987/2006 (Dz.Urz. UE 2018 L 312/14).
 11. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1862 z dnia 28 listopada 2018 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmiany i uchylenia decyzji Rady 2007/533/WSiSW oraz uchylenia rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1986/2006 i decyzji Komisji 2010/261/UE (Dz.Urz. UE 2018 L 312/56).
 12. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1052/2013 z dnia 22 października 2013 r. ustanawiające europejski system nadzorowania granic (EUROSUR) (Dz.Urz. UE 2013 L 295/11).
 13. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1240 z dnia 12 września 2018 r. ustanawiające europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) i zmieniające

- rozporządzenia (UE) nr 1077/2011, (UE) nr 515/2014, (UE) 2016/399, (UE) 2016/1624 i (UE) 2017/2226 (Dz.Urz. UE 2018 L 236/1).
14. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/816 z dnia 17 kwietnia 2019 r. ustanawiające scentralizowany system służący do ustalania państw członkowskich posiadających informacje o wyrokach skazujących wydanych wobec obywateli państw trzecich i bezpaństwowców (ECRIS-TCN) na potrzeby uzupełnienia europejskiego systemu przekazywania informacji z rejestrów karnych oraz zmieniające rozporządzenie (UE) 2018/1726 (Dz.Urz. UE 2019 L 135/1).
 15. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz.Urz. UE 2016 L 119/132).
 16. Decyzja ramowa Rady 2009/315/WSiSW z dnia 26 lutego 2009 r. w sprawie organizacji wymiany informacji pochodzących z rejestru karnego pomiędzy państwami członkowskimi oraz treści tych informacji (Dz.Urz. UE 2009 L 93/23).
 17. Układ z Schengen z 14 czerwca 1985 r. (O.J.L. 2000.239.19) zawartego między Belgią, Francją, Holandią, Luksemburgiem i Niemcami.

Literatura przedmiotu

1. Dragan A., *System Informacyjny Schengen drugiej generacji jako nowoczesne rozwiązanie informatyczne*, „Annales Universitatis Mariae Curie-Skłodowska”, Lublin – Polonia 2015, vol. 62, nr 1.
2. Gajda A., *Interoperacyjność unijnych systemów operacyjnych w zakresie bezpieczeństwa, ochrony granic i zarządzania migracjami*, Kwartalnik Kolegium Ekonomiczno-Społecznego „Studia i Prace” 2019, nr 1(37).
3. Wyligąła H., *Cyfryzacja zarządzania migracjami w Unii Europejskiej*, „Rocznik Bezpieczeństwa Międzynarodowego” 2019, vol. 13, nr 2.

Orzecznictwo

1. Wyrok TSUE z dnia 26 kwietnia 2022 r. w sprawie dotyczącej możliwości tymczasowego przywrócenia przez państwo UE kontroli granicznej na granicach wewnętrznych, sprawy połączone C-368/20 i C-369/20 (*Landespolizeidirektion Steiermark*) (Dz.Urz. UE 2022 C 237/08).

Źródła internetowe

1. GUS, *Ruch graniczny oraz wydatki cudzoziemców w Polsce i Polaków za granicą w 2021 roku* [online:] <https://stat.gov.pl/obszary-tematyczne/ceny-handel/handel/ruch-graniczny-oraz-wydatki-cudzoziemcow-w-polsce-i-polakow-za-granica-w-4-kwartale-2021-roku,13,34.html> [dostęp: 20.09.2022].
2. *Refugees from Ukraine recorded across Europe* [online:] <https://data.unhcr.org/en/situations/ukraine> [dostęp: 25.09.2022].
3. Agencja Unii Europejskiej ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA) [online:] <https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=LEGISSUM:4374366> [dostęp: 05.10.2022].
4. *Common information sharing environment (CISE)*, [online:] https://oceans-and-fisheries.ec.europa.eu/ocean/blue-economy/other-sectors/common-information-sharing-environment-cise_en [dostęp: 02.10.2022].
5. *Projekt: Rozwój systemu Eurosur* [online] <https://piap.lukasiewicz.gov.pl/badanie/projekt-rozwoj-systemu-eurosur/> [dostęp: 03.10.2022].
6. Szymańska J., *Odbudowa strefy Schengen po kryzysach – założenia nowej strategii i wyzwania* [online:] <https://www.pism.pl/publikacje/odbudowa-strefy-schengen-po-kryzysach-zalozenia-nowej-strategii-i-wyzwania> [dostęp: 20.09.2022].
7. Szymańska J., *Scentralizowane systemy informacyjne w zarządzaniu procesami migracyjnymi w UE, PISM 2018* [online:] https://pism.pl/publikacje/Scentralizowane_systemy_informacyjne_w_zarz_dzaniu_procesami_migracyjnymi_w_UE [dostęp: 04.10.2022].

8. Rada UE, *Polityka* [online:] <https://www.consilium.europa.eu/pl/policies/it-systems-security-justice/> [dostęp: 05.10.2022].
9. EUROPOL [online:] <https://www.europol.europa.eu/> [dostęp: 02.10.2022].
10. *Secure Information Exchange Network Application (SIENA)* [online:] <https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena> [dostęp: 03.10.2022].
11. *SLTD database (travel and identity documents)* [online:] <https://www.interpol.int/How-we-work/Databases/SLTD-database-travel-and-identity-documents> [dostęp: 03.10.2022].
12. Szczepańska E., *Nielegalne przekroczenia granicy z Białorusią w 2021 roku* [online:] <https://www.strazgraniczna.pl/pl/aktualnosci/9689,Nielegalne-przekroczenia-granicy-z-Bialorusia-w-2021-r.html> [dostęp: 21.09.2022].

Streszczenie

Jednym z najważniejszych osiągnięć Unii Europejskiej jest utworzenie strefy Schengen. Na obszarze tym zniesiona została kontrola graniczna na granicach wewnętrznych między państwami członkowskimi. Prawidłowe funkcjonowanie Schengen wymaga skutecznego zarządzania granicami zewnętrznymi Unii Europejskiej, wzmocnienia działań, które kompensują braki kontroli wewnątrz strefy. W ramach wzmacniania ochrony granic zewnętrznych niezbędne jest ciągłe doskonalenie służącego temu technologicznego systemu. Należy więc zapewnić współdziałanie systemów informacyjnych (Systemu wjazdu/wyjazdu, Systemu Informacyjnego Schengen, Wizowego Systemu Informacyjnego czy Europejskiego Systemu Informacji i Zezwoleń na Podróż ETIAS), a także cyfryzację procedur na granicach zewnętrznych (np. procedury wizowej)³⁵. W niniejszym

³⁵ J. Szymańska, *Odbudowa strefy Schengen po kryzysach – założenia nowej strategii i wyzwania*, <https://www.pism.pl/publikacje/odbudowa-strefy-schengen-po-kryzysach-zalozenia-nowej-strategii-i-wyzwania> [dostęp: 20.09.2022].

opracowaniu postawiono następujące pytania badawcze: Jakie rozwiązania cyfrowe mogą stosować państwa należące do Unii Europejskiej, by skutecznie zarządzać granicami i bezpieczeństwem wewnętrznym? W jaki sposób informatyzacja może pomóc monitorować migracje? Natomiast teza artykułu brzmi: Wykorzystanie elektronicznych baz danych dla potrzeb kontroli granic pozwoli lepiej zarządzać procesami migracyjnymi w Unii Europejskiej, przyczyniając się tym samym do zwiększenia bezpieczeństwa wewnętrznego.

Słowa kluczowe

migracja, Schengen, SIS, VIS, Eurodac, EES, ETIAS, ECRIS-TCN, EU-LISA, PNR

PRZETWARZANIE DANYCH BIOMETRYCZNYCH A PRAWO DO PRYWATNOŚCI

OLGA JÓZEFczyk

UCZELNIA ŁAZARSKIEGO



0000-0003-2156-7711

Wstęp

Ochrona danych osobowych stanowi zagadnienie, którego znaczenie wzrasta wraz z rozwojem nowych technologii. Sceny, które obecnie znamy np. z filmu „Raport mniejszości”, kiedy główny bohater wchodzi do centrum handlowego i na podstawie skanu siatkówki oka są do niego kierowane spersonalizowane reklamy, mogą się okazać w niedalekiej przyszłości codziennością.

W ostatnich latach obserwujemy dynamiczny rozwój biometrii i systemów na niej opartych, co powoduje, że kojarzy się ona intuicyjnie z rozwojem nowych technologii. Warto mieć jednak na uwadze fakt, że początki biometrii sięgają czasów sprzed naszej ery. Już w społeczeństwach pierwotnych znano i wykorzystywano do identyfikacji cechy biometryczne. Przykładowo na wyspie Gavrinis w Bretanii odkryto wyryte na ścianach jaskiń rysunki, których kształt przypomina linie papilarne. Pierwszą współczesną techniką identyfikacji biometrycznej był natomiast system antropometryczny, służący do identyfikacji przestępców na podstawie wymiarów ich ciała. Metoda ta nie została powszechnie wdrożona na świecie, a jej miejsce zajęła daktyloskopia (porównanie śladów linii papilarnych)¹. Badania nad

¹ K. Czaplicki, *Dokumenty tożsamości. Jawność i bezpieczeństwo*, Legalis 2016.

pozostałymi cechami biometrycznymi (np. wzorem tęczówki oka) rozpoczęły się w drugiej połowie XX w. i nadal trwają.

Biometria stała się najbardziej wiarygodną metodą rozpoznawania osób, co sprawiło, że jej zastosowanie jest obecnie bardzo szerokie. Jej niewątpliwe zalety mogą jednak przysłaniać ryzyka związane z nieprawidłowym przetwarzaniem danych biometrycznych.

Pojęcie danych biometrycznych

Dane biometryczne zostały zdefiniowane normatywnie dopiero w Rozporządzeniu 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)². Zgodnie z treścią art. 4 pkt 14 tego aktu są to dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne. Przykładami takich danych są m.in.:

- a) linie papilarne;
- b) wygląd siatkówki oka;
- c) owal twarzy;
- d) kształt małżowiny usznej;
- e) geometria ręki;
- f) układ naczyń krwionośnych dłoni;
- g) głos i jego barwa;

² Dz.Urz. UE. 2016 L 119/1.

- h) charakter pisma;
- i) sposób poruszania się³.

Ich nazwa nawiązuje do pojęcia „biometria”, które pochodzi od greckich słów *bios* (życie) oraz *metron* (miara) i określa wiedzę polegającą na umiejętności rozpoznawania żywych osób na podstawie ich cech biologicznych⁴.

Z technikami biometrycznymi wiąże się wiele pojęć o charakterze technicznym, które dla pełnego zrozumienia zakresu danych biometrycznych należy w skrócie wyjaśnić. Źródłem danych biometrycznych są próbki biometryczne, np. ślina, krew, ślad odcisku palca. Próbkę tę pozyskuje się ze względu na informację, jaką można z nich wygenerować o cechach biometrycznych. Cechy te są więc zapisane w próbce biometrycznej zawierającej dane biometryczne w postaci pewnych faktów o zmierzonych cechach, np. o cechach fizycznych zmierzonych w pewnej chwili, które wykształciły się w wyniku zachodzenia fizykochemicznych procesów formowania się tkanek. Zbiór cech biometrycznych stanowi natomiast wzorzec biometryczny, który jest punktem odniesienia do przeprowadzenia porównania z cechami biometrycznymi pobranymi w określonym momencie⁵.

Należy wskazać, że dane biometryczne stanowią tzw. dane wrażliwe (uregulowane w art. 9 RODO, tj. dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej), wobec których ustawodawca wprowadził podwyższony standard ochrony⁶.

³ M. Sakowska-Baryła, *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Legalis 2018.

⁴ B. Hołyst, J. Pomikała, *Biometria w systemach uwierzytelniania*, „Biuletyn Wojskowej Akademii Technicznej” 2011, t. 60, nr 4, s. 418.

⁵ M. Bąba, *Próba wyznaczenia zakresu pojęcia danych biometrycznych*, PME 2016, nr 2, s. 26.

⁶ M. Sakowska-Baryła, *op. cit.*

Szczególna atrakcyjność tej kategorii danych wynika z faktu, że pozwalają one na niemal jednoznaczne ustalenie tożsamości osoby, której dotyczą. Dodatkowo cechuje je zasadnicza niezmienność (w przeciwieństwie np. do nazwiska czy adresu zamieszkania).

Pojęcie „przetwarzanie danych osobowych” (w tym także danych biometrycznych) zgodnie z treścią art. 4 RODO pkt 2 oznacza natomiast operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. Katalog ten ma charakter otwarty, a zatem pozwala na łatwiejszą interpretację czy identyfikację zjawiska przetwarzania, jednak brak możliwości przypisania faktycznie występujących operacji do któregośkolwiek z wymienionych zachowań nie przesądza o braku przetwarzania w rozumieniu RODO⁷. W konsekwencji zakres tych czynności jest bardzo szeroki.

Przenosząc powyższą, ogólną definicję przetwarzania danych osobowych na przypadek danych biometrycznych, należy wskazać, że przetwarzaniem takich danych będzie uzyskiwanie wzorca biometrycznego (jednokierunkowe wyodrębnienie z danych biometrycznych w formie nieprzetworzonej kluczowych identyfikatorów biometrycznych w postaci m.in. kodu matematycznego) oraz kojarzenie danych biometrycznych (porównanie wzorca danych biometrycznych z danymi pobranymi do weryfikacji lub identyfikacji tożsamości)⁸.

⁷ *Ibidem*.

⁸ K. Czaplicki, *op. cit.*

Zastosowanie biometrii

Techniki biometryczne służą m.in. weryfikacji tożsamości, autoryzacji dostępu lub uprawnień. Są one wykorzystywane zarówno przez podmioty publiczne, jak i prywatne.

W sektorze publicznym biometria znajduje zastosowanie m.in. w zakresie:

- a) dokumentów paszportowych;
- b) identyfikacji przestępców lub ofiar;
- c) autoryzacji dostępu do instytucji publicznych.

W sektorze prywatnym biometria jest natomiast wykorzystywana m.in. w celu:

- a) ewidencji czasu pracy;
- b) autoryzacji dostępu do pomieszczeń;
- c) autoryzacji transakcji finansowych;
- d) logowania do urządzeń osobistych⁹.

Zaczynając od sektora publicznego, należy wskazać, że typowym przykładem zastosowania biometrii w administracji publicznej są dokumenty paszportowe. Zgodnie z wymogami Rozporządzenia Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie¹⁰, wprowadzono dokumenty paszportowe zawierające co najmniej jedną cechę biometryczną, tj. obraz twarzy zapisany w formie elektronicznej. Ponadto poszczególne państwa mają możliwość wydawania paszportów zawierających drugą cechę biometryczną, czyli dwa płaskie odciski palców.

W sektorze prywatnym biometria znalazła zastosowanie w szczególności w bankowości. Wprowadzenie na mocy Dyrektywy

⁹ A. Mednis, K. Gałęzowska, *Wykorzystanie biometrii w administracji publicznej*, IAP 2015, nr 4, s. 22.

¹⁰ Dz.Urz. UE L 385/1.

Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniającej dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylającej dyrektywę 2007/64/WE¹¹ zasady silnego uwierzytelniania użytkowników elektronicznych usług płatniczych ma na celu wzmocnienie bezpieczeństwa w tym zakresie. W Polsce po raz pierwszy w bankowości wykorzystano biometrię w 2010 r. w bankomatach, które identyfikowały użytkownika na podstawie układu naczyń krwionośnych palców¹².

Innym przykładem użycia biometrii są bramki biometryczne przeznaczone np. do kontroli na lotnisku lub przejściach granicznych. Taką testową bramkę biometryczną opracowali naukowcy z Instytutu Optoelektroniki Wojskowej Akademii Technicznej uczestniczący w projekcie PROTECT (*Pervasive and UseR Focused BiomeTrics BordEr ProjeCT*), realizowanym w ramach programu Horyzont 2020. Kontrola za pomocą bramki polega na skanowaniu twarzy i linii papilarnych palca¹³. Obecnie bramki biometryczne są stosowane m.in. na lotnisku Chopina w Warszawie¹⁴.

Ponadto biometria coraz częściej znajduje również zastosowanie w zakresie korzystania z różnego rodzaju urządzeń elektronicznych, np. tabletów, notebooków, smartfonów, w których często są instalowane czujniki odcisku palca pozwalające na biometryczne związanie urządzenia (i przechowywanych na nim danych) z jego posiadaczem¹⁵.

W niektórych państwach uniwersytety wprowadziły karty identyfikacyjne z zapisanymi danymi biometrycznymi w celu poprawy

¹¹ Dz.Urz. UE L 337/35.

¹² K. Sawicka, *Wykorzystanie biometrii w procesie uwierzytelniania użytkowników elektronicznych usług płatniczych*, MOP 2018, nr 23, s. 1258.

¹³ R. Lewandowski, *Biometria – nowe zastosowania*, PBW 2017, nr 9, s. 152.

¹⁴ Zob. [online:] <https://lotnisko-chopina.pl/pl/aktualnosci-i-wydarzenia/0/936/szczegoly.html> [dostęp: 18.09.2022].

¹⁵ R. Lewandowski, *op. cit.*, s. 152.

jakości kontroli dostępu i efektywnej identyfikacji studentów podczas egzaminów¹⁶.

Zagrożenia dla ochrony prawa do prywatności związane z biometrią

Użycie danych biometrycznych ma w założeniu zapewniać wyższy poziom bezpieczeństwa niż korzystanie z „tradycyjnych” metod, np. PIN¹⁷ czy karty magnetycznej. Jednak czy tak jest w praktyce? Przetwarzanie danych biometrycznych wiąże się z licznymi ryzykami w zakresie ochrony praw człowieka, w tym w szczególności prawa do prywatności.

Zgodnie z art. 8 Konwencji Rady Europy o Ochronie Praw Człowieka i Podstawowych Wolności¹⁸ każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. Ponadto niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób.

Prawo do prywatności stanowi jedno z fundamentalnych praw człowieka, o czym świadczy w szczególności liczba orzeczeń

¹⁶ E. Harinda, E. Ntagwirumugara, *Security & Privacy Implications in the Placement of Biometric-Based ID Card for Rwanda Universities*, „Journal of Information Security” 2015, nr 6, s. 93.

¹⁷ Kod 4-cyfrowy zabezpieczający transakcje dokonywane kartą płatniczą (ang. *personal identification number*).

¹⁸ Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z dnia 4 listopada 1950 r. (Dz.U. z 1993 r. Nr 61 poz. 284).

ETPCz¹⁹ wydanych w zakresie jego respektowania. Przykładowo w 2021 r. wydano ich łącznie 148, z czego najwięcej (53) dotyczyło skarg przeciwko Federacji Rosyjskiej²⁰.

Pod względem przedmiotowym prawo do prywatności dotyczy poszanowania szeroko pojętego „życia prywatnego” rozumianego jako swoboda jednostki w kształtowaniu sposobu swojego życia, samodzielności determinowania swej osobowości i autonomiczność w podejmowaniu tych decyzji²¹.

Problemy w zakresie ochrony prawa do prywatności w związku z przetwarzaniem danych biometrycznych zostały m.in. dostrzeżone przez organy Unii Europejskiej (jeszcze przed wdrożeniem RODO). W 2005 r. opublikowano raport Komisji Europejskiej pt. „Biometria na granicach: ocena wpływu na społeczeństwo”²², opracowany w odpowiedzi na zapotrzebowanie zgłoszone przez Parlament Europejski. Celem raportu było rozważenie w szerszej perspektywie wszelkiego rodzaju konsekwencji społecznych i cywilizacyjnych wywołanych zastosowaniem rozwiązań biometrycznych w różnych obszarach życia człowieka. W efekcie zidentyfikowano konsekwencje w 4 podstawowych aspektach, tj.:

- a) społecznym;
- b) ekonomicznym;
- c) technicznym;
- d) prawnym.

Dla ochrony prywatności szczególne znaczenie ma diagnoza w wymiarze społecznym. Zauważono bowiem, że rozpowszechnienie biometrii może skutkować zasadniczą zmianą relacji

¹⁹ Europejski Trybunał Praw Człowieka.

²⁰ Zob. [online:] https://www.echr.coe.int/Documents/Stats_violation_2021_ENG.pdf [dostęp: 18.09.2022].

²¹ L. Garlicki, P. Hofmański, A. Wróbel, *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom I. Komentarz do artykułów 1–18*, Legalis 2010.

²² Zob [online:] <http://ftp.jrc.es/EURdoc/21585-ExeSumm.pdf> [dostęp: 18.09.2022].

państwo – obywatel, istotnie pomniejszając sfery prywatności i anonimowości obywatela²³.

Należy wskazać, że podstawowa zaleta danych biometrycznych, czyli ich niezmienność, stanowi jednocześnie ich największą wadę. Niemożliwe jest bowiem modyfikowanie, czy też usunięcie ich źródła²⁴. Dane biometryczne mogą ujawniać inne dane wrażliwe, np.:

a) pochodzenie rasowe lub etniczne;

b) dane o stanie zdrowia lub kodzie genetycznym

oraz mogą służyć np. profilowaniu danych osobowych do celów marketingowych i określaniu preferencji konsumentów. Przykładowo, istnieją aplikacje monitorujące stan zdrowia na podstawie analizy danych biometrycznych. Jedną z nich – aplikacja Zdrowie – zbiera dane (np. grupa krwi, fototyp skóry, tętno, liczba kroków) z telefonu iPhone, zegarka Apple Watch i używanych aplikacji, aby umożliwić wyświetlanie postępu w jednym miejscu. Zebrane w ten sposób informacje zostają zaszyfrowane i podlegają profilowaniu, np. służą analizie snu czy aktywności ruchowej²⁵. Ryzykowny w tym przypadku jest fakt, że aplikacje tego typu gromadzą dane z wielu różnych źródeł. Warto w tym miejscu wskazać na wyniki badania przeprowadzonego w 2014 r. na zlecenie Global Privacy Enforcement Network dotyczące przestrzegania polityki prywatności przez wydawców aplikacji mobilnych. Analizie poddano 1211 aplikacji mobilnych; 75% z nich żądała pozwolenia na uzyskanie dostępu do funkcji smartfona lub prywatnych danych użytkownika telefonu, a 59% z nich nie informowała w przejrzysty i zrozumiały sposób o swojej polityce prywatności²⁶.

²³ K. Andres, E. Bielak-Jomaa, M. Jagielski, P. Kawczyński, M. Kasińska, P. Litwiński, A. Sieradzka, K. Wojsyk, *Ochrona danych osobowych medycznych*, Legalis 2018.

²⁴ Opinia Grupy Roboczej Nr 3/2012 z dnia 27 kwietnia 2012 r. w sprawie zmian sytuacji w dziedzinie technologii biometrycznych 00720/12/PL WP 193.

²⁵ Zob. [online:] <https://support.apple.com/pl-pl/HT203037> [dostęp: 18.09.2022].

²⁶ Zob. [online:] <https://www.statista.com/chart/2710/app-privacy/> [dostęp: 18.09.2022].

Pojawiają się także procesy sądowe dotyczące przetwarzania danych biometrycznych. Przykładowo, w amerykańskim stanie Illinois grupa użytkowników Facebooka pozwała ten portal społecznościowy za niezgodne z prawem stanu przetwarzanie danych biometrycznych, pozyskanych dzięki funkcji rozpoznawania twarzy ze zdjęć²⁷. Fotografie użytkowników podlegały analizie w celu stworzenia szablonu wykorzystywanego do porównania z fotografiami i filmami, na których mogą się oni znajdować. Pomysł ten spotkał się z szeroką krytyką społeczną. Sprawa została ostatecznie rozpoznana przez sąd w San Francisco, który orzekł, że Facebook naruszył przepisy ochrony danych biometrycznych (*Biometric Information Privacy Act*)²⁸. Obecnie usługa ta może zostać uruchomiona dopiero po wyrażeniu zgody przez użytkownika²⁹.

Ponadto temat rozpoznawania twarzy został poruszony w Opinii Europejskiego Komitetu Ekonomiczno-Społecznego z dnia 20 lutego 2019 r. pt. „Rewolucja cyfrowa w kontekście potrzeb i praw obywateli”³⁰, gdzie wskazano, że „technologia ta jest coraz tańsza i łatwo dostępna dla wszystkich, co może doprowadzić do sytuacji, w której nie będzie już można zachować anonimowości na ulicy ani robić anonimowo zakupów”.

Przywołane rozpoznawanie twarzy wzbudza liczne emocje, bowiem może służyć nie tylko do określenia tożsamości, lecz także do określenia charakterystycznych cech fizjologicznych i psychologicznych, takich jak pochodzenie etniczne, emocje, samopoczucie.

²⁷ Zob. [online:] <https://www.komputerswiat.pl/aktualnosci/wydarzenia/facebook-pozwany-w-sprawie-nielegalnego-zbierania-danych-biometrycznych/rfbqtvb> [dostęp: 18.09.2022].

²⁸ Zob. [online:] <https://www.eff.org/deeplinks/2018/07/eff-illinois-supreme-court-protect-biometric-privacy> [dostęp: 18.05.2019].

²⁹ Zob. [online:] <https://technologia.dziennik.pl/internet/artykuly/573254,nowy-regulamin-facebooka-rodo-rozpoznawanie-twarzy.html> [dostęp: 18.09.2022].

³⁰ Dz.Urz. UE C 190/17-23.

Twarz zawiera bowiem zestaw cech indywidualnych dla każdego człowieka, do których zaliczamy:

- a) owal twarzy;
- b) kształt czoła;
- c) kształt podbródka;
- d) kształt uszu;
- e) wysokość i szerokość nosa;
- f) szerokość ust.

Ponadto w obrębie twarzy możemy wskazać charakterystycznie rozmieszczone punkty, np. pomiędzy centrami oczu, czubkiem nosa a linią oczu oraz pomiędzy centrami oczu a centrum ust, a także różnego rodzaju pieprzyki, piegi czy blizny. Wszystko to zdradza np. przebyte przez nas choroby, alergię i uczulenia³¹. Skłania także do dalszych wniosków, np. o spekulowane przyczyny blizn (udział w bójce, rany wojenne itp.).

Uzyskanie niejako „w gratisie” dodatkowych danych osobowych powoduje, że dochodzi do ryzyka zmiany celu przetwarzania danych biometrycznych bez wiedzy i zgody osoby, której dane dotyczą. Kwestię tę zdiagnozowała m.in. Grupa Robocza art. 29³² w opinii 3/2012 w sprawie zmian sytuacji w dziedzinie technologii biometrycznych³³ z dnia 27 kwietnia 2012 r., a potwierdzają ją przypadki z praktyki omówione w dalszej części niniejszej pracy.

Dodatkowo kontrowersje wzbudzają poszczególne techniki i rodzaje danych biometrycznych. Największym bezpieczeństwem i unikalnością wzorca cechują się metody bazujące na pomiarze

³¹ K. Czaplicki, *op. cit.*

³² Grupa Robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych, powołana na mocy art. 29 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 (Dz.Urz. UE 1995 L 281/31).

³³ Zob. [online:] http://ec.europa.eu/justice/data-protection/index_en.htm [dostęp: 18.09.2022].

naczyń krwionośnych palca i obrazu tęczówki oka. Za mniej bezpieczną metodę uznaje się natomiast odczyt linii papilarnych, ponieważ – zwłaszcza w początkowej fazie stosowania – wiąże się ona z ryzykiem fałszerstwa (np. kopiowanie odcisku palca na silikonie i wykorzystywanie tak pozyskanego obrazu linii papilarnych do podszycia się pod konkretnego użytkownika)³⁴.

W orzecznictwie ETPCz niejednokrotnie pojawiają się stanowiska dotyczące omawianego problemu. Główną konkluzją z jego analizy jest konieczność ścisłego ustawowego uregulowania kwestii wykorzystania danych biometrycznych.

Na ten temat ETPCz wypowiedział się m.in. w szeroko komentowanym wyroku z dnia 4 grudnia 2008 r. w sprawie *S. i Marper przeciwko Wielkiej Brytanii* (30562/04 i 30566/04)³⁵ dotyczącym przetrzymywania próbek odcisków palców oraz DNA³⁶ skarżących, zebranych na potrzeby postępowań sądowych. Zgodnie z prawem krajowym w Wielkiej Brytanii przechowywanie próbek w celu zapobiegania przestępczości było dozwolone nawet wobec osób, co do których zapadły wyroki uniewinniające (jak w przypadku skarżących). Ponadto przechowywanie tych danych nie podlegało ograniczeniom czasowym, jak również nie stworzono katalogu przestępstw, których zapobieganie usprawiedliwiałoby przetwarzanie takich danych. ETPCz uznał, że stanowiło to zbyt daleko idącą ingerencję w prawa podstawowe i naruszyło postanowienia Konwencji.

W świetle powyższego należy również mieć na uwadze, że zagadnienie to reguluje art. 51 ust. 2 Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.³⁷ Zgodnie z treścią tego przepisu władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać

³⁴ K. Sawicka, *op. cit.*, s. 1258.

³⁵ Zob. [online:] [https://hudoc.echr.coe.int/eng#{"fulltext":\["30566/04"\],"documentcollectionid2":\["GRANDCHAMBER","CHAMBER"\],"itemid":\["001-90051"\]}](https://hudoc.echr.coe.int/eng#{) [dostęp: 18.09.2022].

³⁶ kwas deoksyrybonukleinowy (ang. *deoxyribonucleic acid*).

³⁷ Dz.U. z 1997 r. Nr 78 poz. 483.

innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.

Na ten temat wypowiedział się m.in. Naczelny Sąd Administracyjny w wyroku z dnia 1 grudnia 2009 r.³⁸ dotyczącym przetwarzania danych biometrycznych pracowników przez pracodawcę. Sąd wskazał, że wykorzystanie tego rodzaju danych do kontroli czasu pracy jest nieproporcjonalne do zamierzonego celu ich przetwarzania.

Obecnie (po wejściu w życie RODO) kwestię tę reguluje wprost zasada minimalizacji, zgodnie z treścią której przetwarzanie danych z wykorzystaniem systemu biometrycznego wymaga dokonania oceny, czy dany system jest konieczny do spełnienia określonej potrzeby, czy wykorzystanie określonej technologii biometrycznej warunkuje prawdopodobieństwo skuteczności systemu, a także czy utrata prywatności będąca następstwem stosowania systemu biometrycznego jest proporcjonalna do przewidywanych potrzeb i korzyści.

Zagadnienie danych biometrycznych badał także RPO. Przedmiotem kontroli była weryfikacja wątpliwości związanych z wykorzystywaniem urządzeń rejestrujących tzw. odręczny podpis biometryczny przez operatorów pocztowych przy potwierdzaniu odbioru przesyłek. Niepokój obywateli, którzy zgłaszali ten problem, wynikał z faktu większej mobilności danych przetwarzanych w formie elektronicznej i – co za tym idzie – zwiększeniem ryzyka nieautoryzowanego dostępu. Rzecznik Praw Obywatelskich wystąpił zatem w grudniu 2018 r. z prośbą o wyjaśnienia do PUODO. W odpowiedzi PUODO wskazał, że nie przeprowadzał dotąd badań w zakresie przepływu danych elektronicznych wygenerowanych podczas składania własnoręcznego podpisu na urządzeniu elektronicznym (badań w tym zakresie nie przeprowadzał również uprzednio Generalny Inspektor Ochrony Danych Osobowych).

³⁸ I OSK 249/09, CBOSA.

Jednocześnie PUODO poinformował, że problem ten był analizowany przez organy ochrony danych zrzeszone w ramach Międzynarodowej Grupy Roboczej ds. Ochrony Danych w Telekomunikacji (tzw. Grupy Berlińskiej, której Urząd Ochrony Danych Osobowych jest członkiem). Analiza ta wykazała wiele wątpliwości, w tym m.in. zwróciła uwagę na fakt, że w przypadku aplikacji stosowanych przez niektóre banki czy operatorów telefonicznych po złożeniu własnoręcznego podpisu klient nie ma już nad nim kontroli. Biorąc pod uwagę powyższe, PUODO skonstatował, że konieczne jest przeprowadzenie badań w tym zakresie³⁹. Na chwilę obecną brak jednak informacji, czy zostały one faktycznie podjęte.

Na koniec warto także przywołać działania fundacji Panoptikon, której nazwa nawiązuje do XVIII-wiecznej koncepcji więzienia autorstwa utylitarysty Jeremy'ego Benthama (budynek w kształcie pierścienia, podzielony na cele skazańców, którzy zawsze pozostają w polu widzenia strażnika). Fundacja zidentyfikowała m.in. 7 „grzechów” społeczeństwa nadzorowanego, wśród których znajduje się w szczególności ingerencja w prywatność. Wiele artykułów publikowanych na stronie internetowej Panoptikonu dotyczy tematyki danych biometrycznych⁴⁰. W jednym z nich zwrócono uwagę na fakt, że w mediach pojawia się dużo przykładów wycieków haseł. Regularne zmienianie haseł jest zatem jednym z podstawowych elementów naszego bezpieczeństwa. Niestety nie dotyczy to identyfikacji biometrycznej, ponieważ „swojego ciała tak łatwo nie zmienimy”⁴¹, dlatego przetwarzanie danych biometrycznych powinno odbywać się ze szczególną ostrożnością i rozwagą.

³⁹ Zob. [online:] <https://www.rpo.gov.pl/pl/content/podpis-odbioru-przesesy%C5%82ek-na-tablecie-rpo-pyta-czy-bezpieczne> [dostęp: 18.09.2022].

⁴⁰ Zob. [online:] <https://panoptikon.org/idea> [dostęp: 18.09.2022].

⁴¹ Zob. [online:] <https://panoptikon.org/biometria-w-skarbowce> [dostęp: 18.09.2022].

Wymóg szczególnej ochrony danych biometrycznych

Nieprzypadkowo, jak już wskazano, dane biometryczne są na gruncie RODO traktowane jako tzw. dane wrażliwe, a zatem podlegające szczególnej ochronie. Owa szczególna ochrona polega na tym, że – co do zasady – przetwarzanie takich danych jest zabronione (art. 9 RODO). Od tego zakazu RODO przewiduje wyjątki, np. gdy osoba, której dane dotyczą, wyraziła na to wyraźną zgodę. Wyjątki te nie powinny być jednak interpretowane rozszerzająco.

Zgodnie z RODO przetwarzanie tych danych wymaga przeprowadzenia oceny skutków przetwarzania oraz uwzględnienia zasad ochrony danych w fazie projektowania (ang. *privacy by design*). Taka ocena, zgodnie z treścią art. 35 ust. 7 RODO, powinna zawierać co najmniej:

- a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym – gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
- b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
- c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
- d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia, oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Ponadto poza środkami natury prawnej konieczne jest wdrożenie zabezpieczeń o charakterze technicznym i organizacyjnym. W szczególności zasadne wydaje się zastosowanie rodziny

norm ISO⁴² 27000, będących zestawieniem standardów poświęconych bezpieczeństwu informacji, w szczególności normy od ISO/IEC⁴³ 27001 do ISO/IEC 27006⁴⁴.

Podsumowanie

Podsumowując, należy wskazać, że temat przetwarzania danych biometrycznych wzbudza liczne kontrowersje. Entuzjaści biometrii podkreślają atrakcyjność tej kategorii danych, wynikającą z faktu, że pozwalają one na niemal jednoznaczne ustalenie tożsamości. Sceptycy wyliczają natomiast ryzyka w zakresie ochrony praw człowieka, w tym w szczególności prawa do prywatności. Przykłady z praktyki pokazują, że obawy te bywają zasadne.

Orzecznictwo ETPCz wskazuje na konieczność ścisłego ustawowego uregulowania kwestii wykorzystania tego rodzaju danych. Kluczowe znaczenie ma zwłaszcza zastosowanie zasady minimalizacji, zgodnie z treścią której przetwarzanie danych z wykorzystaniem systemu biometrycznego wymaga dokonania oceny, czy utrata prywatności będąca następstwem jego zastosowania jest proporcjonalna do przewidywanych potrzeb i korzyści.

Stopień bezpieczeństwa i zagwarantowania prywatności regulacji prawnych dotyczących tego rodzaju danych przekłada się również na społeczną akceptowalność biometrii.

⁴² Międzynarodowa Organizacja Normalizacyjna (*International Organization for Standardization*).

⁴³ Międzynarodowa Komisja Elektrotechniczna (*International Electrotechnical Commission*).

⁴⁴ K. Andres, E. Bielak-Jomaa, M. Jagielski, P. Kawczyński, M. Kasińska, P. Litwiński, A. Sieradzka, K. Wojsyk, *op. cit.*, Legalis 2018.

Bibliografia

Akty normatywne

1. 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 119/1).
2. Rozporządzenie Rady (WE) nr 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie (Dz.Urz. UE. L 385/1).
3. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego (Dz.Urz. UE L 337/35).
4. Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z dnia 4 listopada 1950 r. (Dz.U. z 1993 r. Nr 61 poz. 284).
5. Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78 poz. 483).

Literatura przedmiotu

1. Andres K., Bielak-Jomaa E., Jagielski M., Kawczyński P., Krasińska M., Litwiński P., Sieradzka A., Wojsyk K., *Ochrona danych osobowych medycznych*, Legalis 2018.
2. Bąba M., *Próba wyznaczenia zakresu pojęcia danych biometrycznych*, PME 2016, nr 2.
3. Czaplicki K., *Dokumenty tożsamości. Jawność i bezpieczeństwo*, Legalis 2016.
4. Garlicki L., Hofmański P., Wróbel A., *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności. Tom I. Komentarz do artykułów 1–18*, Legalis 2010.

5. Harinda E., Ntagwirumugara E., *Security & Privacy Implications in the Placement of Biometric-Based ID Card for Rwanda Universities*, „Journal of Information Security” 2015, nr 6.
6. Hołyst B., Pomikała J., *Biometria w systemach uwierzytelniania*, „Biuletyn Wojskowej Akademii Technicznej” 2011, t. 60, nr 4.
7. Lewandowski R., *Biometria – nowe zastosowania*, PBW 2017, nr 9.
8. Mednis A., Gałęzowska A., *Wykorzystanie biometrii w administracji publicznej*, IAP 2015, nr 4.
9. Sakowska-Baryła M., *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Legalis 2018.
10. Sawicka K., *Wykorzystanie biometrii w procesie uwierzytelniania użytkowników elektronicznych usług płatniczych*, MoP 2018, nr 23.

Orzecznictwo

1. Wyrok NSA z dnia 1 grudnia 2009 r., I OSK 249/09, CBOSA.

Inne

1. Opinia Grupy Roboczej Nr 3/2012 z dnia 27 kwietnia 2012 r. w sprawie zmian sytuacji w dziedzinie technologii biometrycznych 00720/12/PL WP 193.
2. Opinia Europejskiego Komitetu Ekonomiczno-Społecznego z dnia 20 lutego 2019 r. pt. „Rewolucja cyfrowa w kontekście potrzeb i praw obywateli” (Dz.Urz. UE C 190/17-23).

Źródła internetowe

1. <https://lotnisko-chopina.pl/pl/aktualnosci-i-wydarzenia/0/936/szczegoly.html> [dostęp: 18.09.2022]
2. https://www.echr.coe.int/Documents/Stats_violation_2021_ENG.pdf [dostęp: 18.09.2022]
3. <http://ftp.jrc.es/EURdoc/21585-ExeSumm.pdf> [dostęp: 18.09.2022]

4. <https://support.apple.com/pl-pl/HT203037> [dostęp: 18.09.2022]
5. <https://www.statista.com/chart/2710/app-privacy/> [dostęp: 18.09.2022]
6. <https://www.komputerswiat.pl/aktualnosci/wydarzenia/facebook-pozwany-w-sprawie-nielegalnego-zbierania-danych-biometrycznych/rfbqtvb> [dostęp: 18.09.2022]
7. <https://www.eff.org/deeplinks/2018/07/eff-illinois-supreme-court-protect-biometric-privacy> [dostęp: 18.09.2022]
8. <https://technologia.dziennik.pl/internet/artykuly/573254,nowy-regulamin-facebook-a-rodo-rozpoznawanie-twarzy.html> [dostęp: 18.09.2022]
9. http://ec.europa.eu/justice/data-protection/index_en.htm [dostęp: 18.09.2022]
10. [https://hudoc.echr.coe.int/eng#{"fulltext":\["30566/04"\],"documentcollectionid2":\["GRANDCHAMBER","CHAMBER"\],"itemid":\["001-90051"\]}](https://hudoc.echr.coe.int/eng#{"fulltext":["30566/04"],"documentcollectionid2":["GRANDCHAMBER","CHAMBER"],"itemid":["001-90051"]}) [dostęp: 18.09.2022]
11. <https://www.rpo.gov.pl/pl/content/podpis-odbioru-przesy%C5%82ek-na-tablecie-rpo-pyta-czy-bezpieczne> [dostęp: 18.09.2022]
12. <https://panoptikon.org/idea> [dostęp: 18.09.2022]
13. <https://panoptikon.org/biometria-w-skarbowce> [dostęp: 18.09.2022]

Streszczenie

Celem opracowania jest przedstawienie zagadnienia przetwarzania danych biometrycznych w świetle przepisów regulujących ochronę prawa do prywatności. Użycie danych biometrycznych w założeniu ma zapewniać wyższy poziom bezpieczeństwa niż korzystanie z „tradycyjnych” metod. W praktyce wiąże się to jednak z licznymi ryzykami w zakresie ochrony praw człowieka, co zostało omówione na konkretnych przykładach.

Słowa kluczowe

dane biometryczne, dane osobowe, prywatność, prawa człowieka

INFORMATYZACJA ADMINISTRACJI PUBLICZNEJ W POLSCE – WYZWANIA I PROBLEMY

PAWEŁ ŚWITAL

UNIwersytet Technologiczno-Humanistyczny

IM. KAZIMIERZA PUŁASKIEGO W RADOMIU



0000-0002-7404-5143

Wprowadzenie

Obserwowany zarówno w Polsce, jak i na świecie postęp w zakresie modernizacji administracji publicznej związany jest z procesem informatyzacji administracji publicznej. Zasadniczym celem procesu informatyzacji administracji publicznej jest zapewnienie możliwości elektronicznej obsługi obywateli i innych zainteresowanych podmiotów przez organy władzy publicznej¹. Pandemia COVID-19 uwypukliła w tym zakresie zapotrzebowanie na świadczenie usług w formie elektronicznej. Działania te wskazują również na niski poziom wykorzystania usług elektronicznych. W dobie rozwoju i transformacji technologii cyfrowych jednostki administracji publicznej czynią starania, aby jak najwięcej spraw urzędowych można było realizować przez Internet. Według danych Głównego Urzędu Statystycznego w 2021 r. usługi elektroniczne oferowało obywatelom 99,8% jednostek administracji publicznej, przy czym 28,1% z nich dało możliwość zainstalowania aplikacji na urządzenia mobilne, oferujące e-usługi, a udział w głosowaniach

¹ M. Kotulska, *Wykorzystanie środków komunikacji elektronicznej w postępowaniu administracyjnym*, PPP 2012, nr 9, s. 23.

czy konsultacjach społecznych online zapewniało 26,2% urzędów. Usługi przez Internet świadczyły wszystkie jednostki administracji samorządowej².

Informatyzacja wymaga nieustannych inwestycji państwa w podnoszenie jakości, ale i zapewnienie bezpieczeństwa świadczonych usług publicznych przy użyciu nowych technologii. Jak zauważają Z. Mazur oraz H. Mazur, zakres usług oferowanych w sektorze publicznym (m.in. w administracji rządowej i samorządowej) oraz czas i koszt ich realizacji w dużej mierze zależą od stopnia informatyzacji, integracji i interoperacyjności systemów informatycznych (dostosowania ich do wzajemnej współpracy i wymiany danych umożliwiającej ich dalsze przetwarzanie i wykorzystywanie w postaci elektronicznej)³. Spójność systemowa oraz kompatybilność systemów są zatem jednymi z podstawowych cech, jakimi powinni kierować się twórcy wdrażanych systemów informatycznych.

Elektroniczna administracja powinna umożliwić załatwienie sprawy urzędowej w formie elektronicznej. Kluczowe tu będą wszelkie czynności: od wszczęcia postępowania, kontaktu z urzędem, stanu/etapu załatwianej sprawy, obowiązki informacyjne urzędu, opis procedur urzędowych, standaryzacja systemów, uwierzytelnianie danych, bezpieczeństwo danych, proces wydania elektronicznych decyzji administracyjnych. W celu tak pojmowanego załatwiania spraw elektronicznych wprowadzono wiele e-usług publicznych. Są to m.in. Elektroniczna Platforma Usług Administracji Publicznej (ePUAP), Platforma Usług Elektronicznych Zakładu

² Wykorzystanie technologii informacyjno-komunikacyjnych w jednostkach administracji publicznej w 2021 r., Główny Urząd Statystyczny / Obszary tematyczne / Nauka i technika. Społeczeństwo informacyjne / Społeczeństwo informacyjne / Wykorzystanie technologii informacyjno-komunikacyjnych w jednostkach administracji publicznej w 2021 r. [dostęp: 11.06.2022].

³ Z. Mazur, H. Mazur, *Problemy informatyzacji w sektorze publicznym*, „Nierówności Społeczne a Wzrost Gospodarczy” 2015, nr 44(4), cz. 1, s. 395.

Ubezpieczeń Społecznych (PUE ZUS), portal obywatel.gov.pl, portal biznes.gov.pl, emp@tia⁴. Z usług publicznych może korzystać każdy obywatel, który jest w stanie potwierdzić swoją tożsamość w Internecie. Działanie takie możliwe jest za pomocą profilu zaufanego, który służy jako elektroniczny podpis w komunikacji z administracją publiczną. Szeroka gama usług świadczonych przy użyciu środków elektronicznych, jak i bezpieczna możliwość weryfikacji osób korzystających z usług elektronicznych powinna stać się zachętą do odchodzenia od tradycyjnego korzystania z urzędów i pozwolić rozwinąć elektroniczną administrację w Polsce.

Kierunki rozwoju informatyzacji państwa

Wstąpienie Polski w struktury Unii Europejskiej miało spowodować postęp w dziedzinie e-administracji, głównie dzięki pozyskiwanym funduszom na realizację zamierzonych celów. W 2006 r. ogłoszono pierwszy Plan Informatyzacji Państwa, a następny w 2007 r. Dokumenty te zakładały rozwój e-usług. Istotnym zdarzeniem (unikalnym w wymiarze Unii Europejskiej) było uchwalenie w lutym 2005 r. ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne⁵, mającej za zadanie usytuowanie sektora informatyzacji kraju i budowy społeczeństwa informacyjnego, w głównej mierze przez ustalenie trybu funkcjonowania elektronicznej administracji⁶. Następstwem działań w zakresie informatyzacji było wprowadzenie ustaw: o dostępie

⁴ Z funkcjonalnością systemów i e-usług publicznych można zapoznać się [online:] <https://www.gov.pl/web/cyfryzacja/e-uslugi> [dostęp: 01.06.2022].

⁵ Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2021 r. poz. 2070 z późn. zm.).

⁶ B. Bal-Domańska, *Wstęp do e-administracji. E-obieg dokumentów w administracji publicznej z wykorzystaniem el-Dok-Systemu*, Wrocław 2015, s. 18.

do informacji publicznej⁷, o świadczeniu usług drogą elektroniczną⁸, o usługach zaufania i podpisie elektronicznym⁹.

Dużą rolę odgrywały i odgrywają plany i strategie rozwoju informatyzacji, które określają szczegółowo cele państwa w tym obszarze. Są to m.in. Długookresowa Strategia Rozwoju Kraju „Polska 2030. Trzecia Fala Nowoczesności”¹⁰ oraz Program Zintegrowanej Informatyzacji Państwa¹¹.

Z Długookresowej Strategii Rozwoju Kraju wynika konieczność przyspieszenia w Polsce działań w zakresie przemian technologicznych. Będzie to możliwe przede wszystkim poprzez inwestycje infrastrukturalne w szerokopasmowy Internet, który będzie dostępny dla wszystkich. Zapewnienie dostępności cyfrowej zwiększy szanse rozwoju obszarów peryferyjnych, przyczyniając się do równoważenia terytorialnego rozwoju. Jako drugi element wskazano działania na rzecz przyspieszenia potrzeb używania przez obywateli Internetu. Ma to zostać osiągnięte poprzez rozwój usług elektronicznych oraz e-gospodarki, a także wzrost sprawności państwa w tym zakresie. Priorytetowe będzie tu podejście w ramach zintegrowanej informatyzacji, opartej na logicznym i skutecznym obiegu informacji, wprowadzeniu zasad zarządzania procesowego, neutralności technologicznej państwa oraz efektywności kosztowej. Po zrealizowaniu tych warunków będzie można podjąć działania na

⁷ Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2022 r. poz. 902).

⁸ Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r. poz. 344).

⁹ Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz.U. z 2021 r. poz. 1797).

¹⁰ Uchwała nr 16 Rady Ministrów z dnia 5 lutego 2013 r. w sprawie przyjęcia Długookresowej Strategii Rozwoju Kraju „Polska 2030. Trzecia Fala Nowoczesności”, MP z 2013 r., poz. 121.

¹¹ Program Zintegrowanej Informatyzacji Państwa [online:] <https://www.gov.pl/web/cyfrizacja/program-zintegrowanej-informatyzacji-panstwa> [dostęp: 22.05.2022].

rzecz trzeciego elementu Polski Cyfrowej, którym jest przyrost kompetencji cyfrowych społeczeństwa, zapobiegających nowym typom wykluczeń, np. osób starszych nieużywających obecnie Internetu. Pożądane będzie zatem wprowadzenie takich regulacji technologii cyfrowych, które służyć będą rozwojowi sieciowych form życia publicznego i kapitału społecznego.

Drugi dokument to Program Zintegrowanej Informatyzacji Państwa, w którym za cel główny uznano modernizację administracji publicznej z wykorzystaniem technologii cyfrowych, która będzie nakierowana na potrzebę podniesienia sprawności państwa oraz poprawienie jakości relacji administracji z obywatelami i innymi interesariuszami. Będzie to możliwe przy uwzględnieniu trzech celów szczegółowych, które koncentrują się wokół kluczowych składowych procesu transformacji cyfrowej państwa, zarówno w zakresie sektora publicznego, jak i prywatnego, dzięki ich komplementarnej realizacji. Należą do nich: zwiększenie jakości oraz zakresu komunikacji między obywatelami i innymi interesariuszami a państwem, wzmocnienie dojrzałości organizacyjnej jednostek administracji publicznej oraz usprawnienie zaplecza elektronicznej administracji (ang. *back office*), jak również podniesienie poziomu kompetencji cyfrowych obywateli, specjalistów technologii informacyjno-komunikacyjnej (TIK) oraz pracowników administracji publicznej.

Zaufanie do administracji elektronicznej

Omawiając zagadnienie informatyzacji, nie można pominąć kwestii zaufania do technologii, bowiem brak takiego zaufania może być jedną z przyczyn niskiego poziomu korzystania z elektronicznej administracji. Kluczowa różnica między tradycyjną administracją a e-administracją sprowadza się do zmiany postrzegania roli administracji publicznej, która ze względu na podmiot sprawujący

władzę nad obywatelem jawi się jako instytucja świadcząca usługi administracyjne. Nowe podejście wymaga radykalnych zmian zarówno w postawie pracowników administracji, jak i opracowania i wdrożenia stosownych procedur, ich standaryzacji oraz sposobu działania¹². W życiu codziennym coraz powszechniejsze stają się rozwiązania technologiczne, które ograniczają, zastępują lub eliminują udział człowieka. Dotychczasowe relacje człowiek – człowiek zostają zastępowane relacjami człowiek – technologia¹³. Zaufanie jest relacją obciążoną dużym ładunkiem emocji, w związku z tym nie jest ono stabilne¹⁴.

Zaufanie zostało zdefiniowane m.in. w naukach socjologicznych. Według P. Sztompki zaufanie staje się podstawową strategią radzenia sobie z niepewnością i niemożnością kontrolowania przyszłości. Rozumie się je jako strategię upraszczającą, która pozwala jednostkom zaadaptować się do złożonego środowiska społecznego i tym samym korzystać z szerszej puli możliwości. Ma ono szczególne znaczenie w warunkach niewiedzy lub niepewności związanych z nieznanymi lub niepoznawalnymi działaniami innych¹⁵. Tak rozumiane zaufanie może odnosić się do wdrażania nowych systemów informatycznych oraz zmiany paradygmatu myślenia o wykonywaniu zadań administracji publicznej. W działaniach na rzecz informatyzacji administracji publicznej duży nacisk został położony na zapewnienie możliwości elektronicznej obsługi petentów i innych zainteresowanych podmiotów przez organy władzy publicznej.

¹² J. Drobiazgiewicz, *Oddziaływanie telekomunikacji na administrację* [w:] *Rynek usług telekomunikacyjnych*, red. H. Babis, K. Flaga-Gieruszyńska, Warszawa 2011, s. 397.

¹³ J. Ejdyś, *Determinanty zaufania do technologii*, „Przegląd Organizacji” 2017, nr 12, s. 20.

¹⁴ J. Korczak, *Pozyskiwanie i umacnianie zaufania do władz publicznych przez współadministrowanie* [w:] *Sprawiedliwość i zaufanie do władz publicznych w prawie administracyjnym*, red. M. Stahl, M. Kasiński, K. Wlaźlak, Warszawa 2015, s. 98.

¹⁵ P. Sztompka, *Zaufanie. Fundament społeczeństwa*, Kraków 2007, s. 69–71.

Bezpośrednim skutkiem takich działań będzie powstanie systemu e-administracji (e-government). Ma to na celu ostatecznie usprawnienie funkcjonowania administracji publicznej w Polsce¹⁶.

Podkreślić należy za K. Celarek, że jedną z podstawowych metod usprawniania administracji przez kierowanie jej w stronę komunikacji elektronicznej jest podniesienie świadomości o użyteczności elektronicznych rozwiązań. Chodzi tu zarówno o świadomość społeczeństwa, jak i świadomość pracowników instytucji publicznych¹⁷. Nastawić należy się głównie na gotowość urzędników na zmiany – kultura organizacji w rządzie jest ważnym aspektem e-gotowości. Zmniejszenie oporu urzędników i zwiększenie ich zaangażowania w ustalanie kierunków działania ma wpływ na to, jak szybko zostanie wprowadzony w życie e-government¹⁸. W zaufaniu technologicznym niezwykle ważna jest także bieżąca spójność i stosowanie technologii informacyjno-komunikacyjnych (ICT) przez administrację – zrozumienie aktualnego stosowania ICT może świadczyć o gotowości rządu do zarządzania informacją i projektami e-governmentu, jak również o tym, czy struktura ICT odpowiada globalnym standardom, a ponadto może pozwolić wysiłkom e-administracji, by wzrastały na poprzednich projektach komputeryzacji, które były pomyślne¹⁹.

W zakresie zaufania do administracji elektronicznej i funkcjonujących w niej systemów niezbędne jest podkreślanie korzyści płynących z jej wykorzystania. Wskazać tu można możliwość załatwiania spraw z każdego miejsca, przez całą dobę, siedem dni

¹⁶ R. Biskup, M. Ganczar, *Komunikacja elektroniczna w postępowaniu administracyjnym*, PiP 2008, nr 1, s. 59.

¹⁷ K. Celarek, *Prawne aspekty informatyzacji administracji*, Dąbrowa Górnicza 2009, s. 153.

¹⁸ M. Ganczar, *Informatyzacja administracji publicznej. Nowa jakość usług publicznych dla obywateli i przedsiębiorców*, Warszawa 2009, s. 36–37.

¹⁹ D. Fleszer, *Wokół problematyki e-administracji*, „Roczniki Administracji i Prawa” 2014, nr 14(1), s. 127–128.

w tygodniu, oszczędności czasu na zbędne przemieszczanie się, szczegółowy opis procedur w ramach danego systemu, możliwość wglądu do sprawy na każdym stadium jej rozstrzygania. Tak ukazywana administracja elektroniczna będzie budowała nowy wizerunek korzystania z e-usług i załatwiania spraw obywateli. Szczególną rolą państwa w tym zakresie jest zatem budowa wizerunku elektronicznej administracji, a także kształcenie świadomych pokoleń korzystających z elektronicznej administracji przyszłości.

Interoperacyjność i standaryzacja systemów

Legalną definicję interoperacyjności zawiera art. 3 pkt 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne²⁰. W tym ujęciu interoperacyjność to zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy przez wspierane przez nie procesy biznesowe realizowane za pomocą wymiany danych za pośrednictwem wykorzystywanych przez te podmioty systemów teleinformatycznych. Wynika z tego obowiązek, zgodnie z którym podmioty publiczne do realizacji zadań publicznych mają używać systemów teleinformatycznych, które taką interoperacyjność zapewniają: podmiot publiczny używa do realizacji zadań publicznych systemów teleinformatycznych spełniających minimalne wymagania dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów na zasadach określonych w Krajowych Ramach Interoperacyjności (art. 13 ust. 1). Projekt Krajowych Ram Interoperacyjności określa trzy

²⁰ Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2021 r. poz. 2070 z późn. zm.).

poziomy interoperacyjności: poziom technologiczny – infrastruktura teleinformatyczna (łącza komunikacyjne, platformy komputerowe, systemy operacyjne, oprogramowanie); poziom systemowy – kolekcje danych, oprogramowanie aplikacyjne, oprogramowanie i obiekty prezentacji danych; poziom zadaniowy – obiekty i procedury mające bezpośredni związek z rzeczywistymi zadaniami realizowanymi przez podmioty zainteresowane; poziom ten obejmuje przede wszystkim uwarunkowania organizacyjno-prawne, procesy realizacji zadań oraz wykorzystywane informacje²¹. Ważniejsze rekomendacje Europejskich Ram Interoperacyjności dotyczą przede wszystkim:

- 1) dostępności oznaczającej wielokanałowe udostępnienie treści w formie zrozumiałej dla użytkowników;
- 2) wielojęzyczności – udostępniania treści nie tylko w językach narodowych;
- 3) bezpieczeństwa – dostosowanego do poziomu paneuropejskiego;
- 4) prywatności – ochrony danych osobowych;
- 5) subsydiarności – European Interoperability Framework (EIF)²² działa pomocniczo i nie wnika w działania wewnętrzne państw;
- 6) stosowania otwartych standardów;
- 7) tworzenia rozwiązań wielostronnych – pochodzących z różnych źródeł i od różnych dostawców²³.

Tak założone działania dla systemów informatycznych wskazują także na konieczność dostosowywania systemów do Europejskich

²¹ Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r. poz. 2247).

²² Europejskie Ramy Interoperacyjności.

²³ J. Banasikowska, A. Sołtysik-Piorunkiewicz, *Zasady interoperacyjności i standaryzacji w systemach wszechobecnego e-Government krajów Unii Europejskiej*, „Roczniki Kolegium Analiz Ekonomicznych” 2013, nr 29, s. 17.

Ram Interoperacyjności oraz wdrożenia jednolitych standardów w całej Unii Europejskiej. Polskie e-usługi często nie zawierają możliwości korzystania z nich w innym języku niż język polski. Różna jest także budowa systemu, opis procedur. Dużym utrudnieniem jest również konieczność zakładania wielu odrębnych kont do systemów elektronicznych w celu potwierdzania tożsamości.

Standaryzacja polega na zastosowaniu jednolitych zasad i norm realizacji określonych usług, gwarantuje większą przejrzystość i efektywność wydatkowania środków, a także przyczynia się do skuteczności ich realizacji. Ponadto standardy wpływają na stały rozwój, gdyż odwoływanie się do nich umożliwia poszukiwanie i ulepszanie procesów²⁴. W ustawie z dnia 12 września 2002 r. o normalizacji²⁵ przyjęto definicję normalizacji (standaryzacji) jako działalności zmierzającej do uzyskania optymalnego, w danych okolicznościach, stopnia uporządkowania w określonym zakresie, poprzez ustalanie postanowień przeznaczonych do powszechnego i wielokrotnego stosowania, dotyczących istniejących lub mogących wystąpić problemów. Stosowanie standardów pozwala na wykorzystanie w działaniu aktualnej wiedzy z danej dziedziny i ogranicza możliwe straty. Takie podejście daje możliwość wprowadzenia jednolitego standardu obsługi systemu informatycznego, standaryzacji procedur, jak również wprowadzenia jednolitych wzorów, schematów załatwiania spraw.

²⁴ M. Stachowicz, *Standaryzacja jako czynnik optymalizacji usług świadczonych przez administrację publiczną*, ST 2015, nr 5, s. 67–78.

²⁵ Ustawa z dnia 12 września 2002 r. o normalizacji (t.j. Dz.U. z 2015 r. poz. 1483).

Kompetencje cyfrowe pracowników urzędów administracji

E-administracja i inne innowacyjne rozwiązania elektroniczne, jako narzędzie wymagające podstawowych kompetencji cyfrowych, stają się obecnie jednym z czynników sukcesu wielu państw europejskich. Jak wskazano powyżej, w dzisiejszej sytuacji bardzo ważne są umiejętności cyfrowe, takie jak korzystanie z narzędzi e-administracji²⁶. Według raportu pt. „Społeczeństwo informacyjne w liczbach Ministerstwa Administracji i Cyfryzacji” kompetencje cyfrowe definiujemy jako zespół kompetencji informacyjnych obejmujących umiejętności wyszukiwania informacji, rozumienia jej, a także oceny jej wiarygodności i przydatności oraz kompetencji informatycznych, na które składają się umiejętności wykorzystywania komputera i innych urządzeń elektronicznych, posługiwania się Internetem oraz korzystania z różnego rodzaju aplikacji i oprogramowania, a także tworzenia treści cyfrowych. Na bardziej ogólnym poziomie można zatem powiedzieć, że na kompetencje informatyczne składają się umiejętności związane z prawidłowym użytkowaniem sprzętu, oprogramowania i korzystania z Internetu²⁷. Kompetencje te są niezbędne w zakresie wdrażania administracji elektronicznej. Rozwój kompetencji cyfrowych to nie tylko wymóg kierowany do administracji publicznej i obywateli chcących aktywnie uczestniczyć w oferowanych przez nią możliwościach cyfrowego załatwiania

²⁶ E. Włodyka, *Dlaczego potrzebujemy e-administracji? Rozwój podstawowych umiejętności cyfrowych pracowników administracji na Pomorzu Zachodnim*, „Acta Politica Polonica” 2021, nr 2(52), s. 97.

²⁷ Ministerstwo Administracji i Cyfryzacji. *Społeczeństwo informacyjne w liczbach*, Warszawa 2014 [online:] https://mac.gov.pl/files/spoleczenstwo_informacyjne_w_liczbach_2014_srodek_lekki.pdf [dostęp: 15.06.2022].

wielu spraw urzędowych²⁸, ale do wszystkich obywateli, którzy również w przyszłości będą korzystać z usług elektronicznych.

Pomiar kompetencji cyfrowych nie jest wcale sprawą prostą, ponieważ wymaga rozwiązania przynajmniej dwóch istotnych problemów. Po pierwsze niezbędne jest dobre zdefiniowanie pojęcia kompetencji cyfrowych, a po drugie znalezienie w miarę obiektywnych metod jego pomiaru²⁹. Kompetencje cyfrowe rozumiane są w Zaleceniach Parlamentu Europejskiego i Rady Europy z dnia 18 grudnia 2006 r. w sprawie kompetencji kluczowych w procesie uczenia się przez całe życie jako „umiejętne i krytyczne wykorzystanie technologii społeczeństwa informacyjnego w pracy, rozrywce i porozumiewaniu się”³⁰. Z raportu Najwyższej Izby Kontroli (NIK) przeprowadzonego w 2022 r. pt. „Działania organów administracji publicznej na rzecz podnoszenia kompetencji cyfrowych społeczeństwa”³¹ wynika, że w 2020 r. Ministerstwo Cyfryzacji, prowadząc prace nad projektem Programu Rozwoju Kompetencji Cyfrowych, wskazało, iż główną barierą dla obywateli w korzystaniu z technologii cyfrowych nie są koszty – te wymienia tylko 22% gospodarstw domowych nieużywających sieci), 68% wskazuje na brak potrzeb, a 52% – właśnie na brak umiejętności. Wykazać należy, że umiejętności cyfrowe są niezbędne do skutecznego korzystania z administracji elektronicznej, jak i obsługi spraw petentów administracji.

²⁸ D. Cendrowicz, *Rozwój e-kompetencji w administracji publicznej na przykładzie pomocy społecznej*, E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2021, s. 78.

²⁹ Strategia Rozwoju Społeczeństwa Informacyjnego Województwa Śląskiego 2020+, Katowice 2016, s. 17.

³⁰ Recommendation of the European Parliament and of the Council of 18 December 2006 on key competences for lifelong learning (2006/962/EC) [online:] <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=-:celex:32006H0962> [dostęp: 20.06.2022].

³¹ Raport Najwyższej Izby Kontroli pt. „Działania organów administracji publicznej na rzecz podnoszenia kompetencji cyfrowych społeczeństwa”, Warszawa 2022.

Bez takich kompetencji trudno będzie brać udział w załatwianiu spraw elektronicznych. Pamiętać należy, że rozwój kompetencji jest bardzo dynamiczny i dostosowany do potrzeb zmieniającego się otoczenia społeczno-gospodarczego.

W celu minimalizowania braku umiejętności informatycznych Minister Cyfryzacji opracował trzy programy, których elementem było m.in. podnoszenie kompetencji cyfrowych społeczeństwa, tj. Program Zintegrowanej Informatyzacji Państwa, Program Rozwoju Talentów Informatycznych na lata 2019–2029 oraz Projekt Programu Rozwoju Kompetencji Cyfrowych do 2030 r. W Programie Zintegrowanej Informatyzacji Państwa na lata 2014–2022 podkreślono, że: „Kompetencje cyfrowe stanowią obecnie czwarty zespół umiejętności bazowych, obok umiejętności czytania i pisania, matematycznych i językowych. (...) Sposobem kształtowania kompetencji cyfrowych jest edukacja cyfrowa, nakierowana na potrzeby różnych grup obywateli. (...) umiejętności cyfrowe obywateli stanowią niezbędny czynnik budujący kapitał społeczny (...) oraz podniesienie konkurencyjności gospodarki”³².

Bezpieczeństwo danych i systemów informatycznych

Kluczowym problemem w zakresie informatyzacji jest również bezpieczeństwo informacji, systemów informatycznych, które związane jest z pojęciem cyberbezpieczeństwa w administracji. Pojęcie „bezpieczeństwo informacyjne” nie doczekało się jednoznacznej wykładni. Często bywa błędnie utożsamiane z bezpieczeństwem informatycznym. W rezultacie tego sposobu rozumienia problemu informacja byłaby chroniona jedynie tam, gdzie ma ona postać elektroniczną. Tymczasem na bezpieczeństwo informacyjne składa się wiele innych procesów, w trakcie których informacja

³² Raport Najwyższej Izby Kontroli, *op. cit.*, s. 6.

jest generowana, modyfikowana i przesyłana (także w formie werbalnej)³³. Bezpieczeństwo informacji definiowane jest w normie PN-ISO/IEC 27000:2014 – 2.33 jako zachowanie poufności, integralności i dostępności informacji, dodatkowo można brać pod uwagę inne własności, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność. Skuteczne zarządzanie bezpieczeństwem informacji polega przede wszystkim na zdiagnozowaniu podatności (ryzyk) systemów informacyjnych na zagrożenia będące naruszeniami wyżej wymienionych czynników oraz na znalezieniu i skutecznym wprowadzeniu rozwiązań likwidujących lub minimalizujących istniejące podatności, a następnie na stałym monitorowaniu stanu bezpieczeństwa³⁴.

Należy tu zwrócić uwagę, że czym innym jest naruszenie bezpieczeństwa, a czym innym naruszenie zabezpieczenia – można naruszyć bezpieczeństwo, a więc w tym kontekście któryś z atrybutów bezpieczeństwa informacji, nie naruszając jego zabezpieczeń, w szczególności jeśli tych nie ma lub jeśli są niekompletne (można je ominąć, tj. wejść w interakcję z systemem w inny niż zabezpieczany sposób)³⁵.

Z Raportu NIK pt. „Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych”³⁶ wynika, że „procesy zapewnienia bezpieczeństwa informacji realizowane były w sposób chaotyczny i – wobec braku procedur – intuicyjny”. Spośród sześciu skontrolowanych jednostek tylko Kasa Rolniczego Ubezpieczenia Społecznego (KRUS) wdrożyła System Zapewnienia Bezpieczeństwa Informacji (SZBI), chociaż

³³ K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 22.

³⁴ A. Czarnecki, *Bezpieczeństwo systemów informatycznych* [w:] *Case Studies w Informatyce*, red. I. Bach-Dąbrowska, Warszawa 2015, s. 414.

³⁵ D. Lisiak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016, s. 35.

³⁶ Raport NIK pt. „Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych”, Warszawa 2016, s. 9.

należy zauważyć, że jego funkcjonowanie było również obciążone istotnymi nieprawidłowościami. W większości zbadanych jednostek (wszystkich poza KRUS) prace nad zapewnieniem odpowiednich warunków bezpieczeństwa informacji przetwarzanych w systemach informatycznych nie osiągnęły właściwego poziomu. Świadomość potrzeby zapewnienia bezpieczeństwa informatycznego była w kontrolowanych jednostkach fragmentaryczna i ograniczona. Chociaż same systemy informatyczne oraz przeprowadzane audyty dostarczały informacji dotyczących stanu bezpieczeństwa, to dane te nie były odpowiednio analizowane i wykorzystywane. Bezpieczeństwo danych było postrzegane głównie jako przedmiot odpowiedzialności i domena działu IT, a nie wszystkich komórek realizujących zadania statutowe, co w dużej mierze utrudniało wypracowanie spójnych dla całej instytucji systemów zarządzania bezpieczeństwem informatycznym. Wprawdzie polityka dotycząca bezpieczeństwa była cały czas rozwijana, to jednak nie towarzyszyły jej adekwatne umiejętności pracowników i rozwój narzędzi niezbędnych do jej realizacji. We wszystkich jednostkach sprawozdawczość dotycząca bezpieczeństwa IT była niekompletna, niezrეტelna, a w niektórych przypadkach obciążona błędami.

W zakresie bezpieczeństwa danych, jak i systemów ochrona powinna podlegać maksymalnie najwyższym standardom ze względu na kwestie ochrony danych osobowych obywateli, a także informacji zebranych w systemach elektronicznych. Zapewnienie poczucia bezpieczeństwa systemu wiąże się z pogłębieniem zaufania obywateli do administracji publicznej oraz świadczonych przez nią usług publicznych. W dobie informatyzacji, jak i powszechnego wykorzystywania komputerów i innych urządzeń elektronicznych pozwalających załatwić sprawy urzędowe należy podejmować działania mające w jak największym zakresie zabezpieczyć prawo obywateli do ochrony informacji. Za J. Gerwatowskim należy przyjąć, że techniki stosowane w cyberprzestępczości rozwijają się coraz szybciej, a organy ścigania nie są w stanie zwalczać cyberprzestępczości

przy użyciu przestarzałych narzędzi operacyjnych. Każdy słaby punkt systemów informatycznych może okazać się dla przestępcy potencjalnym atutem³⁷. Dlatego też obywatele powinni podejmować środki ochrony prywatności, jak i poufności danych, a także ostrożności w zakresie przekazywania danych i ewentualnego nieuprawnionego ich wykorzystania w celu identyfikacji i możliwości zrealizowania sprawy online.

Podsumowanie

Informatyzacja administracji związana jest ze zmianą paradygmatu wykonywania usług publicznych. Elektroniczna administracja staje się narzędziem powszechnym. W ostatnich latach zauważalny jest poziom zwiększenia dostępu do sieci Internet, a także metod identyfikacji w systemach informatycznych przy wykorzystaniu profilu zaufanego. Administracja elektroniczna, tak jak i tradycyjna, nie jest wolna od problemów i wad. Jak wskazano w niniejszym opracowaniu, główne obszary dotyczą zaufania do technologii informatycznych, interoperacyjności i standaryzacji usług, kompetencji cyfrowych, czy też bezpieczeństwa danych i systemów informatycznych. Są to nieliczne problemy w zakresie informatyzacji, jednak dość kluczowe z punktu widzenia budowania świadomości wyboru usług elektronicznych. Wskazane w pracy dane potwierdzają, że przed państwem stoi nadal wiele wyzwań mających na celu wprowadzenie skutecznej i bezpiecznej administracji elektronicznej. Szczególny nacisk powinien zostać położony na świadome społeczeństwo informatyczne, potrafiące sprawnie obsługiwać systemy. Administracja elektroniczna musi udowodnić, że przy wykorzystaniu wszelkiego typu zabezpieczeń jest obszarem bezpiecznym

³⁷ J. Gerwatowski, *Bezpieczeństwo informacyjne w jednostkach samorządu terytorialnego*, „Studia Prawnoustrojowe” 2019, nr 44, s. 93.

i przyjaznym, intuicyjnym i łatwym w użyciu. Pomimo wielu wykazanych pozytywnych cech działania administracji warto byłoby skupić się na stworzeniu jednego uniwersalnego systemu, urzędu wirtualnego (cyfrowego), który pozwoliłby na realizowanie usług elektronicznych. Dużą rolę w tym zakresie będą odgrywały prawidłowo realizowane zasady bezpieczeństwa, a także kadry posiadające niezbędne kompetencje cyfrowe. Rolą państwa w tym zakresie powinno być też tworzenie jednolitych zasad obsługi systemów oraz standaryzowanie usług świadczonych elektronicznie. Doświadczenia pandemii COVID-19 pokazują, że przyszłość administracji i świadczenia usług będzie związana z procesem szeroko pojętej informatyzacji, dlatego państwo powinno stworzyć odpowiednie procedury oraz edukować w zakresie korzystania z e-usług publicznych i obsługi systemów zarówno obywateli, jak i pracowników urzędów administracji.

Bibliografia

Akty normatywne

1. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz.U. z 2021 r. poz. 1797).
2. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r. poz. 344).
3. Ustawa z dnia 12 września 2002 r. o normalizacji (t.j. Dz.U. z 2015 r. poz. 1483).
4. Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz.U. z 2022 r. poz. 902).
5. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz

minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2012 r. poz. 2247).

6. Uchwała nr 16 Rady Ministrów z dnia 5 lutego 2013 r. w sprawie przyjęcia Długookresowej Strategii Rozwoju Kraju „Polska 2030. Trzecia Fala Nowoczesności”, MP z 2013 r., poz. 121.

Literatura przedmiotu

1. Bal-Domańska B., *Wstęp do e-administracji. E-obieg dokumentów w administracji publicznej z wykorzystaniem el-Dok-Systemu*, Wrocław 2015.
2. Banasikowska J., Sołtysik-Piorunkiewicz A., *Zasady interoperacyjności i standaryzacji w systemach wszechobecných e-Government krajów Unii Europejskiej*, „Roczniki Kolegium Analiz Ekonomicznych” 2013, nr 29.
3. Biskup R., Ganczar M., *Komunikacja elektroniczna w postępowaniu administracyjnym*, PiP 2008, nr 1.
4. Celarek K., *Prawne aspekty informatyzacji administracji*, Dąbrowa Górnicza 2009.
5. Cendrowicz D., *Rozwój e-kompetencji w administracji publicznej na przykładzie pomocy społecznej*, E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa. Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego, Wrocław 2021.
6. Czarnecki A., *Bezpieczeństwo systemów informatycznych* [w:] *Case Studies w Informatyce*, red. I. Bach-Dąbrowska, Warszawa 2015.
7. Drobiazgiewicz J., *Oddziaływanie telekomunikacji na administrację* [w:] *Rynek usług telekomunikacyjnych*, red. H. Babis, K. Flaga-Gieruszyńska, Warszawa 2011.
8. Ejdyś J., *Determinanty zaufania do technologii*, „Przegląd Organizacji” 2017, nr 12.
9. Fleszer D., *Wokół problematyki e-administracji*, „Roczniki Administracji i Prawa” 2014, nr 14(1).

10. Ganczar M., *Informatyzacja administracji publicznej. Nowa jakość usług publicznych dla obywateli i przedsiębiorców*, Warszawa 2009.
11. Gerwatowski J., *Bezpieczeństwo informacyjne w jednostkach samorządu terytorialnego*, „*Studia Prawnoustrojowe*” 2019, nr 44.
12. Korczak J., *Pozyskiwanie i umacnianie zaufania do władz publicznych przez współadministrowanie* [w:] *Sprawiedliwość i zaufanie do władz publicznych w prawie administracyjnym*, red. M. Stahl, M. Kasiński, K. Właźlak, Warszawa 2015.
13. Kotulska M., *Wykorzystanie środków komunikacji elektronicznej w postępowaniu administracyjnym*, PPP 2012, nr 9.
14. Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2012.
15. Lisiak-Felicka D., Szmit M., *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016.
16. Mazur Z., Mazur H., *Problemy informatyzacji w sektorze publicznym*, „*Nierówności Społeczne a Wzrost Gospodarczy*” 2015, nr 44(4), cz. 1.
17. Stachowicz M., *Standaryzacja jako czynnik optymalizacji usług świadczonych przez administrację publiczną*, ST 2015, nr 5.
18. Sztompka P., *Zaufanie. Fundament społeczeństwa*, Kraków 2007.
19. Włodyka E., *Dlaczego potrzebujemy e-administracji? Rozwój podstawowych umiejętności cyfrowych pracowników administracji na Pomorzu Zachodnim*, „*Acta Politica Polonica*” 2021, nr 2(52).

Inne

1. Program Zintegrowanej Informatyzacji Państwa [online:] <https://www.gov.pl/web/cyfrizacja/> program-zintegrowanej-informatyzacji-panstwa [dostęp: 22.05.2022].
2. Raport NIK pt. „Działania organów administracji publicznej na rzecz podnoszenia kompetencji cyfrowych społeczeństwa”, Warszawa 2022.
3. Raport NIK pt. „Zapewnienie bezpieczeństwa działania systemów informatycznych wykorzystywanych do realizacji zadań publicznych”, Warszawa 2016.

4. Recommendation of the European Parliament and of the Council of 18 December 2006 on key competences for lifelong learning (2006/962/EC) [online:] <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=-celex:32006H0962> [dostęp: 20.06.2022].
5. Strategia Rozwoju Społeczeństwa Informacyjnego Województwa Śląskiego 2020+, Katowice 2016.
6. Wykorzystanie technologii informacyjno-komunikacyjnych w jednostkach administracji publicznej w 2021 roku, Główny Urząd Statystyczny / Obszary tematyczne / Nauka i technika. Społeczeństwo informacyjne / Społeczeństwo informacyjne / Wykorzystanie technologii informacyjno-komunikacyjnych w jednostkach administracji publicznej w 2021 roku [dostęp: 11.06.2022].

Streszczenie

Aktualnie trudno wyobrazić sobie administrację publiczną wykonującą zadania publiczne wyłącznie w sposób tradycyjny. Zarówno zmiany społeczno-gospodarcze, jak i postęp nowych technologii wymuszają zastosowanie narzędzi informatycznych w procesach funkcjonowania urzędów administracji. Powszechniejsze staje się także korzystanie z e-usług. Działania te ukazują problemy, jakie pojawiają się w zakresie informatyzacji administracji publicznej, w tym samorządowej. Celem niniejszego opracowania jest próba identyfikacji głównych problemów w zakresie informatyzacji administracji. Dotyczą one zaufania technologicznego, standaryzacji i interoperacyjności systemów elektronicznych, współpracy między administracją rządową i samorządową, kadr i ich kompetencji cyfrowych, a także bezpieczeństwa systemów i danych w nich zawartych.

Słowa kluczowe

informatyzacja, administracja samorządowa, cyfryzacja, standaryzacja, e-usługi, bezpieczeństwo cyfrowe

CZĘŚĆ II

SĄDOWNICTWO
W DOBIE INFORMATYZACJI

INFORMATYZACJA POSTĘPOWANIA KARNEGO A PRAWO DO OBRONY

RENATA KUŚPIEL

UCZELNIA ŁAZARSKIEGO



0000-0002-5887-4451

W ostatnich latach obserwuje się gwałtowny rozwój nowoczesnych technologii, szczególnie w zakresie informatyki. Szybki postęp technologiczny, powszechna cyfryzacja, rozległe technologie sieciowe oraz błyskawiczna komunikacja w czasie i przestrzeni powodują, że świat cyfrowy przenika się ze światem fizycznym, wpływając na wszystkie dziedziny życia. Informatyzacja zmieniła metody komunikacji, rozszerzyła sposoby wymiany wiedzy oraz rozwinęła różne modele zarządzania przedsiębiorstwami, a innowacyjne rozwiązania sprawiły, że otworzyły się przed nami nowe, nieznane dotąd możliwości. Rewolucja cyfrowa trwa nadal i obejmuje swym zakresem kolejne dziedziny życia, zatem nieuniknione staje się wykorzystanie nowoczesnych technologii również w zakresie funkcjonowania wymiaru sprawiedliwości. Należy podkreślić, że w tak dynamicznie zmieniającej się rzeczywistości niezwykle ważna jest umiejętność tworzenia oraz dostosowania regulacji prawnych do nowych wymogów współczesności z zachowaniem powszechnie obowiązujących zasad.

Wprowadzenie

Prowadząc rozważania na temat sądów powszechnych w dobie informatyzacji, należy również nawiązać do zmian wprowadzonych w procesie karnym. Jednakże w przeciwieństwie do postępowania cywilnego czy administracyjnego można uznać, że informatyzacja postępowania karnego dopiero się rozpoczyna. Stosowanie narzędzi i rozwiązań informatycznych w procesie karnym warunkowane jest przede wszystkim istnieniem wyraźnych przepisów w kpk¹. Nie ma ani ogólnej, systemowej podstawy prawnej statuującej taką możliwość, ani też nie można jej wywodzić pośrednio z innych regulacji lub praktyki sądowej. Przepisy wskazujące na wykorzystanie nowych technologii wprowadzane są w wyniku kolejnych nowelizacji kpk. Głównym celem ostatnich zmian procedury karnej była nie tyle spójna informatyzacja, co przyspieszenie i usprawnienie procesu karnego, zarówno na etapie postępowania przygotowawczego, jak i sądowego. Z tego też powodu dokonane nowelizacje dotyczyły tylko wybranych przepisów. Niektóre z tych zmian odebrane zostały bardzo pozytywnie. Jednak są i takie, które wzbudziły duże kontrowersje, przede wszystkim w zakresie uwarunkowań konstytucyjnych oraz naczelnych zasad procesu karnego, a w szczególności w kontekście jednej z nich – zasady prawa do obrony. Dlatego też przedmiotem niniejszych rozważań są zmiany wprowadzone w postępowaniu karnym w związku z jego informatyzacją i ich wpływ na realizację prawa do obrony.

¹ Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. Dz.U. z 2022 r. poz. 1375).

Zasada prawa do obrony

Prawo do obrony gwarantuje możliwość przeprowadzenia rzetelnego postępowania karnego. Jest standardem demokratycznego państwa prawa i świadectwem prawidłowego funkcjonowania wymiaru sprawiedliwości. Zostało wyrażone przez normy prawa międzynarodowego, przede wszystkim w art. 14 ust. 3 lit. b i d Międzynarodowego Paktu Praw Obywatelskich i Politycznych², jak również w art. 48 ust. 2 Karty Praw Podstawowych³ oraz w Europejskiej Konwencji Praw Człowieka⁴ w art. 6, w którym to określono minimalny standard prawa do rzetelnego procesu karnego. Na gruncie prawa polskiego gwarancja prawa do obrony uregulowana została w art. 42 ust. 2 Konstytucji RP⁵, a także w art. 6 kpk. Ustawa zasadnicza stanowi, że każdy, przeciw komu prowadzone jest postępowanie karne, ma prawo do obrony we wszystkich stadiach postępowania. „Może on w szczególności wybrać obrońcę lub na zasadach określonych w ustawie korzystać z obrońcy z urzędu. Konstytucyjne prawo do obrony należy rozumieć szeroko, jest ono bowiem nie tylko fundamentalną zasadą procesu karnego, ale też elementarnym standardem demokratycznego państwa prawnego. Prawo to przysługuje każdemu od chwili wszczęcia przeciwko niemu postępowania karnego (w praktyce od chwili przedstawienia zarzutów) aż do wydania prawomocnego wyroku, obejmuje również etap postępowania

² Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. z 1977 r. Nr 38 poz. 167).

³ Karta praw podstawowych Unii Europejskiej z dnia 7 grudnia 2000 r. (Dz.U. UE 2016 C 202/389).

⁴ Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (Dz.U. z 1993 r. Nr 61 poz. 284 z późn. zm.).

⁵ Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. z 1997 r. Nr 78 poz. 483 z późn. zm.).

wykonawczego”⁶. Także zgodnie z art. 6 kpk oskarżonemu przysługuje prawo do obrony, w tym prawo do korzystania z pomocy obrońcy, o czym należy go pouczyć. „Przy czym prawo do obrony przysługuje niezależnie od formalnego uzyskania statusu podejrzanego lub oskarżonego”⁷. „Jest to prawo do ochrony jednostki przed wszelkimi ingerencjami w sferę wolności i praw, jakim zagraża bądź ze swej natury powoduje proces karny. Jest to zatem prawo do obrony człowieka, a nie jego roli czy statusu w procesie karnym”⁸. „Zasada prawa do obrony to dyrektywa, w myśl której oskarżony (podejrzany) ma prawo bronić swych interesów w procesie i korzystać z pomocy obrońcy”⁹. Istota tej zasady polega na umożliwieniu odpierania przedstawianych zarzutów, kwestionowania przemawiających przeciwko niemu dowodów, a także przedstawiania dowodów na poparcie własnych twierdzeń. Jest to jedna z najważniejszych gwarancji współczesnego procesu karnego. „Oznacza obronę przed grozącymi konsekwencjami prawnymi, obronę zarówno osobistą, jak i prowadzoną przy pomocy profesjonalnego i wykwalifikowanego obrońcy. Korzystanie z przysługujących oskarżonemu środków obrony jest jego uprawnieniem, a nie obowiązkiem, konsekwencją czego jest stwierdzenie, że nikt nie może zmusić oskarżonego do ich stosowania, ale z drugiej strony każdy ma obowiązek poszanowania uprawnienia do korzystania z prawa do obrony”¹⁰.

⁶ Wyrok TK z dnia 17 lutego 2004 r., SK 39/02, OTK-A 2004, nr 2, poz. 7.

⁷ W. Wróbel, *Konstytucyjne prawo do obrony w perspektywie prawa karnego materialnego* [w:] *Węzłowe problemy prawa karnego kryminologii i polityki kryminalnej. Księga pamiątkowa ofiarowana Profesorowi Andrzejowi Markowi*, red. V. Konarska-Wrzošek, J. Lachowski, J. Wójcikiewicz, Warszawa 2010, s. 225.

⁸ D. Dudek, *Konstytucyjna wolność człowieka a tymczasowe aresztowanie*, Lublin 1999, s. 202.

⁹ S. Waltoś, P. Hofmański, *Proces karny. Zarys systemu*, Warszawa 2020, s. 313.

¹⁰ P. Wiliński (red.), *Polski proces karny*, Warszawa 2020, s. 347; zob. także: P. Wiliński, *Istota, funkcje i zakres zasady prawa do obrony* [w:] *Idem, Zasada prawa do obrony w polskim procesie karnym*, LEX 2006.

W literaturze przedmiotu¹¹ i orzecznictwie¹² prawo do obrony już tradycyjnie rozpatruje się w dwóch aspektach: materialnym – jako prawo do przeciwstawiania się oskarżeniu oraz formalnym – jako możliwość korzystania z pomocy obrońcy. Można skorzystać z tych form łącznie lub z każdej z nich z osobna. „Warto przy tym zaakcentować, że chociaż prawo do obrony w znaczeniu formalnym jest uprawnieniem oskarżonego do posiadania obrońcy, to jednak wszystkie czynności podejmowane przez obrońcę są przejawem prawa do obrony w znaczeniu materialnym”¹³. „Tym samym oskarżony rozszerza zakres obrony materialnej, włączając w nią działania swego obrońcy. Warunki i zakres korzystania z obrońcy stają się wówczas przesłankami obrony formalnej”¹⁴. Wszystkie te możliwości realizacji prawa do obrony stanowią gwarancje procesowe, zapewniające ochronę praw i interesów uczestników postępowania karnego, a zwłaszcza oskarżonego. Istotne jest, aby proces karny zachował tę gwarancję procesową prawa do obrony, podążając za rozwojem technologicznym.

¹¹ Zob.: S. Waltoś, P. Hofmański, *Proces...*, *op. cit.*, s. 318; K. Dudka, H. Paluszkievicz, *Postępowanie karne*, Warszawa 2017, s. 197; J. Skorupka (red.), *Proces karny*, Warszawa 2020, s. 215.

¹² Zob.: postanowienie SN z dnia 22 października 2014 r., V KK 164/14, LEX nr 1541209: „Podobnie należało ocenić także podniesiony w uzupełnieniu kasacji zarzut rażącego naruszenia art. 6 kpk. Nie ulega wątpliwości, że przepis ten statuuje jedną z podstawowych gwarancji procesowych oskarżonego, jaką jest prawo do obrony w sensie formalnym (prawo do korzystania z pomocy obrońcy), jak i prawo do obrony w sensie materialnym (prawo przeciwstawiania się oskarżeniu)”; wyrok SN z dnia 6 grudnia 2016 r., IV KK 242/16, LEX nr 2180104: „Oskarżonemu przysługuje prawo do obrony, i to zarówno w sensie formalnym, jak i w sensie materialnym, w toku całego procesu, we wszystkich jego fazach, a zatem również w postępowaniu przed sądem odwoławczym”.

¹³ K. Dudka, H. Paluszkievicz, *Postępowanie...*, *op. cit.*, s. 197.

¹⁴ P. Wiliński (red.), *Polski...*, *op. cit.*, s. 349.

Informatyzacja postępowania karnego a prawo do obrony w sensie materialnym

Prawo do obrony w ujęciu materialnym „przejawia się w podejmowaniu wszelkich działań w toku trwania procesu skłaniających się ku polepszeniu sytuacji oskarżonego”¹⁵. Jest „rozumiane jako prawo do przeciwstawiania się tezie oskarżenia i roszczeniom cywilnym oraz wszelkim uciążliwościom procesowym”¹⁶. W ramach obrony materialnej wyróżnia się obronę merytoryczną, która polega na odpieraniu zarzutów, oraz obronę procesową, polegającą na podnoszeniu zarzutów i wskazywaniu uchybień proceduralnych. Wskazuje się na obronę czynną opartą na zwalczaniu zarzutów za pomocą składania wyjaśnień (art. 175 kpk) oraz składaniu wniosków o wykonanie czynności dowodowej (art. 167 kpk) czy zaskarżaniu wydawanych w toku procesu orzeczeń (art. 425 kpk). Wyodrębnia się również obronę bierną, „polegającą na milczeniu, czyli odmowie składania wyjaśnień lub też odmowie udzielenia odpowiedzi na zadane przez sąd, a także pełnomocników stron poszczególne pytania”¹⁷. W celu urzeczywistnienia tak sformułowanego prawa do obrony w sensie materialnym oskarżony posiada wiele uprawnień procesowych wynikających z konkretnych norm kpk. Dlatego też każde zmiany przepisów, również te informatyzujące dokonywanie różnych czynności w toku postępowania, wpływają na realizację prawa do obrony.

Jednym z takich uprawnień procesowych jest prawo dostępu do akt postępowania przygotowawczego oraz sporządzania z nich odpisów lub kopii, a również uzyskania uwierzytelnionych odpisów lub kopii w trybie art. 156 § 5 kpk. Zgodnie z tym przepisem prokurator może udostępnić akta w postaci elektronicznej. Możliwość

¹⁵ A. Sakowicz, *Kodeks postępowania karnego. Komentarz*, Warszawa 2016, s. 41.

¹⁶ J. Skorupka (red.), *Proces karny...*, op. cit., s. 215.

¹⁷ *Ibidem*.

taka została wprowadzona nowelą¹⁸ z 2016 r. Przy czym prokurator będzie zobowiązany do rozważenia, czy taka forma udostępnienia akt nie powoduje zagrożenia dla zabezpieczenia prawidłowego toku postępowania lub ochrony ważnego interesu państwa. Rozwinięciem tej formuły jest „konstrukcja przejrzenia akt, także w postaci elektronicznej, przez podmiot uprawniony przed ewentualnym wniesieniem przezeń zażalenia na odmowę wszczęcia bądź umorzenie postępowania przygotowawczego (art. 306 § 1b kpk) oraz konstrukcja przejrzenia akt, także w postaci elektronicznej, gdy zachodzą podstawy do zamknięcia śledztwa i końcowego zaznajomienia podejrzanego z materiałami postępowania (art. 321 § 1 kpk)”¹⁹. Niemniej jednak widać, że postulat usprawnienia postępowania i zastosowania akt w postaci elektronicznej realizowany jest stopniowo. Z kolei udostępnienie akt w takiej postaci pozwala zdecydowanie lepiej i sprawniej realizować prawo do obrony. Pomimo pozytywnej oceny przyjętego rozwiązania warto zwrócić uwagę, że wymaga ono jeszcze doprecyzowania albo wypracowania pewnych standardów. Po pierwsze kpk nie definiuje postaci elektronicznej akt oraz informacji w nich zawartych. Po drugie, jak można zauważyć, istnieją różne możliwości udostępnienia akt w postaci elektronicznej i istotne jest określenie, kiedy miało miejsce ich doręczenie. Jednak kpk całkowicie pomija tę kwestię. Po trzecie nie została również określona forma powiadomienia uczestnika postępowania o możliwości zapoznania się z aktami w formie elektronicznej. Wydaje się, że wymagane byłoby doręczenie pisma, które informuje o takiej sposobności, ale do tego pisma należałoby już zastosować przepisy o doręczeniach tradycyjnych, czy też doręczeniach za pomocą poczty elektronicznej.

¹⁸ Ustawa z dnia 11 marca 2016 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (Dz.U. z 2016 r. poz. 437).

¹⁹ M. Nawrocki, *Informatyzacja postępowania karnego* [w:] *Prawo nowych technologii*, red. K. Flaga-Gieruszyńska, J. Gołaczyński, Warszawa 2021, s. 230–231.

Wprowadzenie nowych rozwiązań nie dotyczy tylko postępowania przygotowawczego, lecz wpływa na wszystkie etapy postępowania karnego. W zakresie dostępności akt kolejnym przykładem informatyzacji jest możliwość uzyskania informacji za pomocą systemu teleinformatycznego o sprawie toczącej się przed sądem karnym. Znowelizowany²⁰ również w 2016 r. art. 156 § 1 kpk przedstawia uprawnienie procesowe oskarżonego mówiące o tym, że stronom, obrońcom, pełnomocnikom i przedstawicielom ustawowym, a za zgodą prezesa sądu również innym osobom, udostępnia się akta sprawy sądowej oraz daje możliwość sporządzenia z nich odpisów lub kopii. W drugim zdaniu przepis ten stanowi, że informacje o aktach sprawy mogą być udostępnione także za pomocą systemu teleinformatycznego, jeżeli względy techniczne nie stoją temu na przeszkodzie. Należy się zgodzić z opinią, że jest to słuszne rozwiązanie, ponieważ wykorzystuje nowe technologie oraz narzędzia komunikacji na odległość, które są już powszechne w innych postępowaniach i obecne w komunikacji z organami państwowymi (m.in. ePUAP²¹)²². Jednakże na kanwie tego przepisu pojawiły się wątpliwości interpretacyjne odnośnie do różnicy między sformułowaniem „akt w postaci elektronicznej” a „informacją o aktach sprawy”. Z jednej strony wskazuje się, że omawiany przepis 156 § 1 kpk *in fine* należy rozumieć jako prawną możliwość udzielenia informacji nie o samych aktach sprawy, ale też o ich zawartości²³.

²⁰ Ustawa z dnia 11 marca 2016 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (Dz.U. z 2016 r. poz. 437).

²¹ Elektroniczna Platforma Usług Administracji Publicznej – system teleinformatyczny, w którym instytucje publiczne udostępniają usługi przez pojedynczy punkt dostępowy w sieci Internet; podstawą prawną funkcjonowania ePUAP jest ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r. poz. 2070) [online:] <https://epuap.gov.pl/wps/portal> [dostęp: 31.08.2022].

²² Zob. też: M. Nawrocki, *Informatyzacja...*, op. cit., s. 230.

²³ *Ibidem*.

Z drugiej zaś strony dostrzega się różnicę między tymi zwrotami. „Odwołując się do wykładni literalnej można ocenić, że przepis ten jest rozumiany jako uzyskanie informacji o aktach sprawy – nie o treści samych akt”²⁴. Właśnie z takim poglądem należałoby się zgodzić, analizując również inne przepisy kpk, bowiem możliwość udostępnienia akt w postaci elektronicznej wskazywana jest w ustawie wprost, tak jak w art. 156 § 5 kpk. Natomiast w art. 156 § 1 kpk ustawodawca nie posłużył się tym zwrotem. Chodzi zatem o udostępnienie ogólnych informacji o aktach, a nie o sposób udostępnienia tych akt. Poza tym w kontekście art. 156 kpk warto również zauważyć, że wykorzystane tu możliwości użycia systemu teleinformatycznego, czy też elektronicznej postaci akt, nie stanowią jednoznacznie normatywnej podstawy dla wprowadzenia elektronicznych doręczeń pism, czy też odpisów orzeczeń i zarządzeń wydanych w danej sprawie, ponieważ przepis ten nie jest *lex specialis* wobec art. 128 § 1 kpk.

Niemniej jednak z możliwością wykorzystania systemu teleinformatycznego oraz udostępnienia akt w formie elektronicznej związany jest temat doręczeń elektronicznych, dla których również istnieją już uregulowania w kpk. Ustanowienie zasad doręczeń ma przede wszystkim charakter gwarancyjny względem uczestników postępowania. Umożliwia udział w rozprawie i posiedzeniu oraz podejmowanie odpowiednich czynności procesowych, a tym samym wpływa na skuteczność realizacji prawa do obrony. Podejmując temat doręczeń elektronicznych w postępowaniu karnym, trzeba jednak zaznaczyć, że aktualnie kpk nie reguluje w sposób kompleksowy rozwiązań w tym zakresie. Należy to ocenić negatywnie, ponieważ skutki, jakie wywołuje ta czynność procesowa, są zbyt istotne, by regulacje w zakresie doręczeń elektronicznych

²⁴ M. Kurowski, *Komentarz do art. 156 [w:] Kodeks postępowania karnego. Tom 1. Komentarz aktualizowany*, red. D. Świecki, LEX 2021. Zob. też: J. Kisiel, *Doręczenia elektroniczne w Kodeksie postępowania karnego*, „Palestra” 2021, nr 9, s. 50.

były wprowadzane w sposób wybiórczy, ograniczony tylko do niektórych pism procesowych. Poza tym „przepisy o doręczeniach są stosowane tylko jednostronnie – pomiędzy sądem a uczestnikami postępowania”²⁵. „Aktualnie kpk nie daje możliwości skutecznego składania przez strony i inne uprawnione osoby pism procesowych drogą elektroniczną lub przy użyciu podpisu elektronicznego”²⁶. Takie stanowisko zostało potwierdzone też w orzecznictwie Sądu Najwyższego, gdzie wyraźnie wskazano, że „nie wywołuje skutku procesowego w postaci wniesienia środka odwoławczego oświadczenie procesowe strony, przesłane w formie dokumentu elektronicznego, albowiem zarówno w procedurze wykroczeniowej, jak i w procedurze karnej taka forma czynności procesowej nie jest przewidziana”²⁷. Przy czym „środek odwoławczy może być wniesiony za pomocą telefaksu, jednak skuteczność tego pisma procesowego warunkuje uzupełnienie wymogu formalnego, polegającego na złożeniu na nim własnoręcznego podpisu przez wnoszącego środek”²⁸.

Ustawodawca, dążąc do wprowadzenia doręczeń elektronicznych, przede wszystkim znowelizował²⁹ art. 119 § 1 pkt 2 kpk, dodając wymóg wskazania w piśmie procesowym obok adresu również numeru telefonu, telefaksu oraz adresu poczty elektronicznej lub złożenia oświadczenia o ich nieposiadaniu. Regulacja ta może wzbudzać pewne wątpliwości. „O ile wskazanie numeru telefonu nie budzi zastrzeżeń, o tyle podanie pozostałych danych powinno być uzależnione od zgody wnoszącego pismo na taką formę

²⁵ H. Mazur, *Doręczenia w procesie karnym XXI wieku*, „Palestra” 2011, nr 3–4, s. 109.

²⁶ M. Kurowski, *Komentarz do art. 132 [w:] Kodeks postępowania karnego. Tom 1. Komentarz aktualizowany*, red. D. Świecki, LEX 2021.

²⁷ Postanowienie SN z dnia 26 marca 2009 r., I KZP 39/08, OSNKW 2009, nr 5, poz. 36.

²⁸ Uchwała SN z dnia 20 grudnia 2006 r., I KZP 29/06, OSNKW 2007, nr 1, poz. 1.

²⁹ Ustawa z dnia 19 lipca 2019 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (Dz.U. z 2019 r. poz. 1694).

kontaktu”³⁰. Z kolei w przypadku art. 119 § 1 kpk już samo przekazanie danych jest uznawane za wyrażenie zgody na taki sposób doręczenia pism oraz stwarza obowiązek odbierania i odczytywania nadawanej tak korespondencji. Stosownie bowiem do art. 132 § 3 kpk, wprowadzonego nowelą³¹ z 2003 r., pismo może być także doręczone za pośrednictwem telefaksu lub poczty elektronicznej. Jednocześnie w takim wypadku dowodem doręczenia jest potwierdzenie transmisji danych. Przy czym w literaturze przedmiotu wskazuje się, że sformułowanie „potwierdzenie transmisji danych” ma tak wiele możliwych znaczeń, że nie sposób ustalić, o które chodziło ustawodawcy. Nie uregulowano bowiem kwestii, w którym momencie dochodzi do skutecznego doręczenia wiadomości za pomocą telefaksu lub poczty elektronicznej. Pod pojęciem „transmisja danych” należy *de facto* rozumieć każde przesłanie danych pomiędzy urządzeniami. „Na gruncie analizowanego przepisu może to oznaczać zarówno samo wysłanie wiadomości przez nadawcę, jak i odebranie tej wiadomości przez odbiorcę”³². Sąd Najwyższy miał możliwość analizy powyższego problemu i orzekł, że „doręczenie pism uczestnikom procesu karnego drogą elektroniczną następuje już z chwilą «pomyślnego» zakończenia procesu transmisji danych, tj. przekazania drogą mailową na wskazany adres jakiegoś dokumentu, a nie dopiero z chwilą gdy odbiorca zapoznał się z treścią przesłanego mu mailem lub faxem dokumentu”³³. W doktrynie dodatkowo podkreśla się, że mimo iż przepis art. 132 § 3 kpk nie przewiduje ograniczenia przedmiotowego w zakresie

³⁰ B. Janusz-Pohl, P. Kosmatka, *Zmiany w prawie karnym procesowym – analiza z perspektywy zasady koncentracji*, „Prawo w Działaniu” 2021, nr 47, s. 18–19.

³¹ Ustawa z dnia 10 stycznia 2003 r. o zmianie ustawy – Kodeks postępowania karnego, ustawy – Przepisy wprowadzające Kodeks postępowania karnego, ustawy o świadku koronnym oraz ustawy o ochronie informacji niejawnych (Dz.U. z 2003 r. Nr 17 poz. 155 z późn. zm.).

³² J. Kisiel, *Doręczenia...*, *op. cit.*, s. 50.

³³ Postanowienie SN z dnia 22 listopada 2018 r., I DSI 9/18, LEX nr 2583145.

doręczenia pism procesowych, co sugerowałoby, że może być stosowany do wszystkich pism procesowych, to nie bez znaczenia pozostaje art. 128 § 1 kpk, który wskazuje, iż doręczenie orzeczeń i zarządzeń następuje tylko w postaci uwierzytelnionych ich odpisów. W konsekwencji „orzeczenia oraz zarządzenia nie mogą być doręczane za pośrednictwem telefaksu lub poczty elektronicznej, zwłaszcza gdy od dnia doręczenia pisma biegnie termin procesowy”³⁴.

Podobne zastrzeżenia dotyczą przesyłania odpisów aktu oskarżenia, ponieważ prawo do informacji o treści zarzutu jest przesłanką realizacji prawa do obrony w ujęciu materialnym. Tymczasem wprowadzona w 2021 r. nowelizacja³⁵ procedury karnej rozszerzyła art. 338 kpk o § 4 i § 5, mówiące o tym, że możliwe jest doręczenie odpisu aktu oskarżenia oskarżonemu na adres poczty elektronicznej. Podobnie, zgodnie z art. 334 § 2a kpk, odpisy aktu oskarżenia mogą być przesłane sądowi w postaci elektronicznej, z wyłączeniem odpisów przeznaczonych dla adresatów, którzy w dniu przesłania sądowi aktu oskarżenia są pozbawieni wolności lub których adresu poczty elektronicznej nie ustalono. „Projektodawca uzasadniał proponowaną zmianę potrzebą przyspieszenia postępowań oraz ograniczenia nakładów finansowych. Natomiast wyłączenie z zakresu zastosowania powyższego przepisu podmiotów pozbawionych wolności lub których adresów e-mail nie udało się ustalić ma mieć dla stron charakter gwarancyjny”³⁶. Podobnie art. 338 § 5 kpk ma pełnić funkcję gwarancyjną wobec doręczenia odpisu aktu oskarżenia w trybie art. 338 § 4 kpk. Skoro bowiem ustawa przewiduje do takiego doręczenia zastosowanie art. 132 § 3 kpk, to

³⁴ M. Nawrocki, *Informatyzacja...*, op. cit., s. 229; zob. też: M. Kurowski, *Komentarz do art. 132 [w:] Kodeks postępowania karnego. Tom 1. Komentarz aktualizowany*, red. D. Świecki, LEX 2021.

³⁵ Ustawa z dnia 20 kwietnia 2021 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz.U. z 2021 r. poz. 1023).

³⁶ B. Janusz-Pohl, P. Kosmatka, *Zmiany...*, op. cit., s. 19.

w takim przypadku dowodem doręczenia odpisu aktu oskarżenia będzie potwierdzenie transmisji danych. Dodatkowo, zgodnie z art. 338 § 5 kpk, o dacie doręczenia odpisu aktu oskarżenia oraz adresie poczty elektronicznej, na który odpis został wysłany, należy zawiadomić adresata za pośrednictwem operatora pocztowego, a w uzasadnionych wypadkach telefonicznie. Wymóg wynikający z art. 338 § 5 kpk ma jednak tylko „charakter informacyjny i nie wpływa na skuteczność doręczenia odpisu aktu oskarżenia, gdyby organ procesowy zaniechał zawiadomienia lub brak było w aktach sprawy potwierdzenia jego odbioru. W przepisie tym mowa jest bowiem o zawiadomieniu o dacie doręczenia, a zatem jest to tylko informacja o dokonanej już czynności doręczenia”³⁷.

Dlatego też dotychczas wprowadzone zmiany w zakresie doręczeń elektronicznych oceniane są negatywnie – przede wszystkim za ich wybiórczość i brak kompleksowego rozwiązania. Poza tym wprowadzone dotąd rozwiązania nie zostały ujęte w ustawie o doręczeniach elektronicznych³⁸, która w sposób spójny reguluje kwestię doręczeń elektronicznych również w postępowaniu karnym. Odnajdziemy tam natomiast przepisy odnoszące się do postępowania karnego, które wejdą w życie dopiero w 2029 r. Tym samym docelowe rozwiązanie dla doręczeń elektronicznych w procesie karnym zostanie dopiero wypracowane. Widząc proponowany zakres zmian w przepisach i odnosząc go do gwarancji prawa do obrony, można stwierdzić, że wpłyną one nie tylko na realizację obrony materialnej, ale również na działania w zakresie obrony formalnej.

³⁷ K. Eichstaedt, *Komentarz do art. 338 [w:] Kodeks postępowania karnego. Tom 1. Komentarz aktualizowany*, red. D. Świecki, LEX 2021.

³⁸ Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (Dz.U. z 2022 r. poz. 569 z późn. zm.).

Informatyzacja postępowania karnego a prawo do obrony w sensie formalnym

Prawo do obrony w ujęciu formalnym wyraża się w możliwości ustanowienia obrońcy z wyboru (art. 83 kpk), jak też w możliwości zawnioskowania o przydzielenie obrońcy z urzędu (art. 78–81 kpk), które przysługuje oskarżonemu i podejrzanemu (art. 71 § 3 kpk). Tym samym oskarżony może wybrać obrońcę bądź też żądać przyznania mu obrońcy z urzędu, gdy nie stać go na poniesienie kosztów działania obrońcy z wyboru. W kontekście obrony formalnej oraz uprawnienia do korzystania z obrońcy z urzędu należy zauważyć i pozytywnie ocenić zmiany³⁹ dokonane w art. 81a § 3 kpk dotyczące zapewnienia w płaszczyźnie normatywnej natychmiastowego podjęcia obrony. W przywołanym przepisie ustawodawca przyjął, że jeżeli okoliczności sprawy wskazują na konieczność natychmiastowego podjęcia obrony, wniosek o wyznaczenie obrońcy, a także inne dokumenty niezbędne do rozpoznania wniosku mogą być przekazane przez organ prowadzący postępowanie przygotowawcze do właściwego sądu za pośrednictwem telefaksu lub poczty elektronicznej. Prezes sądu, sąd lub referendarz sądowy powiadamia w sposób wskazany w art. 137 kpk oskarżonego oraz obrońcę o wyznaczeniu obrońcy z urzędu. A zatem w celu natychmiastowego podjęcia obrony można wykorzystać możliwości, jakie daje informatyzacja. Dodatkowo przepis art. 137 kpk umożliwia wezwanie lub zawiadomienie osób telefonicznie albo w inny sposób, stosownie do okoliczności, pozostawiając w aktach odpis nadanego komunikatu z podpisem osoby nadającej. Niewątpliwie rozwiązanie przyjęte w art. 81a § 3 kpk „usprawnia komunikację między organem prowadzącym postępowanie przygotowawcze a sądem

³⁹ Ustawa z dnia 19 lipca 2019 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (Dz.U. z 2019 r. poz. 1694).

właściwym do rozpoznania wniosku”⁴⁰. Poza tym, jak słusznie zauważa się w literaturze przedmiotu, „ma ono szanse realnie wpłynąć na zapewnienie oskarżonemu szybkiego kontaktu z wyznaczonym z urzędu obrońcą, a tym samym na lepsze zagwarantowanie prawa do obrony”⁴¹. Nowelizacja art. 81a § 3 kpk to niejedynie zmiany w postępowaniu karnym, gdzie można dostrzec wpływ nowych technologii na realizację obrony formalnej.

Ustawą o zmianie ustawy o bezpieczeństwie imprez masowych oraz niektórych innych ustaw⁴² została wprowadzona do kpk „rozprawa odmiejskowiona”, stanowiąca jedną z form prowadzenia postępowania przyspieszonego. Jej założeniem było prowadzenie rozprawy w dwóch różnych miejscach (miejscu przebywania oskarżonego i siedzibie sądu) połączonych za pomocą urządzeń technicznych umożliwiających przekazywanie obrazu oraz dźwięku na odległość. Zgodnie z art. 517b § 2a kpk można odstąpić od przymusowego doprowadzenia do sądu sprawcy ujętego na gorącym uczynku bądź w bezpośrednim pościgu, jeżeli zostanie zapewnione jego uczestniczenie zdalne we wszystkich czynnościach sądowych, w których ma on prawo uczestniczyć, a w szczególności złożenie przez niego wyjaśnień. W takim wypadku we wszystkich czynnościach sądowych przy użyciu urządzeń technicznych bierze udział w miejscu przebywania sprawcy referendarz sądowy lub asystent sędziego zatrudniony w sądzie, w którego okręgu przebywa sprawca. Obrońca natomiast uczestniczy w sposób zdalny w czynnościach sądowych w miejscu przebywania sprawcy. Rozwiązania przyjęte w zakresie „rozprawy odmiejskowanej” były krytykowane szczególnie w kontekście gwarancji rzetelnego procesu sądowego.

⁴⁰ J. Mierzwińska-Lorencka, *Kodeks postępowania karnego. Komentarz do nowelizacji 2019, art. 81(a)*, LEX 2020.

⁴¹ J. Zagrodnik, Ł. Chmielniak, M. Klonowski, A. Rychlewska-Hotel, *Kodeks postępowania karnego. Komentarz praktyczny do nowelizacji 2019, art. 81(a)*, LEX 2020.

⁴² Ustawa z dnia 31 sierpnia 2011 r. o zmianie ustawy o bezpieczeństwie imprez masowych oraz niektórych innych ustaw (Dz.U. z 2011 r. Nr 217 poz. 1280).

Jednak zmian w art. 517b kpk nie wprowadzono. Jednakże mocą ustawy związanej z przeciwdziałaniem rozprzestrzenianiu się epidemii koronawirusa w Polsce ustawodawca zdecydował się rozszerzyć instytucję „rozprawy odmiejscowionej” stosowanej w trybie przyspieszonym na rozprawy prowadzone w postępowaniu zwyczajnym.

Na mocy ustawy z dnia 19 czerwca 2020 r.⁴³ znowelizowano art. 374 kpk dotyczący obecności oskarżonego na rozprawie. Dopuszczono możliwość zdalnego uczestniczenia w rozprawie nie tylko oskarżonego, czy też jego obrońcy, lecz również oskarżyciela publicznego, posiłkowego i prywatnego oraz tłumacza, a tym samym umożliwiono przeprowadzanie rozpraw zdalnych na gruncie postępowania karnego. Obecnie rozprawa może przyjmować cztery formy: stacjonarną, stacjonarną z elementami zdalnymi (kiedy sąd i strony postępowania są na sali, a zdalnie odbywa się przesłuchanie świadków), hybrydową (kiedy sąd i jedna ze stron postępowania są na sali, a druga strona postępowania uczestniczy zdalnie) oraz wirtualną salę rozpraw (kiedy sąd i strony postępowania uczestniczą w rozprawie zdalnie, zdalnie również odbywa się przesłuchanie świadków). Rozprawa w formie stacjonarnej, czy też stacjonarnej z elementami zdalnymi nie jest niczym nowym w postępowaniu karnym. Przesłuchanie świadka przy użyciu urządzeń technicznych jest możliwe już od dawna w trybie art. 177 § 1a kpk. Przy czym należy pamiętać, że takie przesłuchanie odbywa się inaczej niż w postępowaniu cywilnym. Otóż w postępowaniu karnym w tej czynności, w miejscu przebywania świadka, bierze udział referendarz sądowy, asystent sędziego lub urzędnik zatrudniony w sądzie, w którego okręgu świadek przebywa. Regulacja ta

⁴³ Ustawa z dnia 19 czerwca 2020 r. o dopłatach do oprocentowania kredytów bankowych udzielanych przedsiębiorcom dotkniętym skutkami COVID-19 oraz o uproszczonym postępowaniu o zatwierdzenie układu w związku z wystąpieniem COVID-19 (Dz.U. z 2022 r. poz. 171 z późn. zm.).

jest oceniana pozytywnie i wskazuje się, że właśnie obecność referendarza sądowego, asystenta sędziego lub urzędnika nadaje wiarygodności zeznaniom. *Novum* w postępowaniu karnym stanowią rozprawa w formie hybrydowej i w formie wirtualnej sali rozpraw, uregulowane w art. 374 § 3–8 kpk. Tak jak przy „rozprawie odmiejscowionej”, tak i w tej rozprawie bierze udział, w miejscu przebywania strony, referendarz sądowy lub asystent sędziego, zatrudniony w sądzie, w którego okręgu strona przebywa.

Analogicznie do „rozprawy odmiejscowionej” rozwiązania przyjęte dla instytucji rozprawy zdalnej są oceniane negatywnie. Zauważa się „uprzywilejowanie prokuratora wobec innych stron i uczestników procesu, gdyż jego wniosek o umożliwienie mu udziału w rozprawie w formie wideokonferencji jest dla sądu wiążący, co stanowi nieuzasadniony przejaw dominacji oskarżyciela publicznego nad przewodniczącym i sądem”⁴⁴. Zgodnie bowiem z brzmieniem art. 374 § 3 kpk przewodniczący, na wniosek prokuratora, „wyraża zgodę” na jego udział w rozprawie przy użyciu urządzeń technicznych. Poza tym wyraźnie widoczne są ograniczenia w możliwościach realizacji prawa do obrony. Zgodnie z art. 374 § 6 kpk obrońca bierze udział w rozprawie przeprowadzanej w sposób zdalny w miejscu przebywania oskarżonego, chyba że stawi się w tym celu w sądzie. Tym samym ustawodawca pozostawił obrońcy wybór. Jednakże niezależnie od podjętej decyzji zagrożone będzie prawo oskarżonego do obrony, ponieważ jeśli obrońca będzie w miejscu pobytu oskarżonego, poza salą rozpraw, może to wzbudzać wątpliwości w kontekście zachowania wymogów efektywnej obrony i zasady kontrydiktoryjności. Z kolei obecność obrońcy w siedzibie sądu uniemożliwia mu bezpośredni kontakt z oskarżonym. Ustawodawca najwyraźniej dostrzegł ten

⁴⁴ C. Kulesza, *Rozprawa zdalna oraz zdalne posiedzenie aresztowe w świetle konwencyjnego standardu praw oskarżonego*, „Białostockie Studia Prawnicze” 2021, vol. 26, nr 3, s. 213.

problem, dlatego też wprowadził art. 374 § 7 kpk mówiący o tym, że sąd może zarządzić przerwę, aby umożliwić telefoniczny kontakt obrońcy z oskarżonym, chyba że złożenie takiego wniosku w sposób oczywisty nie służy realizacji prawa do obrony. Niestety trudno jest określić, w oparciu o jakie przesłanki sąd miałby podejmować decyzję o odmowie zarządzenia przerwy przy tak generalnie zakreślonym kryterium. Poza tym powstaje dodatkowe pytanie: jak przekonać sąd o realizacji prawa do obrony, nie zdradzając tajemnicy obrończej? „Jest to istotny problem, gdyż biorąc pod uwagę literalne brzmienie tego przepisu, należy uznać, że o zarządzeniu przerwy decyduje sąd (a nie przewodniczący), a więc negatywna decyzja sądu w przedmiocie wniosku obrońcy będzie niezaskarżalna. W związku z powyższym naruszenie prawa do obrony w drodze takiej decyzji może być podniesione jedynie w apelacji na podstawie art. 447 § 4 kpk”⁴⁵. W kontekście art. 374 § 7 kpk pojawił się pomysł istnienia dwóch obrońców, jednak nie może to być rozwiązanie docelowe i stanowiące obowiązujący standard. Powszechną praktyką w toku rozprawy jest konsultowanie się obrońcy i oskarżonego. Przyjęty zdalny tryb rozprawy w sposób oczywisty to uniemożliwia. Sąd Najwyższy zauważył, że prawo do obrony, w tym korzystania z pomocy obrońcy, winno być realne. Sąd nie może dopuścić do wykonywania obowiązków obrońcy w sytuacji wyrażnie wskazującej, że obrona może nie mieć realnego charakteru. „Obecność obrońcy oskarżonego może być uznana za wystarczającą tylko wtedy, gdy obrońca rzeczywiście może wypełniać swoje obowiązki”⁴⁶. Podobnie w kwestii realizacji obrony formalnej wypowiedział się Trybunał Konstytucyjny i wyjaśnił, że „charakter działań obrońcy determinowany jest interesem prawnym oskarżonego, dla którego ochrony przepisy procedury karnej przewidują

⁴⁵ J. Zagrodnik, *Komentarz do art. 374 [w:] Kodeks postępowania karnego. Komentarz aktualizowany*, red. J. Skorupka, Legalis 2018.

⁴⁶ Wyrok SN z dnia 7 lipca 2006 r., III KK 418/05, LEX nr 193010.

szereg koniecznych uprawnień. Uprawnienia obrońcy to nie tylko możliwość przeglądania akt postępowania karnego, czy też zapoznawania się z materiałem dowodowym, ale przede wszystkim kontakt z jego mocodawcą. To na podstawie osobistego kontaktu, obrońca pozyskuje faktyczną wiedzę o czynie sprawcy oraz okolicznościach zdarzenia będącego przedmiotem postępowania, buduje strategię obrony, zgłasza wnioski dowodowe i współdziała z innymi obrońcami występującymi w sprawie⁴⁷. Również zdaniem Helsińskiej Fundacji Praw Człowieka „pozostawienie w rękach sądu możliwości decydowania o tym, kiedy kontakt obrońcy z klientem jest zasadny, stanowił będzie prostą drogę do naruszenia prawa do obrony, a w niektórych sprawach wręcz uznania takiego procesu za nierzetelny”⁴⁸.

W podobny sposób jak rozprawa zdalna zostało ukształtowane zdalne posiedzenie aresztowe, przy czym jego regulacje jeszcze mocniej godzą w prawo do obrony. Zgodnie z art. 250 § 3b kpk można odstąpić od przymusowego doprowadzenia do sądu podejrzanego, jeżeli zostanie zapewniony jego udział w posiedzeniu, w szczególności złożenie przez niego wyjaśnień przy użyciu urządzeń technicznych, umożliwiających przeprowadzenie tego posiedzenia na odległość z jednoczesnym bezpośrednim przekazem obrazu i dźwięku. W takim posiedzeniu również bierze udział, w miejscu przebywania podejrzanego, referendarz sądowy lub asystent sędziego zatrudniony w sądzie, w którego okręgu przebywa podejrzany, lub funkcjonariusz Służby Więziennej, jeżeli podejrzany przebywa w zakładzie karnym lub areszcie śledczym. Natomiast zgodnie z art. 250 § 3d kpk obrońca bierze udział w posiedzeniu zdalnym w miejscu przebywania oskarżonego, chyba że obrońca

⁴⁷ Wyrok TK z dnia 17 lutego 2004 r., SK 39/02, OTK-A 2004, nr 2, poz. 7.

⁴⁸ Uwagi Helsińskiej Fundacji Praw Człowieka z dnia 14 czerwca 2020 r., Druk Senacki nr 142, s. 8 [online:] <https://www.hfhr.pl/wp-content/uploads/2020/06/druk-senacki-nr-142-uwagi-HFPC-1.pdf> [dostęp: 31.08.2022].

stawi się w tym celu w sądzie lub sąd zobowiąże go do udziału w posiedzeniu w budynku sądu z uwagi na konieczność uchylenia ryzyka nierozstrzygnięcia wniosku w przedmiocie zastosowania tymczasowego aresztowania przed upływem dopuszczalnego czasu zatrzymania oskarżonego. Uregulowania te wskazują na ograniczenia w swobodzie wyboru miejsca obrońcy oraz ograniczenie kontaktu z oskarżonym. W wypadku gdy obrońca przebywa w innym miejscu niż oskarżony, kodeks również przewiduje możliwość zarządzenia przez sąd, na wniosek obrony, przerwy na kontakt telefoniczny oskarżonego z obrońcą. Jednakże w tym przypadku, zgodnie z art. 250 § 3e kpk, sąd może nie uwzględnić prośby ze względu na ryzyko nierozstrzygnięcia wniosku o tymczasowe aresztowanie przed upływem dopuszczalnego czasu zatrzymania podejrzanego. Sąd ma bowiem 24 godziny (art. 248 § 2 kpk) na rozpoznanie wniosku w przedmiocie tymczasowego aresztowania, w związku z czym istnieje możliwość, że oskarżony nie będzie mógł skontaktować się z obrońcą, a tym samym nie będzie mógł w pełni realizować swojego prawa do obrony, szczególnie w aspekcie formalnym.

Dopełnieniem regulacji zdalnego posiedzenia aresztowego jest rozwiązanie wprowadzone w celu doręczenia postanowienia o tymczasowym aresztowaniu. Przywołany już art. 248 § 2 kpk wskazuje, że zatrzymanego należy zwolnić, jeżeli w ciągu 24 godzin od przekazania go do dyspozycji sądu nie doręczono mu postanowienia o zastosowaniu wobec niego tymczasowego aresztowania albo nie ogłoszono mu tego postanowienia na posiedzeniu przeprowadzonym w sposób określony w art. 250 § 3b kpk, czyli w trybie zdalnego posiedzenia aresztowego. Zatem ustawodawca wprowadził możliwość „doręczenia” albo „ogłoszenia” postanowienia o zastosowaniu tymczasowego aresztowania. Jednakże art. 41 ust. 3 Konstytucji RP wyraźnie przewiduje tylko jedną ewentualność, a mianowicie doręczenie postanowienia o tymczasowym aresztowaniu. Dlatego też, ze względu na omówione uchybienia, zarówno rozprawa zdalna, jak i zdalne posiedzenie aresztowe są

szeroko krytykowane. Na przedstawione problemy zwróciła uwagę nie tylko Helsińska Fundacja Praw Człowieka, ale również Rzecznik Praw Obywatelskich⁴⁹ oraz Naczelna Rada Adwokacka⁵⁰, wskazując na naruszenia podstawowych gwarancji konstytucyjnych, w tym przede wszystkim prawa do obrony oraz prawa do rzetelnego procesu karnego. Jednakże przepisy te nadal obowiązują, a informatyzacja procesu karnego trwa.

Podsumowanie

Postępowanie karne, wzorem innych procedur, stara się podążać za rozwojem technologicznym i wprowadzać coraz więcej przepisów informatyzujących dokonywanie czynności procesowych. W wyniku kolejnych nowelizacji proces karny *sensu largo* został wzbogacony o rozwiązania umożliwiające wykorzystanie różnych systemów informatycznych. Jak wynika z przeprowadzonej analizy, niektóre z tych zmian odbierane są bardzo pozytywnie, bowiem przyczyniają się do usprawnienia postępowania, ale jednocześnie zachowują gwarancje procesowe, szczególnie w zakresie zasady prawa do obrony. Udostępnienie akt postępowania przygotowawczego w postaci elektronicznej, czy też udostępnienie informacji

⁴⁹ Koronawirus. Uwagi RPO dla Senatu do Tarczy Antykryzysowej 4.0 [online:] <https://bip.brpo.gov.pl/sites/default/files/Opinia%20RPO%20ws.%20Tarczy%20Antykryzysowej%204.0%20dla%20Marsza%20C5%82ka%20Senatu%20C%2012.06.2020.pdf> [dostęp: 31.08.2022].

⁵⁰ M. Gałęski, P. Karlik, *Opinia Komisji Legislacyjnej przy Naczelnej Radzie Adwokackiej dotycząca projektowanego artykułu 34 pkt 4 ustawy o dopłatach do oprocentowania kredytów bankowych udzielanych na zapewnienie płynności finansowej przedsiębiorcom dotkniętym skutkami COVID-19 oraz o zmianie niektórych innych ustaw (druk 382)* [online:] https://www.adwokatura.pl/admin/wgrane_pliki/file-20200608-u-o-doplatach-do-oprecent-kredytow-tarcza-04-sm-24-20-29964.pdf [dostęp: 31.08.2022].

o aktach sprawy za pomocą systemu teleinformatycznego umożliwia realizację prawa do obrony nawet w szerszym zakresie. Jednak zostały również wprowadzone zmiany, które ograniczają dotychczasowe uprawnienia. Z pewnością rozwiązania przyjęte dla rozprawy zdalnej, czy też zdalnego posiedzenia aresztowego wymagają, aby ustawodawca ponownie się nad nimi pochylił i zachował te aspekty, które spełniają swoją funkcję, a pozostałe dostosował do powszechnie obowiązujących zasad. Informatyzacja postępowania karnego jest procesem dynamicznym. Dostrzegamy już kolejne zmiany w zakresie doręczeń elektronicznych. Przy czym tworząc nowe regulacje, należy pamiętać, aby były one zgodne z naczelnymi zasadami procesu karnego i gwarancjami konstytucyjnymi, co jest szczególnie ważne właśnie w postępowaniu karnym, które niezwykle silnie ingeruje w prawa i wolności człowieka.

Bibliografia

Akty normatywne

1. Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz.U. z 1977 r. Nr 38 poz. 167).
2. Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j. Dz.U. z 2022 r. poz. 1375).
3. Ustawa z dnia 10 stycznia 2003 r. o zmianie ustawy – Kodeks postępowania karnego, ustawy – Przepisy wprowadzające Kodeks postępowania karnego, ustawy o świadku koronnym oraz ustawy o ochronie informacji niejawnych (Dz.U. z 2003 r. Nr 17 poz. 155 z późn. zm.).
4. Ustawa z dnia 31 sierpnia 2011 r. o zmianie ustawy o bezpieczeństwie imprez masowych oraz niektórych innych ustaw (Dz.U. z 2011 r. Nr 217 poz. 1280).

5. Ustawa z dnia 11 marca 2016 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (Dz.U. z 2016 r. poz. 437).
6. Ustawa z dnia 19 lipca 2019 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw (Dz.U. z 2019 r. poz. 1694).
7. Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (t.j. Dz.U. z 2022 r. poz. 569 z późn. zm.).
8. Ustawa z dnia 19 czerwca 2020 r. o dopłatach do oprocentowania kredytów bankowych udzielanych przedsiębiorcom dotkniętym skutkami COVID-19 oraz o uproszczonym postępowaniu o zatwierdzenie układu w związku z wystąpieniem COVID-19 (Dz.U. z 2022 r. poz. 171 z późn. zm.).
9. Ustawa z dnia 20 kwietnia 2021 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz.U. z 2021 r. poz. 1023).

Literatura przedmiotu

1. Dudek D., *Konstytucyjna wolność człowieka a tymczasowe aresztowanie*, Lublin 1999.
2. Dudka K., Paluszkievicz H., *Postępowanie karne*, Warszawa 2017.
3. Flaga-Gieruszyńska K., Gołaczyński J. (red.), *Prawo nowych technologii*, Warszawa 2021.
4. Janusz-Pohl B., Kosmatka P., *Zmiany w prawie karnym procesowym – analiza z perspektywy zasady koncentracji*, „Prawo w Działaniu” 2021, nr 4.
5. Kisiel J., *Doręczenia elektroniczne w Kodeksie postępowania karnego*, „Palestra” 2021, nr 9.
6. Konarska-Wrzosek V., Lachowski J., Wójcikiewicz J. (red.), *Węzłowe problemy prawa karnego kryminologii i polityki kryminalnej. Księga pamiątkowa ofiarowana Profesorowi Andrzejowi Markowi*, Warszawa 2010.
7. Kulesza C., *Rozprawa zdalna oraz zdalne posiedzenie aresztowe w świetle konwencyjnego standardu praw oskarżonego*, „Białostockie Studia Prawnicze” 2021, vol. 26, nr 3.

8. Mazur H., *Doręczenia w procesie karnym XXI wieku*, „Palestra” 2011, nr 3–4.
9. Mierzwińska-Lorencka J., *Kodeks postępowania karnego. Komentarz do nowelizacji 2019*, LEX 2020.
10. Sakowicz A., *Kodeks postępowania karnego. Komentarz*, Warszawa 2016.
11. Skorupka J., *Kodeks postępowania karnego. Komentarz aktualizowany*, Legalis 2018.
12. Skorupka J. (red.), *Proces karny*, Warszawa 2020.
13. Świecki D., *Kodeks postępowania karnego. Tom 1. Komentarz aktualizowany*, LEX 2021.
14. Waltoś S., Hofmański P., *Proces karny. Zarys systemu*, Warszawa 2020.
15. Wiliński P., *Polski proces karny*, Warszawa 2020.
16. Wiliński P., *Zasada prawa do obrony w polskim procesie karnym*, LEX 2006.
17. Zagrodnik J., Chmielniak Ł., Klonowski M., Rychlewska-Hotel A., *Kodeks postępowania karnego. Komentarz praktyczny do nowelizacji 2019*, LEX 2020.

Orzecznictwo

1. Wyrok TK z dnia 17 lutego 2004 r., SK 39/02, OTK-A 2004, nr 2, poz. 7.
2. Wyrok SN z dnia 7 lipca 2006 r., III KK 418/05, LEX nr 193010.
3. Uchwała SN z dnia 20 grudnia 2006 r., I KZP 29/06, OSNKW 2007, nr 1, poz. 1.
4. Postanowienie SN z dnia 26 marca 2009 r., I KZP 39/08, OSNKW 2009, nr 5, poz. 36.
5. Postanowienie SN z dnia 22 października 2014 r., V KK 164/14, LEX nr 1541209.
6. Wyrok SN z dnia 6 grudnia 2016 r., IV KK 242/16, LEX nr 2180104.
7. Postanowienie SN z dnia 22 listopada 2018 r., I DSI 9/18, LEX nr 2583145.

Źródła internetowe

1. Gałęski M., Karlik P., *Opinia Komisji Legislacyjnej przy Naczelnej Radzie Adwokackiej dotycząca projektowanego artykułu 34 pkt 4 ustawy o dopłatach do oprocentowania kredytów bankowych udzielanych na zapewnienie płynności finansowej przedsiębiorcom dotkniętym skutkami COVID-19 oraz o zmianie niektórych innych ustaw (druk 382)* [online:] https://www.adwokatura.pl/admin/wgrane_pliki/file-20200608-u-o--doplatach-do-oprecent-kredytow-tarcza-04-sm-24-20-29964.pdf [dostęp: 31.08.2022].
2. *Koronawirus. Uwagi RPO dla Senatu do Tarczy Antykryzysowej 4.0* [online:] <https://bip.brpo.gov.pl/sites/default/files/Opinia%20RPO%20ws.%20Tarczy%20Antykryzysowej%204.0%20dla%20Marsza%C5%82ka%20Senatu%2C%2012.06.2020.pdf> [dostęp: 31.08.2022].
3. *Uwagi Helsińskiej Fundacji Praw Człowieka z dnia 14 czerwca 2020 r., Druk Senacki nr 142* [online:] <https://www.hfhr.pl/wp-content/uploads/2020/06/druk-senacki-nr-142-uwagi-HFPC-1.pdf> [dostęp: 31.08.2022].

Streszczenie

Przedmiotem rozważań w niniejszym opracowaniu są zmiany wprowadzone w postępowaniu karnym w związku z jego informatyzacją i ich wpływ na realizację prawa do obrony. Na skutek kolejnych nowelizacji procedura karna została wzbogacona o rozwiązania umożliwiające wykorzystanie różnych rozwiązań informatycznych. Wprowadzono m.in.: udostępnienie akt postępowania przygotowawczego w postaci elektronicznej, udostępnienie informacji o aktach sprawy za pomocą systemu teleinformatycznego, niektóre rozwiązania dla doręczeń elektronicznych, najnowsze zmiany w zakresie rozprawy zdalnej, czy też zdalne posiedzenie aresztowe. Analiza ostatnich zmian w przepisach postępowania karnego pozwala na ocenę przyjętych rozwiązań i skłania do refleksji nad zachowaniem gwarancji procesowych, szczególnie w zakresie zasady prawa do obrony. W opracowaniu wskazano zasadnicze problemy związane

z realizacją prawa do obrony, ale również przedstawiono rozwiązania, które oceniane są bardzo pozytywnie i pomagają w zagwarantowaniu rzetelnego procesu karnego.

Słowa kluczowe

informatyzacja postępowania karnego, prawo do obrony, doręczenia elektroniczne, rozprawa zdalna, zdalne posiedzenie aresztowe

ELEKTRONICZNE POSTĘPOWANIE WIECZYSTOKSIĘGOWE W KONTEKŚCIE INFORMATYZACJI POSTĘPOWAŃ SĄDOWYCH

MIROŚŁAWA PYTLEWSKA

INSTITUT DE REPUBLICA



0000-0002-0299-055X

Wstęp

Postępująca informatyzacja społeczeństwa zainicjowała rozpoczęcie tego procesu również wobec postępowań sądowych¹. Jego celem było usprawnienie postępowań sądowych, zwłaszcza w odniesieniu do postępowania wieczystoksięgowego, stanowiącego jeden z czynników zapewnienia bezpieczeństwa obrotu nieruchomościami. Początkowym etapem była migracja², czyli przeniesienie treści dotychczasowych ksiąg wieczystych z postaci papierowej do elektronicznej, a następnie wprowadzanie możliwości składania wniosków za pośrednictwem systemu teleinformatycznego³ przez coraz szerszy krąg uprawnionych podmiotów. Zasadą jest złożenie wniosku do sądu na formularzu urzędowym (art. 626² kpc) przez wszystkie podmioty, tj. osoby fizyczne i osoby prawne. Z kręgu osób fizycznych są wyłączeni notariusze, komornicy i naczelnicy urzędów

¹ M. Pytlewska-Smółka, *Elektroniczne postępowanie wieczystoksięgowe*, NPN 2015, nr 4(66), s. 21.

² Ustawa z dnia 14 lutego 2003 r. o przenoszeniu treści księgi wieczystej do struktury księgi wieczystej prowadzonej w systemie informatycznym (Dz.U. z 2003 r. Nr 42 poz. 363).

³ M. Pytlewska-Smółka, *Składanie wniosków za pośrednictwem systemu teleinformatycznego – próba oceny*, NPN 2016, nr 4(70), s. 44.

skarbowych, zobligowani do składania wniosków za pośrednictwem systemu teleinformatycznego⁴. Kolejnym podmiotem, który od dnia 8 sierpnia 2017 r. może składać wniosek za pośrednictwem systemu teleinformatycznego jest Komisja do spraw restryktacji nieruchomości warszawskich utworzona na mocy ustawy z dnia 9 marca 2017 r. o szczególnych zasadach usuwania skutków prawnych decyzji restryktacyjnych dotyczących nieruchomości warszawskich, wydanych z naruszeniem prawa⁵. Informatyzując postępowanie wieczystoksięgowe, wprowadzono art. 626⁴ kpc⁶, zgodnie z którym notariusz, komornik oraz naczelnik urzędu skarbowego składa wniosek o wpis wyłącznie za pośrednictwem systemu teleinformatycznego⁷. Obecnie wnioski o wpis do księgi wieczystej

⁴ H. Ciepla, M. Pytlewska-Smółka, *Elektroniczne postępowanie wieczystoksięgowe w praktyce i orzecznictwie z wzorami wniosków*, Warszawa 2018, s. 124.

⁵ Ustawa z dnia 9 marca 2017 r. o szczególnych zasadach usuwania skutków prawnych decyzji restryktacyjnych dotyczących nieruchomości warszawskich, wydanych z naruszeniem prawa (t.j. Dz.U. z 2021 r. poz. 795).

⁶ Art. 626⁴ kpc zmieniony przez art. 1 pkt 19 ustawy z dnia 15 stycznia 2015 r. (Dz.U. z 2015 r. poz. 218), zmieniającej niniejszą ustawę z dniem 1 lipca 2016 r.

⁷ Założenie konta użytkownika jest obligatoryjne dla podmiotów zobowiązanych do składania wniosków za pośrednictwem systemu teleinformatycznego obsługującego elektroniczne postępowanie wieczystoksięgowe. Zgodnie z § 1 pkt 1 rozporządzenia Ministra Sprawiedliwości z dnia 26 kwietnia 2016 r. w sprawie trybu zakładania i udostępniania konta w systemie teleinformatycznym obsługującym postępowania sądowe (Dz.U. z 2016 r. poz. 637), użytkownikiem konta może być wyłącznie osoba fizyczna, która założyła konto w systemie teleinformatycznym obsługującym postępowanie sądowe. Jednak zgodnie z § 9 pkt 1 projektu rozporządzenia Ministra Sprawiedliwości w sprawie trybu zakładania i udostępniania konta w systemie teleinformatycznym obsługującym postępowanie sądowe, użytkownik mógł przekazać innej osobie uprawnienie do dostępu do konta. Zgodnie z pkt 2 w uzasadnionych przypadkach, w szczególności w razie śmierci użytkownika, prezes sądu mógł udostępnić konto osobie uprawnionej. Zgodnie z pkt 3 udostępnienie konta następuje na wniosek osoby uprawnionej, do wniosku zaś należy dołączyć dokumenty potwierdzające uprawnienie do dostępu do konta – zob. rozporządzenie Ministra Sprawiedliwości z dnia 26 kwietnia 2016 r.

oraz wnioski o założenie księgi wieczystej muszą być obligatoryjnie składane przez wymienione podmioty za pośrednictwem systemu teleinformatycznego⁸.

Wejście w życie ustawy z dnia 9 marca 2017 r. o szczególnych zasadach usuwania skutków prawnych decyzji reptrywatyzacyjnych dotyczących nieruchomości warszawskich wydanych z naruszeniem prawa⁹ (dalej: ustawa reptrywatyzacyjna)¹⁰ doprowadziło do dodania kolejnego podmiotu mogącego składać wnioski wieczystoksięgowe za pośrednictwem systemu teleinformatycznego. Komisja reptrywatyzacyjna jest jedynym organem, który może złożyć wniosek o wpis w dziale II lub III w formie tradycyjnej, na formularzu KW-WPIS, lub wniosek elektroniczny za pośrednictwem systemu teleinformatycznego.

Przeprowadzenie procesu migracji oraz umożliwienie składania wniosków za pośrednictwem systemu teleinformatycznego, jak również informatyczne usprawnienie obsługi biurowej stanowi

w sprawie trybu zakładania i udostępniania konta w systemie teleinformatycznym obsługującym postępowanie sądowe (Dz.U. z 2016 r. poz. 637); akt uznany za uchylony.

⁸ W przyszłości przewiduje się wdrożenie elektronicznego postępowania wieczystoksięgowego wobec wszystkich kategorii wnioskodawców. Zob. Uchwała Nr IX/62/2015 Krajowej Rady Notarialnej z dnia 22 września 2015 r. w sprawie projektu rozporządzenia Ministra Sprawiedliwości w sprawie zakładania i prowadzenia ksiąg wieczystych w systemie teleinformatycznym, s. 1–6 [online:] <https://legislacja.rcl.gov.pl/docs//517/12276357/12307150/12307153/dokument190319.pdf> [dostęp: 17.05.2022 w zakresie treści dokumentu].

⁹ Ustawa z dnia 9 marca 2017 r. o szczególnych zasadach usuwania skutków prawnych decyzji reptrywatyzacyjnych dotyczących nieruchomości warszawskich, wydanych z naruszeniem prawa (Dz.U. z 2017 r. poz. 718).

¹⁰ Zob. uzasadnienie rządowego projektu ustawy o szczególnych zasadach usuwania skutków prawnych decyzji reptrywatyzacyjnych dotyczących nieruchomości warszawskich wydanych z naruszeniem prawa (z dnia 24 listopada 2016 r.), druk sejmowy nr 1056 [online:] <http://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=1056> [dostęp: 23.10.2022 w zakresie treści dokumentu].

element informatyzacji postępowań sądowych. Celem postępowania elektronicznego było ułatwienie i zapewnienie szybszego dostępu do sądu oraz sprawne załatwienie sprawy.

Prowadzenie ksiąg wieczystych

Księgi wieczyste są prowadzone przez sądy rejonowe właściwe ze względu na położenie nieruchomości, zaś obowiązek prowadzenia ksiąg wieczystych należy do zadań władzy publicznej¹¹. Jako że wpisy w księgach wieczystych odzwierciedlają zmiany w stosunkach własnościowych nieruchomości, sprawne funkcjonowanie elektronicznego postępowania wieczystoksięgowego decyduje o bezpieczeństwie obrotu nieruchomościami oraz poszerza jawność formalną ksiąg wieczystych¹². Usprawnieniu postępowań sądowych służyła informatyzacja ksiąg wieczystych, stanowiąca część informatyzacji postępowań sądowych, polegająca na odmiejszczeniu dokonywania wglądu do księgi i pobierania odpisów, zwłaszcza zupełnych¹³. Wdrożenie systemu zinformatyзовanych ksiąg wieczystych umożliwia pełniejsze wykorzystanie zgromadzonych danych¹⁴.

¹¹ J. Kuropatwiński, *Księgi wieczyste. Komentarz do art. 1–58² ustawy o księgach wieczystych i hipotece oraz do art. 626¹–626¹³ k.p.c. Tom I. Komentarz do art. 1–10 ustawy o księgach wieczystych i hipotece*, Płock 2013, s. 21.

¹² M. Pytlewska-Smółka, *Rola uczestników postępowania wieczystoksięgowego w obecnym stanie prawnym oraz w świetle projektów rozszerzających informatyzację postępowania z księgami wieczystymi* [w:] *Rola uczestników postępowań sądowych – wczoraj, dziś i jutro*, t. 2, red. D. Gil, Lublin 2015, s. 126.

¹³ A. Gryszczyńska, *Wpływ informatyzacji na formalną jawność rejestrów sądowych* [w:] *Ewolucja prawa polskiego pod wpływem technologii informatycznych*, red. J. Misztal-Konecka, G. Tylec, Lublin 2012, s. 140.

¹⁴ A. Kościółek, *Elektroniczne postępowanie wieczystoksięgowe*, MoP 2015, nr 14, s. 747.

Zgodnie z art. 1 ustawy z dnia 6 lipca 1982 r. o księgach wieczystych i hipotece¹⁵ księgi wieczyste zakłada się i prowadzi dla nieruchomości, a ponadto księgi prowadzi się w celu ustalenia stanu prawnego nieruchomości. Oznacza to, że dla każdej nieruchomości prowadzi się odrębną księgę wieczystą, tj. odrębnie dla nieruchomości gruntowych, budynkowych i lokalowych.

System teleinformatyczny w postępowaniu wieczystoksięgowym

Pierwszym etapem informatyzacji ksiąg wieczystych była migracja. Zasady i tryb dokonywania migracji księgi wieczystej uregulowano w ustawie z dnia 14 lutego 2003 r. o przenoszeniu treści księgi wieczystej do struktury księgi wieczystej prowadzonej w systemie informatycznym. Zgodnie z art. 2 ust. 2 tej ustawy migracja księgi wieczystej to ogół czynności służących przeniesieniu treści dotychczasowej księgi wieczystej do struktury księgi wieczystej prowadzonej w systemie informatycznym.

Kolejny etap informatyzacji, od dnia 16 czerwca 2010 r., polegał na umożliwieniu przeglądania elektronicznych ksiąg wieczystych przez przeglądarkę dostępną na stronie internetowej <http://ekw.ms.gov.pl>. Natomiast od dnia 1 lipca 2014 r. wprowadzono możliwość samodzielnego drukowania odpisów ksiąg wieczystych, wyciągów z ksiąg wieczystych oraz zaświadczeń o zamknięciu księgi. Na podstawie art. 36⁴ ust. 4 ukwh wydruki te posiadają moc dokumentów wydawanych przez sąd.

Zgodnie z art. 25¹ ust. 1 ukwh księgi wieczyste są zakładane i prowadzone w systemie teleinformatycznym¹⁶, zaś sposób

¹⁵ T.j. Dz.U. z 2022 r. poz. 1728.

¹⁶ Na podstawie art. 25¹ ust. 2 ustawy z dnia 6 lipca 1982 r. o księgach wieczystych i hipotece (t.j. Dz.U. z 2013 r. poz. 707 z późn. zm.) wydano rozporządzenie Ministra

zakładania oraz prowadzenia ksiąg wieczystych w systemie teleinformatycznym uregulowano w rozporządzeniu Ministra Sprawiedliwości z dnia 15 lutego 2016 r. w sprawie zakładania i prowadzenia ksiąg wieczystych w systemie teleinformatycznym¹⁷.

Początkowo w elektronicznym postępowaniu wieczystoksięgowym posługiwano się definicją systemu teleinformatycznego w rozumieniu art. 2 pkt 3 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną¹⁸. Zgodnie z tą regulacją rozumiany on był jako obsługujący postępowanie sądowe i dostępny za pomocą usług internetowych udostępnianych na stronach internetowych

Sprawiedliwości z dnia 15 lutego 2016 r. w sprawie zakładania i prowadzenia ksiąg w systemie teleinformatycznym (Dz.U. z 2016 r. poz. 312). Było ono poprzedzone rozporządzeniem Ministra Sprawiedliwości z dnia 21 listopada 2013 r. w sprawie zakładania i prowadzenia ksiąg wieczystych w systemie informatycznym (t.j. Dz.U. z 2015 r. poz. 1613 z późn. zm.), które straciło moc z dniem wejścia w życie ustawy z dnia 15 stycznia 2015 r. o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz.U. z 2015 r. poz. 218 z późn. zm.). Pierwotnie regulacje dotyczące systemu teleinformatycznego miały wejść w życie – zgodnie z § 136 wskazanego rozporządzenia – dnia 1 kwietnia 2016 r., jednak na podstawie § 1 rozporządzenia Ministra Sprawiedliwości z dnia 26 marca 2016 r. zmieniającego rozporządzenie w sprawie zakładania i prowadzenia ksiąg wieczystych w systemie teleinformatycznym (Dz.U. z 2016 r. poz. 410), termin ten przesunięto na dzień 1 lipca 2016 r. Ustawa z dnia 15 stycznia 2015 r. o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz.U. z 2015 r. poz. 218) zmieniła m.in. ustawę z dnia 6 lipca 1982 r. o księgach wieczystych i hipotece, ustawę z dnia 14 lutego 1991 r. – Prawo o notariacie, ustawę z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji oraz ustawę z dnia 14 lutego 2003 r. o przenoszeniu treści księgi wieczystej do struktury księgi wieczystej prowadzonej w systemie informatycznym (Dz.U. z 2003 r. Nr 4 poz. 363).

¹⁷ Rozporządzenie Ministra Sprawiedliwości z dnia 15 lutego 2016 r. w sprawie zakładania i prowadzenia ksiąg wieczystych w systemie teleinformatycznym (Dz.U. z 2015 r. poz. 312 z późn. zm.).

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

Ministerstwa Sprawiedliwości¹⁹. Następnie system ten zdefiniowano w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne²⁰.

Elektroniczne postępowanie wieczystoksięgowe

Elektroniczne postępowanie wieczystoksięgowe obejmuje rozpoznawanie wniosków w postępowaniu wieczystoksięgowym, a księga wieczysta to nie tylko rejestr praw rzeczowych na nieruchomościach, ale przede wszystkim rejestr publicznych²¹ praw podmiotowych²². Zgodnie z treścią art. 626⁸ § 1 kpc wpis dokonywany jest jedynie na wniosek i w jego granicach, chyba że przepis szczególny przewiduje dokonanie wpisu z urzędu. Stosownie do treści art. 626⁸ § 2 kpc, rozpoznając wniosek o wpis, sąd bada jedynie treść i formę wniosku, dołączonych do wniosku dokumentów²³

¹⁹ Wymogi wniesienia pisma za pośrednictwem systemu teleinformatycznego określono w § 2 ust. 1 pkt 1–5 rozporządzenia Ministra Sprawiedliwości z dnia 20 października 2015 r. w sprawie sposobu wnoszenia pism procesowych za pośrednictwem systemu teleinformatycznego obsługującego postępowanie sądowe (Dz.U. z 2015 r. poz. 1783).

²⁰ Zgodnie z art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, system teleinformatyczny to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci telekomunikacyjnego urządzenia końcowego w rozumieniu przepisów ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz.U. z 2021 r. poz. 2070).

²¹ P. Siciński, *Księgi wieczyste i postępowanie wieczystoksięgowe* [w:] *Praxis. Notariat. Czynności notarialne*, red. A.J. Szereda, Warszawa 2021, s. 1088.

²² H. Ciepla, S. Brzeszczyńska, *Obrót nieruchomościami w praktyce notarialnej, sądowej, egzekucyjnej, podatkowej w wzorami umów*, Warszawa 2018, s. 498.

²³ H. Ciepla, M. Pytlewska, *Podział majątku wspólnego z rozliczeniem praw spółkowych i kredytów frankowych. Regulacje dotyczące małżonków, konkubentów*

oraz treść księgi wieczystej. Natomiast zgodnie z treścią przepisu art. 626⁹kpc sąd oddala wniosek o wpis, jeżeli brak jest podstaw lub istnieje przeszkoda do jego dokonania.

Zgodnie z art. 92 § 4 ustawy – Prawo o notariacie²⁴, jeżeli akt notarialny zawiera przeniesienie, zmianę lub zrzeczenie się prawa ujawnionego w księdze wieczystej albo ustanowienie prawa, które może być ujawnione w księdze wieczystej bądź obejmuje czynność przenoszącą własność nieruchomości, chociażby dla tej nieruchomości nie była prowadzona księga wieczysta, notariusz sporządzający akt notarialny, nie później niż w dniu jego sporządzenia, składa wniosek o wpis w księdze wieczystej za pośrednictwem systemu teleinformatycznego obsługującego postępowanie sądowe. Na żądanie strony czynności notarialnej wniosek może zawierać żądanie dokonania w księdze wieczystej także innego wpisu związanego z czynnością notarialną.

System teleinformatyczny, który funkcjonuje w ramach elektronicznego postępowania wieczystoksięgowego, jest systemem centralnym zarządzanym przez Ministra Sprawiedliwości, zaś złożenie wniosku za pośrednictwem systemu teleinformatycznego związane jest z weryfikacją podmiotów, którym przysługuje ta kompetencja, czyli notariusza, komornika, naczelnika urzędu skarbowego i członka komisji reperytywizacyjnej. Ich weryfikacji dokonuje się poprzez system teleinformatyczny. Podmioty te autoryzują, czyli podpisują składane przez siebie pisma procesowe w elektronicznym postępowaniu wieczystoksięgowym podpisem bezpiecznym, weryfikowanym ważnym kwalifikowanym certyfikatem, w rozumieniu ustawy z dnia 5 września 2016 r. o usługach zaufania oraz

i partnerów związków jednopłciowych. Praktyka sądowa, notarialna i wieczystoksięgowa, Warszawa 2022, s. 218.

²⁴ Ustawa z dnia 14 lutego 1991 r. – Prawo o notariacie (t.j. Dz.U. z 2022 r. poz. 1799 z późn. zm.).

identyfikacji elektronicznej²⁵. W zakresie wniosków przesyłanych za pośrednictwem systemu teleinformatycznego przez notariusza, system weryfikuje dane identyfikacyjne notariusza w odrębnym systemie informatycznym prowadzonym przez samorząd notarialny i Ministra Finansów.

Celem sukcesywnego wdrażania kolejnych etapów informatyzacji ksiąg wieczystych było ułatwienie dostępu do sądu oraz usprawnienie postępowania wieczystoksięgowego poprzez wykorzystanie systemu teleinformatycznego²⁶.

Informatyzacja postępowania wieczystoksięgowego spełnia również rolę ochronną dla obrotu nieruchomościami, bowiem w przypadku wniosków składanych za pośrednictwem systemu teleinformatycznego rękojmia wiary publicznej ksiąg wieczystych zostaje wyłączona już z chwilą zamieszczenia wzmianki. Wzmianka zawiera informację o wniosku w centralnym repertorium wniosków elektronicznych (REP. C). Numer każdej wzmianki o wniosku składa się z oznaczenia centralnego repertorium wniosków elektronicznych (REP. C), czteroznakowego kodu podmiotu składającego wniosek, a także z kolejnego numeru w centralnym repertorium wniosków elektronicznych, którym został oznaczony wniosek, z dodaniem dwóch końcowych cyfr danego roku. Dla notariuszy składających wnioski za pośrednictwem systemu teleinformatycznego przewidziano kod: NOTA, dla komorników: KOMO, dla naczelników urzędów skarbowych: USKA, a KREP dla Komisji do spraw reprivatyzacji nieruchomości warszawskich.

Zaletą informatyzacji jest automatyczne zamieszczanie wzmianek w księgach wieczystych, dzięki czemu rękojmia wiary publicznej ksiąg wieczystych zostaje wyłączona niezwłocznie po

²⁵ Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz.U. z 2021 r. poz. 1797).

²⁶ A. Kościółek, *Elektroniczne postępowanie...*, op. cit., s. 747.

sporządzeniu aktu notarialnego prowadzącego np. do zmiany właściciela nieruchomości.

Znaczenie elektronicznego postępowania wieczystoksięgowego wynika także z powiązania danych ujawnionych w elektronicznych księgach wieczystych z innymi rejestrami i bazami danych. Zgodnie z § 33 rozporządzenia z dnia 15 lutego 2016 r. w sprawie zakładania i prowadzenia ksiąg w systemie teleinformatycznym według pkt 5 Rubryka 2.2 „właściciel” obejmuje: w podrubryce 2.2.5 „osoba fizyczna” następujące pola: szczegółowe dane identyfikujące osobę fizyczną: – zgodnie z lit. h – 2.2.5.8 „PESEL” – numer ewidencyjny PESEL osoby fizycznej, chyba że odrębne przepisy nie przewidują nadawania tego numeru. Zgodnie z art. 6 ust. 1 ustawy z dnia 24 września 2010 r. o ewidencji ludności²⁷ rejestr PESEL jest centralnym zbiorem danych prowadzonym przez ministra właściwego do spraw informatyzacji.

Podmioty zobowiązane do wszczęcia elektronicznego postępowania wieczystoksięgowego są zobligowane do użycia interaktywnych formularzy²⁸. Kolejność składania wniosków za pośrednictwem tego systemu precyzuje § 2 rozporządzenia Ministra Sprawiedliwości z dnia 20 października 2015 r. w sprawie sposobu wnoszenia pism procesowych za pośrednictwem systemu teleinformatycznego obsługującego postępowanie sądowe²⁹. Chwilą wpływu wniosku o wpis złożonego za pośrednictwem systemu teleinformatycznego jest godzina, minuta i sekunda zamieszczenia wniosku w systemie, który pozwala na precyzyjne określenie momentu wniesienia

²⁷ Ustawa z dnia 24 września 2010 r. o ewidencji ludności (t.j. Dz.U. z 2022 r. poz. 1191).

²⁸ Zgodnie z art. 125 § 2¹ kpc pisma niewniesione za pośrednictwem systemu teleinformatycznego nie wywołują skutków prawnych, jakie ustawa wiąże z wniesieniem pisma do sądu.

²⁹ Rozporządzenie Ministra Sprawiedliwości z dnia 20 października 2015 r. w sprawie sposobu wnoszenia pism procesowych za pośrednictwem systemu teleinformatycznego obsługującego postępowanie sądowe (Dz.U. z 2015 r. poz. 1783).

wniosku, co w praktyce pozwoli uniknąć przypadków równoczesnego złożenia wniosków³⁰. Rozwiązanie to zwiększa bezpieczeństwo obrotu nieruchomościami.

Zgodnie z § 2 ust. 1 pkt 1 rozporządzenia Ministra Sprawiedliwości z dnia 20 października 2015 r. wniesienie pisma za pośrednictwem systemu teleinformatycznego przez użytkownika następuje poprzez jego uwierzytelnienie. Zanim to stanie się możliwe, konieczne jest założenie konta w systemie teleinformatycznym, zaś uwierzytelnienie użytkownika polega na jego identyfikacji na potrzeby uzyskania przez niego dostępu do konta, oczywiście w zakresie posiadanych przez niego uprawnień³¹. Konto udostępnia się użytkownikowi wyłącznie po uwierzytelnieniu³², które polega na zweryfikowaniu zadeklarowanej tożsamości. Następuje ono po identyfikacji, czyli zadeklarowaniu (autoryzacji) swojej tożsamości przez użytkownika.

Inicjując elektroniczne postępowanie wieczystoksięgowe, należy mieć na uwadze okoliczność, że formularz wniosku musi być podpisany bezpiecznym podpisem elektronicznym weryfikowanym ważnym kwalifikowanym certyfikatem. Charakteryzuje się on tym, że jest przyporządkowany wyłącznie jednej osobie, a dodatkowo bezpieczeństwo gwarantowane jest przyznaniem tylko tej osobie bezpiecznych urządzeń oraz niepowtarzalnych danych niezbędných do składania podpisu elektronicznego³³.

³⁰ A. Kościółek, *Elektroniczne postępowanie...*, op. cit., s. 752.

³¹ Zgodnie z § 2 pkt 4 rozporządzenia Ministra Sprawiedliwości z dnia 30 listopada 2021 r. w sprawie konta w systemie teleinformatycznym obsługującym postępowanie sądowe (Dz.U. z 2021 r. poz. 2204).

³² Zgodnie z § 4 rozporządzenia Ministra Sprawiedliwości z dnia 30 listopada 2021 r. w sprawie konta w systemie teleinformatycznym obsługującym postępowanie sądowe (Dz.U. z 2021 r. poz. 2204).

³³ A. Kościółek, *Elektroniczne czynności procesowe w sądowym postępowaniu cywilnym*, Warszawa 2012, s. 334. Założeniem bezpiecznego podpisu elektronicznego jest powiązanie z danymi, do których zostaje dołączony, w sposób gwarantujący, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna – zob. *Ibidem*, s. 335–336.

System teleinformatyczny automatycznie weryfikuje wniosek formalnie w odniesieniu do istnienia wskazanej księgi wieczystej oraz badania kompletności wymaganych danych. W przypadku braku pozytywnej weryfikacji wniosek uważa się za niezłożony³⁴. Zgodnie z § 2 ust. 1 pkt 2 projektu rozporządzenia po uwierzytelnieniu użytkownika następuje wprowadzenie treści pisma, a następnie (§ 2 ust. 1 pkt 3) dołączenie załączników, o ile są wnoszone. Kolejnym etapem elektronicznego postępowania wieczystoksięgowego jest opatrzenie pisma bezpiecznym podpisem elektronicznym weryfikowanym za pomocą ważnego kwalifikowanego certyfikatu. Należy mieć na uwadze, że wszystkie wskazane czynności nie oznaczają niewystąpienia braków formalnych wniosku, który pozytywnie przeszedł weryfikację kompletności zawartych danych w interaktywnym formularzu.

Podczas składania wniosków przez wybrane podmioty za pośrednictwem systemu teleinformatycznego mogą pojawić się problemy dotyczące błędów technicznych programu informatycznego. Odnośnie do takich sytuacji wypowiedział się już Sąd Najwyższy w postanowieniu z dnia 24 września 2010 r.³⁵, stwierdzając, że w sytuacji istnienia błędów w systemie informatycznym, uniemożliwiających dokonanie wpisu zgodnego z prawem, sąd nie może odmówić wpisu ani dokonać wpisu niezgodnego z prawem, a zgodnego z programem informatycznym.

³⁴ Zastosowanie powyższego mechanizmu weryfikacyjnego nie wyklucza możliwości wystąpienia w pozytywnie zweryfikowanym wniosku braków formalnych w rozumieniu przepisów proceduralnych – zob. A. Kościółek, *Elektroniczne postępowanie...*, op. cit., s. 750.

³⁵ Postanowienie SN z dnia 24 września 2010 r., IV CSK 82/10, LEX nr 885028.

Znaczenie automatycznego zamieszczania wzmianek dla obrotu nieruchomościami

Dla obrotu nieruchomościami istotne znaczenie ma § 68 ust. 1 rozporządzenia Ministra Sprawiedliwości z dnia 15 lutego 2016 r. w sprawie zakładania i prowadzenia ksiąg wieczystych w systemie teleinformatycznym, zgodnie z którym wzmianka o wniosku złożonym za pośrednictwem systemu teleinformatycznego, obejmująca numer wzmianki, umieszczana jest automatycznie w księdze wieczystej wskazanej we wniosku, z chwilą zarejestrowania wniosku w centralnym repozytorium wniosków elektronicznych. Zgodnie z § 68 ust. 2 tegoż rozporządzenia numer wzmianki o wniosku składa się z oznaczenia centralnego repertorium wniosków elektronicznych (Rep. C), czteroznakowego kodu podmiotu składającego wniosek, kolejnego numeru w centralnym repertorium wniosków elektronicznych, którym został oznaczony wniosek, z dodatkiem dwóch końcowych cyfr danego roku. Zgodnie z § 68 ust. 3 tegoż rozporządzenia określono następujące czteroznakowe kody podmiotów: NOTA – dla notariuszy, KOMO – dla komorników oraz USKA – dla naczelników urzędów skarbowych działających jako administracyjne organy egzekucyjne.

Podsumowanie

Dokonująca się informatyzacja życia społecznego zainicjowała informatyzację postępowań sądowych, a wśród nich postępowanie wieczystoksięgowe. Stało się to możliwe po uprzednim „zmigrowaniu”, czyli przeniesieniu treści ksiąg papierowych do ksiąg elektronicznych. Elektroniczne postępowanie wieczystoksięgowe oraz możliwość składania wniosków za pośrednictwem systemu teleinformatycznego uprościło postępowanie w sprawach dotyczących rozpoznawania wniosków o wpisy

w księgach wieczystych. Stanowi to element bezpieczeństwa obrotu nieruchomościami.

Bibliografia

Akty normatywne

1. Ustawa z dnia 6 lipca 1982 r. o księgach wieczystych i hipotece (t.j. Dz.U. z 2022 r. poz. 1728).
2. Ustawa z dnia 14 lutego 1991 r. – Prawo o notariacie (t.j. Dz.U. z 2022 r. poz. 1799 z późn. zm.).
3. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r. poz. 344).
4. Ustawa z dnia 14 lutego 2003 r. o przenoszeniu treści księgi wieczystej do struktury księgi wieczystej prowadzonej w systemie informatycznym (Dz.U. z 2003 r. Nr 42 poz. 363).
5. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2005 r. Nr 64 poz. 565).
6. Ustawa z dnia 24 września 2010 r. o ewidencji ludności (t.j. Dz.U. z 2022 r. poz. 1191).
7. Ustawa z dnia 15 stycznia 2015 r. o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz.U. z 2015 r. poz. 218 z późn. zm.).
8. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz.U. z 2021 r. poz. 1797).
9. Ustawa z dnia 9 marca 2017 r. o szczególnych zasadach usuwania skutków prawnych decyzji reprivatyzacyjnych dotyczących nieruchomości warszawskich, wydanych z naruszeniem prawa (t.j. Dz.U. z 2021 r. poz. 795).
10. Rozporządzenie Ministra Sprawiedliwości z dnia 21 listopada 2013 r. w sprawie zakładania i prowadzenia ksiąg wieczystych w systemie informatycznym (t.j. Dz.U. z 2015 r. poz. 1613 z późn. zm.).

11. Rozporządzenie Ministra Sprawiedliwości z dnia 20 października 2015 r. w sprawie sposobu wnoszenia pism procesowych za pośrednictwem systemu teleinformatycznego obsługującego postępowanie sądowe (Dz.U. z 2015 r. poz. 1783).
12. Rozporządzenie Ministra Sprawiedliwości z dnia 15 lutego 2016 r. w sprawie zakładania i prowadzenia ksiąg w systemie teleinformatycznym (Dz.U. z 2016 r. poz. 312 z późn. zm.).
13. Rozporządzenie Ministra Sprawiedliwości z dnia 26 kwietnia 2016 r. w sprawie trybu zakładania i udostępniania konta w systemie teleinformatycznym obsługującym postępowanie sądowe (Dz.U. z 2016 r. poz. 637); akt uznany za uchylony.
14. Rozporządzenie Ministra Sprawiedliwości z dnia 26 marca 2016 r. zmieniające rozporządzenie w sprawie zakładania i prowadzenia ksiąg wieczystych w systemie teleinformatycznym (Dz.U. z 2016 r. poz. 410).
15. Rozporządzenie Ministra Sprawiedliwości z dnia 26 kwietnia 2016 r. w sprawie trybu zakładania i udostępniania konta w systemie teleinformatycznym obsługującym postępowania sądowe (Dz.U. z 2016 r. poz. 637).

Literatura przedmiotu

1. Ciepla H., Brzeszczyńska S., *Obrót nieruchomościami w praktyce notarialnej, sądowej, egzekucyjnej, podatkowej z wzorami umów*, Warszawa 2018.
2. Ciepla H., Pytlewska M., *Podział majątku wspólnego z rozliczeniem praw spółkowych i kredytów frankowych. Regulacje dotyczące małżonków, konkubentów i partnerów związków jedнопłciowych. Praktyka sądowa, notarialna i wieczystoksięgowa*, Warszawa 2022.
3. Ciepla H., Pytlewska-Smółka M., *Elektroniczne postępowanie wieczystoksięgowe w praktyce i orzecznictwie z wzorami wniosków*, Warszawa 2018.

4. Gryszczyńska A., *Wpływ informatyzacji na formalną jawność rejestrów sądowych* [w:] *Ewolucja prawa polskiego pod wpływem technologii informatycznych*, red. J. Misztal-Konecka, G. Tylec, Lublin 2012.
5. Kościółek A., *Elektroniczne czynności procesowe w sądowym postępowaniu cywilnym*, Warszawa 2012.
6. Kościółek A., *Elektroniczne postępowanie wieczystoksięgowe*, MoP 2015, nr 14.
7. Kuropatwiński J., *Księgi wieczyste. Komentarz do art. 1–582 ustawy o księgach wieczystych i hipotece oraz do art. 6261–62613 k.p.c. Tom I. Komentarz do art. 1–10 ustawy o księgach wieczystych i hipotece*, Płock 2013.
8. Pytlewska-Smółka M., *Rola uczestników postępowania wieczystoksięgowego w obecnym stanie prawnym oraz w świetle projektów rozszerzających informatyzację postępowania z księgami wieczystymi* [w:] *Rola uczestników postępowań sądowych – wczoraj, dziś i jutro*, t. 2, red. D. Gil, Lublin 2015.
9. Pytlewska-Smółka M., *Elektroniczne postępowanie wieczystoksięgowe*, NPN 2015, nr 4(66).
10. Pytlewska-Smółka M., *Składanie wniosków za pośrednictwem systemu teleinformatycznego – próba oceny*, NPN 2016, nr 4(70).
11. Szereda A.J. (red.), *Praxis. Notariat. Czynności notarialne*, Warszawa 2021.

Orzeczenia

1. Postanowienie SN z dnia 24 września 2010 r., IV CSK 82/10, LEX nr 885028.

Inne

1. Uchwała Nr IX/62/2015 Krajowej Rady Notarialnej z dnia 22 września 2015 r. w sprawie projektu rozporządzenia Ministra Sprawiedliwości w sprawie zakładania i prowadzenia ksiąg wieczystych w systemie

teleinformatycznym [online:] <https://legislacja.rcl.gov.pl/docs//517/12276357/12307150/12307153/dokument190319.pdf> [dostęp: 17.05.2022 w zakresie treści dokumentu].

2. Uzasadnienie rządowego projektu ustawy o szczególnych zasadach usuwania skutków prawnych decyzji reprivatyzacyjnych dotyczących nieruchomości warszawskich wydanych z naruszeniem prawa (z dnia 24-11-2016), druk sejmowy nr 1056 [online:] <http://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=1056> [dostęp: 23.10.2022 w zakresie treści dokumentu].

Streszczenie

Elektroniczne postępowanie wieczystoksięgowe stanowi element informatyzacji postępowań sądowych. Prowadzenie ksiąg wieczystych w systemie teleinformatycznym, a także obligatoryjne (notariusze, komornicy, naczelnicy urzędów skarbowych) oraz fakultatywne (Komisja do spraw reprivatyzacji nieruchomości warszawskich) składanie wniosków w postępowaniu wieczystoksięgowym gwarantuje obrót nieruchomościami.

Słowa kluczowe

księgi wieczyste, elektroniczne postępowanie wieczystoksięgowe, system teleinformatyczny, nieruchomości

WNOSZENIE ORAZ DORĘCZANIE PISM PROCESOWYCH ZA POŚREDNICTWEM ŚRODKÓW KOMUNIKACJI ELEKTRONICZNEJ W POSTĘPOWANIU SĄDOWOADMINISTRACYJNYM

KATARZYNA TOMIŁO-NAWROCKA

UCZELNIA ŁAZARSKIEGO



0000-0001-6477-293X

Wprowadzenie

Z dniem 31 maja 2019 r. weszły w życie art. 4 ustawy z dnia 10 stycznia 2014 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw¹ oraz ustawa z dnia 12 kwietnia 2019 r. o zmianie ustawy – Prawo o postępowaniu przed sądami administracyjnymi oraz niektórych innych ustaw², które wprowadzają możliwość wnoszenia do sądu administracyjnego pism procesowych nie tylko w postaci papierowej, jak to miało miejsce dotychczas, ale również w formie dokumentu elektronicznego.

Zmiany ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi³ w zakresie wnoszenia oraz doręczania pism procesowych za pośrednictwem środków komunikacji elektronicznej w postaci dokumentu elektronicznego w założeniu miały na celu ułatwienie dokonywania czynności w postępowaniu sądowoadministracyjnym. Wprowadzenie do postępowania

¹ Dz.U. z 2014 r. poz. 183 z późn. zm.

² Dz.U. z 2019 r. poz. 934.

³ Dz.U. z 2022 r. poz. 329.

sądowoadministracyjnego instytucji doręczeń pism przy wykorzystaniu środków komunikacji elektronicznej wymuszone zostało niejako przez rozwój technologii oraz metod komunikacji międzyludzkiej. Niniejsze opracowanie ma na celu przedstawienie przede wszystkim praktycznych aspektów omawianej problematyki, które pojawiły się w orzecznictwie sądów administracyjnych.

Definicja dokumentu elektronicznego

Zgodnie z art. 3 pkt 2 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne⁴, dokument elektroniczny jest to stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych. Prawne definicje określają dokument jako treść lub przedmiot bądź informację⁵. Przez treść tego dokumentu należy rozumieć stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej. Tym samym treść, jako zbiór danych, musi spełniać wymagania ustawowe, tj. stanowić odrębną całość znaczeniową oraz być uporządkowana w określonej strukturze wewnętrznej. Ponadto ten zbiór danych powinien zostać zapisany na materiale lub urządzeniu służącym do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej, czyli informatycznym nośniku danych⁶. Dokumentem elektronicznym będzie zatem wyrażenie oświadczenia woli w postaci elektronicznej, podpisane

⁴ Dz.U. z 2021 r. poz. 2070.

⁵ G. Szpor [w:] C. Martysz, K. Wojsyk, G. Szpor, *Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz*, wyd. 2, Warszawa 2015, art. 3.

⁶ Uchwała NSA (7) z dnia 6 grudnia 2021 r., I FPS 2/21, CBOSA; B. Kwiatek, *Dokument elektroniczny w ogólnym postępowaniu administracyjnym*, Warszawa 2020, s. 110–118.

tw. kwalifikowanym podpisem elektronicznym. Natomiast zgodnie z art. 3 pkt 2 ustawy z dnia 18 listopada 2020 r. o doręczeniach elektronicznych⁷ dokument elektroniczny jest dokumentem, o którym mowa w art. 3 pkt 35 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE⁸, czyli każdą treścią przechowywaną w postaci elektronicznej, w szczególności tekst lub nagranie dźwiękowe, wizualne lub audiowizualne.

W postępowaniu sądowoadministracyjnym dokumentem elektronicznym będzie pismo wniesione za pomocą elektronicznej skrzynki podawczej sądu. Dokument sporządzony w formie pisemnej staje się zupełny dopiero w momencie opatrzenia go podpisem, gdyż na tej podstawie jest identyfikowany autor dokumentu⁹. Przepis art. 12b § 1 dodany do ustawy – Prawo o postępowaniu przed sądami administracyjnymi na mocy ustaw nowelizujących, rozszerza zakres dokumentów spełniających wymagania formy pisemnej na takie, które zostały sporządzone techniką elektroniczną. W odniesieniu do tych dokumentów czynnikiem identyfikującym autora pisma ma być bezpieczny podpis elektroniczny weryfikowany za pomocą ważnego kwalifikowanego certyfikatu lub podpis potwierdzony profilem zaufanym ePUAP albo przez zastosowanie innych mechanizmów, o których mowa w art. 20a uidp, jeżeli takie mechanizmy wprowadzi sąd administracyjny¹⁰.

W postępowaniu przed sądami administracyjnymi dokumentem elektronicznym nie będzie natomiast pismo wniesione za pośrednictwem poczty elektronicznej (e-mail) oraz za pośrednictwem telefaksu.

⁷ Dz.U. z 2022 r. poz. 569.

⁸ Dz.Urz. UE L 257/73.

⁹ M. Romańska [w:] *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, wyd. 6, red. T. Woś, Warszawa 2016, art. 12b.

¹⁰ *Ibidem*.

Dla skutecznego dokonania czynności procesowej w wyniku złożenia dokumentu elektronicznego wymagane jest bowiem zachowanie właściwej formy przewidzianej w przepisach ustawy – Prawo o postępowaniu przed sądami administracyjnymi, czyli złożenie pisma przez elektroniczną skrzynkę podawczą (art. 12b § 2 ppsa¹¹). Pojęcie elektronicznej skrzynki podawczej nie jest tożsame z adresem e-mail, choćby ten drugi był dostępny w przestrzeni publicznej¹². Poczta elektroniczna (adres e-mail) stanowi środek komunikacji elektronicznej i jest objęta definicją w art. 3 pkt 4 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne¹³, nie jest jednak tożsama z pojęciem elektronicznej skrzynki podawczej, która stanowi „dostępny publicznie środek komunikacji elektronicznej” i służy „do przekazywania dokumentu elektronicznego”¹⁴. Wniesiona za pośrednictwem skrzynki e-mail korespondencja nie wywołuje skutków prawnych w postępowaniach przed sądami administracyjnymi.

Doręczenie pisma procesowego za pośrednictwem faksu nie jest doręczeniem za pomocą środków komunikacji elektronicznej w rozumieniu przepisów o świadczeniu usług drogą elektroniczną. Zgodnie z treścią art. 2 pkt 4 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną¹⁵ przez świadczenie usługi drogą elektroniczną rozumie się wykonanie usługi świadczonej bez jednoczesnej obecności stron (na odległość), poprzez przekaz danych na indywidualne żądanie usługobiorcy, przesyłanej i otrzymywanej za pomocą urządzeń do elektronicznego przetwarzania, włącznie z kompresją cyfrową, i przechowywania danych, która jest w całości nadawana, odbierana lub transmitowana za pomocą sieci telekomunikacyjnej w rozumieniu ustawy z dnia 16 lipca 2004 r. – Prawo

¹¹ Dz.U. z 2022 r. poz. 329.

¹² Postanowienie NSA z dnia 15 czerwca 2021 r., III OSK 4856/21, CBOSA.

¹³ Dz.U. z 2021 r. poz. 2070.

¹⁴ Postanowienie NSA z dnia 27 kwietnia 2022 r., I OZ 134/22, CBOSA.

¹⁵ Dz.U. z 2020 r. poz. 344.

telekomunikacyjne¹⁶. Faks nie jest urządzeniem informatycznym, gdyż przez tego rodzaju urządzenia należy rozumieć komputery wyposażone w pamięć umożliwiającą zapisywanie i odtwarzanie danych. Z tego względu wysyłanie informacji pomiędzy urządzeniami faksowymi nie może być uznane za komunikowanie się za pomocą urządzeń tworzących zespół teleinformatyczny. W związku z powyższym tego rodzaju komunikowanie się nie może być uznane za świadczenie usług drogą elektroniczną, gdyż nie odbywa się ono za pośrednictwem systemu teleinformatycznego, a to z kolei przesądza o tym, że taki sposób przesyłania pism nie może być stosowany w postępowaniu administracyjnym¹⁷.

Elektroniczna skrzynka podawcza sądu

Wyjaśnić należy, że elektroniczna skrzynka podawcza sądu to „dostępny publicznie środek komunikacji elektronicznej służący do przekazywania dokumentu elektronicznego do podmiotu publicznego przy wykorzystaniu powszechnie dostępnego systemu teleinformatycznego” (art. 3 pkt 17 uidp). Zgodnie z art. 16 ust. 1a tej ustawy podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę, natomiast zgodnie z art. 2 pkt 1 ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną¹⁸ przez adres elektroniczny rozumieć należy oznaczenie systemu teleinformatycznego umożliwiające porozumiewanie się za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej. Elektroniczna skrzynka podawcza, wymagająca spełnienia

¹⁶ Dz.U. z 2022 r. poz. 1648.

¹⁷ Wyrok WSA w Warszawie z dnia 5 grudnia 2006 r., III SA/Wa 1836/06, CBOSA; wyrok WSA w Warszawie z dnia 9 lutego 2018 r., II SA/Wa 968/17, CBOSA.

¹⁸ Dz.U. z 2020 r. poz. 344.

standardów określonych i opublikowanych na ePUAP przez ministra właściwego do spraw informatyzacji, nie jest zatem tożsama z jakimkolwiek adresem elektronicznym czy „urzędową skrzynką mailową”, a funkcjonalność elektronicznej skrzynki podawczej zasadniczo wiąże się z dostarczaniem dokumentów do tzw. podmiotu publicznego. Stosownie do § 8 ust. 1 rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych¹⁹, minister właściwy do spraw informatyzacji umożliwia podmiotom publicznym tworzenie elektronicznych skrzynek podawczych na ePUAP. Doręczenia dokonywane za pomocą ePUAP uważa się za dokonane przez podmiot publiczny lub do podmiotu publicznego, który utworzył na ePUAP elektroniczną skrzynkę podawczą. Należy też podkreślić, że w przypadku odebrania dokumentu elektronicznego przez elektroniczną skrzynkę podawczą podmiotu publicznego poświadczenie przedłożenia jest automatycznie tworzone i udostępniane nadawcy tego dokumentu przez system teleinformatyczny służący do obsługi doręczeń (§ 13 ust. 1 rde). Jeżeli zatem pismo (podanie, wniosek, skarga) zostało przesłane drogą elektroniczną do podmiotu publicznego, zgodnie z warunkami korzystania z platformy ePUAP, to automatyczne wygenerowanie poświadczenia przedłożenia pozwala przyjąć przez nadawcę, że dokument ten wpłynął do urzędu.

Przesłanki dopuszczalności korzystania z doręczeń elektronicznych

Doręczanie pism za pomocą środków komunikacji elektronicznej w postępowaniu sądowoadministracyjnym następuje, zgodnie

¹⁹ Dz.U. z 2018 r. poz. 180.

z art. 74a § 1 i § 2 ppsa, po spełnieniu przez stronę jednego z następujących warunków: wniosła pismo w formie dokumentu elektronicznego przez elektroniczną skrzynkę podawczą sądu lub organu, za pośrednictwem którego składane jest pismo, wystąpiła do sądu o takie doręczenie i wskazała sądowi adres elektroniczny bądź wyraziła zgodę na doręczanie pism za pomocą tych środków i wskazała sądowi adres elektroniczny. Jeżeli strona zrezygnuje z doręczania pism za pomocą środków komunikacji elektronicznej, sąd doręcza pismo w sposób określony dla pisma w formie innej niż forma dokumentu elektronicznego. Oświadczenie o rezygnacji z doręczania pism za pomocą środków komunikacji elektronicznej składa się w formie dokumentu elektronicznego. Samo wpisanie adresu e-mail przez stronę postępowania administracyjnego we wniosku nie jest równoznaczne z wyrażeniem zgody na doręczanie pism w formie dokumentu elektronicznego²⁰. Stronie, która zrezygnuje z doręczania pism za pomocą środków komunikacji elektronicznej, korespondencja sądowa będzie doręczana w sposób tradycyjny.

W przypadku pism doręczanych uczestniczącym w postępowaniu przed sądem prokuratorowi, Rzecznikowi Praw Obywatelskich, Rzecznikowi Praw Dziecka oraz organowi, którego działanie, bezczynność lub przewlekłe prowadzenie postępowania zaskarżono, sąd przesyła pismo bezpośrednio do elektronicznej skrzynki podawczej podmiotu publicznego w rozumieniu uidp, za urzędowym poświadczeniem odbioru. Datą doręczenia tych pism jest data określona w urzędowym poświadczeniu odbioru²¹.

Sąd, kierując korespondencję do organu, który komunikował się z sądem w postaci papierowej, może dowolnie wybrać sposób tej komunikacji. Sąd może bowiem wysłać korespondencję w postaci papierowej, bądź też – kierując się tym, że organy zostały

²⁰ Wyrok WSA w Łodzi z dnia 6 maja 2021 r., III SA/Łd 97/21, CBOSA.

²¹ B. Dauter [w:] A. Kabat, M. Niezgódka-Medek, B. Dauter, *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, wyd. 2, LEX/el. 2021, art. 74(a).

zobowiązane do przyjmowania korespondencji elektronicznej – wysyłać ją za pośrednictwem środków komunikacji elektronicznej²². Stosownie do treści art. 74a § 10 ppsa pisma skierowane do pełnomocnika organu powinny być doręczane na adres elektronicznej skrzynki podawczej organu.

W celu doręczenia pisma w formie dokumentu elektronicznego na adres elektroniczny adresata zostanie wysłane zawiadomienie zawierające informację o możliwości odbioru pisma w formie dokumentu elektronicznego, wraz ze wskazaniem adresu elektronicznego, z którego adresat będzie mógł pobrać dokument i pod którym powinien dokonać potwierdzenia doręczenia dokumentu, a także pouczenie o sposobie odbioru tego pisma i informacja o wymogu podpisania urzędowego poświadczenia odbioru kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym. Datą doręczenia pisma jest data podpisania przez adresata pisma urzędowego poświadczenia odbioru. W przypadku nieodebrania tego pisma, po upływie 7 dni, licząc od dnia wysłania zawiadomienia, na adres elektroniczny adresata zostanie wysłane powtórne zawiadomienie o możliwości odebrania tego pisma. Po upływie 14 dni od dnia przesłania pierwszego zawiadomienia nieodebrana korespondencja sądowa będzie uważana za doręczoną.

Natomiast doręczenie pisma stronie będącej podmiotem publicznym na elektroniczną skrzynkę podawczą tego podmiotu następuje z chwilą wygenerowania urzędowego poświadczenia odbioru (urzędowe poświadczenie przedłożenia), co następuje automatycznie z chwilą wprowadzenia pisma do systemu odbiorcy (§ 8 ust. 3 rde oraz § 13 ust. 1 rde). Dokument w postaci urzędowego poświadczenia przedłożenia (UPP) jest generowany przez system teleinformatyczny podmiotu publicznego i przekazywany nadawcy. W praktyce oznacza to, że jeżeli wniesiono dokument elektroniczny na informatycznym nośniku danych, zgodnie z warunkami korzystania

²² Postanowienie NSA z dnia 21 kwietnia 2022 r., II GZ 105/22, LEX nr 3334836.

z platformy ePUAP, to automatyczne wygenerowanie UPP pozwala przyjąć, że dokument ten wpłynął do urzędu, samo zaś UPP, stosownie do § 11 ust. 1 pkt 1 rde, stanowi potwierdzenie doręczenia dokumentu elektronicznego. A zatem poświadczenie doręczenia przedłożenia (UPP) jest w takim przypadku niezaprzeczalnym urzędowym poświadczeniem odbioru. W obiegu korespondencji pomiędzy podmiotami publicznymi za moment doręczenia należy uznać wprowadzenie korespondencji do systemu informatycznego adresata, kiedy to automatycznie następuje podpisanie urzędowego poświadczenia odbioru w sposób przyjęty w danym systemie²³.

Dla skuteczności zawiadomienia, o którym mowa w art. 74a § 3 ppsa, o możliwości odbioru pisma w formie dokumentu elektronicznego, a w konsekwencji do uznania pisma za doręczone w trybie art. 74a § 8 ppsa, konieczne jest, aby nie tylko to pismo, lecz również dołączone do niego załączniki były opatrzone kwalifikowanym podpisem elektronicznym albo kwalifikowaną pieczęcią elektroniczną. Ta okoliczność powinna w sposób niebudzący wątpliwości zostać udokumentowana przez sąd w aktach sprawy²⁴, bowiem strony mają prawo oczekiwać, że otrzymywane z sądu pisma czy orzeczenia, będą spełniać ustawowe wymogi w zakresie prawidłowego doręczenia²⁵.

Wymogi formalne pisma procesowego wnoszonego w formie dokumentu elektronicznego w postępowaniu sądowoadministracyjnym

Każde pismo procesowe składane w formie dokumentu elektronicznego musi spełniać wymogi pisma procesowego przewidziane

²³ Postanowienie NSA z dnia 27 kwietnia 2022 r., III OZ 264/22, CBOSA.

²⁴ Postanowienie NSA z dnia 23 lutego 2022 r., II GZ 7/22, CBOSA.

²⁵ Postanowienie NSA z dnia 10 czerwca 2022 r., I FZ 265/21, CBOSA.

w art. 46 § 1 i 2 ppsa i zawierać co najmniej: oznaczenie sądu, do którego jest skierowane, imię i nazwisko lub nazwę stron, ich przedstawicieli ustawowych i pełnomocników, oznaczenie rodzaju pisma, osnovę wniosku lub oświadczenia (treść żądania), podpis strony albo jej przedstawiciela ustawowego lub pełnomocnika, wymienienie załączników. Jeżeli jest to pierwsze pismo w danej sprawie, to dodatkowo musi również zawierać oznaczenie miejsca zamieszkania, a w razie jego braku – adresu do doręczeń lub siedziby i adresów stron, ich przedstawicieli ustawowych i pełnomocników.

Ponadto zmiana przepisów ustawy – Prawo o postępowaniu przed sądami administracyjnymi wprowadziła nowe wymogi formalne dla pism procesowych w postępowaniu sądowoadministracyjnym. W celu zapewnienia jednoznacznego określenia stron postępowania oraz ich przedstawicieli wprowadzony został obowiązek wskazywania w pierwszym piśmie procesowym numeru odpowiedniego identyfikatora, tj. numeru PESEL – w przypadku osób fizycznych, a w przypadku osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej – numeru KRS, REGON lub NIP.

Poza wymogami formalnymi pisma w postaci papierowej, pisma procesowe składane drogą elektroniczną muszą zawierać adres elektroniczny oraz zostać podpisane przez stronę albo jej przedstawiciela ustawowego lub pełnomocnika kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym. Zasady te dotyczą także załączników wnoszonych w formie dokumentu elektronicznego. Opatrzanie pisma przewodniego zaufanym podpisem elektronicznym nie skutkuje podpisaniem całego dokumentu elektronicznego, w tym skargi stanowiącej załącznik do tego dokumentu²⁶.

²⁶ Postanowienia NSA z dnia: 9 października 2020 r., I OZ 814/20; 29 października 2020 r., I OZ 814/20; 13 listopada 2020 r., I OZ 884/20; 26 listopada 2020 r., I OZ 938/20 i I OZ 987/20; 9 grudnia 2020 r., I OZ 1032/20; 11 grudnia 2020 r.,

Naczelny Sąd Administracyjny w uchwale z dnia 6 grudnia 2021 r., I FPS 2/21, wskazał, że zgodnie z art. 57 § 1 w zw. z art. 46 § 1 pkt 4 oraz art. 12b § 1 i art. 46 § 2a i 2b ppsa skargę stanowiącą załącznik do formularza pisma ogólnego, podpisanego podpisem zaufanym, przesłanego przez platformę ePUAP, należy uznać za podpisaną jedynie wówczas, gdy została ona odrębnie podpisana podpisem kwalifikowanym, podpisem zaufanym albo podpisem osobistym. Wymóg podpisania skargi ma zatem na celu legitymizację jej treści przez skarżącego albo przez osobę działającą w jego imieniu. Rozważania te pozostają aktualne także w odniesieniu do pisma procesowego składanego przez ePUAP. Podpisanie pisma procesowego, a w szczególności skargi, potwierdza wolę skierowania do sądu administracyjnego środka prawnego o określonej treści. Taka interpretacja zmierza do tego, aby nie było wątpliwości, czy w istocie strona załączyła do pisma ogólnego w platformie ePUAP zamierzoną treść skargi (pisma procesowego). Pewności tej brakuje, gdy podpisane zostało tylko pismo przewodnie, które w swojej treści nie zawiera żadnych elementów skargi (pisma procesowego), ograniczając się do poinformowania o przesłaniu skargi (pisma) jako załącznika do niego²⁷. W związku z tym, zgodnie z art. 57 § 1 w zw. z art. 46 § 1 pkt 4 oraz art. 12b § 1 i art. 46 § 2a i 2b ppsa, skargę (pismo procesowe) stanowiącą załącznik do formularza pisma ogólnego, podpisanego podpisem zaufanym, przesłanego przez platformę ePUAP, należy uznać za podpisaną jedynie wówczas, gdy została ona odrębnie podpisana podpisem kwalifikowanym, podpisem zaufanym albo podpisem osobistym²⁸.

I OZ 1000/20 i I OZ 1003/20; 15 grudnia 2020 r., I OZ 1048/20; 22 marca 2021 r., III OZ 77/21, CBOSA.

²⁷ P. Iżycki, *O wymogu podpisania pisma wniesionego do sądu administracyjnego w formie dokumentu elektronicznego*, ZNSA 2021, nr 6, s. 75–86.

²⁸ Uchwała NSA (7) z dnia 6 grudnia 2021 r., I FPS 2/21, LEX nr 3274617.

Szczegółowe zasady stosowania podpisu elektronicznego określa rozporządzenie eIDAS²⁹, które weszło w życie dnia 1 lipca 2016 r. Stosownie do art. 3 pkt 10 rozporządzenia eIDAS podpis elektroniczny oznacza dane w postaci elektronicznej, które są dołączone lub logicznie powiązane z innymi danymi w postaci elektronicznej i które użyte są przez podpisującego jako podpis. Zgodnie natomiast z art. 3 pkt 11 rozporządzenia eIDAS kwalifikowany podpis elektroniczny oznacza zaawansowany podpis elektroniczny, który jest składany za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego i który opiera się na kwalifikowanym certyfikacie podpisu elektronicznego. Jednocześnie art. 25 ust. 2 tego rozporządzenia wprowadza zasadę, zgodnie z którą kwalifikowany podpis elektroniczny ma skutek prawny równoważny podpisowi własnoręcznemu. Podpis zaufany stosownie do art. 3 pkt 14a uidp to podpis, którego autentyczność i integralność są zapewniane przy użyciu pieczęci elektronicznej ministra właściwego do spraw informatyzacji. Do zapewnienia tej integralności zastosowano zaawansowaną pieczęć elektroniczną weryfikowaną za pomocą kwalifikowanego certyfikatu pieczęci elektronicznej. Zgodnie natomiast z art. 3 pkt 1 i 2 ustawy z dnia 18 września 2001 r. o podpisie elektronicznym³⁰, podpis elektroniczny oznacza dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny. Z kolei bezpieczny podpis elektroniczny to podpis elektroniczny, który: jest przyporządkowany wyłącznie do osoby składającej ten podpis, jest sporządzany za pomocą podlegających

²⁹ eIDAS (ang. electronic IDentification, Authentication and trust Services) – zob. rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (dokument obowiązuje w całej Unii Europejskiej od dnia 1 lipca 2016 r. i jest stosowany bezpośrednio w polskim porządku prawnym).

³⁰ Dz.U. z 2013 r. poz. 262 z późn. zm.

wyłącznej kontroli osoby składającej podpis elektroniczny bezpiecznych urządzeń służących do składania podpisu elektronicznego i danych służących do składania podpisu elektronicznego, a nadto jest powiązany z danymi, do których został dołączony, w taki sposób, że jakakolwiek późniejsza zmiana tych danych jest rozpoznawalna.

Mając powyższe na względzie, wskazać należy, że pismo procesowe doręczone w formie elektronicznej, opatrzone podpisem elektronicznym weryfikowanym za pomocą ważnego certyfikatu, będzie równoważne pod względem skutków prawnych pismom procesowym opatrzonym podpisami własnoręcznymi, chyba że przepisy odrębne będą wymagać właśnie podpisu odręczego.

Podsumowanie

Możliwość wnoszenia przez strony oraz doręczania przez sąd pism procesowych za pośrednictwem środków komunikacji elektronicznej w postępowaniu sądownoadministracyjnym ma niewątpliwie wiele zalet. Zwrócić należy uwagę, że omawiane w niniejszym opracowaniu przepisy weszły w życie w 2019 r., ale ich szersze zastosowanie nastąpiło dopiero w wyniku pandemii. Do zalet takiego obiegu dokumentów należy zaliczyć nie tylko bezpieczeństwo zdrowotne, tak istotne zwłaszcza wobec wątpliwości co do możliwości przenoszenia wirusa drogą papierową, ale również szybkość biegu korespondencji oraz bardzo duże oszczędności, nie tylko dla stron, ale również dla Skarbu Państwa. Niewątpliwie kwestią przyszłości jest uznanie za standard obrotu całej korespondencji w takiej formie, jednak należy ciągle pamiętać o tym, że w sprawach sądownoadministracyjnych wiele osób fizycznych występuje osobiście, bez pomocy profesjonalnego pełnomocnictwa, i często są to osoby ubogie, zaliczane do kategorii osób tzw. wykluczonych cyfrowo. Dopóki ta kwestia nie zostanie rozwiązana całkowicie, nie może być mowy o zastąpieniu obiegu dokumentacji w formie tradycyjnej.

Bibliografia

Akty normatywne

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE (Dz.Urz. UE L 257/73).
2. Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym (t.j. Dz.U. z 2013 r. poz. 262 z późn. zm.).
3. Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2020 r. poz. 344).
4. Ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz.U. z 2022 r. poz. 329).
5. Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (t.j. Dz.U. z 2022 r. poz. 1648).
6. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2021 r. poz. 2070).
7. Ustawa z dnia 10 stycznia 2014 r. o zmianie ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne oraz niektórych innych ustaw (Dz.U. z 2014 r. poz. 183 z późn. zm.).
8. Ustawa z dnia 12 kwietnia 2019 r. o zmianie ustawy – Prawo o postępowaniu przed sądami administracyjnymi oraz niektórych innych ustaw (Dz.U. z 2019 r. poz. 934).
9. Ustawa z dnia 18 listopada 2020 r. o doręczeniach elektronicznych (t.j. Dz.U. z 2022 r. poz. 569).
10. Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (t.j. Dz.U. z 2018 r. poz. 180).

Literatura przedmiotu

1. Dauter B. [w:] A. Kabat, M. Niezgódka-Medek, B. Dauter, *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, wyd. 2, LEX/el. 2021.
2. Iżycki P., *O wymogu podpisania pisma wniesionego do sądu administracyjnego w formie dokumentu elektronicznego*, ZNSA 2021, nr 6.
3. Kwiatek B., *Dokument elektroniczny w ogólnym postępowaniu administracyjnym*, Warszawa 2020.
4. Romańska M. [w:] *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, wyd. 6, red. T. Woś, Warszawa 2016.
5. Szpor G. [w:] C. Martysz, K. Wojsyk, G. Szpor, *Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz*, wyd. 2, Warszawa 2015.

Orzecznictwo

1. Uchwała NSA (7) z dnia 6 grudnia 2021 r., I FPS 2/21, CBOSA.
2. Postanowienie NSA z dnia 9 października 2020 r., I OZ 814/20, CBOSA.
3. Postanowienie NSA z dnia 29 października 2020 r., I OZ 814/20, CBOSA.
4. Postanowienie NSA z dnia 13 listopada 2020 r., I OZ 884/20, CBOSA.
5. Postanowienie NSA z dnia 26 listopada 2020 r., I OZ 938/20, CBOSA.
6. Postanowienie NSA z dnia 26 listopada 2020 r., I OZ 987/20, CBOSA.
7. Postanowienie NSA z dnia 9 grudnia 2020 r., I OZ 1032/20, CBOSA.
8. Postanowienie NSA z dnia 11 grudnia 2020 r., I OZ 1000/20, CBOSA.
9. Postanowienie NSA z dnia 11 grudnia 2020 r., I OZ 1003/20, CBOSA.
10. Postanowienie NSA z dnia 15 grudnia 2020 r. I OZ 1048/20, CBOSA.
11. Postanowienie NSA z dnia 22 marca 2021 r., III OZ 77/21, CBOSA.
12. Postanowienie NSA z dnia 15 czerwca 2021 r., III OSK 4856/21, CBOSA.
13. Postanowienie NSA z dnia 23 lutego 2022 r., II GZ 7/22, CBOSA.

14. Postanowienie NSA z dnia 21 kwietnia 2022 r., II GZ 105/22, LEX nr 3334836.
15. Postanowienie NSA z dnia 27 kwietnia 2022 r., I OZ 134/22, CBOSA.
16. Postanowienie NSA z dnia 27 kwietnia 2022 r., III OZ 264/22, CBOSA.
17. Postanowienie NSA z dnia 10 czerwca 2022 r., I FZ 265/21, CBOSA.
18. Wyrok WSA w Warszawie z dnia 5 grudnia 2006 r., III SA/Wa 1836/06, CBOSA.
19. Wyrok WSA w Warszawie z dnia 9 lutego 2018 r., II SA/Wa 968/17, CBOSA.
20. Wyrok WSA w Łodzi z dnia 6 maja 2021 r., III SA/Łd 97/21, CBOSA.

Streszczenie

Opracowanie stanowi analizę zagadnienia odnoszącego się do wnoszenia oraz doręczania pism za pośrednictwem środków komunikacji elektronicznej.

W pierwszej części tekstu przeanalizowano pojęcie dokumentu elektronicznego. Wskazano także, że e-mail oraz faks nie stanowią środków komunikacji elektronicznej w postępowaniu przed sądami administracyjnymi. W drugiej części tekstu wyjaśniono pojęcie skrzynki podawczej sądu, a w części trzeciej omówiono przesłanki dopuszczalności korzystania z doręczeń elektronicznych. Czwarta część zawiera przedstawienie wymogów formalnych pisma procesowego składanego w formie dokumentu elektronicznego.

W podsumowaniu zwrócono uwagę na kategorię osób tzw. wykluczonych cyfrowo. Dopóki ta kwestia nie zostanie rozwiązana całkowicie, nie może być mowy o zastąpieniu obiegu dokumentacji w formie tradycyjnej.

Słowa kluczowe

dokument elektroniczny, ePUAP, skrzynka podawcza sądu, doręczenie elektroniczne

SĄDOWNICTWO ADMINISTRACYJNE W DOBIE INFORMATYZACJI – OCENA WYBRANYCH ROZWIĄZAŃ I PERSPEKTYWY NA PRZYSZŁOŚĆ

BEATA ZAJĄC-DUTKIEWICZ

UCZELNIA ŁAZARSKIEGO

 0009-0005-8193-5341

BOŻENA DĄBKOWSKA-MASTALEREK

UCZELNIA ŁAZARSKIEGO

 0000-0001-6034-3839

Wstęp

Od dłuższego już czasu obserwujemy rozwój procesu informatyzacji państwa, który ma na celu stworzenie społeczeństwa informacyjnego. Jest to jeden z priorytetów zarówno Polski, jak i Unii Europejskiej. Organy władzy publicznej mają za zadanie zapewnić powszechny dostęp online do informacji publicznych, a także umożliwić załatwianie spraw administracyjnych za pośrednictwem systemów informatycznych.

Opracowanie stanowi analizę możliwości oraz problemów, jakie występują w sądownictwie administracyjnym w związku z wnoszeniem przez strony pism w formie dokumentu elektronicznego, udostępnianiem akt w systemie elektronicznym oraz rozpraw, w których strony postępowania oraz publiczność mogą uczestniczyć, przebywając poza budynkiem sądu (rozprawy zdalne).

Rozważania prowadzone są na podstawie działań podejmowanych w WSA w Gliwicach oraz WSA w Warszawie.

Przedmiot opracowania przedstawiony został z punktu widzenia osób pracujących w sądzie i stykających się na co dzień z problemami dotyczącymi informatyzacji.

Wnoszenie pism w formie dokumentu elektronicznego

Od kilku lat działa system elektroniczny umożliwiający załatwianie spraw administracyjnych poprzez sieć internetową. Taka elektroniczna platforma usług administracji publicznej zwana jest potocznie ePUAP. Podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone w przepisach prawa i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę¹. Ta elektroniczna skrzynka podawcza to nic innego, jak dostępny publicznie środek komunikacji elektronicznej służący do przekazywania dokumentu elektronicznego do podmiotu publicznego przy wykorzystaniu powszechnie dostępnego systemu teleinformatycznego².

Informatyzacja administracji publicznej przekłada się także na informatyzację sądownictwa administracyjnego³. Przejawem tego procesu jest możliwość wnoszenia za pomocą systemu ePUAP pism, w tym skarg do sądów administracyjnych. Przepisy umożliwiające wnoszenie pism elektronicznie do sądów administracyjnych funkcjonują od dnia 31 maja 2019 r., wtedy to określone zostały wszelkie

¹ Art. 16 pkt 1a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2021 r. poz. 2070).

² Art. 3 pkt 17 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz.U. z 2022 r. poz. 902 z późn. zm.).

³ Por. P. Pietrasz, *Informatyzacja polskiego postępowania przed sądami administracyjnymi a jego zasady ogólne*, Warszawa 2020.

wymogi formalne. Procedura wnoszenia pism elektronicznych do sądu jest szczegółowo uregulowana przepisami ustawy – Prawo o postępowaniu przed sądami administracyjnymi. I tak formułę wnoszenia pism w formie elektronicznej określa art. 12b § 2 ppsa. Dokumenty elektroniczne wnosi się do sądu administracyjnego przez elektroniczną skrzynkę podawczą, a sąd doręcza takie dokumenty stronom za pomocą środków komunikacji elektronicznej⁴.

Pisma elektronicznie kierować można więc tylko poprzez platformę ePUAP, nie można kierować do sądu pism poprzez pocztę e-mail. Pismo wysłane na adres elektroniczny sądu (adres e-mail) z pominięciem platformy ePUAP nie wywołuje skutku, który związany jest ze złożeniem wniosku do sądu. Pisma w postępowaniu sądowym to pisma sądowe oraz pisma procesowe. Do pism sądowych należą orzeczenia (wyroki i postanowienia), zarządzenia, protokoły, notatki oraz inne pisma sądowe, w tym zawiadomienia i wezwania. Pisma procesowe zaś to te, które pochodzą od stron postępowania, a sąd, zgodnie z zasadą oficjalności doręczeń, zobowiązany jest doręczać je pozostałym stronom i uczestnikom postępowania⁵. Przepisy ustawy – Prawo o postępowaniu przed sądami administracyjnymi umożliwiają stronom postępowania otrzymywanie pism procesowych w formie elektronicznej bądź papierowej. Sąd administracyjny w celu doręczania pism w postępowaniu przekształca ich postać. A zatem jeśli otrzyma od jednej ze stron postępowania pismo w formie elektronicznej, wówczas sporządza uwierzytelniony wydruk takiego pisma, a następnie przesyła je drugiej stronie, która zdecydowała się na korespondowanie z sądem w formie tradycyjnej, papierowej. Gdy zaś do sądu administracyjnego wpłynie pismo w formie papierowej, urzędnik sporządza jego uwierzytelniony odpis w formie dokumentu elektronicznego (art. 12b

⁴ Art. 74a ppsa.

⁵ Por. B. Dauter, B. Gruszczyński, A. Kabat, M. Niezgódka-Medek, *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, Warszawa 2011, s. 261.

§ 3 pkt 1 i 2 ppsa) i następnie przesyła go stronie korespondującej za pomocą ePUAP. Nie ma więc przeszkód, by w ramach jednego postępowania sądowego każda ze stron korespondowała w innej formie. Jest to jedynie pracochłonne i czasochłonne dla urzędników sądowych.

Należy podkreślić, że przepisy ustawy – Prawo o postępowaniu przed sądami administracyjnymi dotyczące zastosowania środków komunikacji elektronicznej stosuje się odpowiednio do organów. Jest to o tyle istotne, że do organów oraz za ich pośrednictwem składane są pisma w formie dokumentu elektronicznego.

Strona postępowania stosująca formę korespondencji papierową, mimo iż wybrała taką formę korespondencji, jest informowana o warunkach wnoszenia oraz doręczania pism za pomocą środków komunikacji elektronicznej (art. 12b § 4 i 5 ppsa). Jeżeli strona zdecyduje się na korespondencję elektroniczną w pierwszym piśmie kierowanym w formie papierowej do sądu, musi podać swój adres ePUAP. Wygodniejsze i pewniejsze jest więc przy wyborze elektronicznej formy doręczeń wnoszenie pierwszego pisma do sądu drogą elektroniczną poprzez swoją skrzynkę ePUAP, eliminuje to bowiem ryzyko podania niewłaściwego adresu elektronicznego w piśmie wnoszonym w formie papierowej⁶. Jeżeli zaś pismo wniesiono w formie papierowej, a zawiera ono żądanie o doręczanie pism elektronicznie, jednocześnie strona nie podaje adresu elektronicznego, doręczenie pism przez sąd następuje w formie papierowej, na wskazany przez stronę adres, przy czym w pierwszym piśmie sąd poucza o warunku podania adresu elektronicznego w żądaniu doręczania pism środkami komunikacji elektronicznej⁷. W przypadku gdy pismo strony jest wnoszone w formie dokumentu elektronicznego, powinno zawierać adres elektroniczny oraz zostać podpisane przez stronę albo jej przedstawiciela ustawowego lub

⁶ Por. M. Kwietko-Bębnowski, *Informatyzacja sądów administracyjnych*, LEX/el. 2020.

⁷ Art. 46 § 2d ppsa.

pełnomocnika kwalifikowanym podpisem elektronicznym, podpisem zaufanym (art. 46 § 2a ppsa). Jeżeli takie pismo elektroniczne nie zawiera adresu elektronicznego, sąd przyjmuje, że właściwy jest adres elektroniczny, z którego nadano pismo wniesione w formie dokumentu elektronicznego. Pamiętać należy, że zainicjowanie postępowania sądownoadministracyjnego w formie elektronicznej obliguje sąd – do czasu złożenia przez skarżącego oświadczenia odpowiedniej treści (art. 74a § 2 ppsa) – do doręczenia kolejnych pism w danym postępowaniu w formie elektronicznej. Urzędowe poświadczenie odbioru generowane przez system musi bowiem w swej treści zawierać informację o tym, że dalsze pisma w postępowaniu będą doręczane za pomocą środków komunikacji elektronicznej⁸. Korespondując z sądem w formie elektronicznej, zwrócić należy uwagę, a często umyka to stronom postępowania, że w przypadku nieodebrania korespondencji zastosowane będzie doręczenie zastępcze. Jasną sprawą jest, że pismo sądowe doręczone w formie dokumentu elektronicznego obliguje sąd do ustalenia poświadczenia odbioru, zgodnie z art. 74a § 5 ppsa. Datą doręczenia pisma jest data podpisania przez adresata pisma urzędowego poświadczenia odbioru i tu sprawa nie budzi wątpliwości. Jednak należy mieć na uwadze, że w przypadku elektronicznego doręczenia pism także obowiązuje instytucja doręczenia zastępczego. W przypadku nieodebrania korespondencji system wylicza 14 dni od przesłania dokumentu na właściwy, podany przez stronę adres ePUAP i na UPD pojawia się wówczas data doręczenia zastępczego.

Wymagania szczegółowe odnośnie do pism elektronicznych regulują przepisy rozporządzenia Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów

⁸ J.G. Firlus, *Warunki formalne skargi* [w:] *Pełnomocnik w postępowaniu administracyjnym i sądownoadministracyjnym*, red. H. Knysiak-Sudyka, Warszawa 2020, s. 383.

i kopii dokumentów elektronicznych⁹. I tak zgodnie z § 17 ust. 1 tego rozporządzenia pisma wnoszone za pomocą elektronicznej skrzynki podawczej sporządza się w formacie danych XML na podstawie wzorów dokumentów elektronicznych umieszczonych w centralnym repozytorium lub lokalnym repozytorium. Załączniki dodawane do pism zapisuje się w formatach danych i w sposób uwzględniający przepisy wydane na podstawie art. 18 uidp. Należy jednak pamiętać, że załącznik do formularza przesłanego poprzez ePUAP, aby mógł odnieść skutki prawne, musi zostać odrębnie podpisany podpisem elektronicznym.

Kierowanie korespondencji w formie elektronicznej do sądów administracyjnych – problemy praktyczne

W kilkuletniej już praktyce wnoszenia pism do wojewódzkich sądów administracyjnych drogą elektroniczną można zaobserwować ciągle jeszcze zbyt częste problemy zarówno w odniesieniu do sposobu przesyłania dokumentów przez organy administracji publicznej, jak i pism, zwłaszcza skarg wnoszonych przez strony skarżące.

I tak, dość często strony postępowania kierują do sądu korespondencję e-mailem, mimo że o sposobie korespondencji elektronicznej strona jest pouczana w pierwszym kierowanym do niej piśmie. Także na stronie internetowej sądu znajduje się pouczenie, że pismo w formie dokumentu elektronicznego wnosi się wyłącznie przez elektroniczną skrzynkę podawczą sądu¹⁰.

Co bardzo istotne, zasady podpisywania pism elektronicznych dotyczą także załączników wnoszonych w formie dokumentu

⁹ Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (t.j. Dz.U. z 2018 r. poz. 180).

¹⁰ Por. BIP [online:] <http://www.gliwice.wsa.gov.pl/-ePUAP> [dostęp: 07.06.2022].

elektronicznego. I właśnie najczęstszym problemem jest podpisywanie podpisem elektronicznym jedynie pisma przewodniego, zaś załącznik pisma, a jest to przeważnie skarga, nie jest już podpisany przez stronę skarżącą. Pamiętać należy, że brak podpisu pod skargą stanowi jej brak formalny, implikuje konieczność wezwania do jego usunięcia, a nieusunięcie takiego braku formalnego powoduje odrzucenie skargi. W orzecznictwie sądowoadministracyjnym istniały poważne rozbieżności co do tego, czy podpisanie pisma przewodniego jest równoznaczne z podpisaniem załączników tego pisma. I tak wykształciły się dwie przeciwstawne linie orzecznicze. Część sędziów uznawała, że opatrzenie formularza zaufanym podpisem nie skutkuje podpisaniem pisma stanowiącego do niego załącznik. W ramach tej linii sądy powoływały się na możliwość odrębnego podpisania każdego z załączników do korespondencji wysyłanej przez ePUAP poprzez narzędzia zewnętrzne, w tym tzw. podpisywarkę. Zaś pozostali sędziowie odmiennie twierdzili, że złożenie podpisu zaufanego na formularzu obejmuje również załączone do niego pliki. Argumentacja ta opierała się m.in. na zasadach korzystania z ePUAP opublikowanych na oficjalnej stronie tej platformy¹¹. Kwestia ta została uregulowana uchwałą NSA¹². Naczelny Sąd Administracyjny stanął na stanowisku, że należy podpisywać i załącznik, i pismo przewodnie. Podkreślić w tym miejscu trzeba, że wymóg podpisania skargi ma na celu legitymizację jej treści przez skarżącego. Podpisanie skargi potwierdza wolę danej osoby skierowania do sądu administracyjnego środka prawnego o określonej treści. Wymóg ten eliminuje więc wątpliwości, czy w istocie strona załączyła do pisma przewodniego w platformie ePUAP zamierzoną treść skargi, co zapobiega np. podrobieniu skargi, czy

¹¹ Por. A. Kalicińska, A. Stępień, *Zasady podpisywania pism elektronicznych wnoszonych do sądu administracyjnego. Glosa do uchwały NSA z dnia 6 grudnia 2021 r., I FPS 2/21*, „Przegląd Podatkowy” 2022, nr 6, s. 44–45.

¹² Uchwała NSA (7) z dnia 26 grudnia 2021 r. I FPS 2/21, CBOSA.

też zmianie jej treści przez osoby do tego nieuprawnione. Pewności tej brakuje wówczas, gdy podpisane zostało tylko pismo przewodnie, które w swojej treści nie zawiera żadnych elementów skargi, lecz ogranicza się do poinformowania o jej przesłaniu w formie niepodpisanego załącznika do wspomnianego pisma przewodniego¹³. Należy mieć na uwadze fakt, że brak technicznej możliwości podpisania załącznika z poziomu ePUAP nie wyklucza podpisania takiego dokumentu w innym miejscu, za pośrednictwem odrębnej usługi w domenie gov.pl, poprzez tzw. podpisywarkę, a następnie dołączenia do korespondencji. Nie ma więc przeszkód technicznych, aby strona podpisała skargę w formie podpisu zaufanego, podpisu kwalifikowanego.

Często zdarzającym się uchybieniem po stronie skarżących, jak i organów jest przesyłanie do sądu skanów dokumentów papierowych, w tym skarg, czy też odpowiedzi na skargę. Takie sporządzone i podpisane papierowo dokumenty są skanowane i przesyłane do sądu, oczywiście z naruszeniem ustawy – Prawo o postępowaniu przed sądami administracyjnymi. W takiej sytuacji strona wyzywana jest do usunięcia braków formalnych pisma poprzez jego podpisanie.

Kolejnym uchybieniem jest przesyłanie akt administracyjnych przez organy administracji publicznej w złej formie, czyli jako niepogrupowane w sposób zgodny z ustawą.

Problemem jest również weryfikacja prawidłowości podpisu dokumentu elektronicznego. Właściwe byłoby, aby weryfikacja podpisu odbywała się poprzez jedno kliknięcie w systemie EZD (Elektroniczne Zarządzanie Dokumentacją). Niestety podpis taki trzeba weryfikować poprzez kilka programów (np. szafir, PWPW), co jest niekiedy bardzo czasochłonne.

¹³ P. Iżycki, *O wymogu podpisania pisma wniesionego do sądu administracyjnego w formie dokumentu elektronicznego*, ZNSA 2021, nr 6, s. 78–79.

Rozprawy zdalne w sądach administracyjnych

Epidemia COVID-19 spowodowała zmiany w postępowaniu przed sądami administracyjnymi, które miały na celu umożliwienie dbania o swoje sprawy bez konieczności osobistej obecności w siedzibie sądu. Zgodnie z art. 15 zys¹⁴ ustawy o COVID-19¹⁴ rozprawy odbywają się przy użyciu urządzeń technicznych umożliwiających przeprowadzenie rozpraw na odległość z jednoczesnym bezpośrednim przekazem obrazu i dźwięku, z tym że osoby w nich uczestniczące nie muszą przebywać w budynku sądu.

Warunkiem uczestnictwa w rozprawie zdalnej jest złożenie wniosku. Stronie postępowania umożliwia się udział w rozprawie zdalnej, jeśli tylko strona posiada ku temu techniczne możliwości. Udział w rozprawie zdalnej w wojewódzkich sądach administracyjnych odbywa się za pomocą aplikacji komputerowej komunikatora Webex¹⁵.

Sąd doręcza link umożliwiający udział w rozprawie oraz numer telefonu na salę rozpraw w celu zgłaszania ewentualnych nieprawidłowości. Warto pamiętać, że w przypadku uczestniczenia w rozprawie zdalnej nie jest technicznie możliwe składanie dokumentów za pośrednictwem komunikatora Webex.

Odnosnie do pism składanych przez strony w krótkim okresie przed terminem rozprawy pamiętać należy, że pismo procesowe jednej strony musi być przesłane przez sąd innym stronom postępowania. Sytuacja jest prosta, gdy wszystkie strony komunikują się z sądem za pomocą ePUAP. Jeśli choć jedna ze stron nie ma ePUAP,

¹⁴ 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 2020 r. poz. 1842 z późn. zm.), w brzmieniu nadanym przez art. 4 pkt 3 ustawy z dnia 28 maja 2021 r. o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz.U. z 2021 r. poz. 1090).

¹⁵ Rozprawy zdalne w sądach powszechnych odbywają się za pomocą m.in. aplikacji: ZOOM, SCOPIA, JITSI.

to sąd musi doręczyć jej pismo procesowe w formie papierowej. W takiej sytuacji jeśli w sprawie należy uiścić koszty sądowe¹⁶, sąd wzywa wnoszącego pismo do uiszczenia opłaty kancelaryjnej w wysokości 50 groszy¹⁷ za jedną stronę pisma, pod rygorem pozostawienia pisma bez rozpoznania. Dopiero po uiszczeniu opłaty kancelaryjnej i – o czym nie można zapominać – po zaksięgowaniu tej opłaty (co z przyczyn technicznych zajmuje czasem nawet kilka dni) sąd wykonuje odpis pisma oraz przesyła je stronie w formie papierowej za pośrednictwem Poczty Polskiej S.A. Z powyższych przyczyn od przesłania pisma za pomocą ePUAP do doręczenia odpisu tego pisma stronie, która nie posiada ePUAP, może upłynąć nawet kilka tygodni.

Jeśli chodzi o rozprawy zdalne, to należy zaznaczyć, że wnioski i twierdzenia strony uczestniczącej w rozprawie zdalnej są zapisywane w protokole tak samo jak wnioski strony obecnej na sali rozpraw.

Rozprawy zdalne są zatem kolejnym krokiem w stronę informatyzacji postępowania sądowego w sądach administracyjnych. Niewątpliwe zalety rozpraw zdalnych są takie, że strona postępowania może uczestniczyć w rozprawie, przebywając we własnym domu, może ustnie składać wnioski i oświadczenia, słyszy wydane przez sąd orzeczenie kończące postępowanie, a także uzasadnienie podjętego rozstrzygnięcia. Istotne jest również to, że na rozprawie zdalnej może być obecna publiczność. Z praktyki wynika, że dość często osoby niebędące stroną postępowania biorą udział w tego rodzaju rozprawach. Zaletą jest również okoliczność, że ustawodawca nie wyłączył możliwości fizycznej obecności na sali rozpraw tej strony, która nie chce lub nie może łączyć się zdalnie.

¹⁶ Art. 220 § 1 w zw. z art. 235a ppsa.

¹⁷ § 1 ust. 3 rozporządzenia Rady Ministrów z dnia 3 czerwca 2019 r. w sprawie wysokości opłat kancelaryjnych pobieranych w sprawach sądowoadministracyjnych (Dz.U. z 2019 r. poz. 1090).

Wadą rozpraw zdalnych jest na pewno konieczność składania wniosku o przeprowadzenie tego rodzaju rozprawy¹⁸. Link na rozprawę zdalną nie jest zatem udostępniany stronom z urzędu w momencie wyznaczenia terminu rozprawy. Jest on przesyłany dopiero po złożeniu stosownego wniosku.

Postulatem *de lege ferenda* może być umożliwienie uczestnictwa w rozprawie zdalnej na przykład w siedzibie urzędu gminy, w sytuacji gdy strona nie posiada odpowiedniego sprzętu.

Portal akt sądowych sądów administracyjnych

Przejawem zmian, które niesie za sobą informatyzacja sądownictwa administracyjnego jest na pewno system PASSA, czyli Portal Akt Sądowych Sądów Administracyjnych. Służy on udostępnianiu akt sądowoadministracyjnych w systemie teleinformatycznym¹⁹.

Strona postępowania ma możliwość złożenia do sądu administracyjnego wniosku o udostępnienie akt w PASSA. Konieczne jest podanie numeru PESEL osoby, której udostępnione mają być akta sprawy. Zatem w przypadku spółek, fundacji, stowarzyszeń podmioty te muszą upoważnić konkretną osobę fizyczną – pracownika, adwokata, radcę prawnego – do przeglądania akt. Dostęp do akt jest udzielany tej konkretnej osobie, a nie spółce czy fundacji.

Udostępnianie w PASSA jedynie akt sądowych jest jednocześnie największą wadą tego systemu. Pamiętać należy, że to w aktach administracyjnych znajdują się dokumenty, od których zależy merytoryczne rozstrzygnięcie sprawy.

¹⁸ Zob. [online:] [www.bip.warszawa.wsa.gov.pl / rozprawy zdalne / informacje ogólne dotyczące rozpraw jawnych](http://www.bip.warszawa.wsa.gov.pl/rozprawy_zdalne/informacje_ogolne_dotyczace_rozpraw_jawnych) [dostęp: 21.07.2022].

¹⁹ Zob. [online:] [www.bip.warszawa.wsa.gov.pl / Portal Akt Sądowych – PASSA](http://www.bip.warszawa.wsa.gov.pl/Portal_Akt_Sadowych_-_PASSA) [dostęp: 21.07.2022].

Po upływie 6 miesięcy od prawomocnego zakończenia postępowania dostęp do akt sądowych w systemie PASSA jest odbierany.

Od strony technicznej dostęp do akt sprawy przebiega w ten sposób, że urzędnik skanuje wszystkie karty akt sądowych. Następnie wprowadza je do zewnętrznego systemu PASSA. Dziwić może konieczność skanowania każdej karty akt sądowych, jednak pamiętać należy, że w sądach administracyjnych w Polsce akta sądowe prowadzone są w formie papierowej. Zarządzenia sędziów nanoszone są czasem bezpośrednio na pismo wnoszone przez stronę do sądu.

Istotne jest zastrzeżenie, że w przypadku gdy akta sprawy obejmują dane szczególnie wrażliwe w rozumieniu RODO, udostępnić je można wyłącznie stronie, której te dane dotyczą.

Do zalet systemu PASSA zaliczyć można na pewno to, że dostęp do niego jest bezpłatny. Strona postępowania może we własnym domu przeglądać akta sądowe sprawy. Ma zatem dostęp do wszelkich zarządzeń, wezwań czy wydanych orzeczeń. Do tej pory strona mogła jedynie dzwonić do sekretariatu z prośbą o udzielenie konkretnych informacji lub wnioskować o przesłanie jej kopii lub odpisów kart sprawy po uiszczeniu opłaty kancelaryjnej²⁰.

Podsumowanie

Korespondencja elektroniczna jest szybka i bezpłatna, jednak pamiętać należy, że jest to procedura sądowa sformalizowana, zatem zawsze konieczne będzie dochowanie wszystkich warunków określonych przepisami ustawy – Prawo o postępowaniu przed sądami administracyjnymi. Patrząc z punktu widzenia pracowników sądu, często bywa tak, że w ramach jednego postępowania

²⁰ Por. rozporządzenie Rady Ministrów z dnia 3 czerwca 2019 r. w sprawie wysokości opłat kancelaryjnych pobieranych w sprawach sądowoadministracyjnych (Dz.U. z 2019 r. poz. 1090).

korrespondencja elektroniczna z jedną stroną postępowania nakłada się z korespondencją papierową z drugą stroną. Opisana sytuacja podwaja pracę sekretariatu sądu, bowiem wiąże się z koniecznością skanowania, drukowania, uwierzytelniania dokumentów. Z kolei strona postępowania, decydując się na korespondencję elektroniczną, musi posiadać umiejętności związane z utworzeniem dokumentu elektronicznego w systemie informatycznym i podpisywaniem go podpisem elektronicznym – wymaga to wiedzy o zasadach funkcjonowania systemu oraz zaznajomienia się z procedurą ppsa dotyczącą korespondowania z sądem w formie elektronicznej. Nie może zwłaszcza umknąć uwadze strony, że jeśli wnosi skargę w formie załącznika do pisma przewodniego wysłanego za pośrednictwem platformy ePUAP, to istnieje obowiązek podpisania także i tego załącznika. Z pewnością więc możliwość korespondowania elektronicznego z sądem jest bardzo korzystna, jednak należy się liczyć z pewnymi utrudnieniami związanymi ze specyfiką tej formy komunikacji.

Jeśli chodzi o udostępnianie akt w systemie PASSA, autorkom niniejszego opracowania nasuwają się dwa wnioski *de lege ferenda*. Po pierwsze należałoby udostępnić w PASSA wszystkie akta administracyjne, a nie tylko te, które zostały przesłane za pomocą ePACZKI. Drugim postulatem jest udostępnianie dokumentów w PASSA wszystkim stronom postępowania od momentu przekazania skargi do sądu administracyjnego, a zatem bez konieczności składania wniosku.

Podsumowując z kolei rozważania dotyczące rozpraw zdalnych, stwierdzić należy, że dają one możliwość wyboru formy uczestnictwa w rozprawie, co niewątpliwie jest aspektem bardzo pozytywnym. Zdaje się to szczególnie ważne w przypadku spraw rozpoznawanych w Naczelnym Sądzie Administracyjnym i Wojewódzkim Sądzie Administracyjnym w Warszawie. W tych bowiem sądach rozpoznawane są sprawy, których strony zamieszkują lub mają siedzibę w odległych częściach Polski.

Bibliografia

Akty normatywne

1. Ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (t.j. Dz.U. z 2022 r. poz. 329 z późn. zm.).
2. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2021 r. poz. 2070).
3. 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 2020 r. poz. 1842 z późn. zm.).
4. Ustawa z dnia 28 maja 2021 r. o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz.U. z 2021 r. poz. 1090).
5. Rozporządzenie Prezesa Rady Ministrów z dnia 14 września 2011 r. w sprawie sporządzania i doręczania dokumentów elektronicznych oraz udostępniania formularzy, wzorów i kopii dokumentów elektronicznych (t.j. Dz.U. z 2018 r. poz. 180).
6. Rozporządzenie Rady Ministrów z dnia 3 czerwca 2019 r. w sprawie wysokości opłat kancelaryjnych pobieranych w sprawach sądowo-administracyjnych (Dz.U. z 2019 r. poz. 1090).

Literatura przedmiotu

1. Dauter B., Gruszczyński B., Kabat A., Niezgódka-Medek M., *Prawo o postępowaniu przed sądami administracyjnymi. Komentarz*, Warszawa 2011.
2. Iżycki P., *O wymogu podpisania pisma wniesionego do sądu administracyjnego w formie dokumentu elektronicznego*, ZNSA 2021, nr 6.
3. Knysiak-Sudyka H. (red.), *Pełnomocnik w postępowaniu administracyjnym i sądowoadministracyjnym*, Warszawa 2020.

4. Kwietko-Bębnowski M., *Informatyzacja sądów administracyjnych*, LEX/el. 2020.
5. Pietrasz P., *Informatyzacja polskiego postępowania przed sądami administracyjnymi a jego zasady ogólne*, Warszawa 2020.

Orzecznictwo

1. Uchwała NSA (7) z dnia 26 grudnia 2021 r., I FPS 2/21, CBOSA.

Inne

1. Zasady organizacji i przeprowadzania rozpraw w okresie obowiązywania stanu zagrożenia epidemicznego albo stanu epidemii z powodu COVID-19 [online:] <http://www.gliwice.wsa.gov.pl/> [dostęp: 07.06.2022].
2. www.bip.warszawa.wsa.gov.pl / Portal Akt Sądowych – PASSA [dostęp: 21.07.2022].
3. www.bip.warszawa.wsa.gov.pl / rozprawy zdalne /informacje ogólne dotyczące rozpraw jawnych [dostęp: 21.07.2022].

Streszczenie

W opracowaniu przedstawiono analizę możliwości oraz problemów, jakie występują w sądownictwie administracyjnym w związku z wnoszeniem przez strony pism w formie dokumentu elektronicznego, udostępnienia akt sprawy w systemie PASSA (akta elektroniczne) oraz rozpraw, w których strony postępowania oraz publiczność mogą uczestniczyć odmiejscowo (rozprawy zdalne). Rozważania prowadzone są na podstawie działań podejmowanych w Wojewódzkim Sądzie Administracyjnym w Warszawie oraz Wojewódzkim Sądzie Administracyjnym w Gliwicach.

W pierwszej części opracowania dokonano wykładni tych przepisów ustawy – Prawo o postępowaniu przed sądami administracyjnymi, które regulują wnoszenie przez strony pism w formie dokumentu elektronicznego.

Omówiono kryteria, jakie musi spełniać prawidłowo podpisany dokument wniesiony w formie elektronicznej. Zwrócono uwagę na to, czym różni się pismo wniesione w formie dokumentu elektronicznego od e-maila (ePUAP, e-mail), a także jakie skutki procesowe powoduje przesłanie do sądu e-maila, a jakie pisma w formie dokumentu elektronicznego ePUAP. Przedstawiono praktyczne zagadnienia i problemy, z jakimi borykają się strony postępowania oraz sędziowie i urzędnicy. Podniesiono kwestię przesyłania przez organ administracji publicznej do wojewódzkich sądów administracyjnych skarg wniesionych przez stronę skarżącą w formie dokumentu elektronicznego. Przedstawiono najczęstsze problemy wynikające z takich działań.

W drugiej części opracowania rozważono uregulowania dotyczące udostępniania akt sprawy w systemie PASSA. Wyjaśniono, czym jest portal PASSA oraz w jaki sposób dochodzi do odwzorowania papierowych akt sprawy. Opisano możliwości, jakie daje tego rodzaju dostęp, zakres udostępniania akt sprawy, okres, na jaki dostęp taki jest udzielony, a także warunki, jakie musi spełnić strona postępowania, aby go otrzymać. Scharakteryzowano ograniczenia i możliwości, jakie daje nowa regulacja.

W ostatniej części przedstawiono kwestię przeprowadzania w sądach administracyjnych rozpraw odmiejscowych (zdalnych), omówiono związane z tym regulacje prawne oraz praktykę wybranych sądów administracyjnych. Wypunktowano problemy, jak i korzyści wynikające z możliwości brania udziału w rozprawie bez konieczności fizycznej obecności na sali rozpraw. W opracowaniu wskazano na zalety i wady aktualnych rozwiązań prawnych, ograniczenia technologiczne, zaproponowano też zmiany, które usprawniłyby informatyzację sądownictwa administracyjnego w Polsce.

Słowa kluczowe

informatyzacja, rozprawy zdalne, akta elektroniczne, ePUAP, dokument elektroniczny

ELEKTRONICZNE POSTĘPOWANIE UPOMINAWCZE JAKO WZORZEC INFORMATYZACJI POSTĘPOWANIA CYWILNEGO

MAGDALENA ZAWISZA

OKRĘGOWA IZBA ADWOKACKA W WARSZAWIE;

UCZELNIA ŁAZARSKIEGO



0000-0002-6883-5050

Wstęp

Informatyzacja, pojmowana jako proces wprowadzenia nowoczesnych informatycznych metod przetwarzania informacji, mających na celu wsparcie funkcjonowania przedsiębiorstw lub instytucji¹, jest nieodłącznym elementem w procesie kształtowania społeczeństwa informacyjnego². Dostrzegalny wyraźnie od kilku lat przyspieszony postęp technologiczny we wszystkich sferach życia społeczeństwa powoduje bezwzględną konieczność efektywnego udostępnienia przez organy państwa odpowiednich zasobów informacji, a także oferowania szerokiego wachlarza usług publicznych świadczonych w systemie teleinformatycznym. W kontekście poruszanej w niniejszym opracowaniu problematyki wyzwania te dotyczą przede wszystkim procedur wykorzystywanych w postępowaniach toczących się przed organami stosującymi oraz egzekwującymi

¹ P. Adamczewski, *Słownik informatyczny*, Gliwice 2005, s. 102.

² Społeczeństwo informacyjne to społeczeństwo, w którym towarem jest informacja traktowana jako szczególne dobro niematerialne, równoważne lub cenniejsze nawet od dóbr materialnych. Przewiduje się rozwój usług związanych z 3P (przesyłanie, przetwarzanie i przechowywanie informacji) – zob. [online:] https://pl.wikipedia.org/wiki/Spo%C5%82eczne%C5%84stwo_informacyjne [dostęp: 22.09.2022].

powszechnie obowiązujące przepisy prawa. Za S. Kotecką wskazać należy, że sądownictwo można postrzegać jako „system przetwarzania danych. Informacja wpływa do sądu w formie pisma procesowego, jest następnie uzupełniana i weryfikowana poprzez gromadzenie i ocenę danych w trakcie postępowania dowodowego, a rezultatem tych czynności staje się orzeczenie sądowe, czyli rozstrzygnięcie o zebranych danych. Opierając się na prawie materialnym i procesowym, a zatem przy użyciu określonych procedur, sąd zbiera, przetwarza i wartościuje dane, a następnie tworzy dane nowego rodzaju”³.

Wprowadzone do prawa publicznego na przestrzeni ostatnich lat technologie informatyczne stały się niewątpliwie naturalnym narzędziem usprawniającym działalność polskiego wymiaru sprawiedliwości, a w globalnej perspektywie – funkcjonowania organów władzy publicznej, zarówno w sferze szybkości postępowania, jak i jego jakości. Za jedną z największych reform w tym obszarze uznaje się zaś wprowadzenie odrębnego trybu postępowania cywilnego – elektronicznego postępowania upominawczego, które pozostaje dotychczas postępowaniem o największym stopniu informatyzacji.

Charakterystyka elektronicznego postępowania upominawczego

Elektroniczne postępowanie upominawcze (zwane dalej EPU) zostało wprowadzone do polskiego porządku prawnego na mocy ustawy z dnia 9 stycznia 2009 r. o zmianie ustawy – Kodeks

³ S. Kotecka, *Obywatelski wymiar e-sądownictwa w Polsce. O wykorzystaniu technologii informacyjno-komunikacyjnych w relacji interesanta z sądem*, Instytut Spraw Publicznych. Analizy i Opinie, Warszawa 2014, s. 1.

postępowania cywilnego oraz niektórych innych ustaw⁴. Założeniem ustawodawcy było uzupełnienie istniejącego modelu o postępowanie, które przyczyni się do sprawniejszego rozpoznawania roszczeń, dochodzonych w trybie przepisów rozdziału 3 działu V tytułu VII księgi pierwszej części pierwszej Kodeksu postępowania cywilnego. Ponadto jako główny cel zmiany założono odciążenie sądów od rozpoznawania spraw, w których stan faktyczny nie jest skomplikowany i nie wymaga przeprowadzenia postępowania dowodowego⁵.

Elektroniczne postępowanie upominawcze skierowano głównie, lecz podkreślić należy iż nie wyłącznie, do tzw. powodów masowych, zajmujących się działalnością gospodarczą związaną z obrotem wierzytelnościami, których roszczenia są udowodnione dokumentami, najczęściej fakturami bądź rachunkami. Zakres podmiotowy omawianej procedury pozostaje jednak nieograniczony. Z kolei zakres przedmiotowy obejmuje roszczenia pieniężne, w których zastosowanie mają przepisy o postępowaniu upominawczym, o bezspornym i nieskomplikowanym charakterze, bez ograniczeń ze względu na wartość przedmiotu sporu⁶. Komunikacja między powodem i sądem elektronicznym odbywa się wyłącznie w drodze elektronicznej, zaś między pozwanym i sądem elektronicznym w drodze tradycyjnej, chyba że pozwany sam zainicjuje komunikację elektroniczną poprzez wysłanie pisma drogą elektroniczną⁷.

Ustawodawca, wdrażając nową procedurę, oparł jej rozwiązania pod względem prawnym na dotychczasowych regulacjach

⁴ Ustawa z dnia 9 stycznia 2009 r. o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz.U. z 2009 r. Nr 26 poz.156 z późn. zm.).

⁵ Uzasadnienie rządowego projektu ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw, Sejm VI kadencji, druk sejmowy nr 859.

⁶ A. Marciniak (red.), *Kodeks postępowania cywilnego. Tom III. Komentarz do art. 425–729*, Legalis 2020.

⁷ Art. 505³¹ § 1 i 2 ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (t.j. Dz.U. z 2021 r. poz. 1805 z późn. zm.).

postępowania upominawczego, natomiast pod względem technicznym wzorowano się na rozwiązaniach funkcjonujących w Wielkiej Brytanii (ang. *Money Claim Online*) oraz Niemczech (niem. *automatisiertes Mahnverfahren*)⁸.

Money Claim Online (zwana dalej MCO) umożliwia przeprowadzenie postępowania, które inicjowane jest przez wypełnienie prostego formularza umieszczonego na powszechnie dostępnym portalu internetowym. Strona pozwana w celu obrony swoich praw ma możliwość złożenia odpowiedzi na pozew lub wytoczenia powództwa wzajemnego drogą elektroniczną lub tradycyjną. W toku postępowania uczestnicy posiadają możliwość elektronicznego śledzenia przebiegu sprawy⁹. W praktyce okazuje się, że jedynymi wymogami technicznymi stawianymi osobom zainteresowanym skorzystaniem z e-sądu jest posiadanie łącza internetowego i aktualnej wersji przeglądarki, bowiem zrezygnowano z konieczności posługiwania się elektronicznym podpisem. Do rozpoznawania spraw w ramach MCO wyznaczony został tylko jeden sąd – sąd hrabstwa Northampton, który zobowiązany jest do rozpoznania sprawy w ciągu 5 dni od jej przyjęcia. O przeniesieniu sprawy do innego sądu właściwego obie strony informowane są tradycyjną pocztą, którą to przekazywane są im również wszelkie dokumenty oraz potwierdzenia. Pozwany poprzez korespondencję pocztową dowiaduje się także o wniesieniu pozwu¹⁰.

W niemieckim modelu nie wyodrębnia się osobnego postępowania elektronicznego, regulując je w jednolity sposób jako

⁸ Uzasadnienie rządowego projektu ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw, Sejm VI kadencji, druk sejmowy nr 859.

⁹ P. Pęcherzewski, *Angielski sposób na sprawny i prosty e-sąd*, PME – dodatek do MoP 2007, nr 22, s. 39; A. Garlacz, *Money Claim Online – składanie pozwów przez Internet w Anglii i Walii*, e-Biuletyn 2006, nr 3 [online:] http://www.bibliotekacyfrowa.pl/Content/23635/Money_Claim_on_Line_skladanie_pozwow.pdf [dostęp: 24.09.2022].

¹⁰ A. Garlacz, *Money Claim Online...*, op. cit.

fakultatywny rodzaj postępowania upominawczego. Powód, chcąc zainicjować postępowanie elektroniczne, może – ale nie jest zobligowany – wnieść o wydanie nakazu zapłaty poprzez złożenie w wersji papierowej urzędowego formularza udostępnionego na elektronicznych nośnikach danych lub drogą elektroniczną. Sądem właściwym do rozpoznania sprawy w tym trybie jest sąd właściwy ze względu na domicyl powoda. Czynności w postępowaniu upominawczym wykonują wykwalifikowani urzędnicy sądowi, których pozycję można porównać do polskich referendarzy oraz sekretarzy sądowych. Jednakże najbardziej wyróżniającą cechą niemieckiego modelu postępowania jest to, że w zdecydowanej większości sądów proces weryfikacji pozwu, przygotowania i sporządzania nakazu zapłaty (włącznie z jego wystawieniem i doręczeniem powodowi) obsługiwany jest przez zautomatyzowany wewnętrzny sądowy system, który działa samodzielnie, bez uczestnictwa czynnika ludzkiego¹¹.

Polski ustawodawca zastosował jednak rozwiązania analogiczne do pragmatycznego modelu angielskiego, rezygnując przy tym z wyłączenia z udziału czynnika ludzkiego, a w konsekwencji wprowadzenie pełnej automatyzacji w wydawaniu orzeczeń, co ma miejsce w nieco bardziej skomplikowanym germańskim systemie postępowania upominawczego¹². Z MCO zapożyczono m.in. funkcjonalny interfejs EPU oraz powszechnie dostępny sposób identyfikacji uczestników.

EPU jako wzorzec informatyzacji

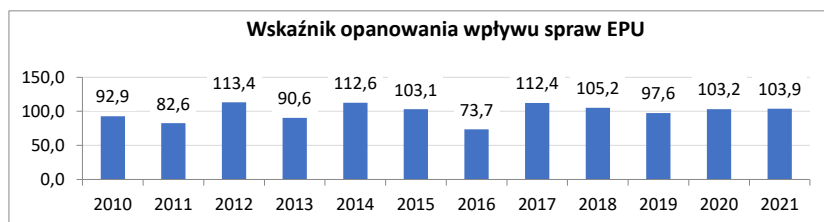
EPU zakłada kompleksową obsługę sprawy poprzez wyodrębniony system elektroniczny, umożliwiający stronom (decydującym się na

¹¹ A. Harast, *Elektroniczne postępowanie upominawcze (sądowe) w wybranych państwach Unii Europejskiej*, MoP 2009, nr 20, Legalis.

¹² K. Jasik-Kuchta, *Proponowane zmiany w polskim elektronicznym postępowaniu upominawczym w świetle rozwiązań Online Civil Money Claims*, MoPH 2018, nr 4, s. 31.

wybór elektronicznego kontaktu z sądem) m.in.: wnoszenie pism procesowych, doręczenia elektroniczne oraz wydawanie orzeczeń przez sąd w formie elektronicznej. Dopuszcza on także możliwość nadania klauzuli wykonalności w formie elektronicznej i złożenia przez wierzyciela wniosku do komornika o wszczęcie egzekucji w formie elektronicznej¹³.

Wśród charakterystycznych przymiotów EPU wyróżnić można: efektywność, szybkość, ekonomikę, powszechność, informatyzację oraz interoperacyjność. Głównym celem elektronicznego postępowania jest zwiększanie efektywności sądownictwa, przez co rozumieć należy przyspieszenie dotychczasowych procedur, a także obniżenie kosztów obciążających wymiar sprawiedliwości, co niewątpliwie potwierdza wskaźnik opanowania wpływu¹⁴, który od kilku lat oscyluje w granicach 100.



Źródło: Informator Statystyczny Wymiaru Sprawiedliwości, EPU – elektroniczne postępowanie upominawcze (e-sąd) 2010–2021 [online:] <https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/> [dostęp: 24.09.2022].

Ponadto z danych Ministerstwa Sprawiedliwości wynika, że w 2021 r. średni czas rozpoznania sprawy przez e-sąd wyniósł 27,5 dnia (w sprawach cywilnych – 25,9 dnia; w sprawach

¹³ Art. 505²⁸ kpc i nast.

¹⁴ Wskaźnik opanowania wpływu jest odniesieniem liczby spraw załatwionych w danym okresie sprawozdawczym lub okresie działania jednostki sprawozdawczej do liczby spraw wpływających (Informator Statystyczny Wymiaru Sprawiedliwości).

gospodarczych – 41,2 dnia; w sprawach z prawa pracy – 54,4 dnia)¹⁵. Nie powinno także budzić wątpliwości, że daleko idąca informatyzacja czynności procesowych w ramach elektronicznego postępowania upominawczego znajduje realne przełożenie na zwiększenie sprawności postępowania sądowego, jednocześnie upraszczając oraz przyspieszając procedurę, w tym związane z nią czynności konieczne do skutecznego wniesienia pozwu, a więc zainicjowania sądowego postępowania.

Dochodzenie swoich praw przed e-sądem wiąże się dodatkowo z finansowymi korzyściami. Po pierwsze należy zauważyć, że z uwagi na elektroniczny charakter postępowania uczestnicy nie muszą ponosić wydatków związanych chociażby z wydrukowaniem oraz powielaniem pism i ich załączników, a także przygotowaniem oraz wysłaniem korespondencji tradycyjną pocztą (np. zakup koperty i znaczka). Po drugie skorzystanie z EPU jest bardziej ekonomiczne niż tradycyjna procedura, bowiem w EPU strony zwolnione zostały od obowiązku ponoszenia opłat sądowych od skarg na orzeczenia referendarzy i zażaleń. Nie ma także potrzeby uiszczenia opłaty skarbowej od pełnomocnictwa¹⁶. Zaś najbardziej korzystne wydaje się rozwiązanie przewidujące wnoszenie wraz z pozwem tylko 1/4 opłaty sądowej¹⁷. Warto w tym miejscu wskazać również na negatywne aspekty finansowe, które związane są z EPU.

¹⁵ Informator Statystyczny Wymiaru Sprawiedliwości, EPU – elektroniczne postępowanie upominawcze (e-sąd) 2010-2021 [online:] <https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/> [dostęp: 24.09.2022].

¹⁶ Z treści art. 1 ust. 1 pkt 2 ustawy z dnia 16 listopada 2006 r. o opłacie skarbowej (t.j. Dz.U. z 2021 r. poz. 1923 z późn. zm.) wynika, że opłacie podlega złożenie dokumentu stwierdzającego udzielenie pełnomocnictwa lub prokury albo jego odpisu, wypisu lub kopii – w sprawie z zakresu administracji publicznej lub w postępowaniu sądowym. W EPU strona lub jej pełnomocnik nie ma obowiązku złożenia dokumentu pełnomocnictwa, jedynie się na nie powołuje (art. 89 § 1¹ kpc), a więc nie ma też obowiązku uiszczenia opłaty skarbowej.

¹⁷ Art. 19 ust. 2 pkt 2 ustawy z dnia 28 lipca 2005 r. o kosztach sądowych w sprawach cywilnych (t.j. Dz.U. z 2022 r. poz. 1125).

Z uwagi bowiem na fakt znacznego pomniejszenia opłaty sądowej wyłączono możliwość uzyskania w tej procedurze sądowego zwolnienia z kosztów sądowych. Ponadto przy opłacaniu pozwu zachodzi konieczność uiszczenia dodatkowej opłaty manipulacyjnej na rzecz operatora systemu płatności.

Za zasadniczą zaletę EPU uznać należy powszechny dostęp do procedury, co w praktyce potwierdza wpływ ponad 2 mln spraw rocznie oraz ponad 25 mln spraw, które trafiły do e-sądu w okresie od 2012 r. do 2022 r.¹⁸ Przypuszczać należy, że o popularności EPU przesądził sposób identyfikacji uczestników postępowania za pomocą zwykłego podpisu elektronicznego. Rozwiązanie to stanowi znaczne ułatwienie dla stron, które zostały zwolnione z obowiązku posługiwania się bezpiecznym, kwalifikowanym podpisem elektronicznym, którego koszty uzyskania i aktualizacji nierzadko mogłyby przewyższać wartość drobnych roszczeń często dochodzonych w postępowaniu upominawczym.

Jak już wcześniej wspomniano, EPU jest najbardziej zinformatywowanym postępowaniem w polskim wymiarze sprawiedliwości. Za pomocą serwisu internetowego strona powodowa wnosi pozew, po czym generowane są elektroniczne akta sprawy. Następnie przy użyciu systemu teleinformatycznego wydawany jest nakaz zapłaty, również tworzy się oraz doręcza korespondencję, nadaje się tytuły wykonawcze, a nawet możliwe jest złożenie wniosku o prowadzenie egzekucji. Rola e-sądu nie ogranicza się tylko do wydania nakazu zapłaty. Obsługujący EPU system teleinformatyczny spełnia zarazem funkcję biura podawczego, organu doręczeńiowego, programu repetytoryjnego, sądowych akt sprawy, repozytorium przechowującego elektroniczne tytuły wykonawcze¹⁹. Oczywiście podej-

¹⁸ Informator Statystyczny Wymiaru Sprawiedliwości, EPU – elektroniczne postępowanie upominawcze (e-sąd) 2010-2021 [online:] <https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/> [dostęp: 24.09.2022].

¹⁹ Ł. Goździaszek, *Informatyczny przełom w postępowaniu cywilnym? Rozważania nad elektronicznym postępowaniem upominawczym*, „Palestra” 2009, nr 9–10, s. 82.

owanie rozmaitych czynności wyłącznie w sposób elektroniczny powoduje typowe zagrożenia charakterystyczne dla nowych technologii, w tym do najbardziej uciążliwych zaliczyć należy przerwy w działaniu portalu, jednakże w dalszym ciągu podejmowane są działania mające na celu usprawnienie systemu, który oceniany jest pozytywnie.

W kontekście interoperacyjności warto dodać, że regulacje elektronicznego postępowania upominawczego od początku zakładały integrację z innymi bazami publicznymi, co wynikało chociażby z konieczności weryfikacji danych numerycznych dotyczących stron²⁰. Na mocy nowelizacji Kodeksu postępowania cywilnego z 2019 r.²¹ numer PESEL jest również wykorzystywany na potrzeby doręczeń w EPU, gdyż w razie niemożności skutecznego doręczenia nakaz zapłaty uznaje się za doręczony, o ile adres, pod którym pozostawiono zawiadomienia, jest zgodny z adresem ujawnionym w rejestrze PESEL²².

Mając na uwadze, że czynności w elektronicznym postępowaniu upominawczym ogniskują się wokół funkcjonalności systemu teleinformatycznego obsługującego to postępowanie, neutralność technologiczna i interoperacyjność są – jak się wydaje – przynajmniej w znacznym zakresie realizowane²³. Powyższe oznacza, że obecnie obowiązujący mechanizm procesowy przewidziany dla elektronicznego postępowania upominawczego umożliwia funkcjonowanie oraz podejmowanie wszelkich czynności procesowych we względnie jednolitym i zamkniętym środowisku informatycznym.

²⁰ Uzasadnienie rządowego projektu ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw, Sejm VI kadencji, druk sejmowy nr 859.

²¹ Ustawa z dnia 4 lipca 2019 r. o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz.U. z 2019 r. poz. 1469).

²² Art. 505³⁴ § 1 kpc.

²³ Ł. Goździaszek, *Elektroniczne postępowanie upominawcze w świetle celów informatyzacji podmiotów publicznych*, PPA 2020, t. CXX/2, s. 343–344.

Podsumowanie – ocena dotychczasowych rozwiązań i perspektywy na przyszłość

Wprowadzenie EPU uważane jest za jedną z ważniejszych reform wymiaru sprawiedliwości przeprowadzonych na przestrzeni ostatnich lat. Znacznie większy niż zakładano wpływ spraw do e-sądu dowodzi, że istnieje społeczne zapotrzebowanie na przystępną, elektroniczną komunikację z wymiarem sprawiedliwości²⁴. Niewątpliwie rozwiązanie to ułatwiło jednostkom dochodzenie swoich praw, umożliwiając tym samym realizację konstytucyjnego prawa dostępu do sądu. Wobec tego wypracowany model postępowania elektronicznego stawiany jest obecnie za wzór dla dalszej informatyzacji cywilnych postępowań sądowych.

EPU w krótkim czasie osiągnęło stabilną i znaczącą rolę w postępowaniu cywilnym. Ponadto pozytywnie wpłynęło na dotychczasową ocenę procedury cywilnej, która wielokrotnie była krytykowana przez przedstawicieli doktryny oraz praktyków prawa, z uwagi na brak jakichkolwiek rozwiązań umożliwiających stronom postępowania teleinformatyczny kontakt z sądem. Powyższe przesądzało o swego rodzaju „zacofaniu” Kodeksu postępowania cywilnego w stosunku chociażby do procedury administracyjnej, która od dawna przewidywała szeroki wachlarz form kontaktowania się z uczestnikami postępowania, w tym również poprzez wykorzystanie komunikacji elektronicznej.

Można zatem stwierdzić, że elektroniczne postępowanie upominawcze stanowi obecnie wzorzec legislacyjny dla konstruowania prawno-informatycznych modeli innych postępowań. O istotnym znaczeniu EPU świadczy chociażby zamiar zastąpienia

²⁴ J. Lora, *Komunikacja sądów z obywatelami – badania empiryczne, wnioski, rekomendacje zmian*, Warszawa, kwiecień 2009 [online:] https://for.org.pl/upload/File/Raporty/Raport_Komunikacja_Sadow_z_obywatelami_WEB_FINAL.pdf [dostęp: 10.04.2022].

nim w przyszłości tradycyjnego, zwykłego postępowania upominawczego. Wykorzystanie EPU jako wzorca będzie skutkowało uspołnieniem prawno-informatycznej koncepcji, która powinna mieć swoje dalsze zastosowanie w szeroko rozumianym postępowaniu cywilnym. Ponadto pozwoliłoby to wykorzystać – na ogół pozytywne – dotychczasowe doświadczenia związane z elektronicznym postępowaniem upominawczym.

Warto zauważyć, że mimo wieloletniego funkcjonowania elektroniczne postępowanie upominawcze, nawet w wypadku postępu informatycznego w konkurencyjnych względem niego postępowaniach cywilnych, posiada perspektywy na przyszłość. Możliwy jest bowiem jego dalszy rozwój, chociażby poprzez zautomatyzowanie orzekania na wzór skrajnie zautomatyzowanego modelu germańskiego, w którym to nakazy zapłaty wydawane są przez wewnętrzny system komputerowy.

Bibliografia

Akty normatywne

1. Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (t.j. Dz.U. z 2021 r. poz. 1805 z późn. zm.).
2. Ustawa z dnia 28 lipca 2005 r. o kosztach sądowych w sprawach cywilnych (t.j. Dz.U. z 2022 r. poz. 1125).
3. Ustawa z dnia 16 listopada 2006 r. o opłacie skarbowej (t.j. Dz.U. z 2021 r. poz. 1923 z późn. zm.).
4. Ustawa z dnia 9 stycznia 2009 r. o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz.U. z 2009 r. Nr 26 poz. 156, z późn. zm.).
5. Ustawa z dnia 4 lipca 2019 r. o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw (Dz.U. z 201 r. poz. 1469).

Literatura przedmiotu

1. Adamczewski P., *Słownik informatyczny*, Gliwice 2005.
2. Goździaszek Ł., *Informatyczny przełom w postępowaniu cywilnym? Rozważania nad elektronicznym postępowaniem upominawczym*, „Palestra” 2009, nr 9–10.
3. Goździaszek Ł., *Elektroniczne postępowanie upominawcze w świetle celów informatyzacji podmiotów publicznych*, PPA 2020, t. CXX/2.
4. Harast A., *Elektroniczne postępowanie upominawcze (sądowe) w wybranych państwach Unii Europejskiej*, MoP 2009, nr 20.
5. Jasik-Kuchta K., *Proponowane zmiany w polskim elektronicznym postępowaniu upominawczym w świetle rozwiązań Online Civil Money Claims*, MoPH 2018, nr 4.
6. Kotecka S., *Obywatelski wymiar e-sądownictwa w Polsce. O wykorzystaniu technologii informacyjno-komunikacyjnych w relacji interesanta z sądem*, Instytut Spraw Publicznych. Analizy i Opinie, Warszawa 2014.
7. Marciniak A. (red.), *Kodeks postępowania cywilnego. Tom III. Komentarz do art. 425–729*, Legalis 2020.
8. Pęcherzewski P., *Angielski sposób na sprawny i prosty e-sąd*, PME – dodatek do MoP 2007, nr 22.

Inne

1. Uzasadnienie rządowego projektu ustawy o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw, Sejm VI kadencji, druk sejmowy nr 859.

Źródła internetowe

1. Garlacz A., *Money Claim Online – składanie pozwów przez Internet w Anglii i Walii*, e-Biuletyn 2006, nr 3 [online:] http://www.bibliotekacyfrowa.pl/Content/23635/Money_Claim_on_Line_skladanie_pozwow.pdf [dostęp: 24.09.2022].

2. Informator Statystyczny Wymiaru Sprawiedliwości, EPU – elektroniczne postępowanie upominawcze (e-sąd) 2010-2021 [online:] <https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/> [dostęp: 24.09.2022].
3. Lora J., *Komunikacja sądów z obywatelami – badania empiryczne, wnioski, rekomendacje zmian*, Warszawa 2009 [online:] https://for.org.pl/upload/File/raporty/Raport_Komunikacja_Sadow_z_obywatelami_WEB_FINAL.pdf [dostęp: 10.04.2022].
4. Społeczeństwo informacyjne [w:] Wikipedia, wolna encyklopedia [online:] https://pl.wikipedia.org/wiki/Spo%C5%82ecze%C5%84stwo_informacyjne [dostęp: 22.09.2022].

Streszczenie

Istotnym krokiem w kierunku informatyzacji postępowania cywilnego było wejście w życie ustawy z dnia 9 stycznia 2009 r. o zmianie ustawy – Kodeks postępowania cywilnego oraz niektórych innych ustaw, która wprowadziła do polskiego porządku prawnego nowe postępowanie odrębne – elektroniczne postępowanie upominawcze.

Procedura ta zakłada kompleksową obsługę sprawy poprzez wyodrębniony system elektroniczny, umożliwiający wnoszenie pism procesowych przez strony postępowania (o ile strona wybierze elektroniczny kontakt z sądem), doręczenia elektroniczne, wydawanie orzeczeń przez sąd w formie elektronicznej. Dopuszcza on także możliwość nadania klauzuli wykonalności w formie elektronicznej i złożenie przez wierzyciela wniosku do komornika o wszczęcie egzekucji w formie elektronicznej²⁵.

Wprowadzenie EPU uważane jest za jedną z ważniejszych reform wymiaru sprawiedliwości przeprowadzonych na przestrzeni ostatnich lat. Znacznie większy niż zakładano wpływ spraw do e-sądu dowodzi, że istnieje społeczne zapotrzebowanie na przystępną, elektroniczną komunikację

²⁵ Art. 505²⁸ kpc i nast.

z wymiarem sprawiedliwości²⁶. Niewątpliwie rozwiązanie to ułatwiło jednostkom dochodzenie swoich praw, umożliwiając tym samym realizację konstytucyjnego prawa dostępu do sądu. Wobec tego wypracowany model postępowania elektronicznego stawiany jest obecnie za wzór dla dalszej informatyzacji cywilnych postępowań sądowych.

W związku z powyższym za uzasadnione należy uznać poddanie analizie wprowadzonego na gruncie polskiego ustawodawstwa modelu elektronicznego postępowania upominawczego. W tym celu przybliżono charakterystykę funkcjonowania systemu, jego funkcję oraz cele, dokonując oceny ich realizacji w praktyce.

Słowa kluczowe

elektroniczne postępowanie upominawcze, informatyzacja, postępowanie cywilne, e-sąd, prawo do sądu

²⁶ J. Lora, *Komunikacja sądów z obywatelami – badania empiryczne, wnioski, rekomendacje zmian*, Warszawa, kwiecień 2009 [online:] https://for.org.pl/upload/File/raporty/Raport_Komunikacja_Sadow_z_obywatelami_WEB_FINAL.pdf [dostęp: 10.04.2022].

NOTA O REDAKTORACH NAUKOWYCH

Bartosz Kotowicz – asystent w Katedrze Prawa Gospodarczego Publicznego na Wydziale Prawa i Administracji Uczelni Łazarskiego w Warszawie, doktorant Uczelni Łazarskiego w Warszawie, członek Centrum Badań Procesu Legislacyjnego Uczelni Łazarskiego w Warszawie; doradca restrukturyzacyjny, właściciel kancelarii prawnej. Odbił aplikację adwokacką przy Okręgowej Radzie Adwokackiej w Warszawie. Prowadzi szkolenia dla administracji publicznej. Autor i współautor wielu publikacji naukowych z zakresu prawa zamówień publicznych, prawa gospodarczego publicznego i prawa administracyjnego.

Angelika Kurzawa – doktor nauk prawnych, adiunkt w Katedrze Prawa Administracyjnego, Konstytucyjnego i Prawa Pracy na Wydziale Prawa i Administracji Uczelni Łazarskiego w Warszawie. Pracuje w Departamencie Prawnym i Rozstrzygania Sporów w Urzędzie Regulacji Energetyki. Prowadzi szkolenia w ramach doskonalenia zawodowego dla radców prawnych w Okręgowej Izbie Radców Prawnych w Lublinie. Wykłada na studiach podyplomowych „Administracja – rejestracja stanu cywilnego” na Katolickim Uniwersytecie Lubelskim oraz „Inżynier Kontraktu” w Uczelni Łazarskiego w Warszawie. Autorka wielu publikacji z zakresu prawa administracyjnego, postępowania administracyjnego i sądownictwa administracyjnego oraz prawa gospodarczego publicznego, w tym prawa energetycznego.

Łukasz Nosarzewski – doktor nauk prawnych, adiunkt w Katedrze Prawa Administracyjnego, Konstytucyjnego i Prawa Pracy na Wydziale Prawa i Administracji Uczelni Łazarskiego w Warszawie.

Radca Prokuratury Generalnej Rzeczypospolitej Polskiej, radca prawny. Odbił aplikację radcowską przy Okręgowej Izbie Radców Prawnych w Warszawie i aplikację legislacyjną w Rządowym Centrum Legislacji.

Doświadczenie zawodowe zdobywał, pracując w prywatnej kancelarii radcy prawnego, Kancelarii Sejmu RP, Biurze Rzecznika Praw Obywatelskich i Kancelarii Prezydenta RP. Prowadzi szkolenia dla administracji publicznej. Autor publikacji z zakresu prawa informacyjnego i zamówień publicznych. Specjalizuje się w dostępie do informacji publicznych, ochronie danych osobowych, ochronie informacji niejawnej, zamówieniach publicznych i postępowaniach sądowych.

Monografia stanowi omówienie wielu interesujących i istotnych zagadnień z zakresu informatyzacji działań administracji publicznej i wymiaru sprawiedliwości. Autorzy podjęli się analizy zagadnień istotnych z punktu widzenia praktyki, podejmując próbę oceny istniejących rozwiązań, jak również wskazania ewentualnych perspektyw rozwoju informatyzacji w poszczególnych grupach zagadnień.

Dr hab. Joanna Smarż, prof. UTH Rad.

Cyfryzacja usług publicznych (procesów społeczno-gospodarczych) może stanowić relewantny prakseologiczny miernik oceny funkcjonowania państwa. Im większy jest zakres informatyzacji, tym z pewnością pełniej realizuje się konstytucyjny postulat optymalizacji sprawności działania instytucji publicznych. W konsekwencji w przyszłości należy antycypować z jednej strony rozrost norm prawnych umożliwiających wykorzystanie technologii informatyczno-komunikacyjnej, natomiast z drugiej strony wynikające stąd praktyczne ale i teoretyczne problemy stosowania prawa. Szczególnie newralgiczne w kontekście omawianego zagadnienia pozostaje odpowiednie wyważenie informatyzacji z publicznymi prawami podmiotowymi i zasadami ogólnymi systemu prawa, takimi jak rzetelność, transparentność, ochrona tajemnicy korespondencji, ochrona danych osobowych, prawo do prywatności, prawo do procesu czy prawo do sądu, przy równoczesnym przeciwdziałaniu wykluczeniu cyfrowemu sporej jeszcze części społeczeństwa. Właśnie m.in. o tym traktuje niniejsza monografia i tutaj znajdują się jej niewątpliwe walory poznawcze oraz eksplanacyjne.

Dr hab. Jan Chmielewski, prof. ALK



ISBN 978-83-66723-59-7



DOI: 10.26399/978-83-66723-59-7