



Uniwersytet
Wrocławski

Otwarte dane i ich ponowne wykorzystywanie w prawie polskim

Wybrane zagadnienia

redakcja

Michał Bernaczyk

Wrocław 2021

Otwarte dane i ich ponowne wykorzystywanie w prawie polskim

Wybrane zagadnienia

Prace Naukowe
Wydziału Prawa, Administracji i Ekonomii
Uniwersytetu Wrocławskiego

Seria: **e-Monografie**

Nr 198



Dostęp online: <https://www.bibliotekacyfrowa.pl/publication/144508>

DOI: [10.34616/144499](https://doi.org/10.34616/144499)

Otwarte dane i ich ponowne wykorzystywanie w prawie polskim

Wybrane zagadnienia

redakcja
Michał Bernaczyk
Uniwersytet Wrocławski
Wydział Prawa, Administracji i Ekonomii
ORCID: [0000-0001-7683-8852](https://orcid.org/0000-0001-7683-8852)

Wrocław 2021

Kolegium Redakcyjne

prof. dr hab. Leonard Górnicki – przewodniczący

dr Julian Jezioro – zastępca przewodniczącego

mgr Aleksandra Dorywała – sekretarz

mgr Ewa Gałyga-Michowska – członek

mgr Bożena Górna – członek

mgr Tadeusz Juchniewicz – członek

Recenzenci: *dr hab. Robert Suwaj, Politechnika Warszawska;*

dr hab. Dariusz Szostek, prof. Uniwersytetu Śląskiego

**© Copyright by Wydział Prawa, Administracji i Ekonomii
Uniwersytetu Wrocławskiego**

Publikacja finansowana ze środków Fundacji Media 3.0.



Korekta: *Magdalena Wojcieszak*

Projekt i wykonanie okładki: *Karolina Drozd*

Skład i opracowanie techniczne: *Aleksandra Kumasza eBooki.com.pl*

Druk: *Agencja Reklamowa TOP, Agnieszka Łuczak*

Wydawca

E-Wydawnictwo. Prawnicza i Ekonomiczna Biblioteka Cyfrowa.

Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego

ISBN 978-83-66601-81-9 (druk)

ISBN 978-83-66601-82-6 (online)

Spis treści

Wstęp	9
ROZDZIAŁ I. PRAWO DOSTĘPU DO OTWARTYCH DANYCH JAKO PRAWO PODSTAWOWE W PRAWIE KRAJOWYM, MIĘDZY- NARODOWYM I UNIJNYM	
Michał Bernaczyk	
Wprowadzenie. Konstytucyjne czy ponadnarodowe gwarancje dostępu do otwartych danych? Kilka uwag o nowym pojęciu „wykorzystywania informacji sektora publicznego” w polskim ustawodawstwie	15
Łukasz Żyła	
Cyfrowy dostęp do informacji i danych o funkcjonowaniu pań- stwa a prawo do informacji jako prawo człowieka	39
ROZDZIAŁ II. PRAKTYCZNE ZAGADNIENIA DOSTĘPU DO INFORMACJI I ICH PONOWNEGO WYKORZYSTYWANIA	
Sylvia Kotecka-Kral	
Interoperacyjność aplikacji mobilnych śledzących kontakty za- każne	95
Adam Haręza	
Dostęp do informacji publicznej rozważany przez pryzmat pro- cesów anonimizacji oraz pseudonimizacji danych	153
Ewa Wojnarska-Krajewska	
Wybrane aspekty prawne scrapowania ze szczególnym uwzględ- nieniem informacji i danych publicznych	209

Wstęp

Nasz świat i życie jest zapisane w danych. Wśród czytelników tej książki znajdują się zapewne Ci, którzy urodzili się w świecie wolnym od cyfryzacji danych i informacji, ale kolejne pokolenia nie znają już tego świata. Przyszłość tego ostatniego również będzie zależeć zarówno od tego, co będziemy w stanie uczynić z otaczającymi nas danymi, jak i po co będziemy je przetwarzać, a wreszcie – jaki stopień swobody w ich pozyskiwaniu i wykorzystywaniu przyznamy jednostkom oraz władzom publicznym. To zaś rozstrzygnie prawo w wielopoziomowym systemie prawa krajowego i międzynarodowego.

Teksty przekazane do niniejszej publikacji dają pewien przekrój problemów, które powinny być brane pod uwagę przy modelowaniu ponownego wykorzystania w mozaice polskich, ustawowych norm materialnych i proceduralnych dotyczących dostępu do szeroko pojętych informacji i danych. Taką okazją staje się niewątpliwie uchwalenie ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego oraz postępująca deprecjacja ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. Aby uzyskać najlepszą i efektywną krajową regulację wyważającą ochronę interesu publicznego i prawo do informacji w epoce cyfrowej, po pierwsze, należałoby powrócić do kwestii podstawowej i określić bądź wykluczyć umocowanie prawa do ponownego wykorzystywania w prawach podstawowych jednostki, zarówno na płaszczyźnie konstytucyjnej, jak

i ponadnarodowej. Dziś unikamy debaty, czy jest to prawo o rodowodzie konstytucyjnym (zob. art. 79 ust. 1 Konstytucji RP *ab initio*), a jeśli tak, to w jakiej relacji pozostaje ono do np. art. 20 lub 54 Konstytucji RP? Czy dotykamy tu w ogóle kwestii praw człowieka do uzyskiwania i rozpowszechniania informacji, czy też mowa tu o swobodzie regulacyjnej ustawodawcy do kreowania nowych usług publicznych wspierających życie kulturalne, obrót gospodarczy lub warunki socjalne? W prawie unijnym ponowne wykorzystywanie poszukuje uzasadnienia w prawie podstawowym jednostki i wobec tego trendu nie wolno przejść obojętnie. Tym zagadnieniom poświęcamy pierwszy rozdział.

Po drugie, dostęp do informacji, ponowne wykorzystywanie należy obserwować w działaniu. Tym zagadnieniem poświęcamy rozdział drugi agregujący zagadnienia praktyczne. Warto przyjrzeć się potencjalnym obszarom kolizji z prawem do ochrony danych osobowych. Duże zbiory danych powinny być przeznaczone do ponownego wykorzystywania z poszanowaniem praw jednostki bez narażania jej na identyfikację. Tymczasem przeciwdziałanie globalnym skutkom pandemii SARS-CoV-2 w formie aplikacji śledzących kontakty (*de facto* przemieszczanie się jednostek) pokazało potencjał (i zagrożenia dla prywatności) płynący z interoperacyjności systemów pozwalających na łączenie danych osobowych, przestrzennych i telekomunikacyjnych. Kluczowe znaczenie ma więc anonimizacja i pseudoanonimizacja przed ich ponownym wykorzystaniem. Wreszcie nie sposób uciec od kwestii ochrony baz danych (publicznych i prywatnych) i przysługującego im zróżnicowanego stopnia ochrony prawnej. W Polsce nie odnotowywano do tej pory przypadków wydawania przez podmioty zobowiązane decyzji administracyjnej o odmowie ponownego wykorzystywania opartej na argumentach zagrożenia dla prawa do baz danych w rozumieniu przepisów ustawy z dnia 27 lipca 2001 r. o ochronie baz danych. Warto zatem przyjrzeć się, w których sytuacjach aktualizują się normy zakazu i dozwoleń związane z eksploatacją cyfrowych baz danych.

Pozostaję z nadzieją, że niniejsza książka przysłuży się specjalistom, naukowcom i studentom chcącym zgłębiać prawne zagadnienia związane z cyfrową rewolucją oraz będzie stanowić wkład w debatę nad jak najlepszymi rozwiązaniami legislacyjnymi towarzyszącymi otwieraniu dostępu do danych.

Redaktor dr hab. Michał Bernaczyk, prof. UWr

Rozdział I

Prawo dostępu do otwartych danych jako prawo podstawowe w prawie krajowym, międzynarodowym i unijnym

Wprowadzenie.

Konstytucyjne czy ponadnarodowe gwarancje dostępu do otwartych danych? Kilka uwag o nowym pojęciu „wykorzystywania informacji sektora publicznego” w polskim ustawodawstwie

The introduction: Constitutional or supranational origin of access to open data? Some conceptual issues on the new “re-use of public sector information” definition in Polish ordinary legislation

Streszczenie: Artykuł wyjaśnia kilka zagadnień pojęciowych wynikających z ewolucji prawa do ponownego wykorzystywania informacji sektora publicznego, rozwiniętego w najnowszej dyrektywie UE 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (dalej jako „dyrektywa 2019/1024”). Mimo faktu, że ponowne wykorzystywanie zostało wprowadzone jako odrębne uprawnienie, zależne od krajowego ustawodawstwa o dostępie do informacji, przechodziło ono stopniową ewolucję w kierunku prawa podstawowego do poszukiwania oraz uzyskiwania cyfrowych informacji i danych wynikającego z Karty praw podstawowych Unii Europejskiej. Ewolucja prawa do ponownego wykorzystywania i jego najnowsza implementacja w ustawie z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego może okazać się ostatnią deską ratunku dla jednostek, prywatnych przedsiębiorców rozczarowanych nieefektywną i względnie anachroniczną ustawą o dostępie do informacji publicznej.

Słowa kluczowe: ponowne wykorzystywanie informacji sektora publicznego, dyrektywa *re-use*, prawo do informacji, dostęp do informacji publicznej, Karta praw podstawowych Unii Europejskiej, Europejska Konwencja Praw Człowieka, Konstytucja RP, dyrektywa 2019/1024

Abstract: The article explains some conceptual issues originating from the evolution of right to re-use of the public sector information, developed in the latest EU directive of 20 June 2019 on open data and the re-use of public sector information (further referred to as the “Directive (EU) 2019/1024”). Despite the fact that re-use was introduced in first Public Sector Information Directive of 2003 as a separate right, dependent on national access to information (freedom of information) laws, it began slow transformation into the fundamental right to seek and receive digital open data & information under EU Charter of Fundamental Rights. Such evolution and the recent implementation in Polish Law on Open Data and Re-Use of Public Sector Information of 11 August 2021 may become a lifeline for individuals, private business disappointed with relatively weak and anachronistic Law on Access to Public Information.

Keywords: re-use of public sector information, Directive (EU) 2019/1024 on open data and the re-use of public sector information, right to information, freedom of information, access to information, The Charter of Fundamental Rights of the European Union, The European Convention on Human Rights, The Constitution of Republic of Poland

1. Cywilizacyjny kontekst ponownego wykorzystywania informacji sektora publicznego

Nasza terażniejszość we wszystkich obszarach życia prywatnego oraz społecznego opiera się na dostępności danych. To, w jaki sposób potrafią z nich korzystać, determinowało rozwój jednostek i społeczeństw jeszcze przed nastaniem epoki cyfrowej, jednak to cyfryzacja i rozwój sieci informatycznych na przełomie XIX i XX w. umożliwiły człowiekowi radykalne uzupełnienie umiejętności kognitywnych poprzez systemy gromadzące, przetwarzające informacje, wspomagając tym samym aktywność człowieka, a nawet zastępując ją w obsłudze obrotu

gospodarczego oraz w relacjach z władzą publiczną¹. Nie ma wątpliwości, że jakość naszego życia będzie zależeć już nie tylko od dostępności danych, ale zapewnienia im cech umożliwiających relatywnie swobodne przetwarzanie. Komisja Europejska prognozuje, że w 2025 r. ludzkość wytworzy 175 zettabajtów danych. Obecnie 80% operacji przetwarzania i analizy danych odbywa się w centrach danych i w ramach scentralizowanej infrastruktury obliczeniowej, a 20% w inteligentnych urządzeniach podłączonych do internetu, takich jak samochody, sprzęty gospodarstwa domowego czy roboty produkcyjne, oraz w obiektach przetwarzania danych znajdujących się w pobliżu użytkownika (tzw. *edge computing* – przetwarzanie danych na obrzeżach sieci z wykorzystaniem architektury rozproszonych zasobów), zaś w perspektywie najbliższych lat tendencja ulegnie odwróceniu². Unia Europejska aspiruje również do pierwszeństwa w wyścigu o sztuczną inteligencję, której zastosowanie ma być osiągnięciem nie tylko pod względem technologicznym, ale i etycznym. Nie należy mieć jednak złudzeń, że rozwój i doskonalenie systemów sztucznej inteligencji jest możliwy bez danych, którymi „uczymy” sztuczną inteligencję. Istotnym posiadaczem danych, „paliwa” do rozwoju są państwa członkowskie i Polska nie stanowi pod tym względem wyjątku. Polska ma obowiązek wdrożyć prawne gwarancje umożliwiające wykonywanie operacji na danych, co na pierwszy rzut oka nie wnosi istotnej zmiany w sferze materialnych oraz proceduralnych praw człowieka i obywatela umożliwiających dostęp do informacji o działalności państwa.

¹ W państwach UE granice zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach wynikają z art. 22 ust. 1 rozporządzenia 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 (Dz. Urz. UE L 119 z 4.05.2016 r., s. 1), dalej jako: RODO.

² Zob. Komunikat z 19 lutego 2020 r. „Europejska strategia w zakresie danych”, COM(2020) 66 final, s. 2.

Sformułowania prawo do informacji i otwarte dane padają często w trakcie opisywania zjawisk z pogranicza partycypacji społecznej, innowacyjnej gospodarki, ale odnoszą się do innych desygnatów. Otwarte dane (podkreślmy, że operujemy słowem „dane”, a nie informacje) odnoszą się do najniższego, najbardziej szczegółowego sygnału, zaś przydana im „otwartość” umożliwia ich ekstrakcję, łączenie w informacje, powielanie i inne techniki związane z tzw. eksploracją danych. Proces ten przebiega współcześnie w przytłaczającej większości przypadków za pomocą technik komputerowych. To, czy jakkolwiek podmiot będzie mieć roszczenie o dostęp do tych danych, a już zwłaszcza o nadanie im cech „otwartości”, zależy od konstytucyjnych i ustawowych uwarunkowań prawa krajowego. Jeżeli w systemie prawnym istnieje norma kompetencyjna nakazująca organom państwa gromadzić dane, utrzymywać informacje, a nadto czynić je otwartymi (w sensie czysto technicznym³), to nie oznacza wcale, że taki nakaz jest korelatem uprawnienia jednostki do korzystania z danych, nie wspominając o ich dostępności (otwartość techniczna nie przekłada się na dostęp jednostki do informacji i swobodę czynienia z niej użytku). Prawo dostępu do informacji jest materią konstytucyjną lub ustawową, aczkolwiek zaliczaną do prawa konstytucyjnego w znaczeniu materialnym⁴. Ponowne wykorzystywanie – w rozumieniu reżimu prawa UE – odnosi się do informacji pochodzącej od podmiotów władzy publicznej, do której zagwarantowano już dostęp. Tkwi w tym pewien paradoks: wykonując prawo Unii Europejskiej (w formie ustawowej implementacji kolejnych dyrektyw: zob. chronologię tych wdrożeń w kolejnym punkcie), polski ustawodawca wypełnia zobowiązania traktatowe i realizuje „otwartość”

³ Do otwartości w aspekcie technicznym odwołują się definicje legalne różnych formatów nadające się do odczytu maszynowego umieszczone w dyrektywie 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (zob. art. 2 pkt 14 i 15 dyrektywy 2019/1024).

⁴ M. Bernaczyk, *The constitutional right to information in Poland: theory and practice*, „International Comparative Jurisprudence” 2019, Vol. 5, No. 1, s. 37-39.

danych, których dostępność wynika z wyłącznej kompetencji państwa członkowskiego⁵.

Sukces instytucji prawnej ponownego wykorzystywania informacji sektora publicznego zależy więc od dostępności danych na zasadach i w trybie prawa krajowego, które mogą się różnić w zależności od szczegółowych rozwiązań przyjętych w poszczególnych państwach. Ilustrując to dosadniej, można to porównać do hipotetycznej sytuacji, w której na obszarze Unii Europejskiej istniałby jednolity, zbudowany na zasadzie rozliczalności prawny system ochrony danych osobowych (co jest faktem prawnym), lecz (i to już założenie czysto fikcyjne) każde państwo członkowskie swobodnie decydowałoby o tym, czym są dane osobowe i co – często wbrew faktycznej naturze określonych danych – identyfikuje istotę ludzką. Zrozumienie tych obszarów regulacyjnych wymaga osadzenia instytucji ponownego wykorzystywania na tle zasady kompetencji powierzonych (art. 5 ust. 2 Traktatu o Unii Europejskiej) oraz uwzględnienia specyfiki reżimu dostępowego w danej jurysdykcji. W Polsce ten ostatni wynika z art. 61, 74 ust. 3 Konstytucji RP oraz ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (dalej jako: u.d.i.p.), natomiast przepisy Konstytucji RP nie dają wyraźnej odpowiedzi na dwa zasadnicze pytania:

- 1) czy w aktualnym ustroju społeczno-gospodarczym (art. 20-22 Konstytucji RP) państwo polskie może być uprawnione z tytułu własności publicznej do zgromadzonej przezeń informacji (dobra niematerialnego);
- 2) jak dalece (i czy w ogóle) państwo polskie może kreować normę pozwalającą na czynienie użytku z informacji, tak aby korzystanie z własności publicznej nie przeradzało się w kamuflowane ograniczenie wolności uzyskiwania informacji i prawa do informacji. Jest

⁵ To, czy jest to kompetencja wyłączna Unii Europejskiej, również może stanowić przedmiot dyskusji. Wydaje się, że państwa członkowskie powinny być gotowe na reinterpretację poglądu o swej wyłączności w kwestii dostępu do informacji, skoro obowiązująca dyrektywa (zob. dalsze uwagi) zaczyna podkreślać związek ponownego wykorzystywania z wolnością uzyskiwania informacji.

to zagadnienie kluczowe w dobie tendencji autokratycznych wyrażających się w dążeniu egzekutywy do kontroli nad środkami przekazu, obiegiem informacji o działalności władz publicznych, a także deprecjacji mechanizmów rozliczalności za sprawowanie władzy publicznej (zarówno w formie sankcji skupionej, jak i sądu opinii publicznej).

Dotychczasowa praktyka polskiego ustawodawcy w rozstrzyganiu powyższych kwestii jest powściągliwa. Ponowne wykorzystywanie informacji sektora publicznego oglądane zarówno z perspektywy „użytkownika” (podmiotu wnioskującego o dane lub korzystającego z bezwłoskowego dostępu do cyfrowych repozytoriów), jak i władz publicznych, nie okazało się rozwiązaniem spektakularnym, rewolucyjnym czy istotnie wpływającym na gospodarke.

Nie można powiedzieć, aby ustawa wzmocniła zakres wolności i praw jednostki, z którymi *re-use* pozostaje w instrumentalnym związku (np. wolność działalności gospodarczej, nauczania, badań naukowych lub dóbr kultury). Nie ma też wyraźnych dowodów, że odrębna regulacja ustawowa doprowadziła do ograniczenia prawa dostępu do informacji publicznej. Rzeczpospolita Polska uniknęła wprowadzania norm kreujących nową kategorię publiczną utożsamianych z „publiczną własnością danych” lub praw *sui generis* należnych państwu. W 2017 r. fundacje ePaństwo oraz Centrum Cyfrowe konkludowały we wspólnym raporcie, że „ustawa o re-use nie zrewolucjonizowała wykorzystywania zasobów publicznych, w tym zasobów dziedzictwa kultury. [...] Można postawić tezę, że mamy do czynienia z dwiema możliwymi odpowiedziami. Albo zasoby publiczne nie są atrakcyjne dla użytkowników, albo brak jest wiedzy na temat tego, jak stosować reguły ponownego wykorzystywania informacji zgodnie z prawem”⁶.

⁶ Raport 2017. Ustawa o ponownym wykorzystywaniu informacji sektora publicznego rok po wejściu w życie, s. 28, https://centrumcyfrowe.pl/wp-content/uploads/2017/06/Reuse_raport_2017.pdf [dostęp: 1.10.2021].

Z kolei z perspektywy Rady Ministrów zagadnienie otwartych danych było jednym z wielu zagadnień w polityce krajowej i europejskiej⁷. Nie można stwierdzić, że w aspekcie normatywnym doszło do uprzywilejowania tej sfery polityki poprzez np. radykalne wyjście poza minimum wymogów przepisanych dyrektywami UE bądź wzmocnienie pozycji ministra ds. informatyzacji. Warto docenić, że w obrębie działu administracji rządowej „informatyzacja” instytucję ponownego wykorzystywania starano się traktować jako zagadnienie niesporne, sektorową nowinkę technologiczną z obszaru tzw. społeczeństwa informacyjnego (zob. art. 12a ustawy z dnia 4 września 1997 r. o działach administracji rządowej⁸). Pozwalało to kolejnym ministrom ds. informatyzacji prowadzić rządowe prace nad implementacją prawa UE, prezentując je jako zagadnienie neutralne politycznie, unikając przy tym zajmowania kategorycznego stanowiska na temat związku informacji posiadanych przez państwo z konstytucyjnymi zasadami ustroju i prawami jednostki⁹. Niemniej

⁷ Stanowisko i proponowane działania Rady Ministrów zawierał Program otwierania danych publicznych – dokument strategiczny określającym kierunki realizacji polityki na rzecz otwierania danych do 2020 r. (przyjęty we wrześniu 2016 r.). Obecnym dokumentem programowym jest „Program otwierania danych na lata 2021-2027” (<https://www.gov.pl/attachment/c42009a8-0354-43f9-88ca-3a057823c6bd>, dostęp: 26.10.2021). Jest to dokument obszerny, ale w zakresie identyfikacji problemów i metod ich rozwiązywania (por. s. 60-62) nie można mówić o nowości. Program nie przedstawia szczegółowo metod wykonania u.d.i.p. oraz ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego.

⁸ T.j. Dz. U. z 2020 r. poz. 1220 ze zm. Dostęp do informacji i otwieranie danych nie zostały ujęte wprost w grupie zadań ministra ds. informatyzacji (w przeciwieństwie do np. „kształtowania polityki państwa w zakresie ochrony danych osobowych”, zob. art. 12a ust. 1 pkt 8 ustawy o działach administracji rządowej), aczkolwiek ponowne wykorzystywanie informacji sektora publicznego jest przesłanką rozwoju społeczeństwa informacyjnego (zob. art. 12a ust. 1 pkt 6 powołanej ustawy) oraz warunkiem wstępnym usług świadczonych drogą elektroniczną (zob. art. 12a ust. 1 pkt 6 powołanej ustawy).

⁹ W praktyce minister ds. informatyzacji był jednak skazany na porażkę, ilekroć pozostali członkowie Rady Ministrów dostrzegali ryzyko utraty prawnej i politycznej kontroli nad informatyzacją bądź zasobami informacyjnymi. Tak należy tłumaczyć m.in. genezę przepisu art. 2 ust. 3 u.d.i.p. (w brzmieniu obowiązującym do 8 grudnia 2021 r.), który ograniczał przekazywanie pod kontrolę ministra ds. informatyzacji informacji gromadzonych w bazach danych administrowanych przez ministra sprawiedliwości (centralna baza ksiąg wieczystych, Krajowy Rejestr Karny, Krajowy Rejestr Sądowy) lub ministra finansów

jednak problem potencjalnej rozdzielności bądź krzyżowania się praw podmiotowych informacyjnych jednostki pochodzących z różnych systemów prawnych (UE i polskiego systemu źródeł prawa) pozostaje, dlatego w dalszej części warto prześledzić, w jaki sposób ewoluowała instytucja ponownego wykorzystywania informacji sektora publicznego. Cel tej zwięzłej charakterystyki opiera się na następującym założeniu: nie można wykluczyć, że w perspektywie czasu ustawowe środki implementacyjne przejmą w całości lub istotnej części funkcję przypisywaną ustawie o dostępie do informacji publicznej.

2. Instytucja ponownego wykorzystywania i jej harmonizacja z polskim reżimem dostępu do informacji posiadanych przez państwo

29 grudnia 2021 r. upływa dziesięć lat od chwili wdrożenia w Polskim porządku prawnym dyrektywy o ponownym wykorzystywaniu informacji sektora publicznego. Wówczas to weszła w życie nowelizacja u.d.i.p. z dnia 16 września 2011 r.¹⁰, która miała na celu wykonanie dyrektywy 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego¹¹.

(Rejestr Należności Publicznoprawnych). Derogacja art. 2 ust. 3 u.d.i.p. jest niewątpliwie krokiem we właściwym kierunku, aczkolwiek pozycja ustrojowa ministra ds. informatyzacji (pomijając oczywistą zależność od prezesa rady ministrów) będzie zależeć od roli przypisywanej mu w ramach projektów związanych z informatyzacją sektora publicznego powierzanych w trybie art. 10c ustawy z dnia 8 sierpnia 1996 r. o Radzie Ministrów (t.j. Dz. U. z 2021 r. poz. 178 ze zm.). W zależności od decyzji premiera rola ministra ds. cyfryzacji może polegać na współwykonawstwie projektów (w charakterze zleceniobiorcy) bądź sprowadzać się do roli organu opiniującego.

¹⁰ Chodzi o ustawę z dnia 16 września 2011 r. o zmianie ustawy o dostępie do informacji publicznej oraz niektórych innych ustaw (Dz. U. Nr 204, poz. 1195).

¹¹ Dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 345 z 31.12.2003 r., s. 90), dalej jako: dyrektywa 2003/98/WE.

W nauce prawa konstytucyjnego odnotowano to wydarzenie z innego powodu aniżeli wykonanie prawa UE lub wzmocnienie praw jednostki. Przeciwnie, na implementacji dyrektywy cieniem położyło się naruszenie konstytucyjnego trybu uchwalania ustaw i próba ograniczenia prawa dostępu do informacji publicznej. W ciągu ostatnich dziesięciu lat utarło się wykorzystywać inicjatywy ustawodawcze lub abstrakcyjną kontrolę konstytucyjności¹² ustaw dotyczących dostępu do informacji

¹² Por. krytyczne uwagi w pkt 4 zdania odrębnego sędziego M. Zubika pod adresem pytania prawnego NSA w sprawie P 25/12 rozstrzygniętej wyrokiem TK z dnia 13 listopada 2013 r. („Postawione przez Naczelnny Sąd Administracyjny pytanie prawne nie służyło również «umacnianiu uprawnień obywateli»”). Podobne kontrowersje towarzyszyły wnioskowi Pierwszej Prezes Sądu Najwyższego z dnia 4 listopada 2013 r. wszczynającego postępowanie przed TK pod sygn. K 58/13. Sprawa nie została merytorycznie rozpoznana wskutek cofnięcia wniosku i umorzenia postępowania, co Pierwsza Prezes SN tłumaczyła rozstrzygnięciem wątpliwości natury konstytucyjnej (kolizji prawa do prywatności z prawem do informacji) w praktyce sądowni-administracyjnej (zob. komunikat Pierwszej Prezes SN Małgorzaty Gersdorf i pismo procesowe do sprawy K 58/13 z dnia 12 kwietnia 2017 r., dostępne pod adresem: http://www.sn.pl/aktualnosci/SiteAssets/Lists/Wydarzenia/New-Form/2017.04.12_Wycofanie.wniosku.TK_K-58_13.pdf [dostęp: 21.09.2021]). Organizacje pozarządowe wskazywały jednak na inny problem, do którego Pierwsza Prezes SN nie odniosła się oficjalnie: ewentualne orzeczenie w sprawie K 58/13 mogło legitymizować prace ustawodawcze nad ograniczeniem jawności życia publicznego zaś składowi orzekającemu miała przewodniczyć osoba nieuprawniona do zasiadania w TK (co potwierdził wyrok ETPCz z dnia 7 maja 2021 r. w sprawie *Xero Flor w Polsce sp. z o.o. v. Poland*, skarga nr 4907/18). Praktyka ustrojowa po wyborach parlamentarnych z 2015 r. nosi wyraźne znamiona ograniczenia sfery autonomii informacyjnej jednostki, co przejawia się przede wszystkim w kierowaniu do Trybunału Konstytucyjnego wniosków (w trybie kontroli abstrakcyjnej) o stwierdzenie niezgodności z Konstytucją RP przepisów ustawy o dostępie do informacji publicznej. Przykładem jest niewątpliwie wniosek grupy posłów koalicji rządzącej z dnia 2 grudnia 2019 r. o stwierdzenie niezgodności z Konstytucją RP przepisu art. 5 ust. 2 u.d.i.p. rozpoznawany przez TK pod sygn. K 21/19. Wniosek pozostaje w bezpośrednim związku z próbami zablokowania opinii publicznej dostępu do tzw. list poparcia dla kandydatów na członków Krajowej Rady Sądownictwa (szerzej o prawnym i politycznym kontekście tej sprawy zob. M. Bernaczyk, *Dostęp do list poparcia kandydatów do Krajowej Rady Sądownictwa jako przykład neutralizacji aksjologicznej Konstytucji RP*, Acta Universitatis Wratislaviensis No. 3978, „Przegląd Prawa i Administracji” 2020, t. 120/1, s. 133-146). Podobny charakter nosi wniosek Pierwszej Prezes SN Małgorzaty Manowskiej z dnia 17 lutego 2021 r. skierowany do TK i rozpoznawany pod sygn. K 1/21. Pozostaje on w zbiegu z praktyką odmowy informowania o statusie osób zaopiniowanych przez KRS i dopuszczonych do służby sędziowskiej w SN. Wszystkie te działania są stwarzają nieodparte wrażenie dążenia do wygaszenia ustawowych podstaw prawnych

publicznej jako pretekst do ograniczania prawa do informacji o działalności władz publicznych (art. 61 Konstytucji RP). Wspomnianą nowelę z dnia 16 września 2011 r. można oceniać jako pierwsze działanie tego typu, skoro wprowadziła ona – nie mające nic wspólnego z wykonaniem dyrektywy 2003/98/WE – ograniczenie dostępu do informacji o działalności władz publicznych ze względu na „ważny interes gospodarczy państwa”, zarówno w sferze polityki zagranicznej, jak i w ramach gospodarowania mieniem Skarbu Państwa (zob. art. 1 pkt 4 noweli z 16 września 2011 r.¹³). Dzięki kontroli następczej zainicjowanej przez Prezydenta RP doszło do wygaszenia epizodycznej mocy obowiązującej tych ograniczeń. Wyrokiem Trybunału Konstytucyjnego z dnia 18 kwietnia 2012 r. (K 33/11) uznano je za niezgodne z Konstytucją RP z powodu naruszenia procedury ustawodawczej, jednakże trzon przepisów o unijnej proveniencji (nieistniejący już rozdział 2a u.d.i.p.), poświęconych „ponownemu wykorzystywaniu informacji sektora publicznego”, wszedł w życie 29 grudnia 2011 r.

Przepisy dotyczące ponownego wykorzystywania pozostały sprawą nie tyle konstytucyjnie niesporną, ile pozbawioną zainteresowania nauki prawa konstytucyjnego. Było to o tyle dziwne, że u.d.i.p. jest zaliczana do źródeł prawa konstytucyjnego (obok ustawowych konkretyzacji praw wyborczych z art. 62, prawa petycji, skarg i wniosków z art. 63). Ustawa o dostępie do informacji publicznej, traktowana jako uszczegółowienie art. 61 ust. 1 Konstytucji RP („prawo do informacji o działalności funkcjonariuszy oraz organów władzy publicznej”), z końcem 2011 r. zaczęła operować dwoma różnymi uprawnieniami w stosunku do „informacji o sprawie publicznej” (art. 1 ust. 1 u.d.i.p.):

umożliwiających wykonywanie prawa do informacji o działalności państwa i legitymizację stanu prawnego uniemożliwiającego weryfikację klientystycznych, korupcyjnych zachowań funkcjonariuszy państwa.

¹³ Ograniczenie dostępu do informacji o sprawach publicznych wprowadzono w formie nowej „tajemnicy dyplomatycznej” zdefiniowanej ogólnie w art. 7 pkt 12 ustawy z dnia 21 stycznia 2021 r. o służbie zagranicznej (Dz. U. z 2021 r. poz. 464).

- 1) każdemu przysługuje prawo dostępu do informacji publicznej (art. 2 u.d.i.p.),
- 2) każdemu przysługuje prawo do ponownego wykorzystywania informacji publicznej (zob. art. 2a u.d.i.p. w brzmieniu obowiązującym od 29 grudnia 2011 r. do 16 czerwca 2016 r.).

Rozdzielenie tych dwóch kwestii w odniesieniu do tego samego idiomatu („informacja publiczna”) przez racjonalnego ustawodawcę oparło się na założeniu Unii Europejskiej, że – w największym uproszczeniu – efekt wiedzy osiągany przez jednostkę dzięki „krajowemu” prawu do informacji jest niewystarczający dla swobodnego przepływu towarów i usług opartych na informacji (preferowaną była informacja cyfrowa nadająca się do automatycznego przetwarzania).

W ten sposób ujawnia się subtelna i teoretyczna różnica pomiędzy tzw. „ponownym wykorzystywaniem informacji sektora publicznego” (prawem podmiotowym wynikającym z prawa wtórnego UE) a krajowym prawem (człowieka, obywatela) do informacji (ew. prawem dostępu do informacji publicznej). Ponowne wykorzystywanie informacji sektora publicznego jest z perspektywy UE zagadnieniem wtórnym wobec dostępu do tej informacji. Dotychczasowa praktyka ustawodawcza i sądowa Unii Europejskiej uniknęła bezpośredniej wypowiedzi, czy stanowienie prawa wtórnego w obrębie dostępu do informacji o działalności państwa (w znaczeniu wyprowadzonym np. z art. 10 EKPCz, art. 61 Konstytucji RP) znajduje się w gestii kompetencji wyłącznych UE lub współdzielonych z państwami członkowskimi. Artykuł 11 ust. 2 Karty praw podstawowych UE definiuje wolność wypowiedzi jako „wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe”, w czym należy upatrywać bezpośrednie nawiązania UE do art. 10 ust. 1 EKPCz¹⁴, ale to

¹⁴ Zob. J. Sobczak, komentarz do art. 11 Karty Praw Podstawowych Unii Europejskiej, [w:] A. Wróbel (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, Warszawa 2020, teza nr 3.

samo w sobie nie daje odpowiedzi na pytanie, czy istnieje „unijne” prawo do (dostępu, „poszukiwania”) informacji posiadanych przez państwa członkowskie, a zwłaszcza wykorzystywania (*re-use*) udostępnionych informacji (bezdyskusyjnie prawo dostępu do informacji istnieje w odniesieniu do instytucji UE; zob. art. 42 Karty praw podstawowych).

Wprawdzie można twierdzić, że do pewnego stopnia zagadnienie to zostało już rozstrzygnięte w samej Karcie, ponieważ zgodnie z art. 52 ust. 2 „w zakresie, w jakim niniejsza Karta zawiera prawa, które odpowiadają prawom zagwarantowanym w europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, ich znaczenie i zakres są takie same jak praw przyznanych przez tę konwencję”. Jednocześnie art. 52 ust. 3 zd. 2 Karty zastrzega, że treść wolności z art. 10 EKPCz ma charakter minimalny i może zostać ukształtowana w prawie UE na wyższym poziomie. Trybunał Sprawiedliwości UE może zatem uznać zbieżność normatywną klauzul art. 10 ust. 1 EKPCz i art. 11 ust. 1 Karty, ale i wyjść poza aktualny dorobek orzecniczy Trybunału strasburskiego. Ostrożność w stawianiu znaku równości między jednym a drugim przepisem może wynikać również z orzecznictwa ETPCz. Sformułowanie „otrzymywanie informacji bez ingerencji władz publicznych” nie doprowadziło w systemie Rady Europy¹⁵ do progresywnego i szybkiego zrekonstruowania prawa do informacji o działalności państwa jako samoistnego uprawnienia jednostki. Wydobywanie z EKPCz prawa do informacji można ocenić jako bardzo powolny proces (jeśli za jurydyczne otwarcie dyskusji przyjmiemy wyrok z dnia 19 lutego 1998 r. w sprawie *Guerra i in. przeciwko Włochom*, skarga nr 14967/89, zaś silne zakotwiczenie prawa do informacji o działalności utożsamimy z wyrokiem z dnia 14 kwietnia 2009 r. w sprawie *Társaság a Szabadságjogokért (TASZ) przeciwko*

¹⁵ Znacznie korzystniej rozstrzygnięto tę kwestię w art. 13 ust. 1 zd. 2 Amerykańskiej Konwencji Praw Człowieka z 1969 r., która pozostawiała mniejszy margines wątpliwości wprost wskazując na prawo do „poszukiwania” informacji nieobecne w leksyce art. 10 EKPCz (zob. także wyrok Międzyamerykańskiego Trybunału Praw Człowieka z 16 września 2006 r., ser. C/151).

Węgrom, skarga nr 37374/05). Mimo aktualnego i bezspornego poglądu o konwencyjnej ochronie prawa dostępu do informacji o działalności państwa, prawo to jest obwarowane w orzecznictwie ETPCz pewnymi ograniczeniami podmiotowymi (np. poszukiwanie informacji w związku z pełnioną rolą *public watchdog*) oraz przedmiotowymi (informacja poszukiwana w interesie publicznym, wymóg istnienia „gotowej” informacji, której wyłącznym dysponentem pozostają władze publiczne)¹⁶.

Unia Europejska podeszła do kwestii otwartości danych ostrożnie, tzn. redukując zarzuty o działanie poza obszarem kompetencji powierzonych przez Państwa Członkowskie i wprowadzając prawo podmiotowe do ponownego wykorzystywania informacji sektora publicznego (po raz pierwszy) w dyrektywie 2003/98/WE¹⁷ **udostępnionej przez państwo członkowskie**. Dyrektywa 2003/98/WE zdefiniowała ponowne wykorzystywanie (ang. *re-use of public sector information*) jako „wykorzystywanie przez osoby fizyczne lub prawne dokumentów będących w posiadaniu organów sektora publicznego, do celów komercyjnych lub niekomercyjnych innych niż ich pierwotne przeznaczenie w ramach zadań publicznych, dla których te dokumenty zostały wyprodukowane”. Od początku też założyła, że zakres normowania nie narusza krajowych reżimów dostępowych (po raz pierwszy zasada ta została podkreślona w motywie 9 nieobowiązującej już dyrektywy 2003/98/WE, następnie w motywie 8 dyrektywy 2013/37/EU, zaś w obecnym stanie prawnym powtórzono ją w motywie 18 dyrektywy 2019/1024 z dnia 20 czerwca 2019 r). Należy przy tym zastrzec, że pierwsze orzeczenia TSUE dotyczące uchybienia obowiązkowi wdrożenia dyrektywy 2003/98/WE nie nakładały, wbrew obiegowym opiniom, obowiązku kategorycznego oddzielenia prawa do informacji od prawa do ponownego wykorzystywania

¹⁶ Zob. rekapitulację poglądów ETPCz na temat wolności uzyskiwania informacji od państwa w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom* (wyrok z dnia 8 listopada 2016 r., skarga nr 18030/11).

¹⁷ Dyrektywa 2003/98/WE, s. 90.

(zob. pkt 6 i 8 wyroku z 27 września 2007 r., sprawa C465/06, *Komisja p. Królestwu Hiszpanii*). Trybunał Sprawiedliwości UE wymagał natomiast przestrzegania zasady pewności prawa i określoności krajowych źródeł prawa, co może wyrażać się zarówno w doprecyzowaniu istniejącego ustawodawstwa o dostępie do informacji, jak i w tworzeniu odrębnej ustawy.

W polskim porządku prawnym odczytywano dyrektywę 2003/98/WE jako konieczność użycia takich środków legislacyjnych, które dzielą oba zagadnienia (dostęp i ponowne wykorzystywanie). W efekcie praktyka sądowniczoadministracyjna zaakceptowała propozycję autora, aby w toku ustalania znaczenia tej instytucji prawnej kierować się wykładnią celowościową (w jej unijnym rozumieniu, podszytym funkcjonalizmem). W rezultacie pod pojęciem prawa do ponownego wykorzystywania należy rozumieć publiczne prawo podmiotowe gwarantujące osobom fizycznym, osobom prawnym i jednostkom organizacyjnym nieposiadającym osobowości prawnej uzyskanie informacji sektora publicznego w celu:

- 1) osiągnięcia przez wnioskodawcę szeroko pojętej korzyści (społecznej lub gospodarczej), która jest uwarunkowana:
 - a) wykonaniem przez podmiot zobowiązany operacji na informacjach publicznych (tzn. szeroko pojętą „obróbką” techniczną lub analityczną informacji publicznej lub jej części, a w szczególności wyszukaniem, przekształceniem, utrwaleniem, replikowaniem w postaci elektronicznej pod kątem indywidualnego przedsięwzięcia komercyjnego lub niekomercyjnego wnioskodawcy)

lub

- b) wyrażeniem przez podmiot zobowiązany zgody na eksploatację informacji publicznych objętych prawami własności intelektualnej (praw autorskich i pokrewnych, włączając formy ochrony *sui generis*), o ile podmiot zobowiązany posiada takie uprawnienia;

- 2) mogącym sięgać dalej niż zmniejszanie niewiedzy lub podnoszenie świadomości prawnej, społecznej, ułatwianie świadomych decyzji w społeczeństwie obywatelskim, udział w debacie publicznej, prawo do krytyki itp.

Drugi człon tej definicji nawiązywał częściowo do postulatów, aby odróżniać „wartość demokratyczną” informacji sektora publicznego od ich „wartości ekonomicznej”¹⁸, ale należy zastrzec, że taki postulat był formułowany z perspektywy ponadnarodowej i bez roztrząsania konstytucyjnego uzasadnienia prawa do informacji w poszczególnych państwach członkowskich. Trawestacja tych postulatów skutkowałą niekiedy nazywaniem w Polsce prawa do ponownego wykorzystywania prawem o charakterze gospodarczym, ekonomicznym itp., ale nie miało to uzasadnienia ani w tekście dyrektywy, ani w krajowych środkach implementacji. Upraszczając, prawo do ponownego wykorzystywania wyrażało się w żądaniu publicznieprawnnej usługi polegającej na odpowiednim przygotowaniu danych do jakiegoś przedsięwzięcia realizowanego przez wnioskodawcę (niekoniecznie w ramach wolności działalności gospodarczej). Pierwotnie podstawowym zagadnieniem leżącym u podstaw wprowadzenia tej instytucji nie był wcale dylemat, „czy udostępniać informacje” (zwane w Polsce „informacjami publicznymi”, ew. „o sprawie publicznej”), lecz „w jaki sposób” udostępniać informacje¹⁹. Tymczasem niektóre państwa członkowskie

¹⁸ K. Janssen, *The Availability of Spatial and Environmental Data in The European Union. At the Crossroads between Public and Economic Interests*, Bedfordshire 2010, s. 64.

¹⁹ Np. K. Janssen pisała (w 2010 r.) np. „ogólnie rzecz ujmując, ponowne wykorzystywanie wiąże się z przetwarzaniem danych, które wykracza poza dostęp do dokumentów celu zapoznania się z jego zawartością. Na przykład naukowiec w celu uzyskania wyników musi przeprowadzić pewne czynności na danych, które uzyskuje z sektora publicznego. W wielu przypadkach wymaga to połączenia ich z innymi danymi lub wynikami innych badań. Sam dostęp do danych lub przeczytanie informacji nie będzie wystarczające. [...] Ponowne wykorzystywanie może być zdefiniowane jako «jakiegokolwiek wykorzystywanie informacji [...] sektora publicznego nie będące wykonywaniem zadania publicznego», jeżeli przyjęto założenie, że to komercyjne lub niekomercyjne wykorzystywanie danych ma gospodarczy cel przynoszący korzyść i wymaga dalszego przetwarzania danych w sposób wykraczający poza samo tylko zapoznanie się z ich zawartością”, K. Janssen, *The Availability...*, s. 66.

(przynajmniej na poziomie tekstu prawnego) już wtedy przewidywały, że uprawniony ma prawo do informacji wyrażonej w cyfrowym formacie i na nośnikach podlegających automatycznemu przetwarzaniu. Zresztą postulat kreślenia linii demarkacyjnej pomiędzy dostępem do informacji a jej ponownym wykorzystywaniem bardzo szybko zmuszał swych zwolenników do przeformułowania pierwotnego stanowiska²⁰.

Powyższe okoliczności przywołuję z intencją zwrócenia uwagi Czytelnika na pewne zjawisko. Otóż nie tylko w nauce, ale również na poziomie prawa UE zmienia się punkt widzenia na traktatowe uzasadnienie ponownego wykorzystywania, które znalazło wyraz w dyrektywie 2019/1024 z dnia 20 czerwca 2019 r. Należy dostrzec w niej wyraźne powiązanie (w motywie 5) prawa dostępu do informacji z art. 11 ust. 1 Karty praw podstawowych. Zgodnie z zasadą powierzenia (art. 5 ust. 1 zd. 1 TUE) granice kompetencji Unii wyznacza zasada przyznania, a wszelkie kompetencje nieprzyznane Unii w Traktatach należą do państw członkowskich (art. 5 ust. 2 zd. 2 TUE). Zasada powierzenia oznacza, że organy UE nie posiadają ogólnej kompetencji prawodawczej o treści zbieżnej ze zdolnością ustawodawczą krajowych parlamentów. Podstawową konsekwencją zasady powierzenia jest konieczność oparcia każdego aktu prawa wtórnego na podstawie traktatowej. Z chwilą wejścia w życie traktatu lizbońskiego (13 grudnia 2009 r.) Karta praw podstawowych uzyskała status identyczny z traktatami (prawem pierwotnym UE), więc wyznacza zakres kompetencji w zakresie ochrony praw podstawowych zagwarantowanych w Karcie (art. 11). Wszystko to prowadzi do hipotezy, że ponowne wykorzystywanie informacji sektora publicznego w dyrektywie 2019/1024 z dnia 20 czerwca 2019 r. zmierza do budowy mechanizmu ochrony wolności wypowiedzi w jej aktywnych przejawach związanych ze swobodą uzyskiwania informacji od państwa członkowskiego. Należy też dodać, że 25 listopada 2020 r. Komisja przedstawiła projekt rozporządzenia w sprawie europejskiego

²⁰ K. Janssen, *The influence of the PSI directive on open government data: an overview of recent developments*, "Government Information Quarterly" 2011, Vol. 28, No 4, s. 450.

zarządzania danymi – akt w sprawie zarządzania danymi (*Data Governance Act*)²¹, co oznacza, że integracja systemów prawnych państw członkowskich UE w zakresie dostępu do danych w celu ponownego wykorzystywania przechodzi podobny proces, co np. ochrona danych osobowych (polegał on na stopniowym zastępowaniu krajowej regulacji przepisami rozporządzenia wiążącymi w całości i stosowanymi bezpośrednio).

Ten proces, oglądany z perspektywy polskiej, może być dobrą wiadomością, ponieważ konsekwentne osłabianie prawa do informacji (publicznej) przy stopniowym wygaszeniu efektywnych środków ochrony sądowej i konstytucyjnej może znaleźć oparcie w prawie Unii Europejskiej i właściwych mu środkach ochrony praw jednostki. Oczywiście to zależy od tego, na ile polskie władze będą skłonne nadal kontestować prawo pierwotne UE, tak jak miało to miejsce w przypadku wyroku TK z dnia 7 października 2021 r. (K3/21).

Abstrahując od powiązania dyrektywy 2019/1024 z ochroną praw podstawowych jednostki w systemie UE oraz Rady Europy, wydaje się, że w sposób niezauważony, niekoniecznie przemyślany przez politycznych architektów, dokonuje się proces wypierania ustawy o dostępie do informacji publicznej przez ustawę z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (ogłoszona w Dz. U. z 2021 r. poz. 1641).

Dnia 29 czerwca 2021 r. Rada Ministrów złożyła do Sejmu rządowy projekt ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (druk nr 1338 Sejmu IX kadencji). Rządowa inicjatywa ustawodawcza jest logiczną konsekwencją związania Polski prawem UE i dyrektywą Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego²². Proces

²¹ <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020P.C0767&from=EN> [dostęp: 17.07.2021].

²² Dz. Urz. UE L 172 z 26.06.2019 r., s. 56.

legislacyjny w parlamencie przebiegał nadzwyczaj sprawnie, nie wzbudzając emocji na spolaryzowanej scenie politycznej, mimo że zakres uchwalonej regulacji dotyczy kwestii dostępu i przetwarzania informacji posiadanych przez państwo. Uchwalona regulacja będzie już odsłoną trzecią regulacji ustawowej poświęconej tzw. ponownemu wykorzystywaniu informacji sektora publicznego. Historię implementacji unijnego reżimu dotyczącego otwierania danych na terytorium polski tworzą następujące ustawy:

1. Nowelizacja ustawy o dostępie do informacji publicznej z 16 września 2011 r.²³, która weszła w życie 29 grudnia 2011 r. Nowelizacja polegała przede wszystkim na uzupełnieniu ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej poprzez dodanie rozdziału 2a („Ponowne wykorzystywanie informacji publicznej” – art. 23a-23i). Była to pierwsza w historii Polski implementacją dyrektywy 2003/98/WE²⁴. Polski rząd i ustawodawca uznali wówczas, że istniejąca ustawa o dostępie do informacji publicznej, w zakresie, w jakim posługuje się pojęciem „informacji o sprawie publicznej”, nakłada się zakresowo na definicję legalną „informacji sektora publicznego” zawartą w dyrektywie. Rozwiązanie było interesujące i co do zasady trafne, ponieważ otwieranie dostępu do danych gromadzonych przez szeroko pojęte państwo może być oparte na krajowej regulacji, którą kolokwialnie nazywany prawem (dostępu) do informacji publicznej. Nie zmienia to jednak faktu, że argumenty państwa członkowskiego UE o „dostrzeganiu przez system prawny prawo dostępu do dokumentów posiadanych przez organy administracji” były dla TSUE niewystarczające. W kontekście dyrektywy 2003/98/WE Trybunał przywołał swe dotychczasowe orzecznictwo dotyczące obowiązków państw członkowskich w zakresie wdrażania dyrektyw: skoro istniejący reżim prawny nie odnosi się wyraźnie, jasno,

²³ Ustawa z dnia 16 września 2011 r. o zmianie ustawy o dostępie do informacji publicznej oraz niektórych innych ustaw (Dz. U. Nr 204, poz. 1195).

²⁴ Dyrektywa 2003/98/WE, s. 90.

wprost do praw podmiotowych jednostki wynikających z pierwszej dyrektywy 2003/98/WE, to nie można mówić o spełnieniu standardów przewidywalności prawa i prawidłowej implementacji (zob. pkt 6 i 8 wyroku z dnia 27 września 2007 r., sprawa C 465/06, *Komisja p. Królestwu Hiszpanii*),

2. Kolejnym źródłem prawa była ustawa z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego (Dz. U. z 2019 r. poz. 1446). Ustawa po raz kolejny wykonywała prawo UE. Unia Europejska zdecydowała się na nowelizację dyrektywy 2003/98/WE (dokonaną dyrektywą Parlamentu Europejskiego i Rady 2013/37/UE z dnia 26 czerwca 2013 r. zmieniającą dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego²⁵), a polska implementacja zrewidowanej dyrektywy derogowała w całości rozdział 2a ustawy o dostępie do informacji publicznej. Ponowne wykorzystywanie wyprowadzono do samodzielnej regulacji ustawowej, chociaż nowy dogmat o odrębności istoty tych regulacji przełamywało centralne repozytorium informacji publicznej pozostawione w art. 9b ust. 1. Rozwiązanie opierało się na założeniu (osobiście oceniam je jako wysoce kontrowersyjne i niepoparte staranną wykładnią art. 61 Konstytucji RP), iż prawo do ponownego wykorzystywania jest prawem podmiotowym całkowicie odrębnym treściowo od prawa dostępu do informacji publicznej (w znaczeniu wynikającym z art. 61 Konstytucji RP). Z politycznego punktu widzenia było to rozwiązanie wygodne, pomagało (nieistniejącemu już) Ministerstwu Cyfryzacji utrzymywać narrację (zarówno wobec opinii publicznej, jak i w obrębie obozu rządzącego), że jest to regulacja z zakresu prawa administracyjnego zwiększająca swobodę działalności gospodarczej, obojętna dla konstytucyjnego statusu jednostki. Łatwość, szybkość, z jaką uchwalono tę ustawę w Sejmie VIII kadencji, zdaje się potwierdzać skuteczność tej taktyki, mimo zarysowujących

²⁵ Dz. Urz. UE L 175 z 27.06.2013 r., s. 1.

się wówczas ostrych podziałów politycznych zapoczątkowanych wybuchem kryzysu konstytucyjnego po wyborach parlamentarnych z 25.10.2015 r.

3. Aktualny system dostępu do informacji sektora publicznego posiadanych przez państwo (wytworzonych lub zgromadzonych przez nie od innych podmiotów publicznych) opiera się na przedłożonym projekcie ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (druk nr 1338 Sejmu IX kadencji). Ustawa z dnia 11 sierpnia 2021 r. opiera się na konstrukcji legislacyjnej i rozwiązaniach zawartych w ustawie z 2016 r., w kluczowych elementach używa identycznego języka prawnego (np. jeśli chodzi o treść podmiotu uprawnionego, treść uprawnienia, jak i podmioty zobowiązane), jednak wskutek poprawki senatora Jana Hamerskiego²⁶ zmieniono zasadniczo pojęcie ponownego wykorzystywania (zob. art. 2 pkt 12 ustawy). Gdyby nie ten drobny (wydawać by się mogło) zabieg, trudno byłoby mówić, że proponowane rozwiązania stanowią rewolucję w stosunku do dotychczasowego stanu prawnego (zob. dalsze uwagi).

Treść projektu przedłożonego Sejmowi nie pozostawiała cienia wątpliwości, że obowiązująca ustawa z dnia 21 sierpnia 2021 r. miała uszczegółowić rozwiązania (znane już ustawie z 2016 r., aczkolwiek zgodnie z wymogami dyrektywy 2019/1024), co wyraża się m.in. w szeregu nowych definicji legalnych konkretyzujących formy utrwalenia i udostępniania informacji sektora publicznego („dane badawcze”, „dane dynamiczne”, „dane o wysokiej wartości”, „interfejs programistyczny aplikacji”) i cechy jakościowe informacji sektora publicznego („otwarte dane”, „format przeznaczony do odczytu maszynowego”). Projekt posługiwał się pojęciem ponownego wykorzystywania, które stanowiło kalkę językową implemmentowanych dyrektyw i oznaczało „wykorzystywanie przez użytkowników informacji sektora publicznego w jakimkolwiek innym celu niż pierwotny publiczny cel, w jakim informacja została wytworzona, przetworzona,

²⁶ Zob. druk Senatu X kadencji nr 469Z z 8 sierpnia 2021 r.

pozyskana lub zgromadzona, z wyjątkiem wymiany informacji sektora publicznego między podmiotami zobowiązanymi wyłącznie w celu realizacji zadań publicznych” (zob. art. 2 pkt 12 rządowego projektu ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, druk Sejmu IX kadencji nr 1338). Jednakże na etapie rozpatrywania ustawy przez Senat definicja legalna uzyskała znacznie zwiększoną formę, przejmując funkcję ustawowej konkretyzacji prawa do informacji z art. 61 Konstytucji RP. Ponowne wykorzystywanie to „wykorzystywanie przez użytkowników informacji sektora publicznego w jakimkolwiek celu, z wyjątkiem wymiany informacji sektora publicznego między podmiotami zobowiązanymi wyłącznie w celu realizacji zadań publicznych”. Język art. 2 pkt 12 ustawy nie pozwala na przełamanie sformułowania „jakiegokolwiek cel” i twierdzenie, że wniosek o ponowne wykorzystywanie nie może dotyczyć informacji posiadanych przez podmioty zobowiązane w celu uzyskania wiedzy o działalności podmiotów (o których mowa w art. 61 ust. 1 zdanie pierwsze i drugie Konstytucji RP). Odwołanie się do obowiązku implementacji prawa UE nie uchybia w żaden sposób innej tezie, że ustawodawca krajowy może w krajowym środku (ustawie lub rozporządzeniu wykonawczym) wychodzić poza standard minimalny i funkcję dyrektywy tak długo, jak nie podważa jej celów. Absorpcja treści prawa podmiotowego skoncentrowanego na czysto politycznym efekcie „wiedzy” (prawa do informacji publicznej) przez prawo do ponownego wykorzystywania z pewnością nie podważa samego pierwotnego celu dyrektywy 2019/1024, jakim jest ułatwianie przetwarzania danych i agregowanie ich w informacje o różnorodnych zastosowaniach.

Otwarte jednak pozostaje pytanie o przestrzeganie ustawy o otwartych danych. Po niespełna 10 latach obowiązywania regulacji w tej materii (przypomnijmy, że pierwsza implementacja weszła w życie 29.12.2011 r.) brakuje spektakularnych przykładów wykorzystywania informacji sektora publicznego, ponieważ wykonanie dotychczasowych przepisów

re-use uzależnione było od potwierdzenia (najczęściej w formie prawomocnego wyroku sądowego), że wnioskowane dane są w istocie dostępne na podstawie ogólnej (u.d.i.p.) bądź szczególnej regulacji dostępowej. Ten „sądowy” warunek będący efektem wykładni systemowej okazuje się już nieaktualny w świetle najnowszej definicji ponownego wykorzystywania. Nie trzeba aż tak skomplikowanych analiz, aby wykazać, że przed sądami administracyjnymi próżno szukać sporów o właściwy format danych, opłaty za przygotowanie do udostępnienia bądź zakres tajemnic ustawowo chronionych ze szczególnym uwzględnieniem paradygmatu danych osobowych lub własności intelektualnej. Zamiast tego przedsiębiorcy bądź organizacje społeczne toczą z organami publicznymi i spółkami Skarbu Państwa spory o pryncypia, tzn. czy ustawa w ogóle znajduje zastosowanie (np. do spółek Skarbu Państwa) i czy wnioskowane informacje (np. cyfrowe dane rozkładowe dotyczące transportu kolejowego, dalekie od zagadnień sensytywnych politycznie) są informacjami publicznymi tudzież informacjami sektora publicznego. Przeciętne rozstrzygnięcie relatywnie nieskomplikowanych zagadnień prawnych trwa przeciętnie trzy lata, co skutecznie paraliżuje jakiegokolwiek model biznesowy uzależniony od danych publicznych. Nie przynosi jednak efektu w postaci udostępnienia danych do ponownego wykorzystywania. Rozliczalność za nieudostępnienie informacji publicznej jest iluzoryczna, zaś w obszarze ponownego wykorzystywania w praktyce nie istnieje. W efekcie powracamy do konstatacji, że wszelkie prawa podmiotowe są warte dokładnie tyle, ile system, który je chroni, zaś sądo-administracyjna ochrona prawa dostępu do informacji sektora publicznego celem ponownego wykorzystywania jest długotrwała i ma ograniczony potencjał w zakresie sporów o faktyczne cechy wnioskowanych danych (interoperacyjność, prawidłowość działania API, niespekutowanie normatywnie określonych formatów danych, itp.).

Bibliografia

- Bernaczyk M., *Dostęp do list poparcia kandydatów do Krajowej Rady Sądownictwa jako przykład neutralizacji aksjologicznej Konstytucji RP*, Acta Universitatis Wratislaviensis No. 3978, „Przegląd Prawa i Administracji” 2020, t. 120/1.
- Bernaczyk M., *The constitutional right to information in Poland: theory and practice*, “International Comparative Jurisprudence” 2019, Vol. 5, No. 1, s. 37-39.
- Janssen K., *The Availability of Spatial and Environmental Data in The European Union. At the Crossroads between Public and Economic Interests*, Bedfordshire 2010.
- Janssen K., *The influence of the PSI directive on open government data: an overview of recent developments*, “Government Information Quarterly” 2011, Vol. 28, No. 4., s. 446-456.
- Sobczak J., komentarz do art. 11 Karty Praw Podstawowych Unii Europejskiej, [w:] A. Wróbel (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, Warszawa 2020, teza nr 3.

Cyfrowy dostęp do informacji i danych o funkcjonowaniu państwa a prawo do informacji jako prawo człowieka

Digital access to information and data on the functioning of the state and the right to information as a human right

Streszczenie: Prawo do informacji oraz samo pojęcie informacji stanowią współcześnie przedmiot zainteresowania wielu dyscyplin naukowych zajmujących się prawami człowieka, prawem konstytucyjnym, prawem administracyjnym, ale także (w kontekście rozwoju społeczeństwa informacyjnego) technologią informacyjną. W niniejszym artykule, poddając krytycznej analizie dotychczasową literaturę z tego zakresu, zamierzam postawić tezę o istotnym wpływie form i trybów cyfrowego dostępu do informacji na funkcjonowanie państwa w zakresie realizacji prawa do informacji jako prawa człowieka, a także dokonać ogólnej analizy przepisów regulujących tę kwestię.

Słowa kluczowe: dostęp do informacji, otwarte dane, administracja cyfrowa, informacja cyfrowa, prawo do informacji, polskie ustawodawstwo

Abstract: The right to information and the concept of information itself are nowadays the subject of interest of many scientific disciplines dealing with human rights, constitutional law, administrative law, but also (in the context of the development of information society) information technology. In this article, subjecting to a critical analysis of the existing literature in this area, I intend to put forward a thesis on the significant influence of the forms and modes of digital access to information on the functioning of the state on the realisation of the right to information as a human right, and to make a general analysis of the provisions regulating this issue.

Keywords: access to information, open data, digital government, digital information, right to information, polish legislation

Wprowadzenie

Wpływ uregulowanych w randze ustawy przepisów określających zasady dostępu do informacji publicznych na realizację prawa do informacji (chronionego w Konstytucji RP) jest oczywisty. To, co jednak winno przykuć uwagę badaczy tematu, to kwestia zupełnie innego rodzaju sposobów posługiwania się informacją przez człowieka w XXI w., w porównaniu do czasów powstawania środków masowego komunikowania się czy też sprzed powstania sieci Internet. Zjawiska związane z tzw. społeczeństwem informacyjnym mają znaczący wpływ na to, jak człowiek funkcjonuje w relacji jednostka-państwo oraz w samym społeczeństwie. System prawny zaś reaktywnie powinien odpowiadać na zmieniającą się rzeczywistość, i można powiedzieć, że odpowiada, ale czy właściwie?

1. „Informacja” a „dane”

Dokonując analizy prawa do informacji, należy na wstępie uściślić przedmiot tego prawa, a tym samym zdefiniować pojęcie informacji. Chociaż język prawny posługuje się terminem informacji, to w żaden sposób go nie definiuje. W polskim porządku prawnym można znaleźć jednak legalne definicje węższego zakresu pojęcia informacji jak informacja jawna czy informacja publiczna. Brak legalnej definicji informacji z pewnością wynika z jej bardzo ogólnego charakteru. Jak przyznaje Jacek Jadacki, „są takie nazwy, o których nie można powiedzieć ani że są nazwami konkretnymi, ani że są nazwami abstrakcyjnymi. Są to mianowicie nazwy, które mają mieszane denotacje, a więc takie, do których należą zarówno konkrety, jak i abstrakty. Do nazw tego rodzaju należą np. nazwy negatywne oraz nazwa najogólniejsza («przedmiot»)”¹. Wydaje się, że do takich nazw zaliczyć można pojęcie informacji. Jej

¹ J.J. Jadacki, *Spór o granice języka*, Warszawa 2002, s. 92.

szeroki zakres użycia w językach specjalistycznych takich nauk, jak fizyka, informatyka, ekonomia, politologia czy naukach o komunikacji, a jednocześnie powszechność używania w języku potocznym uwidacznia niezwykle wieloznaczny i metaforyczny charakter.

W obecnych czasach, gdy nastąpiła znacząca technicyzacja w podejściu do rozumienia informacji (w języku potocznym), gdy informacje są generowane i przetwarzane automatycznie przez maszynę, a ich odbiorcą jest kolejna maszyna, a nie człowiek, wydaje się, że takie definicje mogą okazać się niewystarczające, zwłaszcza w aspektach prawnych. Nie ma także żadnego rozsądnego powodu, żeby relatywizować ogólne pojęcie informacji do obszaru komunikacji językowej². W literaturze podkreśla się, że „dla definiowania terminu informacji większe znaczenie ma zatem ustalenie, czy dany komunikat może/musi być wykorzystany przez człowieka, niż ustalenie sposobu przenoszenia informacji, jej formy, a nawet treści”³. Definicje techniczne obejmują także przekazy informacji, które mogą przyczyniać się do poszerzenia wiedzy czy poznania rzeczywistości. Można odwołać się w tym miejscu do *Encyklopedii PWN*: „informacja [łac.], inform. obiekt abstrakcyjny, który może być w postaci zakodowanej zapisywany (na nośnikach informacji), przesyłany, przetwarzany za pomocą programów komputerowych i używany do sterowania urządzeniami”. Józef Mikułowski-Pomorski podkreśla, iż „w cybernetyce informacją są wszelkie dane zewnętrzne, które mogą być wytwarzane wewnątrz samego systemu, jak np. dane w maszynach cyfrowych i sygnały transmitowane w sieciach”⁴. Jak widać, w definicjach cybernetycznych czy ogólnie definicjach związanych z naukami technicznymi pojawia się także pojęcie danych, które ostatnimi czasy także

² M.J. Schroeder, *Spór o pojęcie informacji*, „Studia Metodologiczne” 2015, nr 34, s. 25.

³ J. Taczkowska-Olszewska, *Dostęp do informacji publicznej w polskim systemie prawnym*, Warszawa 2014, s. 3.

⁴ J. Mikułowski-Pomorski, *Informacja i komunikacja*, Wrocław 1989, s. 45, cyt. za: J. Janowski, *Technologia informacyjna dla prawników i administratywistów*, Warszawa 2013, s. 79.

znalazło miejsce w języku prawnym (np. dane osobowe czy dane publiczne). Należy w tym miejscu ująć pojęcie informacji w szerszy kontekst systemów informacyjnych i podjąć próbę zdefiniowania również pojęcia danych i relacji tych pojęć. Posłużę się tzw. infologiczną teorią Langefora (1973), która wyraźnie rozróżnia informację od danych i uwzględnia wymagania użytkowników informacji. Zdaniem Börjega Langefora informacja może jedynie powstać jako koncept umysłu człowieka w wyniku procesu interpretacji danych, zaś „informacja to proces interpretacji danych w oparciu o nie. Langefors jednocześnie podkreślał jej subiektywność, „tzn. fakt, że z określonych danych, różni ludzie mogą wyciągać różne informacje”⁵. Badacze Thomas H. Davenport i Lawrence Prusak z kolei zauważają, że „dane to zbiór dyskretnych, obiektywnych faktów na temat zdarzeń”. Ich zdaniem dane same w sobie nie niosą żadnego znaczenia, dopiero w procesie interpretacji, przetworzenia mogą przyjąć formę informacji. Dokonuje się to poprzez „kontekstualizację, kategoryzację, kalkulację, korekcję i kondensację”⁶. Można skonstatować, że dane to zbiór symboli, użytych do reprezentowania czegoś. Informacja zaś to zinterpretowane dane. Te same dane mogą więc być interpretowane w różny sposób przez różnych ludzi w zależności od posiadanej wiedzy *a priori*.

Podsumowując za Mariuszem Grabowskim i Agnieszką Zajac: „Dane reprezentują fakty. W systemach zarządzania wspomaganych komputerowo dane są kodowane za pomocą odpowiednich symboli. Mogą być rejestrowane, przetwarzane i przesyłane. Dane są przesyłane do świadomości odbiorcy w postaci komunikatu, zatem każdy komunikat zawiera dane”. Autorzy przyznają, że choć dane same w sobie nie mają znaczenia ani celu, to uporządkowanie i struktura symboli mogą naprowadzać na

⁵ M. Grabowski, A. Zajac, *Dane, informacja, wiedza – próba definicji*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie” 2009, nr 798, s. 6.

⁶ T.H. Davenport, L. Prusak, *Working Knowledge: How Organizations Manage What They Know*, Boston, MA 1998, s. 2-6.

ich ściśle określoną interpretację, zaś informacja nadaje im znaczenie poprzez interpretację. Innymi słowy informacja to dane znajdujące się w komunikacie, zinterpretowane przez odbiorcę, jednocześnie mają one dla interpretatora jakieś znaczenie i wnoszą do jego świadomości pewną nowość. Aby dane mogły przeistoczyć się w informację, niezbędna jest interpretacja odbiorcy. Z kolei informacja zależy od umiejętności interpretacyjnych odbiorcy, czyli ma wymiar subiektywny.

Relacje pojęć danych i informacji można znaleźć w tzw. piramidzie Data-Information-Knowledge-Wisdom (DIKW), schemacie zaproponowanym przez wybitnego amerykańskiego specjalistę z dziedziny badań operacyjnych i systemowych Russella L. Ackoffa, który wyróżnił pięć poziomów poznania: dane – informacja – wiedza – zrozumienie – mądrość. Według Ackoffa dane są produktem obserwacji, nie mając przy tym żadnej wartości, dopóki nie zostaną przetworzone w użyteczną formę informacji. Wiedza to następna warstwa, precyzująca informacje, umożliwiając sterowanie systemem⁷. Chociaż sam diagram i jego rozumienie były odbierane w znacząco różny sposób, to hierarchia ta unaczynia zależności pomiędzy pojęciami danych i informacji⁸. Takie rozumienie danych można odnaleźć w pierwszym Programie Otwierania Danych Publicznych, przyjętym uchwałą Rady Ministrów z dnia 20 września 2016 r.: „dane publiczne – liczby i pojedyncze wydarzenia lub obiekty, na możliwie najniższym poziomie agregacji, które nie zostały poddane przez administrację publiczną przetworzeniu do postaci raportów, wykresów, itp. oraz nie został im nadany odpowiedni kontekst lub interpretacja”. Dane są w tym przypadku określone jako produkt niepoddany interpretacji i nieprzetworzony, odnoszący się do liczb, pojedynczych wydarzeń lub obiektów.

⁷ J.H. Bernstein, *The Data-Information-Knowledge-Wisdom Hierarchy and its Antithesis*, „CUNY Academic Works” 2009.

⁸ M. Brzeziński, J.W. Hołubiec, D. Wagner, *Hierarchiczna struktura poznania: piramida wiedzy*, „Studia i Materiały Polskiego Stowarzyszenia Zarządzania Wiedzą” 2009, nr 19.

Odróżnianie informacji od danych ma istotne znaczenie przy dalszych analizach sposobów i form dostępu do informacji i danych wytwarzanych przez instytucje publiczne. W takim ujęciu tekst prawny będzie informacją publiczną, zaś zawarty w nim ciąg znaków⁹ będzie danymi publicznymi. Zatem wraz z udostępnieniem aktu prawnego jako informacji publicznej udostępniane są jednocześnie dane, które zawiera. Niestety w wielu opracowaniach i publikacjach można napotkać na błędne definicje danych jako np. zapisanych komputerowo informacji czy jako synonimów terminu informacja. Takie błędne założenia prowadzą zazwyczaj do niemających sensu dywagacji oraz błędnych wniosków co do zakresu przedmiotowego udostępniania informacji publicznej.

2. Prawo człowieka do informacji

Francuski prawnik Karel Vasak, przedstawiając koncepcję trzech generacji praw człowieka¹⁰, zaakcentował ich wymiar temporalny. Wydaje się, że prawo do informacji należy zakwalifikować do pierwszej generacji praw człowieka, które jednakowoż jest często także niezbędnym elementem do realizacji innych podstawowych praw człowieka¹¹. Temporalność wyeksponowaną przez Vasaka należy jednak rozumieć w jej całej rozciągłości. W przypadku prawa do informacji jego funkcja była postrzegana na różne sposoby w miarę upływu czasu, zwłaszcza w odniesieniu do informacji o funkcjonowaniu państwa. Prawo dostępu do informacji o funkcjonowaniu państwa w ogóle w kategoriach praw człowieka zaczęło być brane pod uwagę dopiero ostatnimi czasy. Nie ma

⁹ Ciąg znaków w informatyce związany jest z tekstowym typem danych (ang. *string*), który służy do ich przechowywania, nazywany jest także „łańcuchem znaków”.

¹⁰ K. Vasak, *A 30-year struggle; the sustained efforts to give force of law to the Universal Declaration of Human Rights*, „The UNESCO Courier” 1977, Vol. 30, No. 11, <https://unesdoc.unesco.org/ark:/48223/pf0000048063> [dostęp: 11.05.2022].

¹¹ M. McDonagh, *The Right to Information in International Human Rights Law*, „Human Rights Law Review” 2013, Vol. 13, No 1, s. 25-55.

obecnie w doktrynie zgody co do źródła prawa do informacji publicznej. Zdaniem wielu prawników regulacje międzynarodowe wspominają o swobodzie otrzymywania i rozpowszechniania informacji, związanej z wolnością wypowiedzi, a nie o prawie dostępu do informacji publicznej. Takie deklaracje zawarte zostały w Powszechnej Deklaracji Praw Człowieka ONZ z 10 grudnia 1948 r. (PDPCz)¹², Konwencji o ochronie praw człowieka i podstawowych wolności z 4 listopada 1950 r. (EKPCz)¹³, Międzynarodowym Pakcie Praw Obywatelskich i Politycznych z 16 grudnia 1966 r. (MPPOiP)¹⁴. Dlatego na gruncie ochrony praw człowieka obecnie doszukuje się źródeł prawa do informacji publicznej w regulacjach gwarantujących wolność wypowiedzi, w przypadku EKPCz jest to art. 10:

„1. Każdy ma prawo do wolności wyrażania opinii. Prawo to obejmuje wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe. Niniejszy przepis nie wyklucza prawa Państw do poddania procedurze zezwoleń przedsięwzięciom radiowych, telewizyjnych lub kinematograficznych.

2. Korzystanie z tych wolności pociągających za sobą obowiązki i odpowiedzialność może podlegać takim wymogom formalnym, warunkom, ograniczeniom i sankcjom, jakie są przewidziane przez ustawę i niezbędne w społeczeństwie demokratycznym w interesie bezpieczeństwa państwowego, integralności terytorialnej lub bezpieczeństwa publicznego ze względu na konieczność zapobieżenia zakłóceniu porządku lub przestępstwu, z uwagi na ochronę zdrowia i moralności, ochronę dobrego imienia i praw innych osób oraz ze względu na zapobieżenie

¹² A. Przyborowska-Klimczak, *Prawo międzynarodowe publiczne. Wybór dokumentów*, wyd. 7, Lublin 2005, s. 166-171.

¹³ 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.

¹⁴ Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r.

ujawnieniu informacji poufnych lub na zagwarantowanie powagi i bezstronności władzy sądowej”.

Jak już wspomniano, nie zawsze tak było. Początkowa linia orzecznicza Europejskiego Trybunału Praw Człowieka w Strasburgu uznawała, iż wolność wypowiedzi wynikająca z art. 10 EKPCz nie przyznaje jednostce prawa dostępu do dokumentów publicznych, nie nakłada także na państwo obowiązku udostępniania informacji publicznych (patrz sprawa *Guerra i inni przeciwko Włochom*¹⁵ oraz *Leander przeciwko Szwecji*¹⁶). Dopiero w roku 2009 w sprawie *TASZ przeciwko Węgrom* Trybunał wywiódł prawo do informacji publicznej bezpośrednio z art. 10 EKPCz¹⁷ (należy dodać, że podwaliny z pewnością położyła tutaj sprawa *Sdružení Jihočeské Matky przeciwko Republice Czeskiej* z 2006 r.). Węgierskie Zrzeszenie Praw Obywatelskich (Társaság a Szabadságjogokért) zawnioskowało do Sądu Konstytucyjnego o udostępnienie skargi konstytucyjnej, którą złożył członek parlamentu wraz z innymi osobami fizycznymi. W skardze kwestionowano przepisy nowelizacji Kodeksu karnego związane z wykroczeniami w sprawach dotyczących narkotyków. Sąd Konstytucyjny odmówił udostępnienia skargi, twierdząc, że jej akta nie mogą być udostępnione osobom trzecim bez wcześniejszej zgody autora. Sąd Okręgowy w Budapeszcie odrzucił pozew wnioskodawcy. Podniesiono m.in., że treść żądanej przez TASZ skargi nie może być uważana za „informację”, tak więc nie może ona zostać udostępniona w trybie regulacji opartych na prawie dostępu do informacji publicznej. Sąd Apelacyjny podtrzymał w mocy wyrok Sądu Okręgowego. TASZ złożyło skargę do

¹⁵ *Guerra and others v. Italy*, [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-58135%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-58135%22]}) [dostęp: 11.05.2022].

¹⁶ *Leander v. Sweden*, [https://hudoc.echr.coe.int/eng#{%22itemid%22:\[%22001-57519%22\]}](https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-57519%22]}) [dostęp: 17.08.2019].

¹⁷ *Társaság a Szabadságjogokért v. Hungary*, [https://hudoc.echr.coe.int/eng#{%22fulltext%22:\[%22\(%22hungary%22\)%22\],%22kdate%22:\[%222009-03-01T00:00:00.0Z%22,%222009-04-30T00:00:00.0Z%22\],%22itemid%22:\[%22001-92171%22\]}](https://hudoc.echr.coe.int/eng#{%22fulltext%22:[%22(%22hungary%22)%22],%22kdate%22:[%222009-03-01T00:00:00.0Z%22,%222009-04-30T00:00:00.0Z%22],%22itemid%22:[%22001-92171%22]}) [dostęp: 11.05.2022].

ETPCz. W wyroku Trybunał przypomniał na początku, że dotychczas „artykuł 10 nie przyznaje osobom fizycznym prawa dostępu do rejestru zawierającego informacje na temat jego pozycji personalnej, oraz nie nakłada obowiązku na rząd, aby udzielił takich informacji tymże osobom”, jednocześnie uznał, że „prawo do wolności uzyskiwania informacji zabrania rządowi ograniczania komukolwiek otrzymywania informacji, której inni życzą sobie lub chcą mu udzielić”, ostatecznie postanowił, że „miało miejsce pogwałcenie Artykułu 10 Konwencji Europejskiej”. ETPCz finalnie potwierdził konieczność szerokiej interpretacji art. 10 EKPCz, zwracając uwagę, że wolność wyrażania opinii i otrzymywania oraz przekazywania informacji nie może być w pełni realizowana bez faktycznego prawa dostępu do informacji publicznej. Stanowisko ETPCz świadczy o tym, że nie poprzestano na literalnym brzmieniu art. 10 ust. 1 EKPCz, a sytuacja prawna nie została uwzględniona w aspekcie do „wolności od”¹⁸.

W literaturze zauważa się właśnie fakt, że prawo do informacji nie tylko wynika z wolności wypowiedzi, ale że jest także bezpośrednio z nim powiązane, bowiem swoboda wypowiedzi nie może zaistnieć bez uprzedniego pozyskania informacji. Wartościami, które są chronione na podstawie norm dających obywatelom gwarancje dostępu do informacji, są w szczególności jawność, przejrzystość, „prawowitość demokratycznego systemu prawnego”¹⁹.

Na kanwie tzw. instrumentalnego uzasadnienia prawa do informacji podkreśla się, że we współczesnych dokumentach prawo dostępu do informacji zyskuje już rangę prawa samoistnego, które może być realizowane

¹⁸ S. Osowski, B. Wilk, *Od wolności otrzymywania i przekazywania informacji do prawa do informacji (publicznej). Ewolucja orzecznictwa Europejskiego Trybunału Praw Człowieka w zakresie art. 10 Konwencji o ochronie praw człowieka i podstawowych wolności*, „Przegląd Prawa Konstytucyjnego” 2017, nr 2 (36), s. 149.

¹⁹ Projekt Rezolucji Parlamentu Europejskiego z 20.11.2008 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji [wdrożenie rozporządzenia (WE) Nr 1049/2001] przygotowany przez Komisję Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych, 2007/2154 (INI), www.europarl.europa.eu [dostęp: 11.05.2022].

ściśle w powiązaniu z prawem do swobody wypowiedzi. Prawo do informacji staje się jednocześnie egzekwowalne i przybiera postać roszczenia adresowanego do władz publicznych²⁰.

Prawo do informacji publicznej jest prawem powszechnym i przysługującym każdej jednostce niezależnie od tego, czy jest obywatelem danego państwa. Niewątpliwie jest prawem politycznym oraz proceduralnym i pozytywnym, ponieważ rodzi po stronie państwa obowiązek stworzenia mechanizmu jego realizacji i pozwala jednostce żądać tejże realizacji. Dostęp do informacji publicznej jako zasadniczy element funkcjonowania demokratycznego państwa prawa i określający jawność władzy publicznej jako naczelnej zasady wpływającej na właściwe relacje jednostka–państwo ma jednak swoją dłuższą historię, pomimo że dopiero niedawno prawo do informacji publicznej zostało uznane za prawo człowieka. Już w 1766 r. szwedzka ustawa zasadnicza jako pierwsza na świecie gwarantowała prawo publicznego dostępu do dokumentów państwowych²¹.

Prawo do informacji w szerszym ujęciu w polskim porządku prawnym jest chronione w Konstytucji RP i umieszczone zostało w art. 54 wśród wolności i praw osobistych, zaś w art. 61 wśród praw i wolności politycznych. W przeciwieństwie do wolności informacji z art. 54, który ma charakter prawa negatywnego, prawo do informacji publicznej z art. 61, w którym ustrojodawca przyznaje jednostce prawo podmiotowe do określonych informacji, nakłada na władze publiczne pozytywne obowiązki w zakresie gromadzenia i udostępniania informacji:

„1. Obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Prawo to obejmuje również uzyskiwanie informacji o działalności organów samorządu gospodarczego i zawodowego, a także innych osób oraz

²⁰ J. Taczowska-Olszewska, *Dostęp...*, s. 37.

²¹ J.H. Amberg, *Znaczenie zasady jawności dla demokracji*, „Krytyka Prawa” 2018, nr 1, s. 7-19.

jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa.

2. Prawo do uzyskiwania informacji obejmuje dostęp do dokumentów oraz wstęp na posiedzenia kolegiałnych organów władzy publicznej pochodzących z powszechnych wyborów, z możliwością rejestracji dźwięku lub obrazu”.

Dzięki artykułowi 61 prawo do informacji stało się prawem konstytucyjnym i stanowi jedno z podstawowych praw, które ograniczone może być tylko ściśle określonymi wyjątkami:

„3. Ograniczenie prawa, o którym mowa w ust. 1 i 2, może nastąpić wyłącznie ze względu na określone w ustawach ochronę wolności i praw innych osób i podmiotów gospodarczych oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa”.

Konstytucja RP daje główne gwarancje ochrony prawa do informacji w postaci art. 45 (prawo do sądu), art. 80 (prawo wystąpienia z wnioskiem o pomoc w ochronie prawa do informacji do Rzecznika Praw Obywatelskich) oraz art. 79 (możliwość skorzystania z instytucji skargi konstytucyjnej). Należy także pamiętać o możliwości złożenia skargi do Europejskiego Trybunału Praw Człowieka (art. 35 EKPCz) w aspekcie art. 10 EKPCz, przy czym subsydiarny charakter skargi nakłada obowiązek wyczerpania krajowych środków odwoławczych.

3. Społeczeństwo informacyjne

Jako pierwszy terminu „społeczeństwo informacyjne” użył Tadao Umesao (1963 r.) w pracy dotyczącej ewolucyjnej teorii społeczeństwa opartej na „przemysłach informacyjnych”. Termin spopularyzował następnie Kenichi Koyama w pracy *Introduction to Information Theory*. Czym charakteryzuje się społeczeństwo informacyjne? Powszechnie

uznaje się, że jest to społeczeństwo, którego osią napędową jest informacja. Oznacza to, że człowiek:

- wytwarza informację,
- przechowuje informację,
- przekazuje informację,
- pobiera informację,
- wykorzystuje informację²².

Spśród wielu definicji społeczeństwa informacyjnego przywołam tę sformułowaną przez wybitnego polskiego badacza komunikowania masowego Tomasza Gobana-Klasa: „Społeczeństwo informacyjne to społeczeństwo, które nie tylko posiada rozwinięte środki przetwarzania informacji i komunikowania, lecz przetwarzanie informacji jest podstawą tworzenia dochodu narodowego i dostarcza źródła utrzymania większości społeczeństwa”. Na potrzeby niniejszej pracy pominę jednak dogłębną analizę pojęcia społeczeństwa informacyjnego i skutków, jakie ze sobą niesie w odniesieniu do rzeczywistości prawnej oraz społecznej²³. Skupię się natomiast na trzech kluczowych elementach pojęcia społeczeństwa informacyjnego, które okażą się fundamentem w dalszej analizie udostępniania informacji o funkcjonowaniu państwa:

1. Informacja jest towarem, traktowanym jako szczególne dobro niematerialne, równoważne lub cenniejsze od dóbr materialnych.
2. „Symultaniczność przestrzenna obiegu informacji” i jej szybkość obiegu (zanik związku pomiędzy odległością a czasem)²⁴.

²² J. Mączyński, *Globalne społeczeństwo informacyjne – wybrane kwestie adaptacyjne*, [w:] L.W. Zacher (red.), *Rewolucja informacyjna i społeczeństwo. Niektóre trendy, zjawiska i kontrowersje*, Warszawa 1997, s. 18.

²³ T. Goban-Klas, P. Sienkiewicz, *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków 1999, s. 175.

²⁴ J.B. Thompson, *Media i nowoczesność. Społeczna teoria mediów*, przeł. I. Mielnik, Wrocław 2001, s. 29.

3. Przetwarzanie danych i informacji za człowieka przejmują maszyna cyfrowa²⁵.

W dobie społeczeństwa informacyjnego informacja stała się towarem o niezwykle istotnej roli. Największe obecnie przedsiębiorstwa technologiczne swoje główne przychody opierają na monetyzacji danych i informacji, dlatego gromadzenie i przetwarzanie danych i informacji stanowi trzon ich funkcjonowania²⁶. Trudno sobie także wyobrazić działalność jakiegokolwiek ministerstwa państwa, urzędu centralnego czy dziedziny życia bez dostępu do informacji. Aby podejmować decyzje, państwo musi analizować olbrzymie liczby danych i informacji (pomińmy zagadnienie, czy tak się dzieje rzeczywiście). Gromadzenie i przetwarzanie danych jest także niezbędne w relacji jednostka–państwo, np. w korzystaniu z tzw. e-usług publicznych i rozwoju szeroko pojętej e-administracji²⁷.

Zwiększająca się stale szybkość sygnałów i przesyłu informacji wpływa na każdą gałąź życia, ponieważ dane i informacje stanowią obecnie budulec funkcjonowania społeczeństwa. Problemem nie jest już niedosyt informacji, ale jej nadmiar, gdyż dociera ona do nas bez ograniczeń czasu i przestrzeni²⁸. Niewątpliwie prymarne znaczenie ma tutaj rozwój sieci Internet. Wpłynął on nie tylko na zwiększenie szybkości przepływu informacji, ale także na sposoby komunikacji w społeczeństwie²⁹. Internet jednocześnie przewartościował sposoby uczestnictwa w życiu społecznym i publicznym, dając swobodny dostęp do tworzenia sieci relacji społecznych i wymiany informacji. Według Manuela Castellsa, autora

²⁵ M. Campbell-Kelly i in., *Computer: A History of the Information Machine*, Boulder, CO 2013.

²⁶ D. Ciuriak, *The Economics of Data: Implications for the Data-Driven Economy*, Centre for International Governance Innovation, 2018, <https://www.cigionline.org/articles/economics-data-implications-data-driven-economy> [dostęp: 11.05.2022].

²⁷ B. Kasprzyk, *Aspekty funkcjonowania e-administracji dla jakości życia obywateli*, „Nierówności Społeczne a Wzrost Gospodarczy” 2011, nr 23, s. 343-353.

²⁸ P. Tańkowski, *Szybkość informacji*, „Folia Bibliologica” 2009, t. LI, s. 26.

²⁹ M. Graham, W.H. Dutton, *Society and the Internet: How Networks of Information and Communication Are Changing Our Lives*, Oxford 2014, s. 212-227.

pojęcia „społeczeństwo sieciowe”, globalizacja to przede wszystkim swobodny przepływ informacji³⁰. Warto w tym miejscu dodać, że według danych z Głównego Urzędu Statystycznego w 2018 r. w Polsce dostęp do Internetu posiadało 84,2% gospodarstw domowych, zaś w latach, gdy w Polsce zaczęto promulgować akty prawne, prawie 60% obywateli centralnej części kraju nie potrafiło czytać.

Percepcję informacji zmieniły powstanie i rozwój cyfrowych maszyn przetwarzających dane. Pierwsze mechaniczne maszyny liczące powstawały już wiele wieków przed rewolucją przemysłową (mechanizm z Andikityry datowany na lata 150–100 p.n.e.), jednak to powstanie komputera w XX w. spowodowało, że zdołano przekształcić informację w sygnał cyfrowy. Rozwój komputerów sprawił, że człowiek coraz więcej czynności związanych z odbiorem i przetwarzaniem informacji scedował na maszynę. Rozwój maszyn przetwarzających dane i zwiększanie się ich wolumenu przynosi człowiekowi całkowicie nowe możliwości analizy rzeczywistości i jej predykcji. Przykładem jest materiał dziennikarski BuzzFeed News na temat wykorzystywania samolotów szpiegowskich przez władze USA. Dziennikarze wykorzystali dane z 20 tys. lotów dostępnych w serwisie <https://www.flightradar24.com>, następnie stworzyli algorytm, który celnie rozpoznał samoloty szpiegowskie na podstawie podanych wzorców (program wykorzystał tzw. uczenie maszynowe). W ten sposób dziennikarze zidentyfikowali kilkadziesiąt lotów FBI i DHS (Department of Homeland Security). Dane samolotów rządowych służące do wzorców dla algorytmu uzyskano z publicznych baz danych, następnie połączono je z danymi z Flightradar24³¹.

Dalszy rozwój maszynowego uczenia i sztucznej inteligencji spowodował z kolei powstanie zewnętrznych agentów, które analizują informacje za człowieka. Zakłada się, że w przyszłości za człowieka będą

³⁰ M. Castells, *The Rise of the Network Society*, Hoboken, NJ 2011, s. 409-410.

³¹ Dane za stroną internetową: <https://www.buzzfeednews.com/article/peteraldhous/hidden-spy-planes#.atv66XJRgb> [dostęp: 11.05.2022].

podejmować także decyzje (składać oświadczenie woli?)³². W 2016 r. kancelaria prawnicza Baker & Hostetler wykorzystała w swej pracy system sztucznej inteligencji „Ross” jako „adwokata”. Przy zastosowaniu superkomputera Watson firmy IBM system, analizując teksty prawne oraz informacje wejściowe, dokonywał interpretacji prawnych dla działu zajmującego się postępowaniami upadłościowymi³³. Aby jednak systemy przetwarzania informacji, którym człowiek deleguje coraz więcej zadań, funkcjonowały prawidłowo, dane wejściowe powinny być przygotowane w odpowiednich formatach – formatach do odczytu maszynowego (*machine-readable data*)³⁴.

Ostatnimi czasy podkreśla się także olbrzymią liczbę danych generowanych przez człowieka. W projekcie dokumentu przygotowywanego przez Komisję Europejską „A European Strategy for Data”³⁵ podkreśla się, że produkowany zakres i wielkość danych przez człowieka rośnie w niesamowicie szybkim tempie. W 2018 r. człowiek wygenerował 33 zettabajtów (bilion gigabajtów) danych, a prognozuje się, że w 2025 r. będzie to już 175 zettabajtów. Można zauważyć, że rozmiary zbiorów danych i informacji, w tym informacji dotyczących prawa, kompleksowo mogą być analizowane już tylko przy użyciu wydajnych komputerów. Ogromna liczba danych i ich cyfryzacja, czyli zamiana sygnału analogowego na cyfrowy, obejmuje swym zasięgiem obecnie każdą dziedzinę życia³⁶.

Wszystkie te zjawiska zachodzą niezwykle szybko. System prawa musi reaktywnie odpowiadać na zmieniającą się rzeczywistość, i tak też często się dzieje. Przykładem w polskim porządku prawnym odpowiedzi

³² P. Stylec-Szromek, *Sztuczna inteligencja – prawo, odpowiedzialność, etyka*, „Zeszyty Naukowe Politechniki Śląskiej” 2018, z. 123, s. 9.

³³ G. Wierczyński, W.R. Wiewiórkowski, *Informatyka prawnicza*, Warszawa 2016, s. 89.

³⁴ M.E. Williams, *The impact of machine-readable data bases on library and information services*, Information Processing & Management” 1 January 1977, Vol. 13, No 2, s. 95-107.

³⁵ <https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy> [dostęp: 11.05.2022].

³⁶ J. Opila, T. Pełech-Pilichowski, *Problems with the Storing and Presentation of Information*, [w:] W. Cyrul (Ed.), *Information Technology and Law*, Kraków 2014, s. 29.

na zjawiska związane ze społeczeństwem informacyjnym jest ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne czy ustawa z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych, która publikowanie aktów prawnych dopuszcza już tylko w formie elektronicznej za pomocą sieci Internet.

4. Pojęcie informacji publicznej i tryby jej udostępniania w polskim porządku prawnym

Zakres pojęciowy informacji publicznej w polskim prawie został określony w ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198 z późn. zm.). Zgodnie z art. 1 ustawy informacją publiczną jest każda informacja o sprawach publicznych. Precyzując, czym jest desygnat informacji o sprawach publicznych, w wykładni należy się kierować art. 61 Konstytucji RP. W orzecznictwie za informację publiczną uważa się każdą informację wytworzoną przez organy władzy publicznej oraz inne podmioty, które realizują zadania publiczne. Istotny zakres pojęcia informacji publicznej został określony przez WSA w Warszawie w wyroku z dnia 16 listopada 2007 r., II SAB/Wa 68/07: „informacją publiczną będzie każda wiadomość wytworzona lub odnoszona do władz publicznych, a także wytworzona lub odnoszona do innych podmiotów wykonujących funkcje publiczne w zakresie wykonywania przez nie zadań władzy publicznej i gospodarowania mieniem komunalnym lub mieniem Skarbu Państwa”. Charakter informacji publicznej zatem ma nie tylko informacja wytworzona przez ww. podmioty, ale także ta, która się do nich odnosi³⁷. Dotychczas koncentrowałem się na pojęciu informacji publicznej, polski legislator powołał jednak do życia kolejny termin, który w pewien

³⁷ Wyrok WSA w Warszawie z dnia 23 stycznia 2013 r., II SAB/Wa 351/12; wyrok NSA z dnia 7 grudnia 2010 r., I OSK 1774/10; wyrok NSA z dnia 30 października 2002 r., II SA 2037/02; wyrok NSA z dnia 30 października 2002 r., II SAB 181/02.

sposób jest skorelowany z polem semantycznym pojęcia informacji publicznej. Pojęcie informacji sektora publicznego zawarte jest w ustawie z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (dalej: u.o.d.i.s.p.), którą rozumiemy jako „każdą treść lub jej część, niezależnie od sposobu utrwalenia, w szczególności w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej, będącą w posiadaniu podmiotu zobowiązanego”.

Źródłem normatywnym u.o.d.i.s.p. jest dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego, Dz. Urz. L 345/90 z 31.12.2003 r.³⁸ Samo rozróżnienie informacji sektora publicznego (dalej ISP) od informacji publicznej i sposobu dostępu do informacji a ponownego jej wykorzystywania nastrocza wiele problemów. Według Michała Bernaczyka w trakcie implementacji dyrektywy (jeszcze we wcześniejszej ustawie z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego) potraktowano jej cel nie tyle jako „wartość dodaną” do istniejącego krajowego systemu dostępu do informacji, ile jako cel zupełnie odrębny, co ma wynikać z rzekomo odmiennego przeznaczenia informacji³⁹. Autor przyznaje także, że teoretycznie rzecz ujmując, państwo co do zasady nie może odmówić wykorzystywania informacji publicznej, zaś poprzez przepisy u.o.d.i.s.p. może mnożyć bariery proceduralne⁴⁰. Można stwierdzić, że różnica w obrębie tych dwóch pojęć będzie się sprowadzać do postaci informacji/danych, czyli w jakim formacie występują. Zdaniem Bernaczyka państwo, owszem, może wyznaczać granice operacji na informacjach i danych. Autor jednak podkreśla, że „zagadnieniem leżącym u podstaw wprowadzenia instytucji ponownego wykorzystywania nie jest dylemat czy informacje publiczne

³⁸ EUR-Lex - 32003L0098 - EN - EUR-Lex, <https://eur-lex.europa.eu/legal-content/ALL/?uri=CELEX%3A32003L0098> [dostęp: 18.10.2019].

³⁹ M. Bernaczyk, *Prawo do informacji publicznej w Polsce i na świecie*, Warszawa 2014, s. 54.

⁴⁰ *Ibidem*, s. 442.

należy udostępniać, lecz w jaki sposób i w jakiej formie je udostępniać”. Takie też stanowisko odrzucające definiowanie pojęcia ponownego wykorzystywania z art. 23b ust. 2 u.d.i.p. przyjęło się w orzecznictwie⁴¹.

Piotr Sitniewski wskazuje zaś, że działalność nastawiona na uzyskanie określonego przysporzenia, zysku, jakim jest ponowne wykorzystywanie ISP, w sposób naturalny obejmuje swym zakresem szerszy aspekt aniżeli sama jawność, transparentność⁴². Trzeba tutaj nadmienić, że polskie prawo nie różnicuje w tym aspekcie działalności komercyjnej i niekomercyjnej. Ponadto u.o.d.i.s.p. ustala inny rodzaj dostępu do ISP, likwidując możliwość złożenia anonimowego wniosku o ISP oraz teoretycznie ograniczając wykorzystywanie ISP przez dziennikarzy (np. każdorazowe wykorzystanie ISP np. do ich wizualizacji w innym celu wymagać będzie złożenia osobnego wniosku o ponowne wykorzystywanie). Jak zauważa P. Sitniewski, specyficzny sposób utrwalenia określonych ISP może wymagać określenia dodatkowych warunków ponownego wykorzystywania i wcale nie musi stać to w sprzeczności z zasadą generalną domniemania bezwarunkowości zawartą w u.o.d.i.s.p.⁴³

Ustawa o dostępie do informacji publicznej wymienia cztery podstawowe tryby udostępniania informacji publicznych. Zgodnie z art. 7 pkt 1 u.d.i.p. udostępnianie informacji publicznych następuje w drodze:

- 1) ogłaszania informacji publicznych, w tym dokumentów urzędowych, w Biuletynie Informacji Publicznej, o którym mowa w art. 8;
- 2) udostępniania, o którym mowa w art. 10 i 11;
- 3) wstępu na posiedzenia organów, o których mowa w art. 3 ust. 1 pkt 3, i udostępniania materiałów, w tym audiowizualnych i teleinformatycznych, dokumentujących te posiedzenia;
- 4) udostępniania w centralnym repozytorium.

⁴¹ Wyrok NSA z dnia 19 czerwca 2015 r., I OSK 1332/14.

⁴² P. Sitniewski, *Ustawa o ponownym wykorzystywaniu informacji sektora publicznego. Komentarz*, Warszawa 2017, s. 12.

⁴³ *Ibidem*, s. 220.

Za centralne repozytorium odpowiada minister właściwy do spraw informatyzacji. Obecnie jest to serwis dane.gov.pl prowadzony przez ministra właściwego ds. informatyzacji. Samą czynność udostępnienia informacji publicznej w literaturze ujmuje się jako czynność faktyczną administracji. Ustawa o otwartych danych z kolei mówi zasadniczo o dwóch rodzajach dostępu (poza wymienionymi istnieje możliwość złożenia wniosku u ustalenie warunków dla informacji, która już została zainteresowanemu udostępniona), dzięki którym jest możliwe ponowne wykorzystywanie ISP. Pierwszy tryb to ponowne wykorzystywanie ISP udostępnionych w systemie teleinformatycznym, a w szczególności na stronie podmiotowej Biuletynu Informacji Publicznej podmiotu zobowiązanego lub w centralnym repozytorium informacji publicznej, drugi tryb to dostęp do ISP na wniosek o ponowne wykorzystywanie (art. 5 u.o.d.i.s.p.).

5. Dane publiczne

Tak jak w rozdziale pierwszym dokonałem koniecznego rozróżnienia pojęć „informacja” i „dane”, tak w tym miejscu należy odnotować pojęcie danych, które pojawia się w u.d.i.p. Termin dane pojawia się w wielu polskich regulacjach prawnych i jako że, jak zazaczyłem na samym początku pracy, pojęcie „informacje” czy „dane” związane jest z specjalistycznymi dziedzinami i równocześnie z czynnościami „codziennymi” jednostek, rekonstruowanie jego definicji na podstawie tychże regulacji nie przyniesie żadnych korzyści interpretacyjnych. W przepisach możemy bowiem znaleźć takie sformułowania jak dane osobowe, dane dynamiczne, dane badawcze czy bazy danych. W tym miejscu dane będę rozumiał jako zbiór dyskretnych, obiektywnych faktów na temat zdarzeń, z których to informacja dopiero może być wyinterpretowana. W aspekcie informacji o funkcjonowaniu państwa ustawodawca, wyznaczając zakres przedmiotowy dostępu do informacji publicznej, posłużył

się terminem „dane publiczne”. Choć nie sformułowano definicji normatywnej, to w rozdziale 2, w art. 6.1 ust. 4 u.d.i.p. znajdziemy wymienione elementy składowe „danych publicznych”:

- „a) treść i postać dokumentów urzędowych, w szczególności:
 - treść aktów administracyjnych i innych rozstrzygnięć,
 - dokumentacja przebiegu i efektów kontroli oraz wystąpienia, stanowiska, wnioski i opinie podmiotów ją przeprowadzających,
- b) stanowiska w sprawach publicznych zajęte przez organy władzy publicznej i przez funkcjonariuszy publicznych w rozumieniu przepisów Kodeksu karnego,
- c) treść innych wystąpień i ocen dokonywanych przez organy władzy publicznej,
- d) informacja o stanie państwa, samorządów i ich jednostek organizacyjnych”.

Niestety w lit. d) zauważamy definiowanie danych publicznych jako „informacji o stanie państwa”, czyli błąd polegający na zamiennym stosowaniu znaczeń informacji i danych bez polegania na logicznym i naukowym definiowaniu i określaniu korelacji pomiędzy tymi pojęciami.

Z kolei w u.o.d.i.s.p., oprócz posługiwania się przez legislatora pojęciem danych osobowych, można także natrafić na termin „format danych”:

„Art. 10.2. Podmiot zobowiązany, który udostępnia lub przekazuje informacje sektora publicznego w celu ponownego wykorzystywania z użyciem systemów teleinformatycznych, jest obowiązany do stosowania formatów danych oraz protokołów komunikacyjnych i szyfrujących określonych w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 670, 952 i 1005), jeżeli to możliwe w formacie przeznaczonym do odczytu maszynowego wraz z metadanymi, z wyjątkiem art. 13 ust. 1a tej ustawy”.

Nie nadużywając koncepcji rekonstruowania definicji, można przyjąć, że użycie terminu „format danych” i pojęcie samych danych zgadza się

z powszechnym naukowym określaniem korelacji pojęć informacji i danych. Polski ustawodawca jednakże w żadnym innym miejscu nie precyzuje pojęcia danych publicznych czy danych jako składowych informacji publicznej czy informacji sektora publicznego, jak ma to miejsce chociażby w Stanach Zjednoczonych Ameryki. W u.o.d.i.s.p. ustawodawca stwierdza: „Przez informację sektora publicznego należy rozumieć każdą treść lub jej część, niezależnie od sposobu utrwalenia, w szczególności w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej, będącą w posiadaniu podmiotów”. Trudno jednak uznać „część” treści jako dane, ponieważ część ta może zarówno posiadać strukturę, jak i jej nie posiadać, być uporządkowana lub nie i być wreszcie integralną częścią treści w sensie semantycznym lub nie. W kontekście znacznego wpływu nowych technologii i pojęć związanych z informatyką na wiele gałęzi prawa brak takich definicji należy potraktować jako znaczący ubytek w porządku prawnym obejmującym takie dziedziny i czynności, jak wymiana informacji i danych, sprzedaż danych i informacji *etc.*

6. Informacja w postaci elektronicznej

W polskim systemie prawnym nie ma legalnej definicji informacji elektronicznej czy też informacji w postaci elektronicznej (cyfrowej). W ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne znajdziemy natomiast definicję dokumentu elektronicznego: to „stanowiący odrębną całość znaczeniową zbiór danych uporządkowanych w określonej strukturze wewnętrznej i zapisany na informatycznym nośniku danych”. Pomijając fakt, że prawodawca określił wymagania dla dokumentu elektronicznego, których w pewnych okolicznościach dokument taki nie będzie spełniać (np. w trakcie przesyłania dokumentu siecią Internet dokument ten zgodnie z przepisami ustawy przestaje być dokumentem, ponieważ nie jest zapisany na

żadnym nośniku⁴⁴⁾⁴⁵⁾, sam dokument nie wyczerpuje znaczenia pojęcia informacji w postaci elektronicznej. Zgodnie z art. 3 u.d.i.p. prawo do informacji publicznej obejmuje uprawnienia do: 1) uzyskania informacji publicznej, w tym uzyskania informacji przetworzonej w takim zakresie, w jakim jest to szczególnie istotne dla interesu publicznego; 2) wglądu do dokumentów urzędowych; 3) dostępu do posiedzeń kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów. Jak widać, informacja publiczna nie zawsze musi przyjmować postać dokumentu. Ustawa o informatyzacji wskazuje jednak, że ilekroć w przepisach dotyczących informatyzacji zawartych w odrębnych ustawach jest mowa o informacjach w postaci elektronicznej albo informacjach w formie elektronicznej – należy przez to rozumieć, w przypadku wątpliwości interpretacyjnych, dokument elektroniczny, o którym mowa w art. 3 pkt 2 tejże ustawy.

Przed wprowadzeniem ww. definicji dokumentu elektronicznego posługiwano się jego intuicyjnym rozumieniem. Ustawodawca postanowił zdefiniować to pojęcie, jednak zadanie jego definiowania pozostawiono doktrynie. Natomiast dokument elektroniczny to równie szeroka kategoria, która niewątpliwie uzależniona jest silnie od postępu technologicznego. Wydaje się, że pole semantyczne informacji w postaci elektronicznej dokładnie dookreśla *E-podręcznik* udostępniony przez Ministerstwo Cyfryzacji: „O zapisie w postaci elektronicznej mówimy wtedy, gdy do zapisu i odczytu informacji używamy środków technicznych zapisujących informację binarnie, a interpretacji i wyświetlenia (wydrukowania) w formie czytelnej dla człowieka dokonuje się za pomocą odpowiedniego oprogramowania interpretującego binarne zapisy”⁴⁶⁾. Jak wynika z ustawy o informatyzacji, informacja zapisana w postaci elektronicznej to także

⁴⁴⁾ O. Szewczyk, F. Zagórski, *Pseudoeksperci*, „CHIP” 2006, nr 1.

⁴⁵⁾ D. Adamski, M. Kutylowski, *Terminologia ustawy o informatyzacji – niespójności ciągu dalszy*, „Prawo Mediów Elektronicznych” 2006, nr 4.

⁴⁶⁾ *Postać elektroniczna – e-Podręcznik*, https://epodrecznik.mc.gov.pl/mediawiki/index.php?title=Posta%C4%87_elektroniczna [dostęp: 11.05.2022].

„zbiór danych uporządkowanych w określonej strukturze wewnętrznej”. Taki uporządkowany zbiór danych w informatyce określa się także jako plik. Plik jest podstawową jednostką logiczną magazynowania informacji w systemie komputerowym, widoczną dla użytkownika⁴⁷.

7. Format pliku informacji w postaci elektronicznej a prawo do informacji

Format danych definiuje 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 jako „szczegółowo określony sposób zapisania informacji przeznaczonej do przechowywania w pliku komputerowym”. Format dotyczy danych zapisanych i ustrukturyzowanych. Dane zapisane w takiej formie to w informatyce plik komputerowy. Właśnie to, jaką określoną strukturę wewnętrzną ma dany plik komputerowy zawierający informację w postaci elektronicznej, definiuje format pliku⁴⁸. Format to inaczej reguły określające sposób zakodowania informacji w pliku. Sposób ten zależy zaś od zastosowanej aplikacji/programu komputerowego. Specyfikacja czy też inaczej standard struktury takiego formatu może być powszechnie znany i udostępniony publicznie lub utajniony przez właściciela formatu i producenta programu komputerowego⁴⁹. Potocznie nazywa się je odpowiednio formatem otwartym i formatem zamkniętym. Formatem zamkniętym są np. format DOC stworzony i opatentowany przez firmę Microsoft czy PSD stworzony i opatentowany przez firmę Adobe. Pliki z formatami zamkniętymi

⁴⁷ W. Duch, *Fascynujący świat komputerów*, Poznań 1997.

⁴⁸ Format pliku to sposób zakodowania danych, dlatego często mówi się także o formacie danych. Formatu pliku nie należy mylić z rozszerzeniem pliku, który jest jedynie jego określeniem.

⁴⁹ A. Błaszczyk, *Encyklopedia rozszerzeń i formatów plików*, Gliwice 2001.

w większości otwierane i edytowane mogą być jedynie w specjalnie do tego przygotowanych programach. W przypadku pliku DOC jest to program Microsoft Word, w przypadku PSD – program Adobe Photoshop. Oczywiście właścicielami programów są firmy, które stworzyły dany format. W przypadku wymiany informacji zawartych w danym pliku pomiędzy dwoma urządzeniami, aby móc się z nimi zapoznać, na obu urządzeniach musi być zainstalowane odpowiednie oprogramowanie.

Format otwarty w przeciwieństwie do formatu zamkniętego posiada jawną, ogólnodostępną specyfikację oraz strukturę nieograniczoną żadnym prawem związanym z licencjonowaniem, patentami czy znakami towarowymi. Format taki może być otwierany poprzez dowolne oprogramowanie obsługujące dany format. Przykładem formatu z otwartym standardem jest np. ODT – Open Document Text (stworzony w ramach standardu Open Document Format), który może być otwierany, edytowany i zapisywany poprzez bezpłatne programy jak Open Office czy Libre Office oraz inne komercyjne edytory tekstu. Definicję otwartego standardu opublikowała Komisja Europejska w dokumencie „Europejskie Ramy Interoperacyjności wer.1.0” wydanym w 2014 r. Zgodnie z definicją otwarty standard:

- „został stworzony i jest zarządzany przez niedochodową organizację, a jego rozwój odbywa się w drodze otwartego procesu podejmowania decyzji (konsensusu, większości głosów itp.), w którym mogą uczestniczyć wszyscy zainteresowani,
- jest opublikowany, a jego specyfikacja jest dostępna dla wszystkich zainteresowanych bezpłatnie lub po kosztach druku i możliwa dla wszystkich do kopiowania, dystrybuowania i używania bezpłatnie lub w cenie kosztów operacyjnych,
- wszelkie prawa autorskie, patenty i inna własność przemysłowa związane ze standardem są nieodwołalnie udostępnione bez opłat,
- nie ma żadnych ograniczeń w jego wykorzystaniu”⁵⁰.

⁵⁰ Dane za stroną internetową: <https://ec.europa.eu/idabc/servlets/Doccd552.pdf?id=19529> [dostęp: 11.05.2022].

Otwarty standard nie ma legalnej definicji w polskim systemie prawa. Taką definicję wprowadzono jednak w systemach prawnych innych krajów. We Francji definicję otwartego standardu wprowadzono w ustawie nr 2004-575 z dnia 21 czerwca 2004 r. w sprawie zaufania do gospodarki cyfrowej: „Otwarty standard oznacza każdy protokół komunikacji, połączenia lub wymiany oraz każdy interoperacyjny format danych, którego specyfikacje techniczne są publiczne oraz bez ograniczeń dostępu lub wdrażania”⁵¹. Standard ODF jako oficjalny w administracji wprowadzono już m.in. w Danii⁵². W piśmiennictwie podkreśla się także, że otwarte formaty związane są z tzw. neutralnością technologiczną państwa (zasadą równego traktowania przez władze publiczne technologii teleinformatycznych i tworzenia warunków do ich uczciwej konkurencji).

Informacje w postaci elektronicznej można także podzielić na takie, które są możliwe do odczytania przez maszynę, oraz takie, które takiej możliwości nie dają⁵³. Legalną definicję formatu do odczytu maszynowego podaje Foundations for Evidence-Based Policymaking Act of 2018 Stanów Zjednoczonych: „dane w formacie do odczytu maszynowego to dane, które mogą być łatwo przetworzone przez komputer bez interwencji człowieka, przy jednoczesnym zapewnieniu, że żadne znaczenie semantyczne nie zostanie utracone”⁵⁴. Odczyt maszynowy danych znacznie wpływa na rozwój innowacyjnych e-usług. Automatyczne przetwarzanie danych i informacji pozwala na zwiększenie możliwości ich interpretacji.

⁵¹ Ustawa nr 2004-575 z 21 czerwca 2004 r. o zaufaniu do gospodarki cyfrowej, <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=&categorieLien=id> [dostęp: 11.05.2022].

⁵² G. Hillenius, *DK: Danish state administrations to use ODF*, Joinup, <https://joinup.ec.europa.eu/collection/eprocurement/news/dk-danish-state-administrati> [dostęp: 11.05.2022].

⁵³ Należy zwrócić uwagę, że *de facto* każda informacja zapisana cyfrowo może być odczytana przez maszynę. W tym przypadku chodzi jednak o odczyt automatyczny, niewymagający dodatkowych operacji w postaci analizy treści informacji.

⁵⁴ H.R.4174 - 115th Congress (2017-2018): Foundations for Evidence-Based Policymaking Act of 2018, <https://www.congress.gov/bill/115th-congress/house-bill/4174/text> [dostęp: 11.05.2022].

W tym miejscu należy oddzielić pojęcia odczytu maszynowego od sytuacji związanych z możliwością pomocy człowiekowi w odczycie danych i informacji przez maszynę. Z tą sytuacją związane jest pojęcie dostępności (*accessibility*). Informacje odpowiednio sformatowane, w sposób możliwy do odczytu przez maszynę i zaprezentowania ich użytkownikowi, to np. jedyna możliwość zapoznania się z nimi przez osoby niewidome poprzez takie programy jak JAWS czy Window Eye. Niestety pola semantyczne pojęć maszynowego odczytu i dostępności nie wyczerpują całości zagadnień, które pojawiają się w przypadku odbioru informacji przez człowieka za pomocą maszyny. W przypadku odczytu maszynowego mówimy o sposobie sformatowania informacji w taki sposób, aby maszyna mogła odczytać ich znaczenie. W tym przypadku plik DOC nie będzie plikiem odczytu maszynowego, chociaż program komputerowy może łatwo go odczytać i zamienić np. na dźwięk czy też wyekstrahować jego fragment i dokonać wielu operacji. Plikiem do odczytu maszynowego będzie natomiast plik XML, w którym fragmenty tekstu będą zawarte w odpowiednich znacznikach, które to z kolei może odczytać program komputerowy i „zrozumieć” kategorię znaczeniową danego fragmentu tekstu (w rozbudowanych systemach program mógłby np. otrzymać informację, czy dany wyraz to predykat). Z kolei należy zwrócić uwagę, że pojęcie dostępności w praktyce i literaturze pojmowane jest jako dotyczące przede wszystkim osób niepełnosprawnych. Choć w pkt 2 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/2102 z dnia 26 października 2016 r. w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego legislator unijny definiuje dostępność „jako zasady i techniki, jakie powinno się stosować przy projektowaniu, tworzeniu, utrzymywaniu i aktualizowaniu stron internetowych oraz aplikacji mobilnych, tak by były bardziej dostępne dla użytkowników, szczególnie dla osób niepełnosprawnych”, to w polskich przepisach ustawodawca koncentruje się już tylko i wyłącznie na osobach niepełnosprawnych. I choć nie do końca to zgodne z informatycznym

rozumieniem pojęcia formatu do odczytu maszynowego, jako odczyt maszynowy będę rozumiał bardzo szeroki zakres semantyczny tego pojęcia. Jako usprawiedliwienie zwrócę uwagę na stały rozwój programów komputerowych i ich możliwości przetwarzania informacji za człowieka, jak choćby przetwarzanie języka naturalnego (*natural language processing*, NLP), które pozwala na wyekstraktowanie tekstu pliku PDF i wyodrębnienie fragmentów znaczeniowych. Co prawda taki tekst nie zawiera się w znacznikach XML, jednak program komputerowy potrafi go odczytać i dzięki zaawansowanym algorytmom i słownikom „zrozumieć”. Nie będzie zbytnią przesadą stwierdzenie w odniesieniu do wskazanego przypadku, że mamy tutaj do czynienia z odczytem maszynowym pliku.

Efektem przetwarzania danych w formacie do odczytu maszynowego jest na przykład stworzony przez Office for National Statistics bot udzielający odpowiedzi opartych na informacjach publicznych gromadzonych przez tę instytucję⁵⁵. W przypadku funkcjonowania administracji istotne jest także znaczne zwiększenie interoperacyjności i usprawnienie relacji jednostka–państwo (automatyzacja e-usług publicznych).

Jednym z przykładów formatów do odczytu maszynowego i otwartego standardu jest format XML. Dokument w formacie XML to inaczej dokument stworzony na podstawie języka XML (*Extensible Markup Language*, w wolnym tłumaczeniu „Rozszerzalny Język Znaczników”). Język ten jest rekomendowany oraz specyfikowany przez World Wide Web Consortium (W3C) i jest odpowiedzią na zwiększające się wymagania opisu coraz bardziej złożonych informacji elektronicznych prezentowanych w sieci internetowej. Język XML jest językiem tekstowym, oznacza to więc, że dokumenty XML mogą być edytowane w najprostszych edytorach tekstowych, zaś specyfikacje opisujące ten język są opublikowane jako

⁵⁵ <https://www.ons.gov.uk/employmentandlabourmarket/peopleinwork/employmentandemployeetypes/articles/whichoccupationsareathighestriskofbeingautomated/2019-03-25> [dostęp: 11.05.2022].

otwarte standardy⁵⁶. Język XML jest językiem znaczników. Samo pojęcie znacznika (*markup*), na którym opierają się języki znacznikowe takie jak XML, zdecydowanie poprzedza erę komputerów. Znacznik w odniesieniu do dokumentów oznacza informację, będącą instrukcją sposobu przetworzenia poszczególnych części dokumentu. Takie sposoby oznaczania tekstu związane były od początku powstania przemysłu wydawniczego. Poprzez typograficzne przygotowywanie tekstów określano np. krój, stopień czy odmianę pisma.

Wraz z rozwojem wykorzystywania maszyn cyfrowych dokumenty papierowe zaczęły być wypierane przez dokumenty elektroniczne. Oznaczanie sposobów przetwarzania i formatowania dokumentów przybrało więc formę znaczników takich, jakie znamy obecnie. Pierwszym językiem, który pozwalał na oznaczanie sposobu przetwarzania dokumentu, był stworzony w firmie IBM w latach 60. język GML. W późniejszym czasie stał się on podstawą do języka SGML, którego celem było tworzenie i przetwarzanie dużych dokumentów w projektach rządowych, prawnych i przemysłowych w formie możliwej do odczytu przez człowieka. Zarówno język XML, jak i HTML, służący do opisu dokumentów publikowanych w Internecie, wywodzą się właśnie z języka SGML.

Dokument XML to dokument tekstowy, w którym za pomocą znaczników języka XML autor umieścił jakąś informację⁵⁷. Podstawowymi składnikami dokumentu XML są elementy oraz atrybuty, które znajdują się w elementach.

Elementem z atrybutami jest na przykład fragment:

```
<rozporzadzenie data-wydania="1 kwietnia 2011" nazwa="Rozporządzenie">
<tytul>W sprawie zawierania umów</tytul>
</rozporzadzenie>.
```

⁵⁶ *Extensible Markup Language (XML) 1.0 (Fifth Edition)*, <https://www.w3.org/TR/xml/> [dostęp: 11.05.2022].

⁵⁷ P. Kazienko, K. Gwiazda, *XML na poważnie*, Gliwice 2002.

<rozporządzenie> to znacznik o nazwie „rozporządzenie”, natomiast data-wydania=„1 kwietnia 2011” to atrybut o nazwie „data-wydania” i wartości „1 kwietnia 2011”. <tytuł> to znacznik początkowy, „W sprawie zatwierdzania umów” to treść elementu, zaś </tytuł> to znacznik końcowy. Jak widać, struktura takiego tekstu ma postać hierarchiczną, dzięki czemu hierarchiczny akt prawny może zostać zapisany w formie przetwarzalnej maszynowo. W elemencie <tytuł>W sprawie zawierania umów</tytuł> program „będzie wiedział”, że sformułowanie „W sprawie zawierania umów” jest tytułem aktu prawnego. W formacie XML można tworzyć rozbudowane dokumenty, zawierające wiele informacji dostępnych do odczytu automatycznego przez maszynę:

```
<Identification  lims:inforce-start-date="2014-06-04"  lims:fid="720907"
lims:id="720907">
```

```
  <InstrumentNumber>SOR/2005-35</InstrumentNumber>
```

```
  <RegistrationDate>
```

```
    <Date>
```

```
      <YYYY>2005</YYYY>
```

```
      <MM>2</MM>
```

```
      <DD>8</DD>
```

```
    </Date>
```

```
  </RegistrationDate>
```

```
  <ConsolidationDate lims:inforce-start-date="2014-06-04">
```

```
    <Date>
```

```
      <YYYY>2019</YYYY>
```

```
      <MM>6</MM>
```

```
      <DD>22</DD>
```

```
    </Date>
```

```
  </ConsolidationDate>
```

```
  <EnablingAuthority lims:inforce-start-date="2014-06-04" lims:fid="720909"
lims:id="720909">
```

```
    <XRefExternal reference-type="act" link="C-10.4">CANADA TRANS-
PORTATION ACT</XRefExternal>
```

```

</EnablingAuthority>
<LongTitle  lims:inforce-start-date="2014-06-04"  lims:fid="720910"
lims:id="720910">Canadian Transportation Agency General Rules</Long-
Title>
<RegulationMakerOrder>
  <RegulationMaker>P.C.</RegulationMaker>
  <OrderNumber>2005-144</OrderNumber>
  <Date>
    <YYYY>2005</YYYY>
    <MM>2</MM>
    <DD>8</DD>
  </Date>
</RegulationMakerOrder>
</Identification>

```

Strukturę dokumentu XML (np. uściślenie, jakiego typu treść może znaleźć się w danym znaczniku) definiuje się za pomocą standardu DTD (*document type definition*) lub XML Schema. Dokumenty obejmujące definicje XML Schema zapisuje się zazwyczaj w plikach z rozszerzeniami .xsd (od XML Schema Definition). Poprzez schemę XML opisuje się sposób tworzenia dokumentów elektronicznych przez administrację publiczną:

```

<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <xsd:import namespace="http://www.w3.org/2000/09/xmldsig#"
    schemaLocation="http://www.w3.org/TR/xmldsig-core/xmldsig-core-sche-
    ma.xsd" />
  <xsd:element name="OpisWzoru">
    <xsd:element ref="MetadaneWzoru" minOccurs="1" />
    <xsd:element ref="DaneWzoru" minOccurs="1" />
  <xsd:element name="Oswiadczenie" type="xsd:string" />
  <xsd:element name="Wnioskodawca" type="xsd:string" />

```

```
<xsd:element name="SiedzibaWnioskodawcy" type="xsd:string" />  
<xsd:element name="PodstawaPrawna" type="xsd:string" />  
<xsd:element name="DataPublikacji" type="xsd:dateTime" />  
</xsd:schema>
```

Dokumenty XML stanowią warstwę informacyjną dla programów komputerowych. W przypadku analizy tekstów prawnych ściśle osadzonych w języku XML program komputerowy może dokonywać np. zaawansowanych porównań i analiz przepisów prawnych. Język XML uważany jest obecnie za najbardziej uniwersalny język do opisu i udostępniania danych elektronicznych dokumentów, opisuje on np. dokumenty stworzone w takich programach jak Open Office czy MS Office.

Zaawansowanym sposobem udostępnienia informacji i danych publicznych jest także API (*application programming interface*), czyli Interfejs Programistyczny Aplikacji. Rozwiązanie to pozwala na bezpośredni dostęp do bazy danych poprzez wykorzystanie protokołu HTTP. Możliwość pobierania danych poprzez API daje stuprocentową pewność aktualności danych i zgodności z zasobami znajdującymi się w dyspozycji instytucji publicznej. Na świecie coraz więcej krajów decyduje się na udostępnianie swoich zasobów informacyjnych właśnie w taki sposób⁵⁸. W Polsce Ministerstwo Finansów udostępnia poprzez API z baz systemu Besti@ stale aktualizowane dane finansowe JST. Bezpośredni dostęp do baz danych, dzięki możliwości odczytu maszynowego i aktualizacji danych, daje potężne możliwości stałej analizy danych z korzyścią dla obywatela. Korzystając np. z aplikacji wizualizującej na bieżąco dane finansowe miasta, jego mieszkańiec ma łatwy i przejrzysty dostęp do podstawowych informacji na temat funkcjonowania lokalnych władz, jakimi są finanse samorządu, co ma bezpośredni wpływ zarówno na zwiększenie kontroli władzy, jak i angażowanie się w sprawy lokalne.

⁵⁸ D. Jacobson, G. Brail, D. Woods, *Interfejs API. Strategia programisty*, Gliwice 2015.

Oczywiście wcześniej obywatel musi mieć dostęp do odpowiedniego formatu danych i stworzyć aplikację, która te dane przetworzy.

W tym momencie należy podkreślić, że stosowanie wspomnianych wcześniej formatów otwartych oraz do odczytu maszynowego przede wszystkim zwiększa możliwości ich przetwarzania przez obywateli oraz niweluje wszelkie ograniczenia w ich kopiowaniu. Jakość informacji publicznych udostępnianych cyfrowo poprzez Internet ma zaś bezpośredni wpływ na zwiększenie zasięgu dostępności tychże informacji. Prawo dostępu do informacji wcześniej było realizowane przede wszystkim jako dostęp do dokumentów w formie papierowej. Obecnie człowiek funkcjonuje w świecie cyfrowym i udostępnianie informacji wyłącznie w formie papierowej może być nawet uznane za ograniczenie do niej dostępu. Chodzi tutaj nie tylko o konieczność pokonania fizycznej odległości np. do urzędu po to, aby zapoznać się z dokumentami (wyjazd do urzędu musi się odbyć w godzinach jego otwarcia, zaś dostęp online ma miejsce 24 godziny 7 dni w tygodniu), ale przede wszystkim brak możliwości zapisania informacji w sposób cyfrowy, który pozwoli na skopiowanie potrzebnych fragmentów. Łatwość przetworzenia danych i informacji to z kolei jej pełniejsza interpretacja. Można zapytać (w mojej ocenie retorycznie): po co bowiem obywatelowi druk (lub skan) 50 stron projektu budżetu gminy, w którym nie jest w stanie porównać i przeliczyć poszczególnych zadań budżetowych (lub też w najlepszym przypadku musi przepisać do odpowiedniego edytora wszystkie dane)?

Wydaje się, że polski rząd, który był projektodawcą w przypadku wszystkich aktów prawnych, zrozumiał fakt konieczności cyfrowego dostępu do informacji w erze społeczeństwa informacyjnego. Przykładem jest wspomniana wcześniej ustawa z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych, która publikowanie aktów prawnych dopuszcza już tylko w formie elektronicznej za pomocą sieci Internet. Jak wspominałem w rozdziale 3, w latach, gdy w Polsce zaczęto promulgować akty prawne, prawie 60% obywateli

centralnej części kraju nie potrafiło czytać. W 2018 r. w Polsce dostęp do Internetu posiadało 84,2% gospodarstw domowych⁵⁹. Czyż niepublikowanie aktów prawnych w formie elektronicznej nie byłoby ograniczeniem prawa do informacji o obowiązującym prawie? Należy podnieść, że wątpliwości budzi także częste twarde rozgraniczanie treści informacji od jej formy. Owszem, każda informacja, plik zapisany w formie cyfrowej zakodowany jest w tym samym kodzie binarnym. Konkretna informacja to jednak nie kod binarny. Baza z danymi finansowymi zapisana w formie pliku tekstowego txt będzie *de facto* bezwartościowa. A tabela osadzona w pliku PDF dla osoby niewidomej będzie całkowicie niedostępna. Pełny i odpowiedni dostęp do informacji o funkcjonowaniu państwa to niewątpliwie wpływ na rozwój państwa demokratycznego. Można przyznać, że nowe technologie nie wpływają (lub też wpływają w bardzo nikłym stopniu) na treść przekazywanych informacji, ale bez wątpienia na sposób tego przekazu i tym samym oddziałują na dostępność, percepcję i interpretację komunikatu⁶⁰.

8. Elektroniczne udostępnianie informacji publicznej

Zgodnie z art. 7 ust. 1 u.d.i.p. „Udostępnianie informacji publicznych następuje w drodze: 1) ogłaszania informacji publicznych, w tym dokumentów urzędowych, w Biuletynie Informacji Publicznej, o którym mowa w art. 8; 2) udostępniania, o którym mowa w art. 10 i 11; 3) wstępu na posiedzenia organów, o których mowa w art. 3 ust. 1 pkt 3, i udostępniania materiałów, w tym audiowizualnych i teleinformatycznych, dokumentujących te posiedzenia; 4) udostępniania w centralnym repozytorium”.

⁵⁹ GUS, *Spoleczeństwo informacyjne w Polsce w 2018 roku*, <https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczeństwo-informacyjne/spoleczeństwo-informacyjne/spoleczeństwo-informacyjne-w-polsce-w-2018-roku,2,8.html> [dostęp: 11.05.2022].

⁶⁰ W. Cyrul, J. Duda, J. Opila, T. Pelech-Pilichowski, *Informatyzacja tekstu prawa. Perspektywy zastosowania języków znacznikowych*, Warszawa 2014, s. 13.

Jak wynika z *argumentum a rubrica*, podstawowym sposobem realizacji dostępu do informacji publicznej powinien być tryb niewymagający inicjatywy ze strony zainteresowanych podmiotów, czyli tzw. tryb bezwnioskowy. W przypadku bezwnioskowego trybu dostępu do informacji publicznej informacje zapisane w postaci cyfrowej udostępniane są za pomocą sieci Internet (pomijam z powodów oczywistych zagadnienie wstępu na posiedzenia organów, ponieważ materiały z tychże posiedzeń mogą zostać udostępnione albo poprzez sieć Internet, albo poprzez tryb wnioskowy). Informacje publiczne zapisane cyfrowo udostępniane są na stronie Biuletynu Informacji Publicznej lub na stronie centralnego repozytorium (u.o.d.i.s.p umożliwia udostępnianie także poprzez interfejs programistyczny aplikacji). Zgodnie z dyspozycją art. 10 ust. 1 u.d.i.p. informacja udostępniona w BIP lub CRIP nie podlega udostępnieniu na wniosek.

Na stronie internetowej BIP podmioty zobowiązane są do udostępniania informacji dotyczących polityki wewnętrznej i zagranicznej organów władzy publicznej oraz zasad ich funkcjonowania, treści i postaci dokumentów urzędowych dotyczących przebiegu i efektów kontroli oraz wystąpień, stanowisk, wniosków i opinii podmiotów je przeprowadzających, treści innych wystąpień i ocen dokonywanych przez organy władzy publicznej, stanu państwa, samorządów i ich jednostek organizacyjnych, a także majątku publicznego (zob. art. 6 ust. 1 pkt 1-3, art. 6 ust. 1 pkt 4 lit. a tiret drugie i lit. c-d, art. 6 ust. 1 pkt 5 u.d.i.p.). Porównując jednak tryb bezwnioskowy u.o.d.i.s.p, dający możliwość udostępniania danych przez interfejs programistyczny aplikacji (ang. API), w tym przypadku podmiot ma jedynie możliwość, a nie obowiązek, dlatego wnioskujący nie ma w tym zakresie żadnych instrumentów prawnych na uzyskanie danych przez interfejs aplikacji.

Niezależnie od ww. informacji publikowanych obowiązkowo podmioty zobowiązane mogą dodatkowo publikować na stronach BIP również inne informacje publiczne. W literaturze wskazuje się na wyjątkowość powołania BIP, która polegała na podniesieniu strony WWW do rangi

podstawowego „urzędowego” środka przekazu informacji publicznej⁶¹. Jednocześnie w aspekcie praktycznej rzeczywistości prawnej podkreśla się fakt dywersyfikacji cyfrowego dostępu do informacji publicznej poprzez strony WWW niebędące częścią „urzędowego publikatora” oraz takie, które są jego częścią (strony BIP)⁶². Skoro podmiot „może dodatkowo” publikować inne informacje na stronie BIP, to równie dobrze może je publikować na „swojej stronie WWW” zamiast w BIP. Można w tym momencie sformułować pogląd, iż regulacje dotyczące BIP przyczyniły się do osłabienia elektronicznego udostępniania informacji publicznej, aczkolwiek należy zaznaczyć, że fakt odrębnego scharakteryzowania funkcjonalnego strony WWW, na której zamieszczane są istotne informacje publiczne, może się przyczyniać do zwiększenia przejrzystości w możliwości wyszukiwania informacji publicznej przez użytkownika strony. Tym większe może to mieć znaczenie w aspekcie „zalewu” stron internetowych informacjami, mającymi charakter propagandowy, tworzonymi przez departamenty i wydziały zajmujące się marketingiem politycznym⁶³ (PR, rzecznicy prasowi, wydziały promocji) w podmiotach publicznych. Należy także podkreślić, iż nie istnieje żadne prawo podmiotowe, które dawałoby uprawnienie do żądania zamieszczenia informacji publicznej w BIP-ie. Takiego uprawnienia nie przyznaje art. 8 ust. 1 u.d.i.p. Dlatego trzeba stwierdzić, że bezwnioskowe udostępnianie informacji publicznej nie jest publicznym prawem podmiotowym. Wojewódzki Sąd Administracyjny w orzeczeniu II SA/Wa 408/05 stwierdził: „za czynność z zakresu administracji publicznej dotyczącą uprawnień lub obowiązków wynikających z przepisów prawa [...], która podlegałaby zaskarżeniu do sądu administracyjnego nie można uznać sposobu utworzenia i prowadzenia Biuletynu Informacji Publicznej, jak również jego merytorycznej zawartości”⁶⁴.

⁶¹ M. Bernaczyk, *Prawo...*, s. 426.

⁶² *Ibidem*, s. 427.

⁶³ M. Mazur, *Marketing polityczny*, Warszawa 2019.

⁶⁴ Postanowienie WSA w Warszawie z dnia 15 czerwca 2005 r., II SA/Wa 408/05.

Dotychczas zwracało się uwagę, że rola BIP w dostępie do informacji publicznej jest niedostateczna, ponieważ brak jest regulacji zachęcających do publikowania treści poza tymi obligatoryjnymi, a zobowiązane podmioty nie są poddane efektywnej kontroli i często lekceważą obowiązki ustawowe⁶⁵. Kolejnym sposobem udostępniania informacji publicznej wymienionym przez ustawodawcę jest publikacja na stronie internetowej centralnego repozytorium. Zgodnie z art 9a. ust. 1 w centralnym repozytorium udostępniane są informacje „o szczególnym znaczeniu dla rozwoju innowacyjności w państwie i rozwoju społeczeństwa informacyjnego, które ze względu na sposób przechowywania i udostępniania pozwalają na ich ponowne wykorzystywanie w rozumieniu przepisów ustawy z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego [...], w sposób użyteczny i efektywny”. Ustawodawca tego typu informacje publiczne oznacza jako „zasób informacyjny”. Obecnie rolę centralnego repozytorium pełni strona internetowa dane.gov.pl, administrowana przez Ministerstwo Cyfryzacji. Do przekazywania zasobów informacyjnych obowiązane są (art. 9a. ust. 2 u.d.i.p.):

- 1) organy administracji rządowej;
- 2) fundusze celowe;
- 3) Zakład Ubezpieczeń Społecznych;
- 4) Kasa Rolniczego Ubezpieczenia Społecznego;
- 5) Narodowy Fundusz Zdrowia;
- 6) (uchylony)
- 7) państwowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyjątkiem podmiotów, o których mowa w art. 7 ust. 1 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz. U. poz. 1668, z późn. zm.), innych niż państwowe instytuty badawcze.

⁶⁵ G. Szpor, *Prawo dostępu do informacji publicznej jako istotny czynnik rozwoju społeczeństwa informacyjnego*, „Roczniki Geomatyki” 2009, nr 6 (36), s. 93.

Jak widać, zbiór podmiotów zobowiązanych do przekazywania swych zasobów do Centralnego Repozytorium Informacji Publicznej jest zawężony w porównaniu z podmiotami obowiązanyymi do udostępniania informacji publicznej. Michał Bernaczyk zauważa, że cele wyartykułowane w art. 9a ust. 1 u.d.i.p. należy ocenić jako niepotrzebne mnożenie bytów, skoro korespondują one z wyobrażeniem BIP jako bazy danych publicznych – repozytorium cyfrowych dokumentów, co rodzi wątpliwości związane z naruszeniem zasady wyłączności ustawy⁶⁶. Przekazywanie „zasobów informacyjnych” do prowadzonego przez ministra właściwego ds. informatyzacji CRIP nie jest objęte żadną sankcją. W przypadku nieprzekazania zasobów przez dany podmiot może on zostać jedynie „wezwany” do ich przekazania. Powiększanie cyfrowych zbiorów danych publicznych i ich jakości jest w tym przypadku przede wszystkim wynikiem administracyjnego funkcjonowania CRIP (dane.gov.pl). Warto w tym momencie nadmienić o znaczącej obecnie roli serwisu dane.gov.pl jako miejsca, które kreuje pewne standardy udostępniania informacji publicznych⁶⁷.

Kolejnym rodzajem trybu udostępniania informacji publicznej w formie cyfrowej jest udostępnianie na wniosek. Zgodnie z art. 14 ust. 1 u.d.i.p. udostępnianie informacji publicznej na wniosek następuje w sposób i w formie zgodnej z wnioskiem, chyba że środki techniczne, którymi dysponuje podmiot obowiązany do udostępnienia, nie umożliwiają udostępnienia informacji w sposób i w formie określonych we wniosku. Sam wniosek można złożyć w formie elektronicznej, np. poprzez e-mail, co potwierdzono w orzeczeniach Wojewódzkich Sądów Administracyjnych⁶⁸. Dla wnioskującego istotna jest zatem kwestia formy utrwalenia informacji przez podmiot udostępniający. Ustawa o dostępie do informacji publicznej nie daje jasnych wytycznych zarówno co do formy

⁶⁶ M. Bernaczyk, *Prawo...*, s. 435.

⁶⁷ Materiały edukacyjne Otwarte Dane, <https://dane.gov.pl/knowledge-base/education> [dostęp: 11.05.2022].

⁶⁸ Wyrok WSA we Wrocławiu z dnia 20 kwietnia 2018 r., IV SAB/Wr 59/18.

utrwalenia, jak i sposobów udostępnienia, stwierdza natomiast, że podmiot udostępniający informację publiczną zobowiązany jest do przesłania informacji publicznej albo przeniesienia jej na odpowiedni, powszechnie stosowany nośnik informacji (art. 12 ust. 2 pkt 2 u.d.i.p.). Roszczenie wnioskodawcy jest ograniczone przepisem art. 14 ust. 2, który pozwala podmiotowi udostępniającemu na przekazanie informacji w formie innej niż wnioskowana. Naturę przeszkody można wykoncypować z przepisu art. 14 ust. 1, który stwierdza: „chyba że środki techniczne, którymi dysponuje podmiot obowiązany do udostępnienia, nie umożliwiają udostępnienia informacji w sposób i w formie określonych we wniosku”. Ograniczanie przeszkód tylko do tych o naturze technicznej może jednak przyczynić się do znacznego utrudnienia w uzyskaniu informacji w przypadku specyficznego utrwalenia danych informacji przez podmiot. Może się np. okazać, że oprogramowanie przetwarzające informacje eksportuje je tylko do zabezpieczonego formatu, którego nie można przekonwertować na format do odczytu przez wnioskującego, a podmiot nie udostępnia oprogramowania, powołując się na ustawę z dnia 4 lutego 1994 roku o prawie autorskim i prawach pokrewnych⁶⁹.

Elektroniczny dostęp do informacji poprzez sieć Internet oznacza realizację prawa do informacji o funkcjonowaniu państwa 24 godziny przez 7 dni w tygodniu. Dostęp do informacji publicznej online to zwiększenie dostępności podstawowych informacji niezbędnych do prawidłowego funkcjonowania jednostki w państwie. To zatem niewątpliwie pełniejsza realizacja prawa człowieka do informacji publicznej. W literaturze zauważa się nawet zwiększoną podaż informacji elektronicznych dotyczących spraw publicznych, które dzięki nowym technologiom i nowym mediom internetowym udostępniane są wieloma kanałami, często niepublicznymi, jak choćby poprzez aktywność polityków czy urzędników w mediach społecznościowych. Taka sytuacja powoduje, że mówi się

⁶⁹ Zob. wyrok WSA w Warszawie z dnia 3 czerwca 2014 r., II SAB/Wa 179/14.

nawet o prawie do informacji aniżeli o prawie do informacji publicznej chronionej w Konstytucji RP, wskazując, że informacje publiczne w czasach Internetu mieszają się z informacjami niepublicznymi⁷⁰. Należy jednak zwrócić uwagę, że właśnie dostęp do informacji publicznej bezpośrednio od jej źródła, czyli podmiotu publicznego, daje możliwość weryfikowania faktów oraz źródeł informacji na podstawie dokumentów i danych publicznych.

9. Regulacje dotyczące udostępniania informacji w postaci elektronicznej o odpowiedniej jakości

W części tej zajmę się analizą przepisów normujących formy i tryby udostępniania informacji publicznej w postaci elektronicznej, które są jakościowo zgodne z obecnym sposobem funkcjonowania człowieka w aspekcie społeczeństwa informacyjnego. Za jakościowo zgodne przyjmę dwa podstawowe kryteria:

a) możliwość maszynowego odczytywania informacji

Maszynowo odczytywalne informacje to te, które mogą być łatwo przetworzone przez komputer bez interwencji człowieka, przy jednoczesnym zastrzeżeniu, że w trakcie tego procesu żadne znaczenie semantyczne nie zostanie utracone. Plikiem możliwym do odczytu maszynowego będzie więc taki, który program komputerowy może przetworzyć („zrozumieć” jego treść). Przykładem będzie akt prawny zapisany w pliku XML czy bieżące informacje pogodowe udostępnione w pliku JSON poprzez protokół HTTP.

b) otwarty standard

Przyjmując definicję prawodawstwa francuskiego, za otwarty standard będę uważał każdy protokół komunikacji, połączenia lub wymiany

⁷⁰ J. Wawrzyniak, *Paradoksy doktryny i praktyki praw człowieka w dobie globalizacji*, [w:] G. Baranowska [et al.] (red.), *O prawach człowieka. Księga jubileuszowa Profesora Romana Wieruszewskiego*, Warszawa 2017, s. 148.

oraz każdy interoperacyjny format danych, którego specyfikacje techniczne są publiczne oraz bez ograniczeń dostępu lub wdrażania.

Z odpowiednią jakością danych i informacji związany jest termin *open data*. Otwarte dane (*open data*) to dane, które mogą być dowolnie wykorzystywane, ponownie wykorzystywane i rozpowszechniane przez kogokolwiek⁷¹. Sam termin otwartości danych od samego początku swym polem semantycznym obejmował potencjalne możliwości wykorzystania otwartych danych w budowaniu interoperacyjności⁷². Różnego rodzaju dążenia do otwierania danych publicznych powiązane są z kolei z modelem prowadzenia polityki rządu jako *open government*. Model ten zakłada właściwe regulacje i działania państwa w zakresie zwiększenia transparentności poprzez odpowiednie udostępnianie danych i informacji publicznych, dając możliwość ponownego ich wykorzystania⁷³. Działania na rzecz otwartego rządu prowadzi intensywnie Partnerstwo na Rzecz Otwartych Rządów, które zostało formalnie powołane 20 września 2011 r. na marginesie Zgromadzenia Ogólnego Organizacji Narodów Zjednoczonych. Państwami założycielskimi były: Stany Zjednoczone, Brazylia, Indonezja, Meksyk, Norwegia, Filipiny, Republika Południowej Afryki oraz Wielka Brytania. Polska do tej pory nie przystąpiła do tej inicjatywy⁷⁴.

Problematykę dostępności treści udostępnianych w Internecie podejmuje Web Accessibility Initiative (WAI) jako inicjatywa World Wide Web Consortium (W3C). Zbiór dokumentów publikowanych przez WAI o nazwie Web Content Accessibility Guidelines (WCAG) zawiera szczegółowe

⁷¹ *What is Open Data?*, <https://opendatahandbook.org/guide/en/what-is-open-data/> [dostęp: 11.05.2022].

⁷² H. Yu, D.G. Robinson, *The New Ambiguity of "Open Government"*, "SSRN Electronic Journal" 2012, s. 189, <https://doi.org/10.2139/ssrn.2012489>.

⁷³ Należy zwrócić uwagę, że popularne ostatnimi czasy działania na rzecz otwartych danych czy otwartego rządu wcale nie muszą świadczyć o zwiększaniu dostępności do informacji publicznych, ponieważ to ciągle instytucja publiczna decyduje, jakie dane udostępnia, tworząc przy tym narrację „otwartości”, jednocześnie udostępniając np. dwie bazy danych.

⁷⁴ <https://www.opengovpartnership.org/our-members/> [dostęp: 11.05.2022].

zalecenia dotyczące tworzenia dostępnych serwisów internetowych i zamieszczanych na nich treści. Wydaje się, że do tej pory ta inicjatywa ma największy wpływ na zwiększanie dostępności informacji publicznych na całym świecie.

Regulacji dotyczących wskazanych kryteriów nie ma w u.d.i.p., można je natomiast znaleźć w ustawie o otwartych danych. Jak już wspomniałem, prawo ponownego wykorzystywania dotyczy informacji sektora publicznego (ISP), zaś tryb przekazania informacji jest obwarowany dodatkowymi warunkami, które nie mają zastosowania w przypadku dostępu do informacji publicznej. Kwestie zależności u.d.i.p. oraz u.p.w.i.s.p. wymagałyby osobnego omówienia, w tym momencie skupię się na przepisach regulujących odczyt maszynowy i otwarte standardy. U.d.i.p. jedynie w art. 9a ust. 2b dotyczącym funkcjonowania Centralnego Repozytorium zobowiązuje do dostosowania „formatów danych oraz protokołów komunikacyjnych i szyfrujących, umożliwiających odczyt maszynowy do zasad określonych w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2019 r. poz. 700, 730 i 848)”. To jednak w rozporządzeniu minister właściwy do spraw informatyzacji określa „zakres zasobu informacyjnego, mając na względzie szczególne znaczenie określonych informacji publicznych dla rozwoju innowacyjności i społeczeństwa informacyjnego” (art. 9a ust. 3 pkt 2 u.d.i.p.).

Art. 10 u.p.w.i.s.p. stwierdza: „Podmioty zobowiązane, które udostępniają lub przekazują informacje sektora publicznego w celu ponownego wykorzystywania z użyciem systemów teleinformatycznych, są obowiązane do stosowania formatów danych oraz protokołów komunikacyjnych i szyfrujących określonych w przepisach wydanych na podstawie art. 18 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne [...], jeżeli to możliwe w formacie przeznaczonym do odczytu maszynowego wraz z metadanymi”. Jak zauważa Grzegorz Sibiga, przepis ten jedynie

powtarza obowiązki określone w ustawie o informatyzacji, nowością jest natomiast wprowadzenie sformułowania „jeżeli to możliwe w formacie przeznaczonym do odczytu maszynowego wraz z metadanymi”. Jest to niewątpliwie zobowiązanie o miękkim charakterze, jednak dające wnioskodawcy możliwość wnioskowania o informacje lub dane w formacie do odczytu maszynowego, jeżeli takowym instytucja zobowiązana dysponuje. Niestety należy mieć tutaj na uwadze wspomniane wcześniej wątpliwości *de facto* ograniczania dostępu poprzez potencjalne bariery proceduralne w pozyskiwaniu informacji publicznej w trybach u.p.w.i.s.p. Również termin otwarte dane jest wyjaśniony w rzeczonej ustawie – „informacje sektora publicznego udostępniane lub przekazywane w postaci elektronicznej, bezwarunkowo lub z uwzględnieniem warunków, o których mowa w rozdziale 3, kompletne, aktualne, w wersji źródłowej, w otwartym i niezastrzeżonym formacie przeznaczonym do odczytu maszynowego, które są przeznaczone do bezpłatnego ponownego wykorzystywania na tych samych zasadach dla każdego użytkownika, bez konieczności potwierdzania tożsamości przez użytkownika”. Terminu tego jednak w żaden sposób nie można odnieść do ustawy u.d.i.p.

Do kryterium maszynowego odczytu, choć nie wprost, odnosi się natomiast ustawa z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (dalej jako: ustawa o dostępności). Celem ustawy o dostępności jest wdrożenie dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/2102 z dnia 26 października 2016 r. w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego. Przepisy ustawy mają co prawda na celu przede wszystkim zwiększenie dostępności stron internetowych i aplikacji mobilnych podmiotów realizujących zadania publiczne dla osób z ograniczeniami funkcjonalnymi, jednak niejako przy okazji realizują cel zwiększenia jakości informacji publicznych udostępnianych na stronach podmiotów zobowiązanych. Ustawodawca w art. 5 zobowiązał podmioty publiczne do zapewnienia dostępności cyfrowej przez

spełnienie przez ich stronę internetową lub aplikację mobilną wymagań określonych w załączniku do ustawy. Wymagania określone w załączniku do ustawy uznaje się za spełnione, gdy podmiot publiczny zapewnia dostępność cyfrową z uwzględnieniem wymagań określonych w pkt 9, 10 i 11 normy EN 301 549 V2.1.2. Dostępność cyfrowa strony internetowej i aplikacji mobilnej zgodnie z przepisami ustawy ma polegać na zapewnieniu ich funkcjonalności, kompatybilności, postrzegalności i zrozumiałości. Oprócz zwiększenia dostępności samej strony internetowej i aplikacji mobilnej norma EN 301 549 V2.1.2 wylicza także kryteria, jakie powinny spełniać udostępniane dokumenty. Formaty, w których udostępniana jest informacja publiczna, powinny być przede wszystkim możliwe do odczytu przez programy komputerowe wykorzystywane przez osoby niewidome, co oznacza, że powinny mieć możliwość także skopiowania jakiegokolwiek ich fragmentu.

Co warto podkreślić, to fakt zastosowanej sankcji dla instytucji obowiązanych. W ramach nadzoru nad stosowaniem przepisów ustawy minister właściwy do spraw informatyzacji ma prawo składać wystąpienia do podmiotów publicznych w sprawach związanych z dostępnością cyfrową oraz nakładać w drodze decyzji administracyjnej kary pieniężne w sprawach związanych z dostępnością. Dodatkowo zgodnie z art. 18 „każdy ma prawo wystąpić do podmiotu publicznego z żądaniem zapewnienia dostępności cyfrowej wskazanej strony internetowej, aplikacji mobilnej lub elementu strony internetowej, lub aplikacji mobilnej, w tym elementów, o których mowa w art. 3 ust. 2, oraz elementów niedostępnych cyfrowo na podstawie art. 8 ust. 1, albo o jego udostępnienie za pomocą alternatywnego sposobu dostępu, o którym mowa w art. 7”. W przypadku odmowy udostępnienia w odpowiednim formacie informacji publicznej wnioskodawcy przysługuje skarga, do której rozpatrywania stosuje się przepisy Kodeksu postępowania administracyjnego.

Wspomniane wcześniej formaty, na które powołuje się u.p.w.i.s.p., są z kolei zawarte w rozporządzeniu Prezesa 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 (wydanego na podstawie ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne). Wyznaczenie standaryzacji formatów danych używanych na potrzeby komunikacji wynika z potrzeby zapewnienia czytelnego formatu dla adresata-jednostki (formatu do odczytu) oraz z powodu powszechności wymiany informacji poprzez systemy teleinformatyczne⁷⁵. W rozporządzeniu KRI znajduje się więc tabela wyliczająca formaty danych oraz standardy zapewniające dostęp do zasobów informacji udostępnianych za pomocą systemów teleinformatycznych używanych do realizacji zadań publicznych. W tabeli znajdziemy m.in. format Open Document Format for Office Applications (ODF). Oprócz otwartego formatu prawodawca zezwala jednak na korzystanie z formatów zamkniętych, wyliczając formaty komercyjnego podmiotu jak XLS możliwy do edytowania przez program Microsoft Office Excel oraz DOC możliwy do edytowania przez program Microsoft Office Word. W rozporządzeniu KRI natomiast nie odnajdziemy żadnego przepisu odnoszącego się bezpośrednio do formatu umożliwiającego odczyt maszynowy bez względu na format danych. Warto podkreślić, że rozporządzenie to może być istotne także z innego powodu, a mianowicie sposób tworzenia i zapisywania informacji publicznej w konkretnych formatach plików wpływa na możliwość uzyskania dokumentu przetwarzanego przez instytucję zobowiązaną w takim formacie, w jakim wnosi wnioskodawca. Przykładem jest wyrok NSA z dnia 12 września 2013 r. (I OSK 719/13). Skarżący chciał uzyskać formularz danych statycznych dotyczących spraw w Sądzie Apelacyjnym w Warszawie wytworzony w postaci elektronicznej, czyli tej, w której zgodnie z prawem został pierwotnie ten formularz stworzony. Okazało się jednak, że od kilku lat na okres 2-3 lat Ministerstwo

⁷⁵ A. Gałach, *Krajowe ramy interoperacyjności. Systemy informatyczne w administracji publicznej. Wdrażanie i eksploatacja*, Warszawa 2015.

w celu tworzenia, przesyłania i obliczania danych z tych formularzy zamawia u prywatnej firmy program komputerowy, na który otrzymuje pełną licencję. Wnioskujący nie był jednak w stanie odczytać tego formatu lub przekształcić go na format powszechnie stosowany za pomocą żadnego innego programu komputerowego. Tylko ten jeden specyficzny program będący w posiadaniu Ministerstwa Sprawiedliwości był w stanie otworzyć plik z danymi. Sąd orzekł jednak, że program komputerowy nie stanowi informacji publicznej. Stwierdził też, że „program komputerowy jest bowiem narzędziem, którego zastosowanie umożliwi dopiero organowi wytworzenie informacji publicznej”. Tym samym otrzymanie edytowalnego pliku w formie do odczytu maszynowego okazało się niemożliwe, chociaż takowymi plikami dysponowało Ministerstwo. Reguły wyznaczone w KRI mają także znaczenie przy udostępnianiu informacji publicznych w BIP. Zgodnie z § 7 ust. 1 pkt 1 strony Biuletynu spełniają minimalne wymagania dla systemów teleinformatycznych. Zastosowanie tych rozwiązań wiąże się jednak z pewnymi problemami natury technicznej. Zgodnie z art. 8 ust. 6 pkt 3 podmioty udostępniające informacje publiczne w BIP są obowiązane do dołączenia do informacji danych określających tożsamość osoby, która wprowadziła informację do BIP. W praktyce przepis ten uniemożliwia automatyczne wprowadzenie informacji publicznej z innego systemu teleinformatycznego⁷⁶.

Nad poprawą jakości cyfrowej informacji publicznej pracowano dotychczas w Ministerstwie Cyfryzacji, gdzie w ramach grupy roboczej ds. otwartości danych został stworzony Standard Techniczny. Standard ten obecnie jest oficjalnie opublikowany na stronie internetowej gov.pl i ma formę zaleceń, które powinny być stosowane przez instytucje udostępniające informacje publiczne (aczkolwiek sam Standard koncentruje się tutaj na pojęciu danych publicznych). Standard określa odpowiednie formaty danych na podstawie stopni otwartości opublikowanych przez

⁷⁶ K. Świtała, *Prawo do informacji 2.0: propozycje nowego podejścia do informacji publicznej*, „Kwartalnik Prawa Publicznego” 2012, nr 12/2.

Tima Bernersa-Lee (współtwórcy usługi www)⁷⁷. Działania te jednak trudno nawet nazwać prawem miękkim.

Podsumowanie

Jak podaje J. Oleński, „warunkiem sine qua non ładu informacyjnego właściwego dla demokracji i dobrego rynku, oprócz symetrii informacyjnej i bezpieczeństwa informacyjnego, jest spójność prawa dotyczącego informacji”⁷⁸. Właściwe podejście do jakości udostępnianych cyfrowo informacji publicznych wpłynie na „kompletne wdrożenie nowoczesnych rozwiązań gwarantujących jak najpełniejszą realizację konstytucyjnego prawa do informacji o działalności podmiotów publicznych”⁷⁹. Niedyskryminujący i otwarty dostęp do informacji jest obecnie podstawą rozwoju państwa demokratycznego. Polski system prawny niestety jest w tym wymiarze niespójny. Format do odczytu maszynowego służy przede wszystkim do korzystania z informacji publicznych przeznaczonych w szczególności do przetwarzania (aczkolwiek należałoby tutaj wyodrębnić funkcję antydyskryminującą w dostępie do informacji osób niewidomych i niedowidzących) lub ponownego wykorzystywania. Prawo do ponownego wykorzystywania informacji jest zaś związane z różnym przeznaczeniem informacji: demokratycznym, gospodarczym, publicznym. Za M. Bernaczykiem można postawić jednak pytanie, czy wykorzystanie takiej conceptualizacji tego pojęcia ma służyć do rozbudowywania systemów prawnych i zbiurokratyzowania reżimów dostępu do informacji publicznej⁸⁰. Wydaje się, że szczegółowy powód, dla którego

⁷⁷ <http://5stardata.info/en/> [dostęp: 11.05.2022].

⁷⁸ J. Oleński, *Infrastruktura informacyjna państwa w globalnej gospodarce*, Warszawa 2006.

⁷⁹ K. Światała, *Konstytucyjne prawo dostępu do informacji publicznej a rozwój technologii informacyjnych*, „Obserwator Konstytucyjny” 2013, s. 10.

⁸⁰ M. Bernaczyk, *Prawo...*, s. 55.

suweren pozyskuje informacje publiczne, dokonuje ich replikacji, agregacji czy jakichkolwiek operacji możliwych do dokonania z informacją cyfrową, nie powinien być elementem warunkującym sposób dostępu i jakichkolwiek ograniczeń w uzyskiwaniu informacji publicznych. Należy w tym momencie zauważyć pewne dychotomiczne podejście do dostępu do informacji publicznej w aspekcie udostępniania ich elementu składowego, jakim są dane publiczne. Choć coraz częstsze praktyki związane z tzw. otwieraniem danych publicznych przyczyniają się do zwiększania dostępności danych i informacji publicznych, to należy podkreślić, że to reżimy udostępniania informacji publicznych dają gwarancje ochrony konstytucyjnego prawa do informacji o funkcjonowaniu państwa⁸¹. Dodatkowo trzeba nadmienić, że we wszystkich reżimach prawnych można napotkać mieszanie pojęciowe terminów „dane” oraz „informacja”, które to finalnie prowadzi do błędnych interpretacji i wyznaczania treści przedmiotu udostępniania informacji publicznej.

Odnosząc się także do pełnego dostępu do informacji publicznej w czasach społeczeństwa informacyjnego, można przyjąć cele podejścia Access by Design⁸², które dla zapewnienia pełnego dostępu do informacji obejmują:

- podejście proaktywne do udostępniania informacji publicznych,
- rozwijanie współpracy z obywatelami i organizacjami społecznymi,
- otwartość i transparentność wywołującą poczucie odpowiedzialności za sprawy publiczne,
- zwiększenie efektywności pracy i rządzenia organów władzy,
- zwiększenie dostępności informacji publicznej
- zwiększenie jakości informacji.

⁸¹ B.S. Noveck, *Rights-Based and Tech-Driven: Open Data, Freedom of Information, and the Future of Government Transparency*, “Yale Human Rights and Development Law Journal” 2017, Vol. 19, s. 35.

⁸² Koncepcja została sformułowana w 2010 r. przez Komisarz ds. informacji i prywatności prowincji Ontario w Kanadzie Ann Cavoukian.

Obečne przepisy nie dają suwerenowi gwarancji dostępu do informacji w formatach do odczytu maszynowego oraz w otwartych standardach, co sprawia, że obywatel nie ma pewności co do transparentności instytucji publicznych i nie ma możliwości uzyskania informacji w odpowiedniej jakości. Zwraca się uwagę, że regulacje w randze ustawy powinny zastosować klauzulę generalną, zgodnie z którą obywatel winien mieć zagwarantowany aktem normatywnym dostęp do informacji w sposób neutralny technologicznie, czyli w otwartych formatach danych⁸³.

Również podejście proaktywne zawiera wiele wad prawnych. Bezwioskowy (proaktywny) tryb dostępu do informacji publicznej nie daje suwerenowi żadnych środków prawnych jego egzekwowania, trudno więc powiedzieć, że jest podmiotowym prawem publicznym, skoro obywatelowi nie przysługuje żadne roszczenie⁸⁴. Ponieważ zaś samo udostępnienie informacji publicznej jest czynnością materialno-prawną, istnieje problem z weryfikacją jakości tychże informacji⁸⁵. Agnieszka Demczuk zauważa, że obowiązek ustawowy udostępniania informacji publicznej przyspieszył w latach 90., nakładając na instytucje publiczne nowe obowiązki. Zaś najszerszy dostęp do informacji publicznej to realizacja postulatów odnowy administracji publicznej, jej modernizacji, unowocześniania się⁸⁶. Rozwiązania techniczne umożliwiające dostęp do informacji publicznej winny jak najpełniej brać pod uwagę potrzeby użytkowników – obywateli⁸⁷. Przyjmuje się, że w społeczeństwie informacyjnym informacja jest towarem strategicznym, który państwo powinno chronić. Posiadanie odpowiedniej wiedzy stanowi podstawę do

⁸³ <http://prawo.vagla.pl/node/5866> [dostęp: 11.05.2022].

⁸⁴ Postanowienie Naczelnego Sądu Administracyjnego (do 31 grudnia 2003) w Lublinie z dnia 2 lipca 2002 r., II SAB/Lu 10/02.

⁸⁵ M. Folcholc, G. Sibiga (red.), *Główne problemy prawa do informacji w świetle prawa i standardów międzynarodowych, europejskich i wybranych państw Unii Europejskiej*, Warszawa 2014, s. 225.

⁸⁶ A. Demczuk, *Dostęp do informacji publicznej w Polsce. Analiza krytyczna*, „Teki Komisji Politologii i Stosunków Międzynarodowych O.L. PAN” 2010, nr 5, s. 20.

⁸⁷ K. Światała, *Prawo do informacji...*, s. 173.

podejmowania decyzji na wszystkich szczeblach struktury społeczeństwa, od pojedynczego obywatela, przez podmioty prowadzące działalność gospodarczą, po organy władzy publicznej⁸⁸. Dlatego też jednostka, realizując swoje konstytucyjne prawo do informacji, powinna mieć możliwość wyciągania na ich podstawie wniosków (budowania wiedzy) dzięki prowadzonej analizie oraz przetworzeniu informacji i danych. Aby istniała możliwość wykonywania takich operacji, informacja powinna być dostępna w postaci odczytywalnej maszynowo z możliwością skopiowania jej fragmentów. Zagwarantowanie takich sposobów i trybów dostępu do informacji i danych publicznych z pewnością będzie stanowić kolejny niezbędny krok w rozwoju społeczeństwa informacyjnego. Przykłady systemów sztucznej inteligencji, wykorzystujących informacje publiczne i przetwarzających je automatycznie za człowieka, są symptomatyczne w tym aspekcie⁸⁹. W literaturze przyznaje się, że „realizacja w pełni prawa do informacji prawnej, w tym z wykorzystaniem informatyki w tym procesie, jest gwarantem urzeczywistniania praw człowieka w XXI wieku”⁹⁰. Podsumowując, skonstatuję jednak, że gwarancją właściwego „wykorzystania informatyki” w urzeczywistniania prawa do informacji jako prawa człowieka jest dostęp do informacji możliwej do odczytu maszynowego, możliwej do fragmentarycznego skopiowania o otwartym standardzie danych.

⁸⁸ J. Taczkowska-Olszewska, K. Chałubińska-Jentkiewicz M. Nowikowska, *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Warszawa 2019, s. 9.

⁸⁹ R. Weber, *Applying artificial intelligence in the science & technology cycle*, “Information Services & Use” 2019, Vol. 39.

⁹⁰ K. Celarek, *Wykorzystywanie informatyki w procesie udostępniania informacji prawnej oraz jawności prawa gwarancją urzeczywistniania praw człowieka w XXI w.*, „Państwo i Społeczeństwo” 2010, nr 1.

Bibliografia

Pozycje zwarte

- Baranowska G., Gliszczyńska-Grabias A., Hernandez-Polczyńska A., Sękowska-Kozłowska K. (red.), *O prawach człowieka. Księga jubileuszowa Profesora Romana Wieruszewskiego*, Warszawa 2017.
- Bernaczyk M., *Prawo do informacji publicznej w Polsce i na świecie*, Warszawa 2014.
- Błaszczak A., *Encyklopedia rozszerzeń i formatów plików*, Gliwice 2001.
- Campbell-Kelly M., Aspray W., Ensmenger N., Yost J.R., *Computer: a history of the information machine*, Boulder, CO 2013.
- Castells M., *The rise of the network society*, Hoboken, NJ 2011.
- Cyrul W. (ed.), *Information technology and law*, Kraków 2014.
- Cyrul W., Duda J., Opila J., Pelech-Pilichowski T., *Informatyzacja tekstu prawa*, Warszawa 2014.
- Davenport T.H., Prusak L., *Working knowledge: how organizations manage what they know*, Boston, MA 1998.
- Duch W., *Fascynujący świat komputerów*, Poznań 1997.
- Gałach A., *Krajowe ramy interoperacyjności. Systemy informatyczne w administracji publicznej. Wdrażanie i eksploatacja*, Warszawa 2015.
- Goban-Klas T., Sienkiewicz P., *Społeczeństwo informacyjne: Szanse, zagrożenia, wyzwania*, Kraków 1999.
- Graham M., Dutton H.W., *Society and the Internet: how networks of information and communication are changing our lives*, Oxford 2014.
- Bereziński M., Hołubiec J.W., Wagner D., *Hierarchiczna struktura poznania: piramida wiedzy*, „Studia i Materiały Polskiego Stowarzyszenia Zarządzania Wiedzą” 2009, nr 19.
- Jacobson D., Brail G., Woods D., *Interfejs API. Strategia programisty*, przeł. P. Pilch, Gliwice 2015.
- Jadacki J.J., *Spór o granice języka*, Warszawa 2002.
- Janowski J., *Technologia informacyjna dla prawników i administratywistów*, Warszawa 2013.
- Kazienko P., Gwiazda K., *XML na poważnie*, Gliwice 2002.

- Kurose J., Ross K., *Sieci komputerowe*, przeł. T. Walczak, Gliwice 2019.
- Mazur M., *Marketing polityczny*, Warszawa 2019.
- Mączyński J.F., *Rewolucja informacyjna i społeczeństwo. Niektóre trendy, zjawiska i kontrowersje*, Warszawa 1997.
- Mikułowski-Pomorski J., *Informacja i komunikacja*, Wrocław 1989.
- Oleński J., *Infrastruktura informacyjna państwa w globalnej gospodarce*. Warszawa 2006.
- Przyborowska-Klimczak A., *Prawo międzynarodowe publiczne. Wybór dokumentów*, wyd. 7, Lublin 2005,
- Sibiga G. (red.), *Główne problemy prawa do informacji w świetle prawa i standardów międzynarodowych, europejskich i wybranych państw Unii Europejskiej*, Warszawa 2014.
- Sitniewski P., *Ustawa o ponownym wykorzystywaniu informacji sektora publicznego. Komentarz*, Warszawa 2017.
- Taczowska-Olszewska J., *Dostęp do informacji publicznej w polskim systemie prawnym*, Warszawa 2014.
- Taczowska-Olszewska J., Chałubińska-Jentkiewicz K., Nowikowska M., *Retencja, migracja i przepływy danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Warszawa 2019.
- Thompson J.B., *Media i nowoczesność. Społeczna teoria mediów*, przeł. I. Mielnik, Wrocław 2001.
- Wawrzyniak J., *Paradoksy doktryny i praktyki praw człowieka w dobie globalizacji*, [w:] G. Baranowska [et al.] (red.), *O prawach człowieka. Księga jubileuszowa Profesora Romana Wieruszewskiego*, Warszawa 2017.
- Wierczyński G., Wiewiórkowski W.R., *Informatyka prawnicza*, Warszawa 2016.

Pozycje artykułowe

- Adamski D., Kutylowski M., *Terminologia ustawy o informatyzacji – niespójności ciąg dalszy*, „Prawo Mediów Elektronicznych” 2006, nr 4.
- Amberg J.H., *Znaczenie zasady jawności dla demokracji*, „Krytyka Prawa” 2018, nr 1.
- Bernstein J.H., *The Data-Information-Knowledge-Wisdom Hierarchy and its antithesis*, “CUNY Academic Works” 2009.

- Celarek K., *Wykorzystywanie informatyki w procesie udostępniania informacji prawnej oraz jawności prawa gwarancją urzeczywistniania praw człowieka w XXI w.*, „Państwo i Społeczeństwo” 2010, nr 1.
- Ciuriak D., *The Economics of Data: Implications for the Data-Driven Economy*, Centre for International Governance Innovation, 2018, <https://www.cigionline.org/articles/economics-data-implications-data-driven-economy>
- Demczuk A., *Dostęp do informacji publicznej w Polsce. Analiza krytyczna*, „Teki Komisji Politologii i Stosunków Międzynarodowych O.L. PAN” 2010, nr 20.
- Grabowski M., Zając A., *Dane, informacja, wiedza – próba definicji*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie” 2009, nr 798.
- Hillenius G., *DK: Danish state administrations to use ODF*, Joinup, <https://joinup.ec.europa.eu/collection/e-procurement/news/dk-danish-state-administrati>.
- Kasprzyk B., *Aspekty funkcjonowania e-administracji dla jakości życia obywateli*, „Nierówności Społeczne a Wzrost Gospodarczy” 2011, nr 23.
- McDonagh M., *The right to information in international human rights law*, “Human Rights Law Review” 2013, No 13.
- Noveck B.S., *Rights-based and tech-driven: open data, freedom of information, and the future of government transparency*, “Yale Human Rights and Development Law Journal” 2017, Vol. 19.
- Osowski S., Wilk B., *Od wolności otrzymywania i przekazywania informacji do prawa do informacji (publicznej). Ewolucja orzecznictwa Europejskiego Trybunału Praw Człowieka w zakresie art. 10 Konwencji o ochronie praw człowieka i podstawowych wolności*, „Przegląd Prawa Konstytucyjnego” 2017, nr 2 (36).
- Schroeder M.J., *Spór o pojęcie informacji*, „Studia Metodologiczne” 2015, nr 34.
- Stylec-Szromek P., *Sztuczna inteligencja – prawo, odpowiedzialność, etyka*, „Zeszyty Naukowe Politechniki Śląskiej” 2018, z. 123.
- Szewczyk O., Zagórski F., *Pseudoeksperti*, „CHIP” 2006, nr 1.
- Szpor G., *Prawo dostępu do informacji publicznej jako istotny czynnik rozwoju społeczeństwa informacyjnego*, „Roczniki Geomatyki” 2009, nr 7.
- Światała K., *Konstytucyjne prawo dostępu do informacji publicznej a rozwój technologii informacyjnych*, „Obserwator Konstytucyjny” 2013.

Świtała K., *Prawo do informacji 2.0: propozycje nowego podejścia do informacji publicznej*, „Kwartalnik Prawa Publicznego” 2012, nr 12/2.

Tafilowski P., *Szybkość informacji*, „Folia Bibliologica” 2009, Vol. LI.

Vasak V., *A 30-year struggle; the sustained efforts to give force of law to the Universal Declaration of Human Rights*, “The UNESCO Courier” 1977, Vol. 30, No. 11, <https://unesdoc.unesco.org/ark:/48223/pf00000480631977>.

Weber R., *Applying artificial intelligence in the science & technology cycle*, “Information Service & Use” 2019, Vol. 39.

Williams M.E., *The impact of machine-readable data bases on library and information services*, “Information Processing & Management” 1977, nr 13.

Yu H., Robinson D.G., *The new ambiguity of “Open Government”*, “SSRN Journal” 2012, No 178.

Adresy internetowe

<http://5stardata.info/en/>.

<http://www.unic.un.org.pl/prawa-czlowieka/czym-sa-prawa-czlowieka/3129>.

<https://dane.gov.pl/knowledge-base/education>.

https://epodrecznik.mc.gov.pl/mediawiki/index.php?title=Posta%C4%87_elektroniczna.

<https://opendatahandbook.org/guide/en/what-is-open-data/>.

<https://opengovdata.org>.

<https://www.cigionline.org/articles/economics-data-implications-data-driven-economy>.

<https://www.datacoalition.org/policy-issues/open-data/open-government-data-act/>.

<https://www.datacoalition.org/policy-issues/open-data/open-government-data-act/>.

<https://www.hfhr.pl/publication/co-to-sa-prawa-czlowieka/>.

<https://www.opengovpartnership.org/our-members/>.

<https://www.w3.org/TR/xml/>.

Materialy źródłowe

GUS, *Spółeczeństwo informacyjne w Polsce w 2018 roku*, 2019, <https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/spoleczenstwo-informacyjne-w-polsce-w-2018-roku,2,8.html>.

Hearing before the Subcommittee on the Constitution of the Committee on the Judiciary United States Senate on 98 Congress First Session, Washington 1984.

Rozdział II

Praktyczne zagadnienia dostępu do informacji i ich ponownego wykorzystywania

Interoperacyjność aplikacji mobilnych śledzących kontakty zakaźne

Interoperability of mobile applications tracking infectious contacts

Streszczenie: W niniejszym opracowaniu poruszono zagadnienia aplikacji mobilnych śledzących kontakty zakaźne, danych przez nie gromadzonych oraz podmiotów, które mogą mieć do nich dostęp. Niektóre z danych zebranych przy pomocy aplikacji mobilnych zakwalifikowano jako informacje sektora publicznego, które mogą być ponownie wykorzystywane. Na przykładzie polskiej aplikacji STOP COVID – ProteGO Safe omówiono przydatność aplikacji mobilnych do innych celów niż ostrzeganie o kontakcie z osobą zakażoną wirusem SARS-CoV-2. Uwzględniono kontekst interoperacyjności aplikacji mobilnych śledzących kontakty zakaźne, w tym interoperacyjności transgranicznej na obszarze Unii Europejskiej.

Słowa kluczowe: aplikacja mobilna, COVID-19, dane osobowe

Abstract: The study discusses issues of mobile applications tracking infectious contacts, data collected by them and entities that may have access to them. Some of the data collected with the use of mobile applications has been classified as public sector information that can be reused. Using the example of the Polish STOP COVID – ProteGO Safe application, the usefulness of mobile applications for purposes other than warning about contact with a person infected with the SARS-CoV-2 virus was discussed. The context of interoperability of mobile applications tracking infectious contacts, including cross-border interoperability within the European Union, has been taken into account.

Keywords: mobile application, COVID-19, personal data

¹ Adres poczty elektronicznej: sylwia.kotecka-kral@uwr.edu.pl.

1. Dane publiczne

W wyniku wykonywania zadań publicznych gromadzi się, produkuje, reprodukuje i rozpowszechnia szeroki zakres informacji w wielu obszarach działalności, takich jak społeczeństwo, polityka, ekonomia, prawo, geografia, środowisko, pogoda, sejsmiczność (w znaczeniu skłonności danego terenu do występowania naturalnych trzęsień ziemi na danym obszarze)², turystyka, przedsiębiorczość, patenty czy edukacja³. Dane te zwykle się określać mianem publicznych, w odróżnieniu od danych prywatnych⁴, które definiuje nowa polska ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego⁵, uchwalona w wyniku implementacji dyrektywy Parlamentu Europejskiego i Rady (UE) z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego

² Zob. np. <https://www.usgs.gov/> [dostęp: 19.09.2021].

³ Zob. np. Portal Otwartych Danych Unii Europejskiej, <https://data.europa.eu/euodp/pl/data/> [dostęp: 19.09.2021], repozytorium najczęściej używanych dokumentów w krajach członkowskich Unii Europejskiej – *Repository of most commonly used public documents*, https://ec.europa.eu/internal_market/imi-net/repositories/commonly-used-public-documents/index_en.htm [dostęp: 19.09.2021], repozytorium publicznych danych o działalności naftowej na norweskim szelfie kontynentalnym, prowadzone przez Norwegian Petroleum Directorate, <https://www.npd.no/en/about-us/information-services/open-data/> [dostęp: 19.09.2021], estoński portal otwartych danych, <https://opendata.riik.ee/en/andmehulgad/> [dostęp: 19.09.2021], fiński portal otwartych danych, <https://www.avoindata.fi/en> [dostęp: 19.09.2021], repozytorium Statistics Finland, http://www.stat.fi/org/avoindata/index_en.html [dostęp: 19.09.2021], repozytorium danych publicznych Stanów Zjednoczonych Ameryki Północnej, <https://www.data.gov/> [dostęp: 19.09.2021] czy informacji związanych z wirusem SARS-CoV-2 – *Coronavirus (COVID-19)* w USA, <https://www.coronavirus.gov/> [dostęp: 19.09.2021], repozytorium danych National Institut of Standards and Technology (NIST), <https://data.nist.gov/sdp/#/> [dostęp: 19.09.2021].

⁴ Danymi prywatnymi jest każda treść lub jej część, niezależnie od sposobu utrwalenia, w szczególności w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej, będąca w posiadaniu podmiotu innego niż podmiot zobowiązany i przez niego wytworzona, z wyjątkiem danych osobowych (art. 2 pkt 5). Za dane prywatne w rozumieniu ustawowym uznaje się wszelkie treści będące w posiadaniu (i przez nie wytworzone) podmiotów innych niż te, które wymienione zostały w art. 3 ustawy. W szczególności będą to zasoby danych znajdujące się w posiadaniu przedsiębiorców czy też organizacji pozarządowych (i przez nich wytworzone); zob. *Uzasadnienie rządowego projektu ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego*, druk sejmowy nr IX.1338, s. 13.

⁵ Dz. U. z 2021 r. poz. 1641, dalej jako u.o.d.p.w.i.

wykorzystywania informacji sektora publicznego⁶. Przykładem polskiej bazy danych publicznych jest Centralne Repozytorium Informacji Publicznej⁷, które zawiera dane mające potencjał dla rozwoju społeczeństwa informacyjnego i dalszego wykorzystywania w produktach, usługach czy aplikacjach. Powstało ono na podstawie art. 9a ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej⁸; mowa o nim także w art. 5 ustawy z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego⁹. Ostatnia z wymienionych ustaw została uchylona z dniem 8.12.2021 r. przez wspomnianą już ustawę z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, która posługuje się pojęciem „portal danych” w miejsce „Centralnego Repozytorium Informacji Publicznej”. Portal danych został zdefiniowany w jej art. 2 pkt 13 jako prowadzony przez ministra właściwego do spraw informatyzacji, powszechnie dostępny system teleinformatyczny, służący do udostępniania informacji sektora publicznego w celu ponownego wykorzystywania oraz danych prywatnych w celu wykorzystywania. Zmiana nazewnictwa nastąpiła także w ustawie o dostępie do informacji publicznej¹⁰.

W polskim systemie prawnym zamiast pojęcia „dane publiczne” funkcjonuje pojęcie „informacji sektora publicznego”. Informacja sektora publicznego to każda treść lub jej część, niezależnie od sposobu utrwalenia, w szczególności w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej, będąca w posiadaniu podmiotu zobowiązanego (art. 2 pkt 8 u.o.d.p.w.i.); podmioty zobowiązane zostały wskazane w art. 3 tej ustawy. Pojęcie to należy odnieść do definicji „dokumentu” w rozumieniu art. 2 pkt 6 dyrektywy 2019/1024, zgodnie z którym „dokument” oznacza dowolną treść lub dowolną część tej treści niezależnie

⁶ Dz. Urz. UE L 172 z 26.06.2019 r., s. 56. Termin na jej implementację minął 17.07.2021 r.

⁷ <https://dane.gov.pl/pl/> [dostęp: 31.10.2020]; przepisy art. 9a ustawy o dostępie do informacji publicznej weszły w życie z dniem 8.09.2012 r.

⁸ T.j. Dz. U. z 2020 r. poz. 2176.

⁹ T.j. Dz. U. z 2019 r. poz. 1446.

¹⁰ Zob. art. 50 pkt 2-5 u.o.d.p.w.i.

od jej nośnika (papier lub forma elektroniczna lub zapis dźwiękowy, wizualny bądź audiowizualny). Dla jasności wywodów zawartych w niniejszym opracowaniu należy jedynie wskazać, że pojęcie informacji sektora publicznego wyznacza zakres przedmiotowy ponownego wykorzystywania, a dla zakwalifikowania określonej informacji jako informacji sektora publicznego nie ma znaczenia jej treść. Istotne jest natomiast jej utrwalenie oraz fakt posiadania przez podmioty udostępniające lub przekazujące ją w celu ponownego wykorzystywania. Definicja informacji sektora publicznego jest szersza niż pojęcie informacji publicznej i zawiera w sobie informację publiczną oraz inne treści (wykraczające poza zakres pojęcia informacji publicznej), tj. np. zasoby bibliotek, archiwów i muzeów niebędących informacjami publicznymi oraz inne informacje niebędące ani informacją publiczną, ani zasobem bibliotek, archiwów i muzeów¹¹.

W czasach pandemii wywołanej przez wirus SARS-CoV-2¹² do zakresu danych publicznych włączyć należy także dane obrazujące rozprzestrzenianie się choroby COVID-19¹³, a więc dane dotyczące zdrowia publicznego¹⁴. Rozwój społeczeństwa informacyjnego objawiającego się

¹¹ Zob. *Uzasadnienie rządowego projektu ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego*, druk sejmowy nr IX.1338, s. 14-15.

¹² Od ang. *Severe Acute Respiratory Syndrome* – zespół ciężkiej ostrej niewydolności oddechowej.

¹³ Od ang. *Coronavirus Disease 2019*.

¹⁴ „Zdrowie publiczne to nauka i sztuka zapobiegania chorobom, przedłużania życia i promowania zdrowia poprzez zorganizowane wysiłki społeczeństwa”; zob. *WHO European Action Plan for Strengthening Public Health Capacities and Services*, https://www.euro.who.int/_data/assets/pdf_file/0005/171770/RC62wd12rev1-Eng.pdf, s. 5 [dostęp: 18.09.2021], które odwołuje się do dokumentu: *Public health in England. The report of the Committee of Inquiry into the Future Development of the Public Health Function*, London, HMSO, 1988. Zgodnie z polską ustawą z dnia 11 września 2015 r. o zdrowiu publicznym (t.j. Dz. U. z 2021 r. poz. 183) zadania z zakresu zdrowia publicznego obejmują m.in.: monitorowanie i ocenę stanu zdrowia społeczeństwa, zagrożeń zdrowia oraz jakości życia związanej ze zdrowiem społeczeństwa; edukację zdrowotną dostosowaną do potrzeb różnych grup społeczeństwa, w szczególności dzieci, młodzieży i osób starszych; profilaktykę chorób; działania w celu rozpoznawania, eliminowania lub ograniczania zagrożeń i szkód dla zdrowia fizycznego i psychicznego w środowisku zamieszkania, nauki, pracy i rekreacji; analizę adekwatności i efektywności udzielanych świadczeń opieki zdrowotnej w odniesieniu

wszechobecnym wykorzystaniem technologii, także tej, która działa w tle¹⁵ i zbiera dane na temat swoich użytkowników, czy mobilność osób fizycznych spowodowały poważne potrzeby transgranicznego¹⁶ wykorzystywania informacji, również w zakresie zapobiegania rozprzestrzenianiu się chorób zakaźnych. Informacje te są w przeważającym stopniu gromadzone i przechowywane w postaci elektronicznej, w sposób zdecentralizowany (a więc na urządzeniach końcowych użytkownika, takich jak np. smartfony) lub scentralizowany, na serwerach zarządzanych np. przez organy administracji publicznej. Za pomocą aplikacji mobilnych służących do śledzenia kontaktów zakaźnych zbierane są bowiem dane, na podstawie których, pod pewnymi warunkami, chociażby związanymi z liczbą aktywnych użytkowników takich aplikacji, można tworzyć modele rozprzestrzeniania się

do rozpoznanych potrzeb zdrowotnych społeczeństwa; inicjowanie i prowadzenie: działalności naukowej w zakresie zdrowia publicznego, a także współpracy międzynarodowej dotyczącej działalności naukowej w zakresie zdrowia publicznego.

¹⁵ Warto w tym momencie nawiązać do koncepcji *ubiquitous computing*, czyli przetwarzania bez granic lub systemów wszechobecných, oraz *ambient intelligent*. Pierwsze z pojęć oznacza użycie urządzeń komputerowych, w szczególności mobilnych oraz sieci bezprzewodowych we wszystkich możliwych dziedzinach życia. Jest także rozszerzane na zastosowanie urządzeń, o których obecności lub przynajmniej zasadach działania zwykły użytkownik nie wie, jak procesory wbudowane w wiele urządzeń codziennego użytku (tzw. Internet rzeczy). M. Weiser po raz pierwszy zaproponował swoją koncepcję *ubiquitous computing* w 1988 r., a następnie w latach 1991-1993 opublikował jej założenia; zob. M. Weiser, *The Computer for the 21st Century*, <https://web.archive.org/web/20141022035044/http://www.ubiq.com/hypertext/weiser/SciAmDraft3.html> [dostęp: 17.09.2021]. Z kolei *ambient intelligence* przedstawia się jako wizję komputeryzacji otoczenia człowieka, zgodnie z którą „człowiek otoczony będzie przez obliczeniową i sieciową zaawansowaną technologię, która jest świadoma jego obecności, jego osobowości, jego potrzeb i jest zdolna do inteligentnego odpowiadania na indykacje dotyczące pragnień, wyrażone w postaci gestu lub mowy, a nawet do angażowania się w inteligentny dialog; zob. C. Weyrich, *Orientations for WP2000 and beyond*, „ISTAG” 1999, za: J. Banasikowska, A. Sołtysik-Piorunkiewicz, *Zasady interoperacyjności i standaryzacji w systemach wszechobecných e-Government krajów Unii Europejskiej*, „Roczniki Kolegium Analiz Ekonomicznych” 2013, nr 29, s. 13-14.

¹⁶ Przekraczającego granice państw, istniejącego ponad granicami państw; zob. *Słownik języka polskiego PWN*, <https://sjp.pwn.pl/sjp/transgraniczny;2578512.html> [dostęp 19.09.2021], ale także: dotyczącego obszarów po obu stronach granicy, odbywającego się między dwoma państwami ze sobą państwami; zob. B. Dunaj (red.), *Słownik współczesnego języka polskiego*, Warszawa 1996.

wirusa SARS-CoV-2. Służyć one mogą ocenie ogólnej skuteczności środków ograniczających rozprzestrzenianie się COVID-19, ale także być pomocne prywatnym przedsiębiorcom, jak np. apteki czy hurtownie medyczne, do przewidywania zapotrzebowania na środki ochrony indywidualnej przed wirusem SARS-CoV-2, ale i na specjalistyczny sprzęt medyczny, jak respiratory czy ECMO. W dalszej części niniejszego opracowania zostaną poruszone kwestie dostępu podmiotu zarządzającego polską aplikacją śledzącą kontakty zakaźne do zarówno jednostkowych danych zgromadzonych na urządzeniach końcowych użytkowników tejże aplikacji, jak i możliwości dalszego wykorzystania danych przechowywanych na centralnym serwerze do celów związanych z ochroną zdrowia publicznego.

Dnia 11.03.2020 r. Światowa Organizacja Zdrowia ogłosiła, że epidemia wirusa SARS-CoV-2 jest już pandemią¹⁷, co oznacza, że ten rodzaj koronawirusa jest epidemiologicznym zagrożeniem dla całego świata. Wobec ciągle wzrastającej mobilności ludzkiej transgraniczna wymiana danych dotyczących rozprzestrzeniania się wirusa SARS-CoV-2 jest niezwykle istotna dla organów ds. zdrowia publicznego¹⁸ i instytucji badawczych¹⁹ różnych państw.

¹⁷ Zob. *WHO Director-General's opening remarks at the media briefing on COVID-19 - 11 March 2020*, <https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-media-briefing-on-covid-19---11-march-2020> [dostęp: 19.09.2021].

¹⁸ Zgodnie z ustawą z dnia 11 września 2015 r. o zdrowiu publicznym do organów ds. zdrowia publicznego (którym to pojęciem posługują się przedstawiane w niniejszym opracowaniu dokumenty wydane przez organy UE) zalicza się: organy administracji rządowej, zgodnie z kompetencjami określonymi w ustawie z dnia 4 września 1997 r. o działach administracji rządowej (t.j. Dz. U. z 2020 r. poz. 1220), państwowe jednostki organizacyjne, w tym agencje wykonawcze, a także jednostki samorządu terytorialnego, realizujące zadania własne polegające na promocji lub ochronie zdrowia (art. 3 ust. 1). Z analizy dalszych przepisów cytowanej ustawy wynika, że organami ds. zdrowia publicznego są: minister właściwy ds. zdrowia, Narodowy Fundusz Zdrowia, Narodowy Instytut Zdrowia Publicznego – Państwowy Zakład Higieny, jednostki właściwe w sprawach przeciwdziałania uzależnieniom, Instytut Medycyny Wsi, Główny Inspektor Sanitarny, Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy, Główny Inspektor Sanitarny Wojska Polskiego (zob. art. 5 ust. 1 cyt. ustawy).

¹⁹ W polskim systemie prawnym funkcjonuje pojęcie „instytutu badawczego”. Ustawa o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi w zakresie definicji

2. Aplikacje mobilne śledzące kontakty zakaźne

Interoperacyjność aplikacji mobilnych śledzących kontakty zakaźne stanowi część szerszego zagadnienia, dotyczącego balansu pomiędzy koniecznością przekazywania danych o rozprzestrzenianiu się wirusa SARS-CoV-2 do innych systemów informacyjnych, w tym przekazywania transgranicznego, a ochroną danych osobowych i ochroną prywatności użytkowników tych aplikacji – a więc poszanowaniem cyfrowych praw jednostki – i zarządzaniem ryzykiem przy wdrażaniu polityk i inicjatyw dotyczących danych publicznych. Korzystanie z aplikacji mobilnych śledzących kontakty zakaźne może rodzić obawy związane z przetwarzaniem danych osobowych, w tym danych dotyczących zdrowia użytkowników tych aplikacji. Z uwagi na priorytet redakcyjny publikacji, jakim jest osadzenie zasadniczych wątków w obszarze otwartości

tego pojęcia odsyła do art. 1 ust. 1 ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych (t.j. Dz. U. z 2020 r. poz. 1383). Instytutem badawczym jest państwowa jednostka organizacyjna, wyodrębniona pod względem prawnym, organizacyjnym i ekonomiczno-finansowym, która prowadzi badania naukowe i prace rozwojowe ukierunkowane na ich wdrożenie i zastosowanie w praktyce. Do podstawowej działalności instytutu badawczego należy: prowadzenie badań naukowych i prac rozwojowych, przystosowywanie wyników badań naukowych i prac rozwojowych do potrzeb praktyki, wdrażanie wyników badań naukowych i prac rozwojowych. W związku z prowadzoną działalnością podstawową instytut może (m. in.): upowszechniać wyniki badań naukowych i prac rozwojowych, wykonywać badania i analizy oraz opracowywać opinie i ekspertyzy w zakresie prowadzonych badań naukowych i prac rozwojowych, opracowywać oceny dotyczące stanu i rozwoju poszczególnych dziedzin nauki i techniki oraz sektorów gospodarki, które wykorzystują wyniki badań naukowych i prac rozwojowych oraz w zakresie wykorzystywania w kraju osiągnięć światowej nauki i techniki, prowadzić działalność normalizacyjną, certyfikacyjną i aprobową, prowadzić i rozwijać bazy danych związane z przedmiotem działania instytutu, prowadzić działalność w zakresie informacji naukowej, technicznej i ekonomicznej, wynalazczości oraz ochrony własności przemysłowej i intelektualnej, a także wspierającej innowacyjność przedsiębiorstw, wytwarzać w związku z prowadzonymi badaniami naukowymi i pracami rozwojowymi aparaturę, urządzenia, materiały i inne wyroby oraz prowadzić walidację metod badawczych, pomiarowych oraz kalibrację aparatury, prowadzić działalność wydawniczą związaną z prowadzonymi badaniami naukowymi i pracami rozwojowymi; zob. szer. art. 2 cyt. ustawy). Instytut prowadzący badania naukowe i prace rozwojowe w zakresie nauk medycznych uczestniczy w systemie ochrony zdrowia (art. 3 cyt. ustawy).

danych publicznych, nie zostaną omówione szczegółowe kwestie związane z regulacjami prawnymi i rozwiązaniami technicznymi zapewniającymi ochronę prywatności użytkowników aplikacji mobilnych śledzących kontakty zakaźne. W zakresie przetwarzania danych osobowych odesłać należy także do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 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)²⁰.

Na obszarze samej tylko UE obowiązują akty prawne dotyczące zdrowia publicznego w kontekście chorób zakaźnych, jak np. decyzja Parlamentu Europejskiego i Rady nr 1082/2013/UE z dnia 22 października 2013 r. w sprawie poważnych transgranicznych zagrożeń zdrowia oraz uchylająca decyzję nr 2119/98/WE²¹. Ustanowiono w niej szczegółowe przepisy dotyczące nadzoru epidemiologicznego, monitorowania, wczesnego ostrzegania i zwalczania poważnych transgranicznych zagrożeń zdrowia.

Wielu Europejczyków łączy się z Internetem przez urządzenia mobilne, a zatem technologie i dane cyfrowe mają do odegrania ważną rolę w walce z kryzysem wywołanym przez COVID-19. Takie technologie i dane mogą stać się ważnym narzędziem służącym informowaniu społeczeństwa, oferującym organom publicznym, wykonującym zadania z zakresu zdrowia publicznego²², pomoc w ich wysiłkach na rzecz

²⁰ Dz. Urz. UE L 119 z 4.05.2016 r., s. 1; dalej jako: RODO.

²¹ Dz. Urz. UE L 293 z 5.11.2013 r., s. 1.

²² Odnosząc to stwierdzenie do polskich warunków, należy wskazać, że zgodnie z ustawą z dnia 11 września 2015 r. o zdrowiu publicznym, która określa m.in. zadania z zakresu zdrowia publicznego oraz podmioty uczestniczące w realizacji tych zadań, do organów ds. zdrowia publicznego zalicza się: organy administracji rządowej, zgodnie z kompetencjami określonymi w ustawie z dnia 4 września 1997 r. o działach administracji rządowej, państwowe jednostki organizacyjne, w tym agencje wykonawcze, a także jednostki samorządu terytorialnego, realizujące zadania własne polegające na promocji lub ochronie zdrowia (art. 3 ust. 1). Z analizy dalszych przepisów cytowanej ustawy wynika, że organami ds. zdrowia publicznego są: minister właściwy ds. zdrowia, Narodowy Fundusz Zdrowia, Narodowy Instytut Zdrowia Publicznego – Państwowy Zakład Higieny, jednostki właściwe

powstrzymania rozprzestrzeniania się wirusa czy też umożliwiającym organizacjom opieki zdrowotnej wymianę danych dotyczących zdrowia. Fragmentaryczne i nieskoordynowane podejście może jednak ograniczyć skuteczność środków mających na celu walkę z kryzysem wywołanym przez COVID-19, stanowiąc jednocześnie poważne zagrożenie dla jednolitego rynku i podstawowych praw i wolności²³. Aplikacje mobilne mogą pomagać organom ds. zdrowia w monitorowaniu i ograniczaniu pandemii COVID-19 na szczeblu krajowym i unijnym. Mogą udzielać wskazówek obywatelom i ułatwiać organizację opieki medycznej nad pacjentami. Aplikacje umożliwiające śledzenie mogą odgrywać ważną rolę w ustalaniu kontaktów zakaźnych, ograniczaniu rozprzestrzeniania się choroby i przerywaniu łańcuchów zakażeń. W połączeniu z odpowiednimi strategiami wykonywania testów i ustalaniem kontaktów zakaźnych aplikacje te mogą być szczególnie przydatne, jeśli chodzi o dostarczanie informacji na temat poziomu występowania wirusa, ocenę skuteczności środków służących ograniczeniu kontaktów i środków izolacji, oraz mogą wnieść istotny wkład w strategię deeskalacji²⁴.

Wobec powyższego organy UE wydały szereg niewiążących wytycznych i zaleceń, dotyczących gromadzenia danych związanych z rozprzestrzenianiem się COVID-19 poprzez aplikacje mobilne. Są nimi m.in.:

- 1) European Data Protection Board Letter concerning the European Commission's Draft Guidance on apps supporting the fight against the COVID-19 pandemic z 14.04.2020 r.,

w sprawach przeciwdziałania uzależnieniom, Instytut Medycyny Wsi, Główny Inspektor Sanitarny, Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy, Główny Inspektor Sanitarny Wojska Polskiego (zob. art. 5 ust. 1 ustawy o zdrowiu publicznym).

²³ Zalecenie Komisji (UE) 2020/518..., pkt 2 preambuły.

²⁴ Pkt 4 preambuły Zalecenia Komisji (UE) 2020/518.

- 2) European Data Protection Board Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak z 21.04.2020 r.²⁵,
- 3) European Data Protection Board Mandate on geolocation and other contact tracing tools in the context of the COVID-19 outbreak z 7.04.2020 r.²⁶,
- 4) European Data Protection Board Statement in the data protection impact of the interoperability of contact tracing apps z 16.06.2020 r.²⁷,
- 5) Zalecenie Komisji (UE) 2020/518 z dnia 8.04.2020 r. w sprawie wspólnego unijnego zestawu instrumentów ułatwiającego wykorzystanie technologii i danych w celu zwalczania kryzysu wywołanego przez COVID-19 i wyjścia z niego, w szczególności w odniesieniu do aplikacji mobilnych i wykorzystywania zanonimizowanych danych dotyczących mobilności²⁸,
- 6) Komunikat Komisji „Wytyczne dotyczące aplikacji pomocnych w walce z pandemią COVID-19 w odniesieniu do ochrony danych” (2020/C 124 I/01) z 17.04.2020 r.²⁹,
- 7) eHealth Network: Mobile applications to support contact tracing in the EU’s fight against COVID-19. Common EU Toolbox for Member States z 15.04.2020 r.³⁰

²⁵ https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_en [dostęp: 19.09.2021].

²⁶ https://edpb.europa.eu/our-work-tools/our-documents/other/mandate-geolocation-and-other-tracing-tools-context-covid-19_en [dostęp: 19.09.2021].

²⁷ https://edpb.europa.eu/our-work-tools/our-documents/sonstiges/statement-data-protection-impact-interoperability-contact_en [dostęp: 19.09.2021].

²⁸ Zalecenie Komisji (UE) 2020/518 z dnia 8 kwietnia 2020 r. w sprawie wspólnego unijnego zestawu instrumentów ułatwiającego wykorzystanie technologii i danych w celu zwalczania kryzysu wywołanego przez COVID-19 i wyjścia z niego, w szczególności w odniesieniu do aplikacji mobilnych i wykorzystywania zanonimizowanych danych dotyczących mobilności, Dz. Urz. UE L 114 z 14.04.2020 r., s. 7.

²⁹ Dz. Urz. UE C 124 I z 17.04.2020 r., s. 1.

³⁰ https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf [dostęp: 19.09.2021].

2.1. Funkcjonalności aplikacji mobilnych śledzących kontakty zakaźne

Od początku kryzysu wywołanego przez COVID-19 opracowane zostały różne aplikacje mobilne, w tym przez organy publiczne³¹. Decyzja Wykonawcza Komisji (UE) 2020/1023 z dnia 15 lipca 2020 r. zmieniająca decyzję wykonawczą (UE) 2019/1765 w zakresie transgranicznej wymiany danych między krajowymi aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania w związku ze zwalczaniem pandemii COVID-19³² zawiera definicję pojęcia „krajowa aplikacja mobilna służąca do ustalania kontaktów zakaźnych i ostrzegania”. Oznacza ona zatwierdzone na szczeblu krajowym oprogramowanie działające na urządzeniach inteligentnych, w szczególności smartfonach, zaprojektowane zazwyczaj do szeroko zakrojonej i ukierunkowanej interakcji z zasobami internetowymi, które przetwarza dane dotyczące bliskości fizycznej i inne informacje kontekstowe gromadzone za pomocą wielu czujników, w które wyposażone są urządzenia inteligentne (jak np. smartfony), w celu wykrywania kontaktów z osobami zakażonymi SARS-CoV-2 i ostrzegania osób, które mogły mieć styczność z wirusem SARS-CoV-2. Wspomniane aplikacje mobilne mają możliwość wykrywania obecności innych urządzeń korzystających z technologii Bluetooth i wymiany

³¹ Publiczne aplikacje mobilne, skierowane do ogółu użytkowników (nie tylko do profesjonalistów, jakimi są np. lekarze), śledzące kontakty zakaźne: Coronalert (Belgia), Koronavilkku (Finlandia), Coronamelder (Holandia), Stayaway Covid (Portugalia), Protego Safe (Polska), Ostanizdrav (Stay Healthy) – Słowenia, Hoia (Estonia), Virusafe (Bułgaria), Apturi Covid Latvia – SPKC (Łotwa), Immuni (Włochy), Radar Covid (Hiszpania), Covid Tracker Ireland (Irlandia), Corona-Warn-App (Niemcy), Stopcovid (Francja), Virusradar (Węgry), Stop Covid-19 (Chorwacja), Smitte | Stop (Dania), Covidtracker (Szwajcaria), Smittestopp (Digital Contact Tracing) – Norwegia, Sicilia Si Cura (Włochy), Covidmeter (Dania), Rakning C-19 (Islandia), Covtracer (Cypr), Erouška (Czechy), Stopp Corona (Austria), Allertalom – Cercacovid (Włochy); zob. więcej <https://mhealth-hub.org/mhealth-solutions-against-covid-19> [dostęp: 19.09.2021].

³² Dz. Urz. UE L 227 I z 16.07.2020 r., s. 1.

informacji z serwerami wewnętrznymi (ang. *backend servers*) przy użyciu Internetu. Podobną definicję zawiera Zalecenie KE nr 2020/518³³.

Aplikacje śledzące kontakty zakaźne pełnią zazwyczaj trzy funkcje ogólne; pierwszą z nich jest informowanie obywateli i doradzanie im oraz ułatwianie organizacji opieki medycznej nad osobami z objawami, często w połączeniu z kwestionariuszem pozwalającym na postawienie samodzielnej diagnozy; po drugie, ostrzeganie osób znajdujących się w pobliżu osoby zakażonej w celu przerywania łańcuchów zakażeń i zapobiegania ponownemu wystąpieniu zakażeń w fazie „ponownego otwarcia”; oraz po trzecie, monitorowanie i egzekwowanie kwarantanny osób zakażonych, ewentualnie w połączeniu z funkcjami pozwalającymi na ocenę ich stanu zdrowia w okresie kwarantanny. Niektóre aplikacje są dostępne dla ogółu społeczeństwa, zaś inne są przeznaczone wyłącznie dla zamkniętych grup użytkowników i służą śledzeniu kontaktów w miejscu pracy. Organy ds. zdrowia publicznego powinny być zaangażowane na wszystkich etapach selekcji, opracowywania, pilotowania, wdrażania i oceny aplikacji, aby zapewnić najlepszą ochronę zdrowia publicznego z należyтым uwzględnieniem prywatności i ochrony danych. Aplikacje mobilne mają wyraźne mocne strony, które mogą pomóc w uzupełnieniu niedociągnięć nieodłącznie związanych z konwencjonalnym śledzeniem kontaktów zakaźnych, nie polegają bowiem na zdolności osoby do przypomnienia sobie, z kim się kontaktowała, jak blisko i jak długo; rozwiązują też kwestie, jak skontaktować się z nieznanymi osobami, w których obecności przebywała osoba zakażona, np. w kinie czy sklepie. Aplikacje mogą ułatwić śledzenie kontaktów transgranicznych, pod warunkiem że ich interoperacyjność zostanie zapewniona, najlepiej już na etapie projektowania.

W zaleceniu nr 2020/518 Komisja Europejska stwierdza, że niektóre z omawianych aplikacji mobilnych można uznać za wyroby medyczne, w przypadku gdy producent przewiduje ich zastosowanie między innymi

³³ Pkt 3 lit. a Zalecenia Komisji (UE) 2020/518.

do celów diagnozy, zapobiegania, monitorowania, przewidywania, prognozowania, leczenia lub łagodzenia przebiegu choroby, a zatem byłyby one objęte zakresem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2017/745 z dnia 5 kwietnia 2017 r. w sprawie wyrobów medycznych, zmiany dyrektywy 2001/83/WE, rozporządzenia (WE) nr 178/2002 i rozporządzenia (WE) nr 1223/2009 oraz uchylenia dyrektyw Rady 90/385/EWG i 93/42/EWG³⁴ lub dyrektywy Rady 93/42/EWG dotyczącej wyrobów medycznych³⁵. W odniesieniu do aplikacji służących do samodzielnej diagnozy i weryfikacji objawów, jeżeli dostarczają one informacji dotyczących diagnozy, zapobiegania, monitorowania, przewidywania lub prognozowania, należy ocenić ich potencjalną kwalifikację jako wyroby medyczne zgodnie z ramami regulacyjnymi dotyczącymi wyrobów medycznych (dyrektywa 93/42/EWG lub rozporządzenie (UE) 2017/745)³⁶. Aplikacje mobilne, o których mowa, gromadzą więc dane dotyczące zdrowia ich użytkowników³⁷.

Aplikacje mobilne są zaprojektowane tak, aby uzupełniać tradycyjne działania w zakresie śledzenia kontaktów. Podczas oceny skuteczności i bezpieczeństwa aplikacji mobilnych w centrum uwagi powinna znajdować się perspektywa zdrowia publicznego. Aplikacje nie są platformami społecznościowymi do rozpowszechniania społecznych ostrzeżeń lub wzbudzania jakiegokolwiek rodzaju stygmatyzacji osób zakażonych. Wyłącznym celem aplikacji jest, aby organy publicznej opieki zdrowotnej zidentyfikowały osoby, które miały kontakt z osobą zakażoną COVID-19, wezwały je do samokwarantanny, szybko poddały je testom, a także udzieliły im, w odpowiednich przypadkach, informacji o kolejnych etapach, m.in. o tym, co należy robić w przypadku wystąpienia objawów.

³⁴ Dz. Urz. UE L 117 z 5.05.2017 r., s. 1.

³⁵ Dz. Urz. UE L 169 z 12.07.1993 r., s. 1.

³⁶ Zalecenie Komisji (UE) 2020/518..., pkt 13 preambuły.

³⁷ Zgodnie z art. 4 pkt 15 RODO dane dotyczące zdrowia oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.

W działaniach tych nadrzędne znaczenie ma jakość i prawdziwość przetwarzanych danych.

Wytyczne KE dotyczące aplikacji pomocnych w walce z pandemią COVID-19 w odniesieniu do ochrony danych dotyczą wyłącznie dobrowolnie stosowanych aplikacji, które oferują co najmniej jedną z następujących funkcji: przekazywanie osobom fizycznym rzetelnych informacji o pandemii COVID-19; udostępnianie kwestionariuszy do samodzielnej diagnozy i wytycznych dla obywateli (funkcja weryfikacji objawów); ostrzeżenia dla osób, które znajdowały się przez pewien czas w pobliżu osoby zakażonej, w celu przekazania informacji np. o konieczności samoizolacji i o miejscach, gdzie można poddać się badaniu (funkcja ustalania kontaktów zakaźnych i ostrzegania); zapewnienie forum komunikacji między pacjentami i lekarzami w przypadku samoizolacji lub zapewnienie dalszej diagnostyki i doradztwa w zakresie leczenia (wykorzystywanie telemedycyny na szerszą skalę)³⁸. W niniejszym opracowaniu omawiane będą zagadnienia dotyczące dobrowolnie instalowanych aplikacji mobilnych o takich właśnie funkcjonalnościach.

Funkcja weryfikacji objawów to narzędzie przeznaczone dla organów zdrowia publicznego, aby mogły udzielać obywatelom wskazówek dotyczących badań na obecność COVID-19, jak również przekazywać informacje o samoizolacji, sposobach unikania zakażenia innych osób oraz potrzebie zgłoszenia się po pomoc medyczną. Może być ona również uzupełnieniem podstawowej opieki zdrowotnej i zapewniać lepsze informacje na temat wskaźników zakażeń COVID-19 w danej populacji.

Funkcja ustalania kontaktów zakaźnych i ostrzegania to narzędzie pozwalające identyfikować osoby, które znalazły się w pobliżu osoby zakażonej COVID-19, także jeśli chodzi o kontakty transgraniczne, oraz poinformować je o właściwych sposobach działania w takiej sytuacji, np. o potrzebie poddania się kwarantannie w domu czy testom na obecność wirusa.

³⁸ Wytyczne nie obejmują aplikacji mających na celu egzekwowanie obowiązku kwarantanny (w tym aplikacji, których stosowanie jest obowiązkowe).

Śledzenie kontaktów ma szczególne znaczenie. Nie można powiedzieć, że aplikacje mobilne wykonują „śledzenie kontaktów”, ale raczej „śledzenie bliskości” i „powiadamianie o narażeniu”, tj. śledzenie i ostrzeganie użytkowników, którzy byli blisko siebie, co może wspierać śledzenie kontaktów. Większość z nich jest oparta na technologii Bluetooth, która umożliwia wykrywanie bliskości, ale nie pozwala na śledzenie lokalizacji. Istnieją także aplikacje oparte na technologii GPS. Z punktu widzenia ochrony danych osobowych i prywatności, ale także samych funkcji aplikacji, dane dotyczące lokalizacji nie są konieczne ani zalecane, np. przez Europejską Radę Ochrony Danych, do celów aplikacji służących do śledzenia kontaktów. Gromadzenie danych o przemieszczaniu się osób fizycznych w ramach aplikacji służących do ustalania kontaktów zakaźnych naruszałoby zasadę minimalizacji danych ustanowioną w RODO. Dodatkowo stwarzałoby poważne zagrożenia dla bezpieczeństwa i prywatności ich użytkowników. Informacja o bliskości pomiędzy użytkownikami aplikacji może przecież zostać pozyskana bez ustalania ich lokalizacji. Ten rodzaj aplikacji nie wymaga – i stąd też nie powinien obejmować – wykorzystywania danych o lokalizacji. Europejska Rada Ochrony Danych podkreśla, że jeśli chodzi o wykorzystanie danych o lokalizacji, zawsze rekomendowane jest przetwarzanie danych zanonimizowanych, zamiast danych osobowych³⁹. Dane o lokalizacji uważane za

³⁹ Anonimizacja oznacza wykorzystanie zestawu technik w celu usunięcia możliwości powiązania danych ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną pomimo wszelkich „rozsądnych” starań. Ten „test racjonalności” musi uwzględniać zarówno obiektywne aspekty (czas, środki techniczne), jak i elementy kontekstowe, które mogą się różnić w zależności od przypadku (rzadkość zjawiska, biorąc pod uwagę m.in. gęstość zaludnienia, charakter i ilość danych). Jeśli dane nie przejdą tego testu, nie zostały zanonimizowane, a zatem pozostają w zakresie RODO. Ocena odporności anonimizacji zależy od trzech następujących kryteriów: wyodrębnienia (wyzolowanie konkretnej osoby z większej grupy na podstawie danych); możliwości powiązania (powiązanie dwóch wpisów dotyczących tej samej osoby); oraz wnioskowania (wydedukowanie, z istotnym prawdopodobieństwem, nieznanych informacji na temat konkretnej osoby). Zgodnie z definicją zawartą w art. 2 pkt 1 u.o.d.p.w.i. anonimizacja to proces zmiany informacji sektora publicznego w informacje anonimowe, które nie odnoszą się do zidentyfikowanej lub możliwej do zidentyfikowania

zanonimizowane mogą w rzeczywistości nie być anonimowe. Ślady mobilności osób fizycznych są ze swej natury wysoce skorelowane i niepowtarzalne. W związku z tym mogą one być podatne na próby deanonimizacji w określonych okolicznościach⁴⁰. Pojęcie anonimizacji jest często źle rozumiane i mylone z pojęciem pseudonimizacji. Według art. 4 pkt 5 RODO „pseudonimizacja” oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej⁴¹. Podczas gdy anonimizacja umożliwia wykorzystanie danych bez żadnych ograniczeń, dane pseudonimiczne wciąż są objęte zakresem RODO. Dane nie mogą zostać zanonimizowane same w sobie, tj. anonimizować można jedynie całe zbiory danych. W tym sensie każdy zabieg na pojedynczym schemacie danych (z wykorzystaniem szyfrowania lub jakichkolwiek innych matematycznych przekształceń) można uznać za pseudonimizację⁴².

Technologia mobilna do obsługi śledzenia kontaktów została po raz pierwszy zastosowana w Singapurze. Używana tam aplikacja *Trace Together*

osoby fizycznej, lub proces zmiany danych osobowych w dane anonimowe w taki sposób, że identyfikacja osoby, której dane dotyczą, nie jest lub już nie jest możliwa.

⁴⁰ Zob. Y.-A. de Montjoye, C.A. Hidalgo, M. Verleysen, V.D. Blonde, *Unique in the Crowd: The privacy bounds of human mobility*, DOI: 10.1038/srep01376, <https://web.media.mit.edu/~yva/papers/deMontjoye2013unique.pdf>

[dostęp: 19.09.2021]; A. Pyrgelis, C. Troncoso, E. De Cristofaro, *Knock Knock, Who's There? Membership Inference on Aggregate Location Data*, <https://arxiv.org/pdf/1708.06145.pdf> [dostęp: 19.09.2021].

⁴¹ Zob. szerzej P. Litwiński, P. Barta, M. Kawecki, komentarz do art. 4, [w:] P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018, s. 207-208; K. Witkowska-Nowakowska, komentarz do art. 4 pkt 5, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 203-208.

⁴² Zob. *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak*, s. 5-7.

jest pobierana dobrowolnie i gromadzi przez Bluetooth dane o innych urządzeniach, które znajdowały się w pobliżu urządzenia użytkownika⁴³.

Komisja zaleca dobrowolne korzystanie z aplikacji. Zgodnie z dyrektywą 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)⁴⁴ narzucenie obowiązku stosowania aplikacji wiążącego się z prawami do poufności komunikacji, o których mowa w jej art. 5, jest możliwe jedynie w drodze przepisów prawa, które są konieczne, właściwe i proporcjonalne w celu ochrony pewnych celów szczególnych.

Skuteczność aplikacji mobilnych zależy od wielu czynników, m.in. stopnia ich wykorzystania przez użytkowników, czyli odsetka ludności korzystającej z urządzenia mobilnego, a wśród nich odsetka osób, które pobrały aplikację i wyraziły zgodę na przetwarzanie dotyczących ich danych osobowych i nie wycofały jej. Szczególnie narażone na infekcję wirusem SARS-CoV-2 są osoby starsze, które nie zawsze korzystają z urządzeń mobilnych, podobnie jak osoby z dysfunkcjami fizycznymi czy psychicznymi. Inne ważne czynniki skuteczności aplikacji mobilnych śledzących kontakty zakaźne to zaufanie obywateli, że dane będą chronione z wykorzystaniem odpowiednich zabezpieczeń i stosowane wyłącznie w celu ostrzegania osób, które mogły być narażone na kontakt z wirusem. W tym zakresie konieczna jest odpowiednia polityka komunikacji, a zwłaszcza szeroko zakrojona kampania informacyjna. Duże znaczenie dla skuteczności aplikacji śledzących kontakty zakaźne mają: zatwierdzenie tych aplikacji przez organ ds. zdrowia, zdolność organów ds. zdrowia do podejmowania działań na podstawie danych generowanych przez aplikacje, integracja i wymiana danych z innymi systemami i aplikacjami oraz transgraniczna i międzyregionalna interoperacyjność

⁴³ Zob. szerzej: <https://www.tracetogether.gov.sg/> [dostęp: 17.09.2021].

⁴⁴ Dz. Urz. UE L 201 z 31.07.2002 r., s. 37.

z innymi systemami. Aplikacje muszą być częścią kompleksowej strategii zdrowia publicznego w celu zwalczania pandemii, obejmującej m.in. testowanie, a następnie ręczne śledzenie kontaktów w celu usunięcia wątpliwości. Stosowaniu aplikacji powinny towarzyszyć środki wspierające, aby zapewnić, że informacje dostarczane użytkownikom są dostosowane do ogólnego kontekstu działań skierowanych przeciwko pandemii, a wysyłane alerty mogą być przydatne dla publicznego systemu opieki zdrowotnej. W przeciwnym razie aplikacje te mogą nie przynieść w pełni oczekiwanego rezultatu.

2.2. Polska aplikacja mobilna STOP COVID – ProteGO Safe

Większość państw członkowskich UE posiada publiczne aplikacje do śledzenia kontaktów zakaźnych; niektóre z nich oparte są na wykorzystaniu technologii udostępnionej przez prywatne spółki technologiczne⁴⁵. W kwietniu 2020 r. Apple i Google ogłosiły zamiar udostępnienia interfejsów programowania aplikacji śledzących kontakty zakaźne, czyli „systemu powiadomień o narażeniu” (*Exposure Notification System*), w celu obsługi aplikacji, które przyjmują zdecentralizowaną architekturę, będącą jednym z podejść przewidzianych w tzw. wspólnym zestawie narzędzi⁴⁶. Interfejsy API zostały wydane 22 maja 2020 r. Aby zapewnić zgodność rozwiązania interoperacyjnego opracowanego przez Sieć

⁴⁵ Zob. Repozytorium aplikacji mobilnych śledzących kontakty zakaźne dostępnych w państwach europejskich, <https://mhealth-hub.org/mhealth-solutions-against-covid-19> [dostęp: 19.09.2021]. Lista aktualnych inicjatyw w tym zakresie, obrazująca m.in. dane takie jak data uruchomienia aplikacji, sposób przechowywania danych (scentralizowany, zdecentralizowany), dobrowolność instalacji znajduje się w dokumencie *Mobile applications to support contact tracing in the EU's fight against COVID-19, Progress reporting June 2020*, https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_202006progress_report_en.pdf, s. 5 [dostęp: 17.09.2021].

⁴⁶ Zob. *eHealth Network Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States*, https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf [dostęp: 19.09.2021].

e-Zdrowie z interfejsami API, odbyły się oddzielne dyskusje na poziomie technicznym między poszczególnymi państwami członkowskimi i Komisją a Google i Apple.

Polską aplikacją śledzącą kontakty zakaźne jest STOP COVID – ProteGO Safe⁴⁷. Regulamin ProteGO Safe stanowi, iż korzystanie z aplikacji możliwe jest bez ograniczeń terytorialnych⁴⁸. Aplikacja została udostępniona 17.04.2020 r.⁴⁹ przez Ministerstwo Cyfryzacji⁵⁰. Dostępna jest poprzez Sklep Play (dla urządzeń z systemem operacyjnym Android, stworzonym przez Google) lub AppStore (dla urządzeń z systemem operacyjnym iOS, wytworzonym przez Apple). Celem aplikacji nie jest powiadamianie organów ds. ochrony zdrowia, a użytkowników aplikacji o ryzyku epidemiologicznym wynikającym z kontaktu z osobą zakażoną.

Administratorem danych osobowych zbieranych przez aplikację jest Główny Inspektor Sanitarny⁵¹, natomiast aplikację wytworzono na zlecenie Ministra Cyfryzacji. Do przetwarzania danych osobowych w STOP COVID – ProteGO Safe zastosowanie znajduje art. 11 RODO, gdyż cel przetwarzania nie wymaga identyfikacji, zatem użytkownicy STOP COVID

⁴⁷ Zob. <https://www.gov.pl/web/koronawirus/protegosafe> [dostęp: 19.09.2021]; dalej jako: ProteGO Safe.

⁴⁸ Zob. § 4 ust. 2 Regulaminu STOP COVID – ProteGO Safe v. 4.8, <https://www.gov.pl/web/protegosafe/dokumenty> [dostęp: 19.09.2021].

⁴⁹ Informacja zawarta w opisie aplikacji w sklepie Google Play; w repozytorium aplikacji mobilnych śledzących kontakty zakaźne dostępnych w państwach europejskich widnieje data 20.04.2020 r., z kolei na stronie <https://dane.gov.pl/pl/application/1244,protego-safe> [dostęp: 19.09.2021]: 23.04.2020.

⁵⁰ Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2021 r. poz. 670) w art. 19e-19j reguluje publiczną aplikację mobilną – jednakże jedynie taką, której celem jest pobranie, przechowywanie i prezentacja dokumentów elektronicznych przechowywanych na urządzeniach mobilnych, co ma pozwolić na zastąpienie użycia odpowiednich dla tych czynności dokumentów nieelektronicznych. Aplikacja ProteGO Safe nie mieści się zatem w ramach tej regulacji i nie może być nazywana publiczną aplikacją mobilną w rozumieniu ustawy o informatyzacji. Zob. także G. Kubalski, M. Małowiecka, *Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz*, Warszawa 2019, Legalis, komentarz do art. 19e-19j.

⁵¹ Zob. § 2 pkt 5 Regulaminu STOP COVID – ProteGO Safe.

– ProteGO Safe nie są identyfikowani⁵². Dane osobowe przetwarzane są na podstawie art. 6 ust. 1 lit. e RODO w związku z zadaniem realizowanym w interesie publicznym polegającym na zapobieganiu, przeciwdziałaniu i zwalczaniu COVID-19 wynikającym z art. 1, 2, 3, 6 oraz 8a ust. 1, 4 i 5 ustawy z dnia 14 marca 1985 r. o Państwowej Inspekcji Sanitarnej⁵³. Dane osobowe dotyczące zdrowia użytkownika są przetwarzane także na podstawie art. 9 ust. 2 lit. i RODO w zw. z zadaniem publicznym polegającym na zapobieganiu, przeciwdziałaniu i zwalczaniu COVID-19 wynikającym z art. 1, 2, 3, 6 oraz 8a ust. 1, 4 i 5 ustawy o PIS, gdyż przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi na podstawie prawa państwa członkowskiego⁵⁴. Już w tym miejscu należy zasignalizować, że dane dotyczące zdrowia są przetwarzane wyłącznie na urządzeniu końcowym użytkownika i żaden z podmiotów zaangażowanych w wytwarzanie czy zarządzanie aplikacją ProteGO Safe nie ma do nich dostępu⁵⁵.

Korzystanie z aplikacji ProteGO Safe jest bezpłatne i obejmuje swym zakresem moduł triażu, moduł analityczny, moduł dziennik zdrowia, wsparcie w profilaktyce i zapobieganiu zarażeniu, informowanie o istotnych informacjach związanych z pandemią COVID-19, „przypominacz” bezpiecznych zachowań i nawyków codziennej higieny oraz informowanie o bieżącym statusie powiatu (status żółty lub czerwony). W ramach ProteGO Safe możliwe jest ustalenie czynników ryzyka infekcji, tworzenie i prowadzenie historii medycznej, istniejących schorzeń, aktualnej farmakoterapii oraz prowadzenie dziennika profilaktyki. ProteGO Safe przekazuje użytkownikom informacje i wytyczne WHO oraz GIS, ale przekazywane

⁵² Zob. § 2 pkt 4 Regulaminu STOP COVID – ProteGO Safe.

⁵³ Dz. U. z 2019 r. poz. 59; dalej jako: ustawa o PIS. Zob. także § 3 ust. 3 Polityki prywatności STOP COVID – ProteGO Safe v. 4.8.

⁵⁴ Zob. § 3 ust. 4 Polityki prywatności STOP COVID – ProteGO Safe.

⁵⁵ Kwestia ta zostanie poruszona także w dalszej części niniejszego opracowania.

informacje nie mają charakteru konsultacji medycznej lub świadczenia zdrowotnego (w tym w szczególności medycznego lub farmaceutycznego)⁵⁶.

Najbardziej interesujący z punktu widzenia tematyki niniejszego opracowania jest moduł analityczny aplikacji, zdefiniowany jako funkcjonalność ProteGO Safe umożliwiająca zapisywanie, tworzenie historii oraz analizowanie spotkania urządzenia⁵⁷ użytkownika⁵⁸ z innymi urządzeniami użytkowników aplikacji.

Moduł analityczny ma charakter dobrowolny, a zatem to od działania użytkownika zależy, czy zostanie uruchomiony; możliwe jest korzystanie z aplikacji ProteGO Safe bez aktywowania modułu analitycznego. Usługi przewidziane w tym module świadczone są przy użyciu technologii Bluetooth i wymagają włączenia modułu Bluetooth w urządzeniu, a także odpowiednio dla urządzeń z systemem operacyjnym Android: włączenia systemowej opcji rejestrowania narażenia na COVID-19 oraz udzielenia zgody na lokalizację (w zakresie modułu Bluetooth, ProteGO Safe nie wykorzystuje danych GPS), a dla urządzeń z systemem operacyjnym iOS: zaznaczenia opcji „rejestrowanie narażenia na COVID-19”. W celu skutecznego korzystania z pełnej funkcjonalności modułu analitycznego należy pozostawić uruchomioną aplikację w tle. Aplikacja uruchomiona w tle będzie skanować otoczenie w poszukiwaniu urządzeń innych użytkowników aplikacji, jak również sama będzie podlegać skanowaniu przez inne urządzenia. Urządzenie użytkownika aplikacji

⁵⁶ Zob. § 3 ust. 1 Regulaminu STOP COVID – ProteGO Safe v. 4.8. Każdy z modułów zdefiniowany jest w § 2 Regulaminu.

⁵⁷ Elektroniczne urządzenie, za pośrednictwem którego użytkownik uzyskuje dostęp do STOP COVID – ProteGO Safe (tablet, smartfon itp.) z aktywnym modułem Bluetooth, systemem Android 5.0 lub wyższym z dostępem do sklepu Google Play albo z systemem iOS w wersji nie niższej niż 13.5 z dostępem do sklepu AppStore. Moduł analityczny będzie działał jedynie w urządzeniach z systemem Android 6.0 wspierających technologię BLE lub wyższym albo z systemem iOS w wersji nie niższej niż 13.5; zob. § 2 pkt 21 Regulaminu STOP COVID – ProteGO Safe v. 4.8.

⁵⁸ Osoba posiadająca pełną zdolność do czynności prawnych, która po zaakceptowaniu Regulaminu i Polityki prywatności korzysta z STOP COVID – ProteGO Safe; zob. § 2 pkt 22 Regulaminu STOP COVID – ProteGO Safe v. 4.8.

zapisuje historię spotykanych urządzeń, na których jest zainstalowana aplikacja. Dane osobowe w postaci historii spotykanych urządzeń pozostają na urządzeniach użytkowników przez 14 dni.

Konsultant Centrum Kontakt⁵⁹, przekazując telefonicznie informację o zarażeniu COVID-19 osobie chorej⁶⁰, zapyta, czy jest ona użytkownikiem ProteGO Safe. Jeżeli osoba chora jest użytkownikiem ProteGO Safe, konsultant Centrum Kontakt zaproponuje wprowadzenie do ProteGO Safe kodu PIN w celu anonimowego potwierdzenia, że urządzenie należy do osoby chorej i zainicjowania procesu przekazania komunikatu o narażeniu na zakażenie innym użytkownikom aplikacji (poprzez przesłanie klucza diagnostycznego). Wprowadzenie kodu PIN inicjuje proces wysłania klucza diagnostycznego na serwer ProteGO Safe, który następnie przekazuje klucz diagnostyczny do urządzeń użytkowników aplikacji⁶¹; na serwer łądowane są wyłącznie dane dotyczące bliskich kontaktów osoby, u której badanie potwierdziło zakażenie COVID-19⁶². Serwer ProteGO Safe to infrastruktura chmurowa utrzymywana przez Operatora Chmury Krajowej służąca do przekazania klucza diagnostycznego do urządzeń użytkowników. Klucze diagnostyczne są przechowywane na serwerze STOP COVID – ProteGO Safe w postaci zaszyfrowanej przez 14 dni⁶³. Kod PIN to generowane losowo i aktywne przez pół godziny alfanumeryczne hasło przekazywane użytkownikowi, który jest osobą chorą, przez konsultanta Centrum Kontakt. Kod PIN może być

⁵⁹ Jednostka powiadamiająca telefonicznie o wyniku testu na COVID-19 oraz przekazująca kod PIN użytkownikom aplikacji i udzielająca informacji związanych z COVID-19; zob. § 2 pkt 3 Regulaminu STOP COVID – ProteGO Safe v. 4.8.

⁶⁰ Osoba fizyczna, posiadająca pełną zdolność do czynności prawnych, która uzyskała pozytywny wynik testu na COVID-19. Osoba chora nie musi być użytkownikiem; zob. § 2 pkt 14 Regulaminu STOP COVID – ProteGO Safe v. 4.8.

⁶¹ Zob. § 3 ust. 3 Regulaminu STOP COVID – ProteGO Safe v. 4.8.

⁶² Zob. P. Litwiński, A. Leńczuk, A. Krzyżak, A. Siwek, *Raport z audytu prywatności aplikacji ProteGO Safe przeprowadzonego na zlecenie Ministerstwa Cyfryzacji*, Barta, Litwiński. Kancelaria Radców Prawnych i Adwokatów Spółka Partnerska, 5.08.2020 r., <https://www.gov.pl/web/protegosafe/dokumenty> [dostęp: 19.09.2021], s. 46.

⁶³ Zob. § 2 pkt 19 Regulaminu STOP COVID – ProteGO Safe v. 4.8.

wprowadzony do ProteGO Safe w celu anonimowego potwierdzenia, że urządzenie należy do osoby chorej i zainicjowania procesu przekazania klucza diagnostycznego do serwera ProteGO Safe⁶⁴. Po otrzymaniu przez urządzenie użytkownika aplikacji klucza diagnostycznego moduł analityczny dokonuje analizy, porównując klucz diagnostyczny z danymi historycznymi dotyczącymi spotkań innych urządzeń z zainstalowaną aplikacją zapisanymi lokalnie na urządzeniu użytkownika w celu oceny ryzyka narażenia na zarażenie COVID-19. Jeśli analiza prawdopodobieństwa zarażenia COVID-19 wykaże wysokie lub średnie ryzyko narażenia na zakażenie COVID-19, status użytkownika w aplikacji zmieni się odpowiednio⁶⁵. Wprowadzenie przez użytkownika kodu PIN do ProteGO Safe jest dobrowolne⁶⁶.

Z analizy wyżej powołanych fragmentów regulaminu ProteGO Safe wynika, że tylko osoby zweryfikowane przez służby medyczne jako chore na COVID-19 mogą zainicjować proces wysyłania swoich kluczy diagnostycznych na serwer ProteGO Safe, aby możliwe było wysłanie ostrzeżenia innym użytkownikom. Konieczne jest bowiem wpisanie do aplikacji ProteGO Safe, zainstalowanej na urządzeniu, kodu PIN, otrzymanego od pracownika Centrum Kontakt. Takie rozwiązanie gwarantuje poprawność danych. Przetwarzanie niepotwierdzonych danych potęgowałoby chaos, gdyż użytkownicy otrzymywaliby fałszywe powiadomienia o możliwym zarażeniu⁶⁷.

Moduł analityczny jest oparty na *Privacy-Preserving Contact Tracing API* wytworzonym oraz udostępnionym przez gigantów technologicznych Google oraz Apple. Informacje generowane przez moduł analityczny wraz z wynikami jego pracy są przechowywane lokalnie na

⁶⁴ Zob. § 2 pkt 8 Regulaminu STOP COVID – ProteGO Safe v. 4.8.

⁶⁵ Zob. § 3 ust. 4 Regulaminu STOP COVID – ProteGO Safe v. 4.8.

⁶⁶ Zob. § 3 ust. 5 Regulaminu STOP COVID – ProteGO Safe v. 4.8.

⁶⁷ Zob. *Technologia w walce z koronawirusem – 7 filarów zaufania*, <https://panoptykon.org/7-filarow-zaufania> [dostęp: 19.09.2021].

urządzeniu przez 14 dni. Google oraz Apple w swojej dokumentacji⁶⁸ zapewniają, że stosują najwyższe standardy bezpieczeństwa, aby chronić anonimowość użytkowników⁶⁹.

Polityka prywatności STOP COVID – ProteGO Safe⁷⁰ w zakresie funkcjonalności i opisu działania modułu analitycznego dodaje, że klucz diagnostyczny wysłany z urządzenia na serwer STOP COVID – ProteGO Safe nie będzie zawierać danych umożliwiających identyfikację ani informacji o urządzeniach, z którymi użytkownik miał styczność. To użytkownik będzie decydować o tym, czy chce oznaczyć swoje urządzenie jako urządzenie osoby chorej, co zainicjuje wysłanie anonimowego klucza diagnostycznego na serwer STOP COVID – ProteGO Safe, a następnie do innych użytkowników aplikacji. Każda z aplikacji po otrzymaniu klucza diagnostycznego dokonuje automatycznej analizy spotkań poprzez odpowiednie porównanie otrzymanego klucza diagnostycznego z historią spotkań urządzeń z zainstalowaną aplikacją z ostatnich 14 dni. Analiza wykonywana jest niezależnie na urządzeniu każdego użytkownika, brana jest w niej pod uwagę w szczególności odległość użytkowników (siła sygnału) oraz czas przebywania w pobliżu osoby zakażonej i w jej wyniku może zostać zmieniony status aktualnej grupy ryzyka.

Z dokumentacji udostępnionej przez Ministerstwo Cyfryzacji na stronie internetowej <https://www.gov.pl/web/protegosafe/dokumenty> wynika, że Minister Cyfryzacji dysponuje informacjami o liczbie przesłanych na serwer ProteGO Safe kluczów diagnostycznych oraz dacie ich wysłania. Znanie Ministrowi Cyfryzacji i Głównemu Inspektorowi Sanitarnemu, który jest administratorem danych osobowych w ramach aplikacji ProteGO Safe, „są dane przetwarzane w aplikacji i związane z wykorzystywaniem serwera zapewniającego przekazywanie Użytkownikom komunikatów,

⁶⁸ <https://www.google.com/covid19/exposurenotifications/> oraz <https://developer.apple.com/documentation/exposurenotification> [dostęp: 17.09.2021].

⁶⁹ Zob. § 2 pkt 11 Regulaminu STOP COVID – ProteGO Safe v. 4.8.

⁷⁰ Polityka prywatności STOP COVID – ProteGO Safe v. 4.8., <https://www.gov.pl/web/protegosafe/dokumenty> [dostęp: 17.09.2021].

jak UID – losowy identyfikator Urządzenia Użytkownika oraz średni czas korzystania z Aplikacji przez Użytkowników (dane statystyczne, których nie można powiązać z poszczególnymi użytkownikami)”⁷¹. Aplikacja ProteGO Safe uzyskuje dostęp do informacji przechowywanych na urządzeniu użytkownika jedynie wtedy, gdy w wyniku odebrania informacji z serwera ProteGO Safe o kluczu diagnostycznym osoby chorej, bazując na wbudowanych skryptach analitycznych, porównuje otrzymany klucz z identyfikatorami kontaktów, które zostały przez nią odnotowane, w celu ustalenia ryzyka⁷². Dane otrzymane od użytkowników z pozytywnym wynikiem testu na obecność COVID-19 są przetwarzane centralnie, a klucz diagnostyczny osoby chorej przechowywany jest na serwerze ProteGO Safe przez okres 14 dni. Dane osobowe użytkownika oraz inne informacje wprowadzone do aplikacji ProteGO Safe przez użytkownika, jak np. dane dotyczące zdrowia, są przechowywane lokalnie, czyli na urządzeniu końcowym użytkownika, i nie są wymieniane z serwerami centralnymi czy urządzeniami końcowymi innych użytkowników. Przyjęto zatem hybrydowy model przechowywania danych, posiadający zarówno element modelu scentralizowanego, jak i zdecentralizowanego. Serwery są odseparowane od siebie – serwer nadający anonimowe identyfikatory urządzenia użytkownika oraz serwer przesyłający klucze diagnostyczne nie są ze sobą połączone. Identyfikacja osób chorych na COVID-19 jest więc niemożliwa z perspektywy aplikacji ProteGO Safe i serwerów ProteGO Safe⁷³. Serwer ProteGO Safe nie umożliwia przechowywania lub połączenia (porównania) identyfikatorów urządzenia użytkownika z kluczami diagnostycznymi.

W zakresie audytowania realizacji zasad *privacy by design* i *privacy by default* w aplikacji ProteGO Safe stwierdzono, że dane nie podlegają

⁷¹ Zob. § 3 ust. 6 pkt 1 Polityki prywatności ProteGO Safe.

⁷² Zob. P. Litwiński, A. Leńczuk, A. Krzyżak, A. Siwek, *Raport...*, s. 19.

⁷³ *Ibidem*, s. 16.

autouzupełnianiu z innych źródeł. Aplikacja nie jest powiązana i nie może zostać sparowana np. z kontami w mediach społecznościowych⁷⁴.

W komunikacji pomiędzy urządzeniami użytkowników przekazywane są dane zakodowane w kluczu diagnostycznym, umożliwiające wskazanie ryzyka transmisji wirusa SARS-CoV-2 od użytkownika, u którego wykryto obecność wirusa lub chorobę COVID-19. Udostępnianiu może podlegać klucz diagnostyczny, zawierający informację o chorym użytkowniku oraz o tymczasowych identyfikatorach jego urządzenia, przy czym sygnał odbierany przez aplikację jest przez nią interpretowany automatycznie, bez wskazywania użytkownikom, które z zarejestrowanych spotkań stanowiło podstawę zagrożenia zakażeniem, zatem nie dochodzi do udostępnienia danych osoby chorej lub innego użytkownika. Dla innych podmiotów, w tym Głównego Inspektora Sanitarnego czy Ministra Cyfryzacji, który zarządza serwerem ProteGO Safe, dane te są anonimowe w rozumieniu art. 11 RODO⁷⁵. Aplikacja ProteGO Safe przechowuje na urządzeniu użytkownika informacje, które można podzielić na dwie grupy: po pierwsze, informacje niezbędne dla zapewnienia funkcjonalności modułu Triażu, dziennika zdrowia i modułu analitycznego; po drugie, informacje niezbędne dla zapewnienia bezpieczeństwa aplikacji i danych w niej zapisanych, w szczególności w zakresie plików *cookies* dostarczonych przez Cloudflare w celu ochrony przed atakami DDOS⁷⁶.

ProteGO Safe gromadzi informacje niezbędne dla zapewnienia możliwości przeprowadzania analiz dotyczących aplikacji, w celu umożliwienia dalszego rozwoju aplikacji i doskonalenia jej, przy zastosowaniu technologii Google Analytics. Wykorzystywana technologia Google Analytics w projekcie ProteGO Safe nie umożliwia analizowania sposobu korzystania z aplikacji, a jedynie daje informacje statystyczne dotyczące liczby pobrań, modeli telefonów (aby efektywniej dobierać

⁷⁴ *Ibidem*, s. 17.

⁷⁵ *Ibidem*, s. 14.

⁷⁶ *Ibidem*, s. 18.

zasoby usług utrzymania w zakresie obsługi błędów) i przybliżonej lokalizacji pobrania (chodzi głównie o kraj pobrania aplikacji)⁷⁷.

Zastanowienia wymagają kwestie, czy dane, którymi dysponuje GIS, można, po pierwsze, zaliczyć do kategorii danych otwartych, czyli informacji sektora publicznego udostępnianych lub przekazywanych w postaci elektronicznej, bezwarunkowo lub z uwzględnieniem warunków, o których mowa w rozdziale 3 u.o.d.p.w.i., kompletnych, aktualnych, w wersji źródłowej, w otwartym i niezastrzeżonym formacie przeznaczonym do odczytu maszynowego, które są przeznaczone do bezpłatnego ponownego wykorzystywania na tych samych zasadach dla każdego użytkownika, bez konieczności potwierdzania tożsamości przez użytkownika, a po drugie – czy GIS ma podstawy prawne do przekazywania tych danych innym podmiotom publicznym w celu realizacji zadań związanych ze zdrowiem publicznym w okresie pandemii COVID-19.

3. Używanie danych z aplikacji śledzących kontakty zakaźne do innych celów niż ostrzeganie osób, które mogły mieć styczność z SARS-CoV-2

Powoływane we wcześniejszej części niniejszego opracowania akty prawne, wytyczne i zalecenia organów UE, jak również Regulamin i Polityka prywatności polskiej aplikacji ProteGO Safe wskazują, że podstawą prawną przetwarzania danych osobowych przez aplikacje mobile śledzące kontakty zakaźne jest niezbędność przetwarzania danych do wykonania zadania realizowanego w interesie publicznym, polegającego na ochronie przed poważnymi, wewnątrz krajowymi, jak i transgranicznymi zagrożeniami zdrowotnymi. Konkretyzując, zadanie to ma na celu zapobieganie, przeciwdziałanie i zwalczanie COVID-19 poprzez umożliwienie poszczególnym osobom fizycznym śledzenia kontaktów

⁷⁷ *Ibidem*.

zakaźnych, powiadamianiu ich o tym, że znalazły się one w bliskiej odległości od osoby, która ostatecznie została uznana za nosiciela wirusa, w celu jak najszybszego przerwania łańcucha zakażenia.

Przypomnieć jednak należy, że w wyniku szukania balansu pomiędzy koniecznością zyskania akceptacji społecznej do używania aplikacji mobilnych śledzących kontakty zakaźne i związanych z tym ochroną danych osobowych oraz prywatności użytkowników a koniecznością opamowywania pandemii COVID-19 organy UE wybrały rozwiązania chroniące dane i prywatność użytkowników, co zdaje się, ograniczyło jednocześnie możliwości wykorzystania tych danych przez organy ds. zdrowia publicznego. Dane, którymi dysponuje polski GIS jako administrator danych osobowych w ramach ProteGO Safe, można określić jako szczątkowe – w porównaniu z tymi, które są (lub mogą być) gromadzone za pomocą tej aplikacji (w zależności od stopnia wykorzystania jej różnych funkcjonalności przez poszczególnych użytkowników). Tymi danymi są: informacje o liczbie przesłanych na serwer ProteGO Safe kluczy diagnostycznych oraz daty ich wysłania, a także dane przetwarzane w aplikacji i związane z wykorzystywaniem serwera zapewniającego przekazywanie użytkownikom komunikatów, jak UID – losowy identyfikator urządzenia użytkownika oraz średni czas korzystania z aplikacji przez użytkowników (dane statystyczne, których nie można powiązać z poszczególnymi użytkownikami)⁷⁸. Bez wątpienia dane te spełniają kryteria definicji pojęcia „informacja sektora publicznego”, zawartej w u.o.d.p.w.i. GIS powinien udostępniać te dane do ponownego wykorzystywania. Obecnie dane dotyczące zarówno liczby wysłanych kluczy z ostatnich 7 dni, jak i od początku funkcjonowania aplikacji są dostępne w trybie bezwnioskowym jedynie w aplikacji ProteGO Safe w zakładce *Home*⁷⁹.

⁷⁸ Zob. § 3 ust. 6 pkt 1 Polityki prywatności ProteGO Safe.

⁷⁹ Nie można ich znaleźć np. na stronie internetowej <https://www.gov.pl/web/protego-safe> czy <https://dane.gov.pl/>. Na stronie <https://dane.gov.pl/pl/application/1244,protego-safe> [dostęp: 19.09.2021] znajduje się tylko opis aplikacji wraz z linkiem do jej pobrania.

Otwarte dane to dane o szczególnym znaczeniu dla rozwoju innowacji w państwie i rozwoju społeczeństwa informacyjnego, wytworzone przez sektor publiczny lub prywatny, działający w celu realizacji zadań publicznych. Jak już wspomniano, pojęcie to zostało zdefiniowane w art. 2 pkt 11 u.o.d.p.w.i. Dane, nawet zanonimizowane, służące ochronie zdrowia publicznego w czasie pandemii wywołanej przez wirus SARS-CoV-2, są danymi o szczególnym znaczeniu i mogą prowadzić do wytworzenia nowych usług⁸⁰. Nieco na marginesie rozważań odnotować należy, że pojęcie „otwartych danych publicznych” zostało po raz pierwszy zdefiniowane przez grupę zwolenników otwartego rządu na spotkaniu w Se wastopolu w Kalifornii w 2007 r. Otwarte dane rządowe (*Open Government Data*) to filozofia, a coraz częściej zbiór polityk, która promuje przejrzystość, odpowiedzialność i tworzenie wartości poprzez udostępnianie wszystkim danych sektora publicznego. W 2007 r. zespół trzydziestu specjalistów z różnych dziedzin zdefiniował także kryteria (warunki) otwartości danych⁸¹. W 2012 r. sformułowana została prosta,

⁸⁰ Byłyby to dane dynamiczne w rozumieniu art. 2 pkt 8 dyrektywy 2019/1024, a więc „dokumenty w formie cyfrowej podlegające częstym aktualizacjom lub aktualizacjom w czasie rzeczywistym, w szczególności ze względu na ich zmienność lub szybką dezaktualizację; dane wygenerowane przez czujniki zasadniczo uznaje się za dane dynamiczne”.

⁸¹ Są nimi: 1) kompletność; 2) źródłowość; 3) aktualność; 4) dostępność niezależna od platformy informatycznej wykorzystywanej przez użytkownika (neutralność technologiczna); 5) przetwarzalność maszynowa (publikowanie w ustrukturyzowany sposób wraz z opisem struktury pliku, np. w formie metadanych); 6) udostępnienie w sposób niedyskryminujący (dostępność dla każdego, bez konieczności rejestracji czy podpisywania umów); 7) otwarty format plików (pełna specyfikacja formatu ma być dostępna za darmo w sieci); 8) dostępność bez ograniczeń licencyjnych (np. prawa autorskiego, patentowego, tajemnicy handlowej); zob. T. Kulsiwicz, *Redukcja pozaprawnych barier ponownego wykorzystywania informacji sektora publicznego*, [w:] A. Piskorz-Ryń (red.), *Jawność i jej ograniczenia*, t. V. *Dostęp i wykorzystywanie*, Warszawa 2015, s. 202. Kryteria podstawowe uzupełnione zostały później przez kilka warunków dodatkowych. Są nimi: wymagania bezpłatnej dostępności *on-line* danych w stałej lokalizacji sieciowej i w stabilnym formacie, opatrzenia danych potwierdzeniami autentyczności i integralności, otwartości z definicji, odpowiedniego udokumentowania, bezpieczeństwa dla użytkowników oraz wykorzystania inicjatyw obywatelskich przy zbieraniu danych i projektowaniu mechanizmów ich udostępniania.

pięciostopniowa skala poziomu otwartości danych, nazwana *5-Star Open Data*⁸². W 2015 r. wydano Międzynarodową kartę otwartych danych⁸³.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024, dotycząca ponownego wykorzystywania informacji sektora publicznego, reguluje także „otwarte dane”, co podkreślono już w jej tytule. Ma to przede wszystkim wymiar aksjologiczny; ponowne wykorzystywanie służy polityce publicznej otwierania danych. Prawodawca UE położył nacisk również na konieczność udostępniania danych w czasie rzeczywistym, w formatach nadających się do maszynowego przetwarzania, co ma służyć rozwijaniu innowacyjnych produktów, usług i aplikacji z wykorzystaniem nowoczesnych technologii, takich jak sztuczna inteligencja czy Internet rzeczy⁸⁴.

Jak już kilkakrotnie wspomniano, GIS nie posiada danych identyfikujących zakażonych użytkowników aplikacji ProteGO Safe, ich wieku, aktualnego samopoczucia zdrowotnego, stanu zdrowia, w tym chorób współistniejących, na które zapadli i które mogą przyczynić się do cięższego przebiegu COVID-19 lub większego ryzyka zgonu na tę chorobę zakaźną, danych adresowych czy lokalizacji użytkowników. Z pomocą danych pozyskanych z polskiej aplikacji nie jest więc możliwe określenie, czy wirus SARS-CoV-2 przenosi się, a jeśli tak, to w jakim stopniu intensywności (jak szybko), na inne grupy wiekowe niż osoby starsze. Dane te albo nie są w ogóle gromadzone (jak np. dane o lokalizacji), albo są przetwarzane na urządzeniu końcowym użytkownika (np. smartfonie), do których GIS ani MC nie mają dostępu. W odniesieniu do danych gromadzonych bezpośrednio z urządzenia końcowego zastosowanie znajduje art. 5 ust. 3 dyrektywy 2002/58. W związku z tym dostęp dostawcy usługi łączności elektronicznej, którym jest Minister Cyfryzacji, do informacji przechowywanej na

⁸² Skala zaproponowana przez Tim Bernersa-Lee dostępna jest na stronie internetowej <http://5stardata.info/en/> [dostęp: 17.09.2021].

⁸³ *International Open Data Charter*, zob. https://opendatacharter.net/wp-content/uploads/2015/10/opendatacharter-charter_F.pdf [dostęp: 19.09.2021].

⁸⁴ Zob. D. Sybilski, *Dane o wysokiej wartości – nowy rodzaj informacji sektora publicznego*, „Informacja w Administracji Publicznej” 2019, Nr 4, s. 11.

urządzeniu końcowym (np. do ankiety samooceny stanu zdrowia w aplikacji ProteGO Safe) jest dozwolony tylko wtedy, gdy użytkownik wyraził na to zgodę lub dostęp jest niezbędny dla usługi społeczeństwa informacyjnego, o którą wyraźnie poprosił. Ograniczenia praw i obowiązków przewidzianych w dyrektywie 2002/58 są co prawda możliwe na mocy jej art. 15, ale może stać się tak jedynie wtedy, jeżeli stanowią one niezbędny, odpowiedni i proporcjonalny środek w ramach społeczeństwa demokratycznego dla osiągnięcia wyraźnie określonych celów⁸⁵. Nie ma zatem podstaw prawnych do dostępu Ministra Cyfryzacji (dostawcą publicznie dostępnej usługi łączności elektronicznej w publicznych sieciach łączności w UE) czy Głównego Inspektora Sanitarnego (administratora danych gromadzonych przez aplikację) do danych przechowywanych na smartfonach użytkowników aplikacji ProteGO Safe. Nie są uprawnione sugestie, jakoby MC czy GIS mogli tymi danymi dysponować bez zgody użytkowników i przekazywać je np. inspekcjom sanitarnym w celu ułatwienia prowadzenia tzw. dochodzeń epidemiologicznych.

Na zagadnienie związane z aplikacjami mobilnymi służącymi do śledzenia kontaktów zakaźnych można bowiem spojrzeć nieco szerzej niż przez pryzmat ostrzegania osób fizycznych (użytkowników aplikacji) o kontakcie z osobą chorą na COVID-19, co jest podstawowym celem aplikacji śledzących kontakty zakaźne. Aplikacje posiadające funkcjonalność samodzielnej diagnozy oraz weryfikacji objawów chorobowych mogłyby dostarczać istotnych informacji na temat liczby osób wykazujących objawy choroby COVID-19, w podziale na wiek i tydzień roku, pochodzących ze ściśle określonych obszarów, na których dana aplikacja jest w powszechnym użyciu (oczywiście gdyby gromadzono dane o lokalizacji użytkowników).

Mimo ograniczonego zakresu gromadzonych danych, zanonimizowane i zagregowane dane pochodzące z aplikacji śledzących kontakty

⁸⁵ Zob. szerzej: W.R. Wiewiórowski, *Rola Unii Europejskiej w koordynacji zastosowania narzędzi informatycznych do walki z pandemią*, „Europejski Przegląd Sądowy” 2020, nr 6, LEX.

zakaźne, w połączeniu np. z informacjami na temat częstości występowania choroby COVID-19, zbieranymi przez organy ds. ochrony zdrowia, chociażby bez użycia narzędzi elektronicznych, hipotetycznie można byłoby wykorzystać, przykładowo, do oceny skuteczności środków społecznych i środków w zakresie ograniczania kontaktów społecznych, wprowadzania ograniczeń związanych z pandemią wirusa SARS-CoV-2 na danym obszarze kraju, a także ustalania zapotrzebowania na środki ochrony indywidualnej czy specjalistyczny sprzęt medyczny i liczby placówek służby zdrowia, które powinny specjalizować się w leczeniu COVID-19 w danym regionie kraju, ale pod warunkami określonymi w art. 6 i art. 9 dyrektywy 2002/58⁸⁶. Dane te hipotetycznie mogłyby być użyte przez inne niż GIS organy sektora publicznego. W takiej sytuacji nie można mówić o „ponownym wykorzystaniu” (ang. *re-use*) informacji. Zgodnie z definicją zawartą w art. 2 pkt 11 dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1024 w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego ponowne wykorzystywanie oznacza wykorzystywanie przez osoby fizyczne lub podmioty prawne dokumentów będących w posiadaniu (m.in.) organów sektora publicznego do celów komercyjnych lub niekomercyjnych innych niż ich pierwotne przeznaczenie w ramach zadań publicznych, dla którego to celu dokumenty te zostały wyprodukowane, z wyjątkiem wymiany dokumentów między organami sektora publicznego służącej wyłącznie wykonywaniu ich zadań publicznych. Ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego zawiera, co oczywiste, podobną w treści definicję⁸⁷. W zakresie definicji ponownego wykorzystywania nie mieści się zatem wykorzystywanie danych zebranych przez aplikację ProteGO Safe i znajdujących się na centralnym serwerze (a nie na urządzeniach końcowych

⁸⁶ Zob. szerzej: W.R. Wiewiórowski, *Rola Unii Europejskiej...*

⁸⁷ Ponowne wykorzystywanie oznacza wykorzystywanie przez użytkowników informacji sektora publicznego w jakimkolwiek celu, z wyjątkiem wymiany informacji sektora publicznego między podmiotami zobowiązanymi wyłącznie w celu realizacji zadań publicznych (art. 2 pkt 12).

użytkowników aplikacji mobilnych) przez organy publiczne zajmujące się np. ochroną zdrowia publicznego. Ponownym wykorzystywaniem byłoby użycie tych danych np. przez podmioty z sektora prywatnego.

Ustalanie kontaktów zakaźnych oznacza, że organy ds. zdrowia publicznego szybko identyfikują wszystkie osoby, z którymi kontaktował się pacjent z pozytywnym wynikiem badania na obecność wirusa SARS-CoV-2, proszą je o pozostanie w domu i szybko badają i izolują te osoby, jeżeli wystąpią u nich objawy. Funkcja śledzenia kontaktów zakaźnych jest więc przydatna zarówno dla jednostek, jak i organów zdrowia publicznego. Może ona również odgrywać ważną rolę w zarządzaniu środkami ograniczającymi rozprzestrzenianie się wirusa w fazie deeskalacji. Jej wpływ można zwiększyć za pomocą strategii wspierającej szerzej zakrojone testowanie osób z łagodnymi objawami COVID-19. Obie te funkcje mogą również stanowić istotne źródło danych dla organów zdrowia publicznego i ułatwić przekazywanie takich danych krajowym organom epidemiologicznym oraz ECDC⁸⁸. Ułatwiłoby to zrozumienie sposobów rozprzestrzeniania się choroby oraz, w połączeniu z wynikami badań, oszacowanie wartości predykcyjnej wyniku dodatniego dla objawów z układu oddechowego w danej społeczności i zapewnienie informacji na temat poziomu występowania wirusa.

Tymczasem ogromna większość dochodzeń epidemiologicznych w Polsce wykonywana jest przez organy do spraw ochrony zdrowia środkami konwencjonalnymi, bez użycia aplikacji mobilnych czy innego rodzaju technologii wspierającej. Opierają się one głównie na relacjach osób zakażonych, które nie zawsze mogą być prawdziwe z powodu ulotności pamięci ludzkiej, jak i intencji zachowania ich w tajemnicy, np. z powodu złamania zakazów przemieszczania się czy udziału w określonych zgromadzeniach. Jak już wielokrotnie wskazywano w niniejszym opracowaniu, aplikacje śledzące kontakty zakaźne nie umożliwiają identyfikacji użytkowników

⁸⁸ Zob. <https://www.ecdc.europa.eu/en> [dostęp: 19.09.2021].

między sobą ani identyfikacji użytkowników, którzy mieli kontakt z osobą zakażoną, przez organy do spraw ochrony zdrowia czy pozostałych użytkowników aplikacji. Rozwiązanie to podyktowane zostało chęcią wzmocnienia zaufania do tego rodzaju aplikacji poprzez zapewnienie wysokiego stopnia ochrony prywatności ich użytkowników. Przypomnieć należy, że w Polsce administratorem danych osobowych, który samodzielnie ustala cele i sposoby przetwarzania danych osobowych w ramach ProteGO Safe, jest Główny Inspektor Sanitarny. Gdyby osoby mające kontakt z osobami zakażonymi, znanymi przecież organom ds. ochrony zdrowia z imienia i nazwiska, również były identyfikowane, przeprowadzanie dochodzeń epidemiologicznych, a w konsekwencji nakładanie obowiązku kwarantanny czy wykonywanie testów na obecność wirusa SARS-CoV-2, byłoby o wiele szybsze i łatwiejsze, a przez to walka z rozpowszechnianiem się COVID-19 stałaby się bardziej skuteczna. Warunkiem takiego założenia jest jednak aktywne korzystanie z aplikacji, aktywowanie modułu analitycznego oraz wpisanie kodu PIN do aplikacji przez znaczną część społeczeństwa, a nie jedynie jego niewielki odsetek⁸⁹, a przede wszystkim – podstawa prawna do korzystania przez dostawcę aplikacji (Ministra Cyfryzacji) – i podmioty, którym przekazywałby dane – z danych zgromadzonych na urządzeniu końcowym użytkownika, czyli zgoda użytkownika. Obecnie użytkownik nawet nie ma możliwości wyrażenia takiej zgody, nie istnieje system przekazywania danych zgromadzonych przy pomocy aplikacji na urządzeniu końcowym do jakiegoś systemu informacyjnego organów ds. ochrony zdrowia.

⁸⁹ Tylko niecałe 2% Polaków zainstalowało do tej pory rządową aplikację do śledzenia kontaktów z osobami zakażonymi koronawirusem; zob. D. Maciejasz, *Polacy nie zaufali rządowej aplikacji do walki z pandemią. A ci, którzy ją mają, nie raportują zakażeń*, „Gazeta Wyborcza” 2.09.2020, <https://wyborcza.pl/7,156282,26260940,aplikacja-tropiaca-wirusa-w-wirtualnym-schowku-polacy-nie-chca.html> [dostęp: 20.09.2021]. Dnia 26.10.2020 r. do Prezesa rady Ministrów wpłynęła interpelacja nr 13367 w sprawie aplikacji ProteGO Safe; do czasu zakończenia prac nad niniejszym opracowaniem nie udzielono odpowiedzi na interpelację; <https://www.sejm.gov.pl/sejm9.nsf/InterpelacjaTresc.xsp?key=BUUE8Y> [dostęp: 20.09.2021].

W przypadku dużej popularności tych aplikacji krajowe organy ds. zdrowia publicznego mogłyby zdecydować się na wykorzystanie zanonimizowanych danych pochodzących z aplikacji do celów nadzoru syndromicznego nad COVID-19 w ramach podstawowej opieki zdrowotnej. Nadzorem syndromicznym (ang. *syndromic surveillance*) jest monitorowanie częstości występowania pojedynczych objawów lub ich zespołów bez odnoszenia ich do specyficznych chorób. Taki system służy do wczesnego wykrywania epidemii (ognisk epidemicznych), szczególnie z wielu źródeł. Jest wprowadzany w przypadkach masowych zgromadzeń lub w stanach zagrożenia bioterrorystycznego⁹⁰.

W przepisach ustawy o PIS nie wskazano, że Główny Inspektor Sanitarny jest zobowiązany do zarządzania aplikacją śledzącą kontakty zakaźne. Spoczywa na nim obowiązek zarządzania systemem wymiany informacji w ramach systemów wymiany informacji, o których mowa w przepisach wykonawczych wydanych na podstawie art. 2 ust. 2 ustawy o PIS, w zakresie dotyczącym zadań PIS. Rozporządzenie Ministra Zdrowia z dnia 17 października 2014 r. w sprawie systemów wymiany informacji w zakresie dotyczącym zadań Państwowej Inspekcji Sanitarnej⁹¹ określa: wykaz systemów wymiany informacji w zakresie dotyczącym zadań PIS (wśród których znajduje się System Nadzoru Epidemiologicznego nad Chorobami Zakaźnymi) oraz zasady zarządzania przez Głównego Inspektora Sanitarnego wymianą informacji.

Główny Inspektor Sanitarny zarządza wymianą informacji w zakresie systemów, którymi zarządza, przez: zbieranie danych, zapewnianie ciągłej, wielostronnej i szybkiej wymiany danych w sposób, który zapewni kompletność i niezbędną jakość informacji, określanie jednolitych zasad oceny ryzyka sanitarnego i epidemiologicznego, organizowanie specjalistycznych

⁹⁰ Zob. A. Zieliński (red.), *Słowniczek terminów epidemiologicznych*, „Przegląd Epidemiologiczny” <http://www.przeglądepidemiol.pzh.gov.pl/słowniczek-terminow-epidemiologicznych> [dostęp: 20.09.2021].

⁹¹ Dz. U. z 2014 r. poz. 1474 ze zm.

szkoleń w zakresie gromadzenia i przetwarzania danych w tych systemach oraz ich obsługi, administrowanie i utrzymywanie centralnych baz danych tych systemów, z wyłączeniem Systemu Wczesnego Ostrzegania o Niebezpiecznej Żywności i Paszach (RASFF) w Polsce. Natomiast w § 2 pkt 10 zd. 2 Regulaminu ProteGO Safe znajduje się następujące postanowienie: „Minister Cyfryzacji w oparciu o porozumienie wspiera GIS w rozwoju i utrzymaniu STOP COVID – ProteGO Safe”. Wydaje się, że biorąc pod uwagę wskazane akty prawne, a więc ustawę o PIS i rozporządzenie Ministra Zdrowia z dnia 17 października 2014 r. w sprawie systemów wymiany informacji w zakresie dotyczącym zadań PIS, obecnie GIS nie ma prawnej podstawy do takiej formy zarządzania aplikacją śledzącą kontakty zakaźne, która obejmuje pobieranie z danych z serwera ProteGO Safe, następnie przekazywanych do innych systemów informacyjnych w celu realizacji zadań PIS, ani do systemów informacyjnych innych organów ds. ochrony zdrowia.

Tymczasem podejście polegające na maksymalnym wykorzystaniu, oczywiście w granicach zakreślonych przez prawo, danych posiadanych przez organy publiczne, jest zgodne z ideą tzw. otwartego rządu. Rząd jest otwarty (*Open Government*), gdy uwalnia technologię i napędza innowacje w granicach dostępnego prawodawstwa i w równowadze z interesem krajowym i publicznym. Podejście otwarte domyślnie (*open by default*) opisuje zakres, w jakim sprawny i proaktywny rząd (czy szerzej – organy administracji publicznej) wykorzystuje i współużytkuje cyfrowe technologie i narzędzia do komunikowania się, angażowania, współpracy i budowania mostów między wszystkimi podmiotami w celu gromadzenia spostrzeżeń w kierunku bardziej opartego na wiedzy sektora publicznego. Obejmuje to nie tylko dostarczanie bodźców do promowania współpracy i innowacji (np. otwarte dane rządowe, *open source*), poszanowanie cyfrowych praw obywateli (np. przepisów dotyczących ochrony danych osobowych, prywatności, bezpieczeństwa, poufności), ale także otwieranie i współtworzenie procesów rządowych (np. cykl życia polityki,

świadczenie usług publicznych i uruchamianie ICT)⁹². Pojęcie „rząd oparty na danych” (*data driven government*) oznacza rząd (czy szerzej – organy administracji publicznej), który zapewnia, że dane sektora publicznego są udostępniane wewnątrz i na zewnątrz sektora publicznego w sposób godny zaufania, z zachowaniem jasnych zasad ochrony, prywatności, bezpieczeństwa i zasad etycznych dla interesu narodowego i publicznego. Aby ułatwić dzielenie się nimi, rządy budują właściwe podstawy, ustanawiając jasne polityki, które mogą pomóc w przystąpieniu do rządu, promując tym samym integrację sektora publicznego. Rządy oparte na danych przełamują silosy polityczne, promując spójność polityk związanych z danymi, w tym w zakresie ochrony danych, otwartych danych i sztucznej inteligencji, zapewniają wiodącą rolę w rozwoju polityk dotyczących danych i budują zarządzanie potrzebne do promowania koordynacji i odpowiedzialności. Obejmują one międzysektorowe standardy danych oraz replikowalne i skalowalne infrastruktury danych, które ułatwiają szybki i bezpieczny dostęp do danych oraz ich wymianę⁹³.

Dyrektywa 2019/1024, zgodnie z brzmieniem jej art. 1 ust. 4, pozostaje bez uszczerbku dla krajowych i unijnych przepisów dotyczących ochrony danych osobowych, w szczególności RODO i dyrektywy 2002/58/WE, a także odpowiadających im przepisów prawa krajowego. Przy podejmowaniu decyzji w sprawie zakresu i warunków ponownego wykorzystywania dokumentów sektora publicznego zawierających dane osobowe, np. w sektorze zdrowia, wymagane może być przeprowadzenie oceny skutków dla ochrony danych zgodnie z art. 35 RODO⁹⁴. Proces otwierania danych publicznych powinien podlegać odpowiednim zasadom także w zakresie ochrony prywatności, przejrzystości, etyki i praw cyfrowych, w tym w przypadkach, gdy informacje zawarte w indywidualnym

⁹² Zob. *OECD Open, Useful and Re-usable data (OURdata) Index: 2019*, <http://www.oecd.org/governance/digital-government/ourdata-index-policy-paper-2020.pdf>, s. 14 [dostęp: 20.09.2021].

⁹³ Zob. *ibidem*, s. 13-14.

⁹⁴ Pkt 53 preambuły dyrektywy 2019/1024.

zbiorze danych samodzielnie nie stwarzają ryzyka identyfikacji lub wskazania osoby fizycznej, natomiast mogą stwarzać takie ryzyko, gdy informacje te są połączone z innymi dostępnymi informacjami.

4. Zdolność aplikacji mobilnych śledzących kontakty zakaźne do transgranicznej wymiany danych

Jednym z czynników warunkujących otwartość danych publicznych jest ich interoperacyjność. Ma ona także zasadnicze znaczenie z punktu widzenia rozprzestrzeniania się wirusa SARS-CoV-2, który nie respektuje granic państwowych. W celu umożliwienia wykrywania bliskich kontaktów między użytkownikami różnych aplikacji służących do ustalania kontaktów zakaźnych (scenariusz, który jest najbardziej prawdopodobny wśród osób przemieszczających się między krajami/regionami) należy zadbać o interoperacyjność między aplikacjami w poszczególnych państwach. Współpraca między nimi, opracowanie, testowanie, wdrażanie i stosowanie interoperacyjnych interfejsów elektronicznych zwiększy wydajność i bezpieczeństwo usług skierowanych na ochronę zdrowia publicznego. Jeżeli osoba zakażona pozostaje w kontakcie z użytkownikiem aplikacji śledzącej kontakty zakaźne z innego państwa, np. członkowskiego UE, powinno być możliwe transgraniczne przekazywanie danych osobowych takiego użytkownika organom ds. zdrowia w jego państwie członkowskim, w zakresie, w jakim jest to absolutnie niezbędne. Krajowe organy ds. zdrowia nadzorujące łańcuchy zakażeń powinny mieć możliwość wymiany z innymi państwami lub regionami interoperacyjnych informacji na temat użytkowników, u których wykryto obecność wirusa, aby móc zaradzić transgranicznym łańcuchom zakażeń.

Pojęcie „interoperacyjność” to w najogólniejszym znaczeniu „zdolność do współdziałania”. Interoperacyjność jest rozumiana na trzech wzajemnie na siebie oddziałujących płaszczyznach: interoperacyjności

organizacyjnej, interoperacyjności informacyjnej oraz interoperacyjności technicznej.

Interoperacyjność organizacyjna oznacza uzyskanie możliwości efektywnego współdziałania podmiotów publicznych, jednostek i przedsiębiorców – co dotyczy zwłaszcza zdolności współdziałania podczas czynności administracyjnych realizowanych przy wsparciu systemów teleinformatycznych. Interoperacyjność informacyjna to zdolność do efektywnej wymiany informacji pomiędzy podmiotami publicznymi, jednostkami i przedsiębiorcami, rozumianej zarówno w wymiarze zgodności syntaktycznej danych (sposobu opisu struktury przesyłanych danych), jak i spójności semantycznej informacji. Syntaktyczna zgodność opisu danych stanowi podstawę dla uzyskania zgodności semantycznej informacji. Uzyskanie pełnej spójności informacyjnej systemów teleinformatycznych pozwoli uniknąć niejednoznaczności interpretacji przesyłanych informacji, co powinno zapewnić wyższy poziom bezpieczeństwa informacyjnego, w tym teleinformatycznego dla systemów teleinformatycznych wykorzystywanych do realizacji zadań publicznych. Interoperacyjność techniczna rozumiana jest w wymiarze technologii wymiany danych pomiędzy systemami teleinformatycznymi administracji publicznej a jednostkami i biznesem. Poziom interoperacyjności technicznej jest zrozumiąły głównie dla programistów⁹⁵.

Interoperacyjność zapewnia szereg konkretnych korzyści: zwiększa elastyczność, umożliwiając „mieszanie i dopasowywanie” komponentów poszczególnych usług publicznych, zwiększa opłacalność, umożliwiając ponowne wykorzystanie istniejących komponentów i możliwości, tworzy wirtualnie zintegrowane systemy, które są łatwiejsze w użyciu w różnych organizacjach i regionach lub krajach, a także ułatwia tworzenie nowych możliwości poprzez komponowanie nowych funkcji z już istniejących.

⁹⁵ Zob. B. Szafranski, G. Bliźniuk, J. Karnowski, Z. Świerczyński, R. Weydman, L. Żurek (red.), *Interoperacyjność i bezpieczeństwo systemów informatycznych administracji publicznej*, Katowice 2006, s. 20-21.

Dokumentem o priorytetowym znaczeniu dla interoperacyjności w UE są Europejskie Ramy Interoperacyjności (*European Interoperability Framework – EIF*). W czerwcu 2002 r., podczas szczytu w Sewilli, przedstawiciele rządów krajów członkowskich UE przyjęli dokument *eEurope Action Plan 2005*⁹⁶, który zobowiązywał kraje członkowskie do przygotowania ram interoperacyjności, umożliwiających dostarczanie paneuropejskich usług *e-Government* obywatelom i przedsiębiorcom. W lipcu 2003 r. uznano, że założenia Europejskich Ram Interoperacyjności stanowią kluczowy element rozwoju usług e-Administracji w Europie. Pierwsza wersja EIF została wydana w listopadzie 2004 r. w ramach programu *Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens (IDABC)*⁹⁷. Zalecano w nich rządów państw członkowskich tworzenie krajowych ram interoperacyjności w spójności z EIF, aby umożliwić interoperacyjność wspólnotową. Od grudnia 2009 r. prace nad EIF były kontynuowane w ramach programu *Interoperability Solutions for European Public Administrations (ISA)*⁹⁸. W 2017 r. program ten został zastąpiony, poprzez Komunikat Komisji z dnia 23 marca 2017 r. do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, *Europejskimi Ramami Interoperacyjności – strategią wdrażania*⁹⁹, czyli tzw. Nowymi Europejskimi Ramami Interoperacyjności.

⁹⁶ <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2002:0263:FIN:EN:PDF> [dostęp: 19.09.2021].

⁹⁷ Zob. <https://wayback.archive-it.org/12090/20200210174143/https://ec.europa.eu/idabc/> [dostęp: 19.09.2021].

⁹⁸ Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z 16.12.2010 r. *W kierunku interoperacyjności europejskich usług użyteczności publicznej*, COM/2010/0744 final, https://eur-lex.europa.eu/resource.html?uri=cellar:f132547a-7d66-4626-8eb6-9f7428394de7.0022.03/DOC_1&format=PDF [dostęp: 19.09.2021].

⁹⁹ COM(2017) 134 final, <https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52017DC0134&from=PL> [dostęp: 19.09.2021].

Regulują one przede wszystkim sposób, w jaki zasady i modele interoperacyjności powinny być stosowane w praktyce. Zaktualizowane zalecenia dotyczące interoperacyjności zostały uściślone, położono większy nacisk na otwartość i zarządzanie informacjami, przenoszenie danych, zarządzanie interoperacyjnością i zintegrowane świadczenie usług. Ważniejsze rekomendacje Nowych Europejskich Ram Interoperacyjności dotyczą przede wszystkim: dostępności – oznaczającej wielokanałowe udostępnienie treści w formie zrozumiałej dla użytkowników, wielojęzyczności – udostępniania treści nie tylko w językach narodowych, bezpieczeństwa – dostosowanego do poziomu paneuropejskiego, prywatności, w tym ochrony danych osobowych, subsydiarności – EIF działa pomocniczo i nie wnika w działania wewnątrznarodowe, stosowania otwartych standardów, preferowania oprogramowania o otwartym kodzie źródłowym, tworzenia rozwiązań wielostronnych, pochodzących z różnych źródeł i od różnych dostawców. Szczególnie duży nacisk w Europejskich Ramach Interoperacyjności kładzie się na realizowanie ich założeń przez wybieranie w projektach *e-Government* otwartych standardów oraz wolnego oprogramowania o otwartym kodzie źródłowym¹⁰⁰.

Zgodnie z treścią zaleceń Sieci e-Zdrowie z 15.04.2015 r.¹⁰¹ funkcjonowanie aplikacji śledzących kontakty zakaźne powinno spełniać wymagania interoperacyjności, sprecyzowane w *eHealth Interoperability Framework* z 23.11.2015 r.¹⁰² Ramy te są zatwierdzone przez Sieć

¹⁰⁰ Według Europejskich Ram Interoperacyjności otwarte standardy powinny charakteryzować się następującymi cechami: zostały przyjęte przez organizację *not-for-profit*, a ich rozwój będzie opierał się na otwartej procedurze decyzyjnej dostępnej dla każdej zainteresowanej strony, zostały opublikowane, a opłaty za korzystanie ze standardu są niskie i nie stanowią bariery w dostępie do standardu, własność intelektualna standardu lub jego części udostępniona jest bez pobierania dodatkowych opłat, a sposób udostępnienia nie może być zmieniony, nie ma żadnych ograniczeń w ponownym wykorzystaniu standardu.

¹⁰¹ Zob. *Mobile applications to support contact tracing in the EU's fight against COVID-19 Common EU Toolbox for Member States* z 15.04.2020 r., https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf [dostęp: 19.09.2021].

¹⁰² https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20151123_co03_en.pdf [dostęp: 19.09.2021].

e-Zdrowie i składają się z następujących warstw: prawnej i regulacyjnej; organizacyjnej (polityka i proces opieki); semantycznej (dane i informacje); technicznej (aplikacje i infrastruktura)¹⁰³. Przykładowo zalecenie IOP-04 stanowi, że organy zdrowia publicznego powinny uzgodnić protokoły wymiany informacji o łańcuchach transgranicznych kontaktów, zwłaszcza o zarażonych mających kontakt z osobami z innych państw. Nie należy oczywiście zapominać o podstawach prawnych przekazywania danych, w tym danych osobowych i danych osobowych dotyczących zdrowia, pomiędzy różnymi systemami informacyjnymi czy podmiotami. Stworzenie możliwości wymiany danych na poszczególnych poziomach interoperacyjności (organizacyjnej, informacyjnej i technicznej) nie warunkuje legalności tego procesu.

Wytyczne dotyczące interoperacyjności dla zatwierdzonych aplikacji mobilnych do śledzenia kontaktów w UE, przyjęte przez Sieć e-Zdrowie w dniu 13 maja 2020 r.¹⁰⁴, opisują interoperacyjność aplikacji mobilnych służących do śledzenia kontaktów i związanych z nimi procedur jako ich zdolności do wymiany między sobą minimum informacji niezbędnych do ostrzeżenia poszczególnych użytkowników aplikacji, bez względu na to, gdzie się znajdują w UE, zgodnie z procedurami określonymi przez organy zdrowia publicznego, jeżeli znajdował się w pobliżu innego użytkownika, który powiadomił aplikację, że przeszedł pozytywne testy na obecność COVID-19¹⁰⁵. Wytyczne dotyczące interoperacyjności dla zatwierdzonych aplikacji mobilnych do śledzenia kontaktów w UE określają ponadto, że ostrzeżenie i działania następcze powinny być zgodne z procedurami określonymi przez organy zdrowia publicznego, z oceną potencjalnego wpływu na prywatność i bezpieczeństwo oraz z zastosowaniem odpowiednich zabezpieczeń. Po wdrożeniu odpowiednich

¹⁰³ Zalecenie nr IOP-01.

¹⁰⁴ Zob. *eHealth Network Interoperability guidelines for approved contact tracing mobile applications in the EU*, https://ec.europa.eu/health/sites/health/files/chealth/docs/contact-tracing_mobileapps_guidelines_en.pdf [dostęp: 20.09.2021].

¹⁰⁵ Zob. *eHealth Network Interoperability...*, s. 5.

rozwiązań technicznych aplikacje krajowe będą działać bezproblemowo, gdy użytkownicy będą podróżować do innego uczestniczącego państwa członkowskiego. Osoba podróżująca do innego kraju członkowskiego nie będzie zatem zmuszona do instalacji kolejnej aplikacji śledzącej kontakty zakaźne. Wytyczne dotyczące interoperacyjności aplikacji śledzących kontakty zakaźne mają charakter niewiążący, są one często w doktrynie określane mianem „prawa miękkiego”.

Postanowienia dotyczące interoperacyjności znajdują się także w Regulaminie ProteGO Safe. Zgodnie z brzmieniem jego § 2 pkt 6 poprzez „Interoperacyjność lub Ostrzeganie w Europie” rozumie się funkcjonalność ProteGO Safe umożliwiającą wymianę kluczy pomiędzy użytkownikiem a użytkownikami innych aplikacji mobilnych, podobnych do ProteGO Safe, które są wspierane przez inne państwa członkowskie UE i współpracują w ramach bramy federacyjnej (o której za chwilę będzie mowa). Dzięki interoperacyjności użytkownicy mogą otrzymać informację o potencjalnym narażeniu na zakażenie w związku z potencjalnym kontaktem z użytkownikami innych aplikacji mobilnych, podobnych do ProteGO Safe. Z kolei § 3 pkt 7 Regulaminu ProteGO Safe stanowi, że Interoperacyjność (Ostrzeganie w Europie) ma charakter dobrowolny. Interoperacyjność (Ostrzeganie w Europie) jest świadczona za pośrednictwem bramy federacyjnej. W celu skutecznego korzystania z Interoperacyjności należy wyrazić odpowiednią zgodę w aplikacji. Zgoda wyrażona przez użytkownika dotyczy wysyłania i odbierania kluczy w stosunku do wszystkich aplikacji mobilnych, podobnych do ProteGO Safe. Zgodę można w każdej chwili wycofać, bez wpływu na wysłane i odebrane klucze, które zostały wysłane lub odebrane przed cofnięciem zgody. Po wyrażeniu zgody klucze wysyłane są do aplikacji podobnych do ProteGO Safe. Historia spotykanych urządzeń, na których jest zainstalowana aplikacja podobna do ProteGO Safe, będzie przechowywana w bramie federacyjnej przez 14 dni. Nie są oczywiście wymieniane dane identyfikujące użytkowników aplikacji czy dane dotyczące ich stanu zdrowia, nawet jeśli zostały przez użytkowników

wprowadzone do aplikacji. Tego rodzaju dane są przechowywane lokalnie, na urządzeniach końcowych użytkowników.

Komisja wspiera prace państw członkowskich nad rozszerzeniem interoperacyjności również na scentralizowane aplikacje do śledzenia. Aby wesprzeć dalsze usprawnianie systemu, Komisja stworzyła usługę bramy, czyli interfejs umożliwiający wydajne odbieranie i przekazywanie odpowiednich informacji między krajowymi aplikacjami do śledzenia kontaktów i serwerami¹⁰⁶.

W kwietniu 2020 r. KE ogłosiła zamówienie na utworzenie, utrzymanie i funkcjonowanie środowiska współpracy wspierającego ocenę techniczną technologii proponowanych do zwalczania COVID-19 pod względem ich skuteczności, bezpieczeństwa, prywatności, dostępności i interoperacyjności oraz dostosowania do zestawu narzędzi UE. W wyniku tego zamówienia w maju 2020 r. utworzono punkt przeglądu technicznego (reviewfacility.eu)¹⁰⁷.

Decyzja Wykonawcza Komisji (UE) 2020/1023 z dnia 15 lipca 2020 r. zmieniająca decyzję wykonawczą (UE) 2019/1765 w zakresie transgranicznej wymiany danych między krajowymi aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania w związku ze zwalczaniem pandemii COVID-19¹⁰⁸ wprowadziła do regulacji prawnych pojęcie bramy federacyjnej (*Federation Gateway*), czyli bramy sieciowej obsługiwanej przez Komisję za pomocą bezpiecznego narzędzia IT, która służy do odbierania, przechowywania i udostępniania minimalnego zbioru danych osobowych między serwerami wewnętrznymi państw członkowskich w celu zapewnienia interoperacyjności krajowych aplikacji mobilnych służących

¹⁰⁶ Zob. *Mobile applications to support contact tracing in the EU's fight against COVID-19. Progress reporting June 2020*.

¹⁰⁷ Zob. <https://reviewfacility.eu/xwiki/bin/view/Utilities/ProjectFeatureMatrix/> [dostęp: 17.09.2021].

¹⁰⁸ Dz. Urz. UE L 227 I z 16.07.2020 r., s. 1.

do ustalania kontaktów zakaźnych i ostrzegania¹⁰⁹. *European Proximity Tracing – An Interoperability Architecture for contact tracing and warning apps* z 2.09.2020 r.¹¹⁰ to dokument, w którym zaproponowano gotową do wdrożenia architekturę usługi bramy federacyjnej. Przystąpienie państw członkowskich do usługi Europejskiej Bramy Federacyjnej wymagało odpowiedniego poziomu zaufania i zwrócenia dużej uwagi na bezpieczeństwo, integralność i autentyczność dalszej wymiany danych¹¹¹. Usługa bramy federacyjnej jest najmniej złożonym i najbardziej niezawodnym sposobem połączenia zaplecza wszystkich różnych krajowych aplikacji do śledzenia zbliżeniowego kontaktów zakaźnych. Brama federacyjna akceptuje klucze diagnostyczne ze wszystkich krajów, buforuje je tymczasowo i udostępnia je do pobrania dla wszystkich krajów. Ponadto wszystkie *backendy* mogą być natychmiast informowane, jeśli dostępne są nowe dane, dzięki czemu opóźnienia transmisji są minimalne.

Na mocy powoływanej decyzji wykonawczej nr 2020/1023 Sieć e-Zdrowie zyskała także nowy obowiązek, a mianowicie zapewnienia państwom członkowskim wytycznych dotyczących transgranicznej wymiany danych osobowych za pośrednictwem bramy federacyjnej między krajowymi aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania¹¹². Dodano przepisy dotyczące transgranicznej

¹⁰⁹ Zgodnie z § 2 pkt 2 Regulaminu ProteGO Safe v. 4.8. Brama federacyjna to brama sieciowa obsługiwana przez Komisję Europejską za pomocą bezpiecznego narzędzia IT, która służy do odbierania, przechowywania i udostępniania minimalnego zbioru danych osobowych między serwerami wewnętrznymi państw członkowskich UE w celu zapewnienia interoperacyjności krajowych aplikacji mobilnych służących do ustalania kontaktów zakaźnych i ostrzegania. Brama federacyjna umożliwia Interoperacyjność. Dzięki bramie federacyjnej możliwe jest wysyłanie oraz odbieranie kluczy pomiędzy użytkownikiem a użytkownikami innych aplikacji mobilnych, podobnych do ProteGO Safe. Klucze wysyłane są za pośrednictwem bramy federacyjnej, a okres przechowywania kluczy wynosi 14 dni.

¹¹⁰ https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interop_architecture_en.pdf [dostęp: 19.09.2021].

¹¹¹ Zob. *European Interoperability Certificate Governance – A Security Architecture for contact tracing and warning apps* z 2.09.2020 r., https://ec.europa.eu/health/sites/health/files/ehealth/docs/mobileapps_interop_certificate_governance_en.pdf [dostęp: 19.09.2021].

¹¹² Zob. art. 4 ust. 1 lit. h.

wymiany danych między krajowymi aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania za pośrednictwem bramy federacyjnej (art. 7a). Jeżeli dane osobowe są wymieniane za pośrednictwem bramy federacyjnej, przetwarzanie ogranicza się do celów dotyczących ułatwienia interoperacyjności krajowych aplikacji mobilnych służących do ustalania kontaktów zakaźnych i ostrzegania w ramach bramy federacyjnej oraz zapewnienia ciągłości procesu ustalania kontaktów zakaźnych w kontekście transgranicznym. Dane osobowe, o których mowa, są przekazywane do bramy federacyjnej jako dane spseudonimizowane. Pseudonimiczne dane osobowe wymieniane oraz przetwarzane za pośrednictwem bramy federacyjnej obejmują jedynie następujące informacje: klucze przekazane przez krajowe aplikacje mobilne służące do ustalania kontaktów zakaźnych i ostrzegania w okresie do 14 dni poprzedzających datę przesłania kluczy; dane dziennika dotyczące kluczy zgodnie z protokołem specyfikacji technicznych stosowanym w państwie pochodzenia kluczy; weryfikację zakażenia; państwa będące przedmiotem zainteresowania oraz państwo pochodzenia kluczy¹¹³.

Wyznaczone organy krajowe lub organy rządowe przetwarzające dane osobowe za pośrednictwem bramy federacyjnej są współadministratorami danych przetwarzanych za pośrednictwem bramy federacyjnej. Podział odpowiednich obowiązków między współadministratorami przebiega zgodnie z załącznikiem II decyzji wykonawczej (UE) 2019/1765 (dodany na mocy decyzji wykonawczej nr 2020/1023). Każde państwo członkowskie, które chce uczestniczyć w transgranicznej wymianie danych między krajowymi aplikacjami mobilnymi służącymi do ustalania kontaktów zakaźnych i ostrzegania, przed przystąpieniem zawiadamia Komisję o swoim zamiarze i wskazuje organ krajowy lub organ rządowy

¹¹³ Dnia 14.09.2020 r. rozpoczęto testowanie infrastruktury bramy federacyjnej. Komisja rozpoczęła testy między serwerami zaplecza oficjalnych aplikacji z Czech, Danii, Niemiec, Irlandii, Włoch i Łotwy a nowo utworzonym serwerem bramy; zob. *Coronavirus: Commission starts testing interoperability gateway service for national contact tracing and warning apps*, https://ec.europa.eu/commission/presscorner/detail/en/IP_20_1606 [dostęp: 19.09.2021].

wyznaczony jako odpowiedzialny administrator. Komisja Europejska jest podmiotem przetwarzającym dane osobowe, które podlegają przetwarzaniu za pośrednictwem bramy federacyjnej. Do kompetencji Komisji jako podmiotu przetwarzającego należy zapewnienie bezpieczeństwa przetwarzania – w tym przesyłu i przechowywania – danych osobowych w ramach bramy federacyjnej oraz wypełnianie obowiązków podmiotu przetwarzającego określonych w załączniku III. Skuteczność środków technicznych i organizacyjnych mających na celu zapewnienie bezpieczeństwa przetwarzania danych osobowych za pośrednictwem bramy federacyjnej jest regularnie sprawdzana i oceniana przez Komisję oraz przez organy krajowe upoważnione do dostępu do bramy federacyjnej. Bez uszczerbku dla decyzji współadministratorów o zakończeniu przetwarzania za pośrednictwem bramy federacyjnej brama federacyjna ulega dezaktywacji najpóźniej 14 dni po zakończeniu przekazywania kluczy za jej pośrednictwem przez wszystkie połączone krajowe aplikacje mobilne służące do ustalania kontaktów zakaźnych i ostrzegania.

Nieco upraszczając, można podsumować, że interoperacyjność jest do pewnego stopnia czynnikiem zagrażającym bezpieczeństwu teleinformatycznemu, ponieważ automatyzuje wymianę informacji przez nowe, wspólne kanały dystrybucji o różnym stopniu ochrony¹¹⁴. Uznając jednakże prymat interoperacyjności, trzeba stwierdzić, że warunkiem budowy i wdrożenia systemów interoperacyjnych jest skuteczne zagwarantowanie wymaganych rygorów bezpieczeństwa informacji w nich przetwarzanych. Z tego powodu ramy interoperacyjności muszą uwzględniać względy bezpieczeństwa, a także ochronę danych osobowych i prywatności.

¹¹⁴ Zob. B. Szafrński [et al.] (red.), *Interoperacyjność i bezpieczeństwo...*, s. 56.

5. Interoperacyjność aplikacji mobilnych śledzących kontakty zakaźne a prawo do ochrony danych osobowych i prawo do prywatności

Zdaniem Europejskiej Rady Ochrony Danych (dalej jako: EROD) umożliwienie udostępniania danych o osobach, które zostały zdiagnozowane lub pozytywnie przebadane („dane o infekcji”) za pomocą interoperacyjnych aplikacji śledzących kontakty zakaźne, powinno być uruchamiane tylko przez dobrowolne działanie użytkownika i tak się właśnie dzieje. Osoby, których dane dotyczą, muszą mieć kontrolę nad swoimi danymi. Cel, jakim jest interoperacyjność, nie powinien być używany jako argument do rozszerzenia gromadzenia danych osobowych¹¹⁵.

Zapewnienie interoperacyjności różnych wdrożeń jest technicznie trudne i może wymagać znacznych nakładów finansowych i inżynierskich. Aby zapewnić minimalną wymianę i przetwarzanie danych zgodnie z wymogami RODO, twórcy aplikacji do śledzenia kontaktów zakaźnych musieli uzgodnić wspólny protokół i kompatybilne struktury danych. Zatem w przypadku aplikacji, które już mają wspólne ramy lub przynajmniej tę samą podstawę technologiczną, cel interoperacyjności mógł być łatwiejszy do osiągnięcia niż w przypadku tych, które ich nie miały. W rzeczywistości, ze względu na różnice między podejściami, w praktyce może okazać się niemożliwe wdrożenie interoperacyjności bez nieproporcjonalnych kompromisów.

Interoperacyjność doprowadzi do dodatkowego przetwarzania i ujawnienia niektórych danych dodatkowym podmiotom. W tym miejscu opracowania należałoby odwołać się do polskiej aplikacji, a konkretnie do rodzaju danych, jakie ona przetwarza. Jak zawsze osoby, których dane dotyczą, muszą zostać poinformowane o każdym dodatkowym przetwarzaniu ich

¹¹⁵ Zob. *Statement of EDPB on the data protection impact of the interoperability of contact tracing apps* Adopted on 16 June 2020, https://edpb.europa.eu/sites/default/files/files/file1/edpb_statementinteroperabilitycontacttracingapps_en_0.pdf, s. 2 [dostęp: 10.05.2022].

danych osobowych oraz o stronach zaangażowanych w ich przetwarzanie¹¹⁶. Użytkownicy powinni zawsze dobrze rozumieć, na czym polega korzystanie z aplikacji i powinni zachować kontrolę nad swoimi danymi. Najpóźniej w momencie uzyskania danych osobowych przez administratora (administratorów) osoba, której dane dotyczą, musi otrzymać jasne informacje o dodatkowym przetwarzaniu związanym z wykorzystaniem interoperacyjności. W tym miejscu należy poinformować użytkownika o warunkach i zakresie przetwarzania danych. Nadal obowiązują standardowe zasady dotyczące przejrzystości; informacje powinny być podane jasnym i prostym językiem. Obejmuje to informacje o tym, jak udostępnione dane będą przetwarzane przez odbierającą interoperacyjną aplikację do śledzenia kontaktów.

Najważniejsze dla tematyki interoperacyjności w kontekście ochrony danych osobowych i prywatności jest Oświadczenie EROD w sprawie interoperacyjności aplikacji służących do ustalania kontaktów zakaźnych, przyjęte w dniu 16 czerwca 2020 r. Poniżej pokrótce zostaną przedstawione jego postanowienia.

Nadal mają zastosowanie te same podstawy prawne, o których mowa w wytycznych EROD nr 04/2020. W przypadku wyrażenia zgody konieczne będzie zebranie dodatkowej zgody na przetwarzanie interoperacyjne spełniające wszystkie jego wymagania. W szczególności cel przetwarzania musi być konkretny, a zatem wystarczająco szczegółowy. Jeżeli różni administratorzy danych w aplikacjach służących do śledzenia kontaktów korzystają z różnych podstaw prawnych, mogą być wymagane dodatkowe środki w celu realizacji praw osoby, której dane dotyczą, związanych z podstawą prawną. W przypadku danych dotyczących

¹¹⁶ Obowiązek informacyjny wynika z art. 13 RODO, w przypadku gdy administrator pozyskuje dane od osoby, której dane dotyczą, i z art. 14 RODO, jeśli pozyskał dane w sposób inny niż od osoby, której dane dotyczą; zob. szer. np. J. Łuczak, komentarz do art. 13, [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie...*, s. 477 i n.; P. Litwiński, P. Barta, M. Kawecki, komentarz do art. 13, [w:] P. Litwiński (red.), *Rozporządzenie UE...*, s. 361 i n.

zdrowia stosuje się art. 9 RODO, więc administratorzy będą musieli polegać na jednym z wymienionych w tym przepisie wyjątków dopuszczających przetwarzanie szczególnych kategorii danych osobowych.

W opinii EROD każda operacja lub zestaw operacji, których celem jest zapewnienie interoperacyjności oprócz przetwarzania pod kątem funkcjonalności aplikacji na poziomie państwa członkowskiego, musi być oceniana oddzielnie od wcześniejszych lub późniejszych operacji przetwarzania ze względu na dodatkowy cel przetwarzania danych. Dlatego dodatkowe przetwarzanie należy postrzegać jako oddzielne przetwarzanie. W przypadku tej oddzielnej operacji przetwarzania stronami mogą być indywidualni administratorzy lub współadministratorzy, którzy mogą korzystać z podmiotów przetwarzających. Jakikolwiek dalsze przetwarzanie podejmowane po wymianie identyfikatorów (obliczanie ryzyka narażenia na zakażenie, powiadamianie o zidentyfikowanych kontaktach itp.) odbywałoby się w ramach odrębnego administrowania przez otrzymującego dostawcę aplikacji.

Konieczne będzie określenie odpowiednich ról, relacji i obowiązków współadministratorów w odniesieniu do osoby, której dane dotyczą, a następnie informacje te powinny zostać udostępnione osobie, której dane dotyczą. Będzie to miało wpływ na zakres oceny skutków dla ochrony danych, która musi być wykonywana, w tym przetwarzanie do celów interoperacyjności. Przetwarzanie w celu zapewnienia interoperacyjności może zostać powierzone podmiotowi przetwarzającemu, który spełnia warunki art. 28 RODO.

Każde rozwiązanie interoperacyjne musi ułatwiać osobom, których dane dotyczą, wykonywanie ich praw. Tam, gdzie wykonanie praw jest możliwe, nie powinno stać się bardziej uciążliwe dla osób, których dane dotyczą i powinno być jasne, do kogo osoby, których dane dotyczą, powinny się zwrócić, aby skorzystać ze swoich praw. Ograniczenia w wykonywaniu praw osoby, której dane dotyczą, są możliwe na podstawie wyjątków określonych w art. 119 i art. 23 RODO.

Interoperacyjność nie powinna prowadzić do zwiększonego gromadzenia informacji z powodu braku skoordynowanego podejścia. Należy to jasno przekazać użytkownikowi przed udostępnieniem danych. Interoperacyjność nie powinna prowadzić również do obniżenia bezpieczeństwa danych i ochrony danych osobowych.

EROD zaleca, aby dostawcy aplikacji służących do śledzenia kontaktów zakaźnych wzięli pod uwagę każdy wzrost zagrożeń bezpieczeństwa informacji spowodowany dodatkowym przetwarzaniem i zaangażowaniem dodatkowych podmiotów. Dotyczy to w szczególności bezpieczeństwa przesyłanych danych w celu ewentualnego połączenia między serwerami. W szczególności środki dotyczące zagrożeń bezpieczeństwa związanych z interoperacyjnością, które mają wpływ na prawa i wolności osób fizycznych, muszą zostać uwzględnione w ocenie skutków dla ochrony danych.

Kiedy dostawcy rozważają, w jaki sposób zapewnić interoperacyjność swoich aplikacji do śledzenia kontaktów, powinni w miarę możliwości zapewnić, że nie prowadzi to do obniżenia poziomu jakości lub dokładności danych. Interoperacyjność w przypadku dużych rozbieżności może prowadzić do utraty jakości danych (np. błędne wnioski z oceny ryzyka narażenia na zakażenie wirusem SARS-CoV-2 powodujące nieproporcjonalnie niskie przypisanie oceny ryzyka), co może prowadzić do wzrostu fałszywie pozytywnych wyników. Te dodatkowe zagrożenia dla dokładności danych będą musiały zostać jasno przekazane osobom, których dane dotyczą. Środki wprowadzone w celu zapewnienia dokładności danych muszą zostać utrzymane w systemie interoperacyjnym.

Stworzenie interoperacyjnej sieci aplikacji nie jest trywialne. Choć może to zwiększyć ich skuteczność, może również wymagać poważnych zmian w aplikacjach już istniejących lub opracowywanych. Z punktu widzenia ochrony danych interoperacyjność jest możliwa, jeśli przestrzegane są zalecenia zawarte w Wytocznych EROD nr 04/2020. Przekazywanie informacji i kontroli osobom, których dane dotyczą, zwiększy ich zaufanie do rozwiązań i ich potencjalnego wykorzystania.

6. Wnioski

Przetwarzanie danych dotyczących zdrowia jest co do zasady zabronione, z wyjątkami wynikającymi z art. 9 RODO. Jednym z nich jest niezbędność przetwarzania takich danych ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, przewidujących odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową¹¹⁷. Aplikacje śledzące kontakty zakaźne, spełniające warunki określone w licznych unijnych aktach prawnych, wytycznych i zaleceniach im poświęconych, nie zostały przewidziane jako instrumenty obowiązkowe dla społeczeństwa; ich używanie opiera się na zasadzie dobrowolności. Ponadto nie wymieniają one z serwerami centralnymi, w tym obsługującymi wymianę danych ponad granicami państw, danych osobowych umożliwiających identyfikację użytkowników i w ogóle nie gromadzą danych o ich lokalizacji – co zapewnia wysoki stopień ochrony danych osobowych i prywatności, a w konsekwencji zmierzać ma do wysokiego zaufania społecznego do tego narzędzia. Wiele danych osobowych, w tym danych dotyczących zdrowia użytkowników aplikacji mobilnych śledzących kontakty zakaźne, przechowywanych jest lokalnie, na urządzeniach końcowych tychże użytkowników, do których dostawca aplikacji mógłby mieć dostęp jedynie pod warunkami określonymi w dyrektywie 2002/58, do czego obecnie nie ma podstaw prawnych w prawie krajowym.

Wobec faktu, że wirus SARS-CoV-2 nadal się rozprzestrzenia, być może należy rozważyć dwie podstawowe kwestie dotyczące tzw. krajowych

¹¹⁷ Zob. art. 9 ust. 2 lit. i RODO.

aplikacji mobilnych śledzących kontakty zakaźne. Po pierwsze – czy celowe byłoby identyfikowanie przez organy ds. ochrony zdrowia osób, które poprzez taką aplikację zostały powiadomione o tym, że miały styczność z osobą zakażoną wirusem SARS-CoV-2 w celu skierowania ich na kwarantannę? Przy pozytywnej ocenie takiego rozwiązania należałoby liczyć się z jeszcze bardziej poważnym spadkiem akceptacji społecznej dla używania aplikacji śledzącej kontakty zakaźne (przy założeniu, że nadal jej używanie będzie dobrowolne). Po drugie, czy administrator danych osobowych przetwarzanych przez aplikację mobilną nie powinien móc w sposób zgodny z prawem (a więc wymagana byłaby zmiana prawa w tym zakresie) wykorzystać tych danych do celów nadzoru epidemiologicznego, łącznie z ich ujawnieniem w odpowiednich systemach informatycznych, którymi zarządza? Obecnie dane takie jak wiek użytkownika aplikacji (określony w przedziałach) czy choroby współistniejące, na które cierpi użytkownik, są przechowywane wyłącznie na urządzeniu użytkownika i organy ds. ochrony zdrowia nie mają do nich dostępu. Działanie związane z użyciem danych zebranych przez aplikację mobilną w innych systemach (tele)informatycznych także jest interoperacyjnością i należy je wiązać z koncepcją tzw. otwartego rządu. Otwarty rząd to nie tylko struktury zbudowane i działające w sposób transparentny, lecz dzielące się danymi z obywatelami i innymi strukturami państwa i samorządu. O interoperacyjności czy organach administracji publicznej opartych na danych należy bowiem mówić nie tylko w kontekście wymiany danych poza granicami kraju, ale także w sytuacjach wewnątrz krajowych. Podjęcie decyzji w przedmiocie dysponowania danymi użytkowników aplikacji śledzących kontakty zakaźne wymagałoby przeprowadzenia oceny skutków dla ochrony danych i oceny skutków dla ochrony prywatności.

Podsumowując, należy stwierdzić, że dane użytkowników urządzeń wygenerowane przez aplikacje śledzące kontakty zakaźne, takie jak ilość kluczy diagnostycznych przesłanych na serwer centralny i daty ich wysłania, stanowią informacje sektora publicznego, ponieważ zostały zebrane

podczas wykonywania zadania publicznego związanego z ochroną zdrowia publicznego i znajdują się w dyspozycji podmiotu zobowiązanego do udostępniania lub przekazywania informacji sektora publicznego w celu ponownego wykorzystywania, zgodnie z art. 3 u.o.d.p.w.i. Powinny one podlegać ponownemu użyciu, zwłaszcza w celu koordynacji systemu ochrony zdrowia, łącznie z ich ujawnieniem w odpowiednich systemach informacyjnych, którymi zarządza GIS. Warto także rozważyć identyfikację osób, które miały kontakt z osobą zakażoną wirusem SARS-CoV-2 i korzystającą z aplikacji mobilnych śledzących kontakty zakaźne. Dane pozwalające ustalić tożsamość osób „z kontaktu” powinny być znane jedynie upoważnionym pracownikom organów ds. ochrony zdrowia, w celu podjęcia wobec tychże osób określonych czynności związanych z przerwaniem transmisji wirusa SARS-CoV-2. Działający przy ministrze ds. zdrowia krajowy punkt kontaktowy wspólnotowego systemu wczesnego ostrzegania i reagowania dla zapobiegania i kontroli zakażeń oraz chorób zakaźnych, do którego zadań należy wymiana informacji oraz koordynacja działań w zakresie zapobiegania oraz zwalczania zakażeń i chorób zakaźnych z państwami członkowskimi Unii Europejskiej, Komisją Europejską oraz Europejskim Centrum do Spraw Zapobiegania i Kontroli Chorób, także powinien mieć, w sytuacjach przewidzianych ustawą z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi¹¹⁸, dostęp do danych zgromadzonych przez aplikację śledzącą kontakty zakaźne (lub też wymieniać te dane). W przypadku wystąpienia choroby zakaźnej, której zwalczanie wymaga podjęcia skoordynowanego działania wspólnotowego, krajowy punkt kontaktowy wspólnotowego systemu wczesnego ostrzegania i reagowania przekazuje Europejskiemu Centrum do Spraw Zapobiegania i Kontroli Chorób lub punktom kontaktowym państw członkowskich Unii Europejskiej dane osoby podejrzanej o zakażenie lub zachorowanie, zakażonej lub chorej na chorobę zakaźną, tylko w przypadku gdy jest to

¹¹⁸ T.j. Dz. U. z 2021 r. poz. 2069.

niezbędne do podjęcia przez te podmioty działań służących zapobieganiu i kontroli chorób zakaźnych i wyłącznie w zakresie niezbędnym do zapewnienia skuteczności tych działań.

Zgłosić należy także postulat szerszej dostępności, zwłaszcza w trybie bezwioskowym, informacji sektora publicznego związanych z używaniem aplikacji mobilnych śledzących kontakty zakaźne, jak np. liczba jej pobrań ze sklepów internetowych, liczba użytkowników, którzy wyrazili zgodę na śledzenie kontaktów zakaźnych, liczba osób, które odwołały zgodę na śledzenie kontaktów zakaźnych, liczba kluczy diagnostycznych przesłanych na serwer centralny i daty ich wysłania. Kod źródłowy polskiej aplikacji, oparty na oprogramowaniu *open source*, został upubliczniony i może być poddany jak najszerszym badaniom przez osoby, które posiadają odpowiednią wiedzę. Natomiast każdy jest w stanie dokonać samodzielnej analizy danych ilościowych, o których mowa.

Biorąc pod uwagę interes publiczny, może zaistnieć potrzeba dostosowania prawa krajowego, aby przewidywać udostępnianie danych stanowiących informację sektora publicznego innym usługom. Nie należy jednak zapominać, że w przypadku każdego wprowadzanego środka zwiększającego bezpieczeństwo w zakresie zdrowia publicznego należy ocenić, czy mniej inwazyjna alternatywa może osiągnąć ten sam cel oraz zapewnić, że każdy zastosowany środek jest zgodny z prawem, skuteczny i proporcjonalny. Zasada ograniczenia celu wymaga, aby cele przetwarzania danych zostały wystarczająco uszczegółowione, aby wykluczyć dalsze przetwarzanie do celów niezwiązanych z zarządzaniem kryzysem zdrowotnym COVID-19.

Bibliografia

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

- Bielak-Jomaa E., Lubasz D. (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.
- Dunaj B. (red.), *Słownik współczesnego języka polskiego*, Warszawa 1996.
- Kubalski G., Małowiecka M., *Ustawa o informatyzacji działalności podmiotów realizujących zadania publiczne. Komentarz*, Warszawa 2019.
- Kulisiewicz T., *Redukcja pozaprawnych barier ponownego wykorzystywania informacji sektora publicznego*, [w:] A. Piskorz-Ryń, *Jawność i jej ograniczenia*, t. V. *Dostęp i wykorzystywanie*, Warszawa 2015.
- Litwiński P. (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018.
- Litwiński P., Leńczuk A., Krzyżak A., Siwek A., *Raport z audytu prywatności aplikacji ProteGO Safe przeprowadzonego na zlecenie Ministerstwa Cyfryzacji przez Barta, Litwiński Kancelaria Radców Prawnych i Adwokatów Spółka Partnerska w dniu 5.08.2020 r.*, <https://www.gov.pl/web/protegosafe/dokumenty>.
- Maciejasz D., *Polacy nie zaufali rządowej aplikacji do walki z pandemią. A ci, którzy ją mają, nie raportują zakażeń*, „Gazeta Wyborcza” 2.09.2020.
- de Montjoye Y.-A., Hidalgo C.A., Verleysen M., Blonde V.D., *Unique in the Crowd: The privacy bounds of human mobility*, DOI: 10.1038/srep01376, <https://web.media.mit.edu/~yva/papers/deMontjoye2013unique.pdf>.
- Pyrgelis A., Troncoso C., De Cristofaro E., *Knock Knock, Who's There? Membership Inference on Aggregate Location Data*, <https://arxiv.org/pdf/1708.06145.pdf>.
- Słownik języka polskiego PWN*, <https://sjp.pwn.pl/sjp>.
- Sybilski D., *Dane o wysokiej wartości – nowy rodzaj informacji sektora publicznego*, „Informacja w Administracji Publicznej” 2019, Nr 4.
- Szafrąński B., Bliźniuk G., Karnowski J., Świerczyński Z., Weydmann R., Żurek L. (red.), *Interoperacyjność i bezpieczeństwo systemów informatycznych administracji publicznej*, Katowice 2006.
- Weiser M., *The Computer for the 21st Century*, <https://web.archive.org/web/20141022035044/http://www.ubiq.com/hypertext/weiser/SciAm-Draft3.html>.
- Weyrich, C., *Orientations for WP2000 and beyond*, “ISTAG” 1999.

Wiewiórowski W.R., *Rola Unii Europejskiej w koordynacji zastosowania narzędzi informatycznych do walki z pandemią*, „Europejski Przegląd Sądowy” 2020, nr 6.

Zieliński A. (red.), *Słowniczek terminów epidemiologicznych*, „Przegląd Epidemiologiczny”, <http://www.przegl Epidemiol.pzh.gov.pl/slowniczek-terminow-epidemiologicznych>.

Dostęp do informacji publicznej rozważany przez pryzmat procesów anonimizacji oraz pseudonimizacji danych

Access to public information in view of anonymisation and pseudonymisation

Streszczenie: Artykuł jest poświęcony zagadnieniom danych oraz informacji (w warstwie teoretycznej) oraz problematyce dostępu do informacji publicznej w kontekście zastosowania procesów składających się na anonimizację danych oraz pseudonimizację danych osobowych. Prócz definicji obu pojęć artykuł zawiera wyjaśnienie różnic między tymi procesami, a także uszczegółowienie rodzajów, cech czy też metod ich realizacji.

Słowa kluczowe: informacja, dane, informacja publiczna, anonimizacja, pseudonimizacja

Abstract: The article is devoted to the theory of data and information and addresses an access to the public information in the context of anonymisation and pseudonymisation of personal data. The article also explains the differences between the two processes and details types, features and methods of anonymising and pseudonymising data.

Keywords: data, information, public information, anonymisation, pseudonymisation

1. Informacja w służbie społeczeństwa informacyjnego

Ubiegłe stulecie wraz z jego barwną i złożoną historią cechowało dążenie do radykalnych przeobrażeń o charakterze politycznym, gospodarczym i społecznym, których źródeł powinno się upatrywać w procesach

o proveniencji rewolucyjnej. Dotykały one różnorodnych sfer życia człowieka, niosąc ogromne przeobrażenia i wdrażając nieznane dotąd formy organizacyjne.

Fenomenem ubiegłego wieku było zjawisko (ruch), które w lawinowym tempie dokonało kompleksowej transformacji zbiorowości ludzkich, kreując w efekcie tzw. społeczeństwa informacyjne. Zastanawiające, że działania państw i jednostek – określane mianem rewolucji informatycznej – były i pozostają niemal niezauważane przez podmioty (osoby) będące ich docelowymi adresatami.

Praca wielu ludzi jest obecnie trwale zespolona i skoordynowana z funkcjonowaniem komputerów. W relacjach pomiędzy człowiekiem i maszyną można wyróżnić przynajmniej trzy szczególne przypadki symbiozy¹: maszyna zastępuje człowieka w określonych czynnościach poznawczych (np. czujniki, detektory rejestrujące zmienne parametry otoczenia), człowiek konstruuje maszynę, aby uzupełnić swoje ograniczone zdolności poznawcze (np. mikroskop), wreszcie – maszyna kontynuuje pracę zapoczątkowaną przez istotę ludzką (sytuacja hipotetyczna, w której urządzenie po zapoznaniu się z informacją początkową rozpocznie wykorzystywanie jej dla własnego poznania, bez dalszego udziału człowieka).

Konwergencja technologiczna, komputeryzacja, postęp cywilizacyjny i industrialny wyzwalają nieuniknioną potrzebę refleksji prawnofilozoficznej, zdolnej choć w niewielkim stopniu zaspokoić potrzebę badań i dyskursu dotyczącego problematyki społeczeństwa informacyjnego, nazywanego często telematycznym, sieciowym, postindustrialnym bądź postmodernistycznym².

¹ Szerzej na ten temat: M. Hetmański, *Internet jako maszyna cybernetyczna*, [w:] R. Skubisz (red.), *Internet 2000*, Lublin 2000, s. 431 i n.

² Szerzej na ten temat: P.J. Durka, *Komputer. Internet. Cyfrowa rewolucja*, Warszawa 2000; A.M. Wilk, *Polska wobec wyzwań społeczeństwa informacyjnego*, [w:] R. Skubisz (red.), *Internet 2000...*, s. 143 i n.; A. Toffler, *Trzecia fala*, przeł. M. Kłobukowski, Warszawa 2001; D. Bell, *The Coming of Post-industrial Society*, New York 1973; M. Castells, *The*

Już na początku lat siedemdziesiątych Daniel Bell zaobserwował i opisał specyficzną transformację społeczeństwa, w wyniku której miała nastąpić „epoka postindustrialna”, a w konsekwencji informacyjna³. Zjawisko ujmowane jako determinizm technologiczny (według Dominique Vincka) występuje w dwóch wersjach – autonomii rozwoju techniki oraz jej olbrzymiego wpływu na życie społeczne⁴.

Problematyka społeczeństwa informacyjnego, pojęcia stworzonego i spopularyzowanego stosunkowo niedawno, cieszy się wielkim zainteresowaniem niemalże w każdej dyscyplinie nauki. Jest tematem podejmowanym nie tylko przez naukowców, ale również przez dziennikarzy, literatów, a nawet przez polityków. Choć zagadnienie społeczeństwa informacyjnego charakteryzuje się niebywale zawiłą i zmienną strukturą, często bywa przedmiotem komentarzy licznych autorów publikacji naukowych i *quasi*-naukowych.

Podstawowym składnikiem omawianej materii jest bez wątpienia informacja. Stanowi ona spoiwo wszelkich rozważań powiązanych z kwestią społeczeństwa informacyjnego, a co za tym idzie – z Internetem, nowoczesnymi technologiami, prawnymi, politycznymi i społecznymi formami aktywności społecznej. Wprawdzie korzenie nauki o informacji sięgają czasów dawnych, lecz jej niewątpliwym renesansem jest okres po II wojnie światowej, w którym rozpoczęły się wielkie przemiany naukowo-techniczne. Ze swojej natury omawiana nauka przybiera postać interdyscyplinarną i jest immanentnie powiązana z technologią informacyjną, stanowiącą gwarant i motor wszelkich przemian obecnych społeczeństw

Rise of the Network Society, Oxford 1996; M. Castells, *The information Age: Economy, Society and Culture*, Oxford 2000.

³ Por. F. Fukuyama, *Wielki wstrząs. Natura ludzka a odbudowa porządku społecznego*, przeł. H. Komorowska, Warszawa 2000, s. 13.

⁴ D. Vinck, *Sociologie des sciences*, Paris 1995, za: J. Kulpińska, *Od społeczeństwa postindustrialnego do społeczeństwa informacyjnego – koncepcje i dyskusje*, [w:] L.H. Haber (red.), *Polskie doświadczenia w kształtowaniu społeczeństwa informacyjnego: dylematy cywilizacyjno-kulturowe (materiały ogólnopolskiej konferencji naukowej. Kraków, 28 września 2001 r.)*, Kraków 2002, s. 2, <http://www.uci.agh.edu.pl/agh/dep/wnss/konferencje/doc>.

oraz, co równie istotne, jest aktywnym uczestnikiem nowych ewolucji społecznych⁵.

Można wywieść tezę, że społeczeństwo informacyjne pełni rolę *sui generis* kultury prawnej. Brak zastosowania pojęcia system prawa, dziedzina prawa lub dział prawa wiąże się z próbą uwypuklenia czynników aksjologicznych w tej materii. Wynikają one nie tylko z podstaw mających bezpośrednie uzasadnienie w wartościach, ale też przyzwyczajaję, deontologii, czy nawet przypadkowości⁶. Cechą zauważalną społeczeństwa informacyjnego pojmowanego jako kultura prawna byłyby:

- a) konwergencja czynników materialnych;
- b) niezależność od przestrzeni terytorialnej;
- c) szybkość krystalizacji deontologii i aksjologii;
- d) nieznane dotąd procedury prawne i instytucje statyczne;
- e) oparcie podstaw normatywnej kwalifikacji na określeniu granic zasadniczych pojęć.

Nowe zjawiska technologiczne w dziedzinie przesyłania danych i informacji modelują sfery wzajemnych ludzkich oddziaływań⁷. Na tym gruncie zasadzają się zwyczaje i potrzeby regulacji prawnych. Komunikacja elektroniczna doprowadziła do powstania zbiorowości, w której koegzystencja przybrała nową jakość⁸. Poza tym przekaz ma charakter

⁵ Są to trzy cechy charakterystyczne tej dyscypliny, niezmiennie we wszystkich okresach jej rozwoju. Zostały wskazane przez T. Saracevica, byłego przewodniczącego American Society for Information Science and Technology, obecnego dziekana School of Communication, Information nad Library Studies w Rutgers, the State University of New Jersey, w wygłoszonym na początku lat 90. referacie o pochodzeniu, ewolucji i zależności nauki o informacji. Podają za: B. Sosińska-Kalata, *Czym jest dziś nauka o informacji?*, [w:] B. Sosińska-Kalata, K. Materska, W. Gliński (red.) *Spółeczeństwo informacyjne i jego technologia*, Warszawa 2004, s. 9.

⁶ F.W. Gees, *From sectoral systems of innovation to socio-technical systems: Insights about dynamics and change from sociology and institutional theory*, "Research Policy", Vol. 33, Iss. 6-7, September 2004, s. 897-920.

⁷ J. Ober, *Etyka w rozwoju informatyki*, „Nauka” 1999, nr 1, s. 152.

⁸ Dla przykładu P.J. Durka, *Komputer...*, *passim*; A.M. Wilk, *Polska wobec wyzwań...*, s. 143 i n.; A. Toffler, *Trzecia fala...*, *passim*; D. Bell, *The Coming...*, *passim*; M. Castells, *The Rise...*, *passim*; M. Castells, *The information Age...*, *passim*; W. Kilian, *Wprowadzenie*,

znacznie bardziej subiektywny⁹. Konwergencja technologiczna i upowszechnienie się technologii sprzyjały oderwaniu się od czynników narodowości, pochodzenia czy terytorializmu. Podstawowe instytucje organizacji społecznych stają się mniej zasadnicze w swej konstrukcji, a czasem nawet anachroniczne. Problematyka jurysdykcji jest tego najgłębszym dowodem. Ludzkie stosunki kwalifikowane jurydycznie są w przestrzeni nowych zjawisk poddane innemu wartościowaniu. Pomimo fragmentarycznego charakteru opisów tych zjawisk jest użyteczne także na gruncie nauk prawnych wysunięcie hipotezy społeczeństwa informacyjnego. Podstawową korzyścią płynącą z jej zastosowania jest wdrożenie nowych metod analizy normatywnej, które oddać mogą przemożną usługę praktyce. Takie ujęcie ludzkiej zbiorowości wywodzi się z uświadomienia intensywności społecznych oddziaływań i nowej płaszczyzny dla ich urzeczywistniania – cyberprzestrzeni. Zasięg nowej formy koegzystencji jednostek, kwalifikowanej wybiórczo i niespójnie przez normy prawne, jest wręcz globalny. Jego układ jest równoległy i „niekonkurencyjny” w stosunku do desygnatów innych form opisu ludzkich zbiorowości¹⁰. Mimo że włączamy się w jego byt poprzez uruchomienie środków komunikacji określonego rzędu, ma on charakter permanentny ze względu na skalę konsekwencji swych oddziaływań. Należy oczekiwać, że fundamentalne instytucje prawne organizujące i urzeczywistniające egzystencję społeczeństw będą ulegać przemianom, których ramy określały nurty ewolucji modelu zbiorowości informacyjnej¹¹.

[w:] J. Gołaczyński (red.), *Prawne i ekonomiczne aspekty komunikacji elektronicznej*, Warszawa 2003, s. 17 i n.

⁹ A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 39. Wymiana informacji ma zawsze charakter interpersonalny.

¹⁰ Niekonkurencyjna oznacza, że nie tworzy odrębnego bytu materialnego (fizycznego), lecz w istocie kreuje odrębny byt niematerialny (cyfrowy) wynikający z budulca cyberprzestrzeni, czyli danych i informacji, traktowanych zgodnie z cybernetycznymi koncepcjami w kategorii odrębnego bytu, obok materii i energii.

¹¹ A. Lekka-Kowalik, *Demokracja i autonomia jednostki w globalnej infrastrukturze informacyjnej*, „Nauka” 1999, nr 1, s. 126 i n.

Konstrukcja współczesnego modelu społeczeństwa informacyjnego, którego niezaprzeczalnym katalizatorem są technologie stosowane podczas komunikacji elektronicznej, przybierającej w wyniku konwergencji formę cyfrową, wyzwała potrzebę refleksji nad fenomenem informacji¹².

2. Pojęcie i cechy informacji oraz danych

Na początku rozważań należy przyjąć, że nie jest możliwe stworzenie jednej – uniwersalnej definicji informacji¹³. Nie ulega jednak wątpliwości, iż każde ujęcie zagadnienia wnosi dodatkowy komponent, który powiązany z całością przybliży do kompleksowego zrozumienia tematu.

Informacja przestała być traktowana wyłącznie jako wiadomość, stając się immanentnym kodem tkwiącym w każdej rzeczy, który „wyjęty z niej tworzy rzeczy samoistne”¹⁴. Postrzegana jest jak odrębny byt fizyczny. Buduje przestrzeń podporządkowaną specyficznym zasadom. Nawet sztuka, będąc przyjemnością wizualną i abstrakcyjną, jest zarazem wysublimowanym zbiorem informacji. N. Wiener, „ojciec cybernetyki”, nadał jej odrębny, autonomiczny status, czyniąc zeń trzeci elementarny składnik rzeczywistości: „Informacja jest informacją, nie zaś materią i nie energią”¹⁵. Stała się zasadniczym składnikiem otaczającej nas przestrzeni i co równie ważne – nie musi to być przestrzeń rzeczywista.

¹² Wskazane jest w tym miejscu zaakcentować, że istnieje nadal ogromna dysproporcja w podejściu do zagadnienia „informacji” pomiędzy przedstawicielami interpretacji ogólnych i ilościowych charakterystycznych w środowiskach przyrodniczo-filozoficznych a koncepcjami szczegółowymi i jakościowymi reprezentowanymi przez przedstawicieli nauk humanistycznych. Abstrahując od kwestii, iż liczni autorzy tworzą coraz to nowsze definicje, wzbogacając i tak już bogaty zbiór teorii dotyczących opisywanej problematykę. Szerzej na ten temat w dalszej części artykułu.

¹³ W. Taras, *Informowanie obywateli przez administrację*, Wrocław-Warszawa-Kraków 1992, s. 12-13.

¹⁴ Szerzej na ten temat: A.J. Kościański, *Spółeczeństwo informacyjne: propozycje konceptualizacji*, „Kultura i Społeczeństwo” 1999, nr 3 (lipiec–wrzesień).

¹⁵ N. Wiener, *Cybernetyka czyli sterowanie i komunikacja w zwierzęciu i maszynie*, przeł. J. Mieścicki, Warszawa 1971, s. 173.

Niezbędne dla zrozumienia natury informacji jest przejście do kwestii pojęciowych. Zagadnienia te są trudne, zważywszy, że autorzy prac związanych z teorią informacji lub naukami pokrewnymi stronią od konstruowania definicji, uciekając się najczęściej do metod opisowych. Wskazane jest też zaakcentowanie istnienia ogromnej dysproporcji w podejściu do zagadnienia „informacji” między przedstawicielami interpretacji ogólnych i ilościowych, charakterystycznych w środowiskach przyrodniczo-filozoficznych, a koncepcjami szczegółowymi i jakościowymi, reprezentowanymi przez przedstawicieli nauk humanistycznych¹⁶. Dodatkowo tworzone są coraz to nowsze definicje, wzbogacając i tak już bogaty zbiór teorii dotyczących opisywanej problematyki. Tytułem przykładu można wskazać¹⁷:

- 1) ilościową teorię informacji Claude’a E. Shannona;
- 2) nieprobabilistyczną teorię Andrieja N. Kołmogorowa (informacja jako pojęcie nieprobabilistyczne, zawarte w algorytmach)¹⁸;
- 3) teorię Ralpa Windona L. Hartleya (traktującą o pojemności informacyjnej układu ją przekazującego);
- 4) jakościową teorię informacji Mariana Mazura;
- 5) teorię pragmatyczną Klemensa Szaniawskiego;
- 6) semantyczną wykładnię informacji Józefa Olesińskiego.

3. Analiza wybranych definicji informacji

W warstwie semantycznej przez informację można rozumieć: zalecenie, zezwolenie, zakaz, nakaz, każdy opis i sprawozdanie bądź instrukcje

¹⁶ Szerzej na ten temat: M. Hetmański, *Spoleczny charakter informacji*, [w:] B. Chyrowicz (red.), *Spoleczeństwo informatyczne: szansa czy zagrożenie?*, Lublin 2003, s. 14-15.

¹⁷ Za: B. Stefanowicz, *Informacja*, Warszawa 2004, s. 9.

¹⁸ Nieprobabilistyczny – pojęcie probabilistyki powiązane jest z naukami matematycznymi traktującymi o prawdopodobieństwie. Stąd „nieprobabilistyczne” oznacza nieprawdopodobne. Więcej na temat algorytmów probabilistycznych: Z. Płoski, *Słownik encyklopedyczny. Informatyka*, Wrocław 1999.

i wzorce działania, które mogą być wykorzystane do spowodowania określonego postępowania adresata tej informacji¹⁹. Niekiedy informacja jest utożsamiana z pojęciem wiadomości bez względu na formę i proklamowaną treść²⁰. W znaczeniu terminologicznym i potocznym informacja to też powiadomienie, komunikat, wiadomość czy wskazówka²¹. Informacja jest „zdolna przybrać” dowolną postać: obrazu, rysunku, planu, wykresu, mapy, nagrania muzycznego czy zapisu nutowego. Jest nią zatem wszystko to, co przyjmuje uporządkowaną formę energii lub materii²². Bywa, że termin ten dotyczy instytucji trudniących się udzielaniem wskazówek, porad, zaleceń, w zakresie swoich kompetencji i wiedzy.

Szerokie ujęcie zagadnienia zakłada, że informacja stanowi odwzorowanie mnogości i zróżnicowania otaczającej człowieka rzeczywistości. Informacja jest: „różnorodnością, jaką jeden obiekt zawiera o innym obiekcie”²³. W zależności od dziedziny nauki i układu zbudowanego co najmniej przez dwa składniki (czyli obserwatora i obiekt poddany obserwacji) informacja przybiera postać sygnałów, bodźców lub struktury materii.

Przez informację można rozumieć także „ilościową miarę dowolnego kanału komunikacyjnego, przez który przesyłany jest komunikat”²⁴. W takim ujęciu wiąże się ona ze zróżnicowanym sygnałem (kodowanym i dekodowanym) w procesie komunikacji, który stanowi jedynie konkretny jej nośnik, sam zaś informacją nie jest. Miara (zawartość) informacji w komunikatach jest natomiast uzależniona od stopnia prawdopodobieństwa jego pojawienia się, badanego w odniesieniu do innych komunikatów

¹⁹ Szerzej na ten temat: H. Greniewski, *Cybernetyka niematematyczna*, Warszawa 1969, s. 29 i 206; H. Greniewski, M. Kempisty, *Cybernetyka z lotu ptaka*, Warszawa 1963, s. 9 i n.

²⁰ Szerzej na ten temat: J. Nowakowski, W. Sobczak, *Teoria informacji*, Warszawa 1978; W. Piróg, *Zagadnienia informacji i dokumentacji naukowej*, Warszawa 1978.

²¹ M. Szymczak (red.), *Słownik języka polskiego PWN*, t. I, Warszawa 1996.

²² Szerzej na ten temat: R. Tadeusiewicz, *Spoleczność Internetu*, Warszawa 2002, s. 35.

²³ L. Kulikowski, *Informacja i świat, w którym żyjemy*, Warszawa 1978, s. 44.

²⁴ M. Hetmański, *Spoleczny charakter...*, s. 15.

– słowem, im rzadziej pojawiają się dane komunikaty, tym więcej informacji ze sobą niosą²⁵.

Informacje muszą zostać zakodowane i zdekodowane przez podmioty uczestniczące w akcie komunikacji, aby mogły być przesyłane oraz właściwie zrozumiane. Pomijając błędy popełniane przy wysyłaniu i odczytaniu treści przesyłanej informacji, można założyć sytuację, w której nadawca i adresat, posługując się określonym doбором znaków, swobodnie wymieniają informacje. Te znaki można zgodnie z semiotyką Ch.S. Peirce'a²⁶ podzielić na:

- 1) ikony (ilustracje przedmiotów odniesione na zasadzie podobieństwa);
- 2) indeksy (reprezentacje wskazujące występowanie przedmiotu);
- 3) symbole (konwencjonalne i wieloznaczne odniesienia do przedmiotów).

Rozpatrywana w ogólności wymiana informacji obejmuje zatem rozmaite sposoby, m.in.²⁷:

- 1) synchroniczny (np. rozmowa telefoniczna);
- 2) asynchroniczny (np. faks, telegram, list);
- 3) równoległy (np. konferencja z udziałem urzędów przesyłających dźwięk i obraz);
- 4) szeregowy (np. przekazywanie kolejno od jednego do drugiego odbiorcy informacji wysłanej przez nadawcę);
- 5) wielodostępny (np. media, Internet);
- 6) sekwencyjny, czyli restrykcyjny (np. służbowy obieg informacji).

Informacja jest także niejednolicie pojmowana na gruncie cybernetyki. W ujęciu ogólnym – jako stan układów wyróżniony przez badacza

²⁵ Paradoksalnie na szczycie tak utworzonej piramidy usytuowane są wiadomości o sensacyjnym zabarwieniu, najniżej zaś przysłowia. Por. *ibidem*, s. 15-16.

²⁶ Szerzej na ten temat: A. Watson, A. Hill, *Dictionary of Communication and Media Studies*, London 1991, za: S. Juszczak, *Komunikacja człowieka z mediami*, Katowice 1998, s. 44.

²⁷ Szerzej na ten temat: M. Bazewicz, A. Collen, *Methodological Foundations of Human Activity Systems and Informatics*, Wrocław 1995.

spośród innych jego stanów (np. wybrany element ze zbioru komunikatów o normach lub zachowaniach prawnych)²⁸. Natomiast w znaczeniu szczegółowym – jako treść przekazywana przez pewnego nadawcę, której człowiek lub zbudowane przez niego urządzenie jest odbiorcą będącym w stanie ją przyjąć i przetworzyć. Informacja staje się kategorią subiektywną, zależną od świadomości człowieka lub zdolności nadanej przez człowieka percepcji automatu czy formy, w jakiej się ją przekazuje (np. cenna dla nadawcy informacja zakomunikowana adresatowi nierozumiejącemu języka nadawcy staje się bezużytecznym zbiorem dźwięków, podobnie w przypadku wprowadzenia do maszyny matematycznej zakodowanej informacji w niezrozumiałym dla urządzenia języku)²⁹.

Norbert Wiener traktuje informację jako: „treść zaczerpniętą ze świata zewnętrznego w procesie dostosowania się do niego naszych zmysłów”³⁰. Bódcze i sygnały docierające do istoty ludzkiej za pomocą zmysłów, jakimi dysponuje, mogą być rejestrowane i utrwalane, następnie dekodowane i rozumiane. Z tego względu sygnały doń docierające cechuje zawartość informacyjna, mimo że „ich entropia, określana w stosunku do innych sygnałów przez dany podmiot jest różna, to informacja odebrana przez człowieka jest ostatecznie negentropią (czyli entropią ze znakiem minus)”³¹.

Opisane statystyczne ujęcie informacji skorelowane jest z termodynamiczną wykładnią układu izolowanego, w którym zaobserwować można procesy różnicowania się stanów energetycznych. Zgodnie bowiem z drugą zasadą termodynamiki w przypadku procesów przebiegających nieodwracalnie entropia uniwersum procesu wzrasta. Odpowiednio, gdy

²⁸ Szerzej na ten temat: A. Malinowski, *Wstęp do badań cybernetycznych w prawoznawstwie*, Warszawa 1977, s. 116 i n.

²⁹ Szerzej na ten temat: H. Rot, *Podstawy cybernetyki i informatyki prawniczej*, Wrocław 1983, s. 64 i n.

³⁰ N. Wiener, *Cybernetyka a społeczeństwo*, przeł. O. Wojtasiewicz, Warszawa 1961, s. 18.

³¹ M. Hetmański, *Spoleczny charakter...*, s. 18.

proces lub reakcja przebiegają odwracalnie (tzn. nie wykazują tendencji do przebiegu w żadnym kierunku), zmiana entropii w uniwersum procesu jest równa zeru³². Z tego powodu każdy przejaw różnicowania się układu jest przejawem jego malejącej entropii (określanej mianem negentropii), która przez zróżnicowanie prawdopodobieństwa jego produktów stanowi informację samego układu.

Wywód ów należy uzupełnić wyjaśnieniem, że Wiener odnosił swoje obserwacje do układów otwartych powiązanych ze środowiskiem zewnętrznym, a dokładniej społeczną koegzystencją ludzi. Przy takich założeniach II zasada termodynamiki nie znajduje pełnego odzwierciedlenia, odnosi się bowiem do układów w pełni hermetycznych, w których tendencja do lokalnego przeciwdziałania entropii oraz jej modulacji nie ma miejsca (realnego wpływu)³³.

Autor zwrócił także uwagę na urządzenia techniczne służące i wspierające człowieka podczas odbierania wskazanych i wyróżnionych sygnałów o informacyjnej zawartości. Jego zdaniem współpraca człowieka z maszynami zdolnymi do rejestrowania, gromadzenia i przetwarzania informacji wpływa pozytywnie na wzrost informacji³⁴.

Oryginalną koncepcję cybernetyczną zaprezentował Marian Mazur. Za informację uznał związek między stanami tego samego zbioru, przy jednoczesnej ścisłej odpowiedzialności między: „stanami zbioru obrazów, a stanami zbioru oryginałów, skutkującej powstaniem informacji identycznych w obydwu zbiorach”³⁵. Aby w pełni zrozumieć myśl autora, niezbędny jest drobny komentarz. W otoczeniu człowieka zachodzą różne zmiany; społeczeństwo dowiaduje się o nich za pośrednictwem komunikatów złożonych z elementarnych sygnałów odczytywanych przez odpowiednie rejestratory, służące do kumulacji tych komunikatów

³² Szerzej na ten temat: G.M. Barrow, *Chemia fizyczna*, przeł. J. Kuryłowicz, Warszawa 1978, s. 158 i n.; S. Bursa, *Chemia fizyczna*, Warszawa 1979, s. 226 i n.

³³ Szerzej na ten temat: M. Hetmański, *Spółeczny charakter...*, s. 16.

³⁴ N. Wiener, *Cybernetyka a społeczeństwo...*, s. 33 i n.

³⁵ M. Mazur, *Cybernetyczna teoria układów samodzielnych*, Warszawa 1966, s. 37 i n.

w formie skojarzeń³⁶. Zakładając, że społeczeństwo ma pewną skończoną liczbę rejestratorów odbierających sygnały z otoczenia, można przyjąć, że między stanami zbioru oryginałów (zespół obiektów i stanów rzeczywistego świata „energomaterialnego”) a stanami zbioru obrazów (zespół oznakowań, jakie członkowie określonego społeczeństwa przyporządkowują odpowiednim elementom świata rzeczywistego) zachodzi odpowiedniość³⁷.

Niektórzy badacze problemu traktują informację jak metaenergię, czyli impuls energetyczny regulujący ilość energii w materii, a co za tym idzie – w poszczególnych układach i systemach (np. fizycznych, biologicznych), a także w reakcjach między nimi³⁸. Taka definicja niewątpliwie pomocna dla przedstawicieli nauk ścisłych nie znajduje zastosowania podczas analizy reakcji zachodzących w zbiorowościach ludzkich. Wyjątek stanowią podejmowane przez człowieka raptowne działania (decyzje), „zainicjowane” informacją będącą metaenergią.

Niebywale trafnie kompleksową „naturę” informacji przedstawił Mieczysław Bazewicz. W ujęciu autora informacja jest pojęciem abstrakcyjnym, pozbawionym wagi, niezajmującym przestrzeni i niemożliwym do bezpośredniej obserwacji. Postrzegana jest wyłącznie przez pryzmat ludzkich zachowań i pracę, określana zaś przez powszechnie obserwowane i dostrzegalne atrybuty (np. genetyczne, biochemiczne i neurologiczne)³⁹.

Wyjaśnienia wymaga także zagadnienie elektronicznej formy informacji, która w postaci analogowej lub cyfrowej może być przesyłana przez różne urządzenia elektroniczne. Z technicznego punktu widzenia jest to uzależnione od rodzaju sygnału, czyli zmiennej w czasie i przestrzeni

³⁶ Szerzej na ten temat: J. Kossecki, *Cybernetyka społeczna*, Warszawa 1981, s. 163.

³⁷ *Ibidem*, s. 164 i n.

³⁸ Szerzej na ten temat: P. Davis, *Bóg i nowa fizyka*, przeł. P. Amsterdamski, Warszawa 1996; G. Harmon, *The measurement of information*, „Information Processing and Management” 1984, nr 1-2.

³⁹ Szerzej na ten temat: M. Bazewicz, *Wizja społeczeństwa ery komunikacji, informacji i wiedzy XXI wieku*, Wrocław 2000, s. 182 i n.

wielkości fizycznej, transmitującej dane (np. sygnał elektryczny, akustyczny, optyczny)⁴⁰. Jednakże sygnał nie jest desygnatem pojęcia informacji, może on bowiem nieść pewną „porcję” informacji bądź nie nieść jej w ogóle⁴¹. Zasadniczo za pośrednictwem sygnałów określone „podmioty” mogą uczestniczyć w komunikacji i wymianie informacji, należy jednak zaakcentować, że wiadomość wypływająca ze źródła przechodzi przez urządzenie transmitujące i zostaje zamieniona na określony rodzaj sygnału, aby mogła mimo zakłóceń zostać zdekodowana i odebrana przez odbiorcę⁴². Sygnał pełni więc funkcję „nośnika” strumienia informacji.

Sygnał jako zjawisko fizyczne można opisać przez podanie określonej funkcji zależnej od czasu. Jeśli przyjmuje ona dowolne wartości, mamy do czynienia z funkcją (sygnałem) analogową, która w matematycznym opisie jawi się w postaci tzw. funkcji ciągłej. W rezultacie obserwowany z perspektywy człowieka świat przybiera postać analogową, gdyż wszelkie otaczające go zjawiska przyrody wykazują proporcjonalną systematyczność – ciągłość następujących po sobie stanów. Rzeczywistość nie zmienia się bowiem „skokowo” (np. z czerni na biel)⁴³, lecz każda zmiana jest procesem przechodzenia przez wiele etapów pośrednich.

Analogicznie jeżeli dopuszczalne wartości lub ich przedziały uznać za wartości liczbowe, to sygnał określa się jako cyfrowy. Z tego powodu zbiór wartości wielkości cyfrowej jest zbiorem przeliczalnym, gdyż wielkość cyfrowa w danym przedziale swej zmienności przyjmuje skończoną liczbę wartości⁴⁴. W zapisie cyfrowym stosuje się więc zawsze skończoną liczbę symboli. W tej postaci każdą informację można przedstawić

⁴⁰ Szerzej na ten temat: W. Traczyk, *Układy cyfrowe. Podstawy teoretyczne i metody syntezy*, Warszawa 1982, s. 11.

⁴¹ Szerzej na ten temat: J. Ekel, *Decyzyjnoinformacyjny model czynności ludzkich*, [w:] J. Koziński (red.), *Problemy psychologii matematycznej*, Warszawa 1971, s. 295 i n.

⁴² Por. C.E. Shannon, *A Mathematical Theory of Communication*, s. 2, http://free.art.pl/fotografie/teoria_obrazu/shannon.pdf.

⁴³ Szerzej na ten temat: N. Negroponte, *Cyfrowe życie. Jak się odnaleźć w świecie komputerów*, Warszawa, 1997, s. 16 i n.

⁴⁴ Szerzej na ten temat: W. Głocki, *Układy cyfrowe*, Warszawa 1996, s. 9.

w formie elementarnych jednostek zwanych bitami. Bit jest: „elementem składowym DNA informacji, nie ma koloru, rozmiaru ani wagi, przybiera jedynie dwa stany istnienia: włączony/wyłączony, prawda/fałsz, góra/dół, czarny/biały, tak/nie”⁴⁵. Komputery i inne elektroniczne urządzenia wykorzystują tę stosunkowo najprostszą z możliwych kategorii⁴⁶:

- 1) namagnesowanie i roznamagnesowanie (w przypadku powierzchni dysku lub dyskietki);
- 2) prąd płynie bądź nie płynie (np. podczas pracy komputera);
- 3) światło odbija się lub nie (od powierzchni płyty CD-ROM).

W przypadku reprezentacji informacji ilościowej wygodnie jest nadać bitowi interpretację arytmetyczną (0, 1)⁴⁷. Przetwarzanie pojedynczych bitów jest rzadko wykorzystywane. W praktyce podstawowym działaniem urządzeń cyfrowych jest przetwarzanie całych łańcuchów bitów o ustalonej długości wektorów⁴⁸. Za pomocą ciągów bitów tworzących liczbę binarną można zapisać bardziej skomplikowane dane, liczby i znaki alfabetu⁴⁹. W ten sposób można scharakteryzować dowolną wielkość (np. tekst, obraz, dźwięk), a następnie zakodować dane, wprowadzane później do komputera, skanera, kamery cyfrowej lub innego urządzenia⁵⁰. Obecna technologia cyfrowa pozwala na zapisanie, przetworzenie i przesyłanie ogromnej ilości informacji⁵¹. Opisany w wielkim uproszczeniu i skrócie system binarny (dwójkowy) wykorzystywany do reprezentowania informacji w formie cyfrowej pozwala na uproszczenie budowy układów

⁴⁵ N. Negroponte, *Cyfrowe życie...*, s. 15.

⁴⁶ P.J. Durka, *Komputer...*, s. 49.

⁴⁷ Szerzej na ten temat: J. Biernat, *Architektura komputerów*, Wrocław 2002, s. 52.

⁴⁸ Np. wektor 8-bitowy to bajt (*byte*), 4 bity tworzą półbajt (*nibble* lub *tetrada*). *Ibidem*.

⁴⁹ Szerzej na ten temat: D. Madej, K. Marasek, K. Kuryłowicz, *Komputery osobiste*, Warszawa 1987, s. 12.

⁵⁰ Szerzej na ten temat: A. Lach, *Dowody elektroniczne w procesie karnym*, Toruń 2004, s. 25.

⁵¹ Bit – najmniejsza jednostka informacji używana w odniesieniu do sprzętu komputerowego. Bajt (ang. *byte*) to najmniejsza adresowalna jednostka pamięci komputerowej, składająca się z bitów. Jednostkami wyrażającymi ilość informacji większej od bajta są kilobajt, megabajt, gigabajt itd.

elektronicznych, z których zbudowane są komputery, a także podwyższenie jakości pracy oraz niezawodności działania urządzeń elektronicznych (np. przez korekcję błędów). Zalety tego systemu sprawiły, że stał się on dominującym sposobem reprezentacji informacji przez komputery.

Na gruncie teorii informacji, zgodnie z klasyfikacją zaproponowaną przez Warrena Weavera, prócz poziomu analiz formalnych (umożliwiających ustalenie ilości informacji za pomocą konwencjonalnej jednostki miary, czyli wspomnianego bitu) można wskazać też poziom semantyczny i pragmatyczny⁵². W pierwszym znaczeniu informacja jest pojmowana jako treść przekazywana przez nadawcę odbiorcy w formie komunikatu, w drugim definicja kładzie nacisk na jej rolę przy oddziaływaniu na odbiorcę, biorąc pod uwagę jego możliwości percepcyjne⁵³.

Wykładnia analizowanego pojęcia często jest przedmiotem zainteresowania nauk psychologicznych. Punkt ciężkości w psychologicznej interpretacji informacji położony jest jednak na reakcję nadawców i odbiorców podczas komunikacji interpersonalnej. Informacja częstokroć bywa ujmowana jako środek redukujący przez kreowanie alternatywnych rozwiązań, stan niepewności odnośnie do desygnatów i ich właściwości⁵⁴. Definicje psychologiczne są, niestety, obarczone poważną wadą, mianowicie pomijają zagadnienia dotyczące procesów funkcjonowania informacji oraz jej przyczynowo-skutkowego przebiegu.

Współczesne teorie informacji niejednokrotnie stawiają znak równości między informacją a nieprzewidywalnością (generującą systemy chaotyczne)⁵⁵. Jeśli wiadomość nie wnosi nic nowego, to znaczy nie udziela odpowiedzi bez względu na rodzaj i przedmiot pytania lub abstrakcyjnego

⁵² Szerzej na ten temat: J. Petzel, *Informatyka prawnicza: zagadnienia teorii i praktyki*, Warszawa 1999, s. 36 i n.

⁵³ *Ibidem*, s. 37 wraz z podaną w przypisach literaturą.

⁵⁴ Szerzej na ten temat: T. Newcomb, R.H. Turner, P.E. Converse, *Psychologia społeczna*, przeł. H. Muszyński [et al.], Warszawa 1970, s. 205-206.

⁵⁵ Szerzej na ten temat: A. Rothert, *Między porządkiem a chaosem*, Warszawa 2006; D. de Kerckhove, *Inteligencja otwarta*, przeł. A. Hildebrandt, Warszawa 2001, s. 16.

zagadnienia, to nie zawiera informacji, która ze swojej istoty musi stanowić *novum* dla odbiorcy. Staje się swoście traktowanym i nieuporządkowanym strukturalnie substratem wiedzy.

Informacja bywa również traktowana w kategoriach „dobra”, a nawet „towaru”, będącego przedmiotem obrotu gospodarczego⁵⁶. Z dużą dozą prawdopodobieństwa można antycypować błyskawiczny wzrost znaczenia i roli informacji w nowoczesnych gospodarkach, uzależnionych obecnie od rozwoju nowoczesnych form i środków komunikacji społecznej. Współczesne doświadczenia i badania niezbicie dowodzą, że informacja stała się składnikiem wytwórczym, stanowiąc dużą część wartości dodanej większości dóbr i usług⁵⁷. Stąd kraje o rozbudowanej infrastrukturze teleinformatycznej i wyposażone w nowoczesne technologie zdolne do przesyłania, gromadzenia i przetwarzania dużych porcji informacji uzyskują i konsekwentnie podtrzymują dystans ekonomiczny wobec pozostałych państw, które nie rozwijają tego sektora gospodarki.

Jeśli informacja jest czynnikiem wykorzystywanym w celu osiągnięcia zysku, to bez wątpienia jest rodzajem kapitału. Ostatecznie jest ona szczególną odmianą kapitału informacyjnego, ponieważ⁵⁸:

- 1) szybko się dezaktualizuje, co skutkuje jej deprecjacją;
- 2) wykorzystanie przez różnych użytkowników (adresatów) nie powoduje jej zużycia;
- 3) jest mobilna – błyskawicznie przesyła się ją w czasie i przestrzeni.

Informacja to także korelat władzy. Jak stwierdził Umberto Eco: „Kto dysponuje informacją, ten dysponuje realną władzą”. Wgląd do określonych informacji przez osoby niepowołane niewątpliwie może nieść

⁵⁶ Szerzej na ten temat: D. Gill-Tarnowska, *Dobra i usługi informacyjne – informacja jako towar*, [w:] A. Szewczyk (red.), *Informacja – dobra lub zła nowina*, Szczecin 2004, s. 533–538; B. Przybylska, *Informacja jako towar*, [w:] A. Szewczyk (red.), *Informacja...*, s. 559–563.

⁵⁷ Szerzej na ten temat: E. Niedzielska, *Próba systematyzacji procesów rozwoju systemów informacyjnych*, „Wiadomości Statystyczne” 1986, nr 4, s. 20 i n.

⁵⁸ B. Stefanowicz, *Informacja...*, s. 79.

za sobą różnorakie zagrożenia. Dostęp do informacji jest uwarunkowany głównie jej wartością, jej różnicowanie zaś dotyczy nie tylko treści, lecz uwzględnia również kategorie odbiorców, warunkując konieczność ochrony wyselekcjonowanej informacji⁵⁹. Zgodnie z koncepcją J.W. Burcha informacja stanowi najskuteczniejszą broń w batalii z konkurencyjnym światem, ci bowiem, którzy nią dysponują, uzyskują swoiście pojmowaną władzę i przewagę zarówno nad jednostkami, jak i państwem⁶⁰. Prawo do informacji bywa utożsamiane nie tylko z prawem obywatelskim, lecz również z naturalnym prawem człowieka, które jednocześnie gwarantuje i zabezpiecza prawo do poznawania otaczającej nas rzeczywistości, budując na trwałe poczucie społecznego ładu informacyjnego⁶¹.

4. Informacja a dane

W tym kontekście wskazana wydaje się refleksja nad pozornie tożsamymi pojęciami, którymi są dane i informacje. Przez dane należy rozumieć przedstawienie faktów, pojęć albo poleceń w ustalony sposób, umożliwiające ich przesyłanie, analizę lub przetwarzanie przez ludzi albo automatycznie (program komputerowy jest specjalną kategorią danych, podobnie jak notatki, obrazy, jeżeli są dostatecznie sformalizowane i spełniają powyższy wymóg)⁶². Natomiast informacja to wywołany danymi efekt, zamierzony lub doświadczony przez ich użytkowników. Uzyskanie

⁵⁹ Już na początku XXI stulecia około 20% informacji przetwarzanej cyfrowo podlegało ochronie. Szerzej na ten temat: E. Kuriata, *Wirusy komputerowe. Mechanizmy infekcji i środki ochrony*, Wrocław 1999, s. 14.

⁶⁰ Szerzej na ten temat: T. Goban-Klas, *Uniwersytet a mass media*, „Forum Akademickie” 1996, nr 2.

⁶¹ J. Oleński konstatuje: „Prawo do prawdy stanowi podstawę społecznego ładu informacyjnego w cywilizacji łacińskiej i to w całej jej historii, zwłaszcza zaś we współczesnych systemach demokratycznych opartych na jej zasadach”. J. Oleński, *Ekonomika informacji. Metody*, Warszawa 2003, s. 17.

⁶² Za: *Recommendation of the Council of the OECD concerning Guidelines for the Security of Information Systems*, OECD/GD (92) 10, Paris 1992.

informacji, w tym informowanie innych, polega na posługiwaniu się danymi, które przybierają charakter subiektywny, ponieważ są uzależnione od czynników społeczno-kulturowych oraz ekonomicznych⁶³. Syntaktyka, semantyka i pragmatyka statuuja strukturę informacji, kwalifikując ją do określonego zbioru symboli⁶⁴, których znaczenie każdorazowo należy ustalać w wyniku naszej subiektywnej ich interpretacji.

Rozdźwięk między omówionymi pojęciami logicznie jest nieunikniony. Informacja nie może być wyłącznie zbiorem danych – surowym materiałem inkorporującym dane. W pojęciu informacji zawiera się bowiem dodatkowo subiektywny efekt interpretacji danych opisujący określony stan rzeczywistości oraz usytuowany w opozycji do neutralnych semantycznie danych⁶⁵. W dobie transmisji teleinformatycznych dane są zbiorem bitów i bajtów, które nie muszą mieć logicznego związku, w przeciwieństwie do informacji, która zawsze ma znaczenie – jest użyteczna. Przy tak obranych założeniach wydaje się, że myśl Léona Brillouina, traktująca informację jako zbiór danych, nie wyraża w pełni jej funkcji oraz istoty⁶⁶.

Ze zbioru cech informacji wynika, że można pojmować jej naturę różnorodnie. Matematyczna teoria informacji kładzie nacisk na sposób oraz ilość transmitowanej informacji (ustalanej za pomocą konwencjonalnej jednostki miary, czyli opisanego wcześniej bitu), przesyłanej kanałami łączności za pośrednictwem sygnału fizycznego⁶⁷. Teorie językowe analizują logiczne, semantyczne i pragmatyczne powiązania tekstów, z kolei teorie systemowe uwidaczniają wzajemne relacje i zależności informacji

⁶³ Szerzej na ten temat: A. Adamski, *Prawo karne...*, s. 38.

⁶⁴ Szerzej na ten temat: K. Dobrzeńcki, *Prawo a etos cyberprzestrzeni*, Toruń 2004, s. 16.

⁶⁵ C. Stoll napisał: „Dane jako takie nie są informacją, podobnie jak pięćdziesiąt ton cementu nie jest drapaczem chmur. Dane to ziarenka piasku bez logicznego związku”. C. Stoll, *Krzemowe remedium*, przeł. T. Hornowski, Poznań 2000, s. 226-227.

⁶⁶ Por. L. Brillouin, *Nauka a teoria informacji*, przeł. S. Mazurek, J. Szklanny, Warszawa 1969, s. 17.

⁶⁷ Szerzej na ten temat: J. Petzel, *Informatyka...*, s. 36 i n.

w dziedzinie badanego systemu, zaś cybernetyczne teorie eksponują sprzężenie zwrotne informacji wraz z wszelkimi zmianami stanów panującymi w określonym systemie⁶⁸.

Każda definicja w pewien sposób wyłania sens informacji. Jej istotą i naczelną funkcją zarazem jest pogłębianie ludzkiej wiedzy, doświadczenia i budowanie coraz to szerszego wyobrażenia o otaczającej nas rzeczywistości. Bez względu na fizyczny charakter wydobywania informacji (np. w sposób wzrokowy, słuchowy, smakowy), dziedzinę nauki czy właściwości metrologiczne (np. mierzalne, jak wiek, waga, i niemierzalne, jak kolor, zawód)⁶⁹ jej rolą jest wzbogacenie ludzkiej myśli. Forma zaś uzależniona jest od stopnia rozwoju cywilizacji. Początkowo były to przekazy werbalne, następnie treści utrwalane w kamieniu, później wynalazek Gutenberga aż do obecnego cyfrowego (niematerialnego) przekazu informacji. Każda informacja powstaje bowiem i jest rozpoznawalna przez odbiorcę jako wynik sygnałów służących przesyłaniu lub gromadzeniu wiadomości, przy założeniu, iż docierające doń sygnały są prawidłowo dekodowane, a także użyteczne i kompletne⁷⁰. Przy tak obranych założeniach ekspozycyjność, jakość i ilość informacji jest dla adresata współczynnikiem naturalnym.

Związek między informacją a wiedzą jest ewidentny, niemniej pojęcia te nie są tożsame. Sam dostęp do informacji bez odpowiedniej ich analizy i umiejętności abstrakcyjnego myślenia nie stanowi gwarancji poszerzenia bądź nawet zdobycia wiedzy. Informacja jest elementarnym budulcem wiedzy, stymulatorem i niezbędnym składnikiem procesów myślowych. Stanowi „wewnętrzną strukturę odpowiadającą i koordynującą procesy rozgrywane się w umyśle człowieka”⁷¹.

⁶⁸ Szerzej na ten temat: J. Gołaczyński (red.), *Prawne i ekonomiczne aspekty...*, s. 15.

⁶⁹ Por. W. Sobczak, W. Malina, *Metody selekcji informacji*, Warszawa 1978, s. 9 i n.

⁷⁰ Szerzej na ten temat: A. Pomykański, *Informacja na potrzeby innowacji*, Warszawa 1976, s. 15.

⁷¹ R. Pettersson, *What is Information Design?*, Pittsburgh, PA 1998, s. 107.

Informacja prócz funkcji poznawczej jest też czynnikiem sterującym niemalże wszelakimi zjawiskami społecznymi. Ponadto jest czynnikiem kulturotwórczym, integracyjnym, opiniotwórczym, wychowawczym oraz motywacyjnym⁷². Informacja i jej zasoby (jest ona bowiem wielkością mierzalną) stanowią amorficzne tworzywo o nieokiełznanej sile oddziaływania.

5. Właściwości informacji cyfrowej

Na podstawie poczynionych uwag warto wyróżnić reprezentatywne właściwości informacji i jej wpływ na cywilizację w dobie XXI stulecia⁷³:

- 1) daje się gromadzić, przetwarzać, tworzyć i udostępniać, w celu efektywnego wykorzystania i koordynowania procesów podejmowania decyzji;

⁷² Szerzej na ten temat: B. Stefanowicz, *Informacja...*, s. 65-81.

⁷³ Szerzej na ten temat: e-Europe: An information society for all – An Action Plan to be presented in view of the Sevilla Europe Council, 21/22 June 2002; OECD 1999 – OECD Workshops on the Economics of the Information Society: A Synthesis of Policy Implications, OECD, Paris 1999; e-Polska – Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce na lata 2001-2006, Ministerstwo Infrastruktury, www.mi.gov.pl; e-Polska 2006 – Plan działań na rzecz rozwoju społeczeństwa informacyjnego w Polsce, Ministerstwo Infrastruktury, <http://www.mi.gov.pl>; e-Polska – Strategia informatyzacji Rzeczypospolitej Polskiej, Ministerstwo Nauki i Informatyzacji, <http://www.kbn.pl>; Proponowane kierunki rozwoju społeczeństwa informacyjnego w Polsce do 2020 r., Ministerstwo Nauki i Informatyzacji, <http://www.kbn.pl>; *Spółeczeństwo informacyjne to też zjawisko prawne*, „Gazeta IT” 2 października 2003, nr 9 (17); P. Mullan, *Information Society: Frequency un-asked questions*, <http://www.spiked-online>; C. Shapiro, H. Varian, *Information Rules: A Strategic Guide to the Network Economy*, Cambridge 1998; A. Lekka-Kowalik, *Ukryte założenia społeczeństwa informacyjnego*, [w:] T. Zasępa (red.), *Internet – fenomen społeczeństwa informacyjnego*, Częstochowa 2001; A.M. Wilk, *Polska wobec wyzwań...*; J. Kropiwnicki, *Budowa cywilizacji informacyjnej jako filar długookresowej strategii dla Polski do roku 2025*, [w:] T. Zasępa (red.), *Internet – fenomen...*; T. Goban-Klas, P. Sienkiewicz, *Spółeczeństwo informacyjne: szanse, zagrożenia, wyzwania*, Kraków 1999; Z. Topolewski, *Komputerowe zabezpieczenie poufności informacji w zarządzaniu*, Wrocław 2002; J.J. Szymona, *Wolność i własność w Internecie*, [w:] R. Skubisz (red.), *Internet – problemy prawne*, Lublin 1999; J. Oleński, *Ekonomika informacji*, t. 1, Warszawa 2001.

- 2) jako integralny składnik wytwórczy stanowi znaczną część wartości dodanej większości dóbr i usług;
- 3) podobnie jak inne zasoby (tzn. pieniądź, ziemia i praca) posiada swoją wartość;
- 4) ma niematerialną – cyfrową postać oraz jest przekazywana za pomocą urządzeń teleinformatycznych;
- 5) jest pozbawiona ekskluzywnego charakteru, może być bowiem powielana bez uszczuplania swoich zasobów (liczba informacji nie zmniejsza się w toku jej wykorzystywania);
- 6) cechują ją właściwości synergiczne (wartość sumy informacji jest większa niż suma jej elementów składowych, co bezpośrednio wiąże się z pojęciem jakości informacji);
- 7) znacząco wpływa na współczesną organizację społeczeństwa i funkcjonowanie jego instytucji;
- 8) powielenie jej jest wyjątkowo łatwe, tanie i szybkie, natomiast „kopia” przybiera charakter idealny, ponieważ nie różni się jakością od „oryginału”;
- 9) jej obieg kształtuje świadomość oraz standardy nowoczesnego społeczeństwa;
- 10) stanowi najcenniejsze dobro XXI w., jej zabezpieczenie zaś przed próbami przechwycenia lub ingerencji w jej integralność często wymaga przedsięwzięcia wyjątkowych środków ostrożności.

Elektroniczna postać informacji ma nie tylko ogromny wpływ na stosunki społeczne, lecz przede wszystkim na globalny rynek i mechanizmy ekonomiczne, cechujące się nowatorskimi trendami (np. zwiększenie znaczenia produkcji pozaprzemysłowej, pozarynkowej czy niewłasnościowej, podejmowanej częstokroć w ramach indywidualnych przedsięwzięć)⁷⁴.

⁷⁴ Szerzej na ten temat: Y. Benkler, *Bogactwo sieci. Jak produkcja społeczna zmienia rynki i wolność*, przeł. R. Próchniak, Warszawa 2008, s. 19 i n.

Z powodu cech informacji cyfrowej niebywale trudno jest dokonać jednoznacznego rozgraniczenia produktu cyfrowego od usługi świadczonej w tej formie. Informacja bowiem może spełniać równocześnie obie funkcje (np. można posiadać informację przez uzyskanie do niej dostępu lub nabyć prawo jej skopiowania)⁷⁵. Z technologicznego punktu widzenia produkt cyfrowy niczym się nie różni od usługi cyfrowej. Różnica jest jednakże fundamentalna, gdyby wskazany przykład rozważać na gruncie ekonomicznym. Nie bez znaczenia pozostaje także wpływ informacji cyfrowej na modele społecznych relacji.

6. Informacja a prawo administracyjne

Informacja badana poprzez pryzmat nauki prawa administracyjnego może być definiowana w znaczeniu czynnościowym oraz przedmiotowym. W pierwszym kontekście dotyczy prawnych form działania administracji⁷⁶. Zależnie od przyjętych w doktrynie rozmaitych klasyfikacji można ją zakwalifikować do działań faktycznych o charakterze informacyjnym⁷⁷. Wśród tych działań można wyróżnić dwie zasadnicze grupy: działania informacyjne podejmowane w obrębie struktury organizacyjnej administracji publicznej oraz podejmowane poza nią⁷⁸. Pierwsze wiążą się z koniecznością zapewniania niezbędnej sprawności organów administracyjnych, stąd działania informacyjne mają na celu gwarancję dostatecznego

⁷⁵ W. Cellary, *Techniki internetowe*, Poznań 2005, s. 20-21.

⁷⁶ G. Szpor, *Informacja w zagospodarowaniu przestrzennym. Zagadnienia administracyjno-prawne*, Katowice 1998, s. 21.

⁷⁷ Stworzona w doktrynie prawa koncepcja działań faktycznych uznaje je za dopuszczalną, niewadliwą, uzupełniającą działania prawne administracji publicznej kategorię działań podejmowanych na podstawie i w granicach obowiązujących przepisów prawnych. Można zastosować klasyfikację działań faktycznych, która obejmuje dwa sektory: formy działań faktycznych w stosowaniu prawa oraz pozostałe formy działań faktycznych, w tym o charakterze informacyjnym. Szerzej na ten temat: A. Błaś, [w:] J. Boć (red.), *Prawo administracyjne*, Wrocław 2007, s. 339-350.

⁷⁸ *Ibidem*, s. 347.

poziomu koordynacji, kontroli, nadzoru oraz szybkości podejmowanych w łonie administracji działań. Z kolei działania z drugiej grupy zapewniają realizację podstawowych praw podmiotowych obywateli, mających prawo do uzyskania wyczerpującej informacji na tematy związane z funkcjonowaniem aparatu państwowego oraz istotnymi interesami prywatnymi i zawodowymi.

W prawie administracyjnym przedmiotowe ujęcie pojęcia informacji jest wyrażane przez określenie dokonywanej czynności, np. pozyskiwanie, przetwarzanie, gromadzenie czy udzielanie informacji⁷⁹. Poszczególne czynności są opisane w przepisach prawnych, w różnym znaczeniu i kontekście. Należy podkreślić, że cały proces stanowienia oraz stosowania prawa może być traktowany „jako proces przetwarzania informacji faktualnych i prawnych przyjmując, że w odniesieniu do zagadnień prawnych informacją jest wszelki komunikat werbalny sformułowany w danym kodzie językowym, którego treścią jest wiadomość, pytanie, nakaz, zakaz lub przyzwolenie określonego działania lub zaniechania”⁸⁰. Wraz z obowiązkiem publikowania prawa składają się one na mechanizm kreacji normatywnej w państwie będący szeroko pojmowanym procesem informacyjnym, obejmującym gromadzenie, przetwarzanie, udostępnianie informacji.

Rozważając zaś wpływ informacji na zakres czynności podejmowanych przez podmioty administrujące (stąd wykraczając poza nawias administracji publicznej), można przyjąć, że realizacja zadań tych podmiotów spoczywa na odpowiednim wykorzystaniu informacji. Całokształt działań prawnych obejmujących administrację publiczną można opisać, stosując deskrypcję opartą na operacjach dotyczących informacji (na jej gromadzeniu, udostępnianiu, utrwalaniu, przekształcaniu i przekazywaniu)⁸¹.

⁷⁹ G. Szpor, *Informacja w zagospodarowaniu...*, s. 24.

⁸⁰ W. Lang, A. Mrózek, *Proces stosowania prawa jako proces przetwarzania informacji*, „Państwo i Prawo” 1970, nr 7, za: G. Szpor, *Informacja w zagospodarowaniu...*, s. 25.

⁸¹ Szerzej na ten temat: G. Sibiga, *Stosowanie technik informatycznych w postępowaniu administracyjnym ogólnym*, Warszawa 2019, s. 14-15 wraz z podaną tam literaturą.

Informacja pełni zatem wiele funkcji, które to z kolei można zakwalifikować do konkretnej kategorii. Określona informacja może pełnić rolę⁸²: informacyjną, decyzyjną, sterowania albo konsumpcyjną, natomiast w ramach tych kategorii można wyłaniać subkategorie, np. wyodrębniać funkcje procesów informacyjnych⁸³, to znaczy generowania, gromadzenia, przechowywania, przetwarzania, przekazywania, udostępniania, interpretacji, wykorzystania czy usuwania. Cel takiej klasyfikacji jest uzależniony od obranego modelu procesów informacyjnych lub systemu informacyjnego. Regulacje prawne są natomiast uzupełnieniem przyjętych mechanizmów w ramach założonego modelu.

7. Informacja publiczna a prawo administracyjne

Zagadnienie *e-government*, czyli elektronicznego rządu lub elektronicznej administracji publicznej (zwanej też e-administracją bądź elektronicznym zarządzaniem, a nawet elektronicznym państwem), jest pojmowane w sposób niejednolity zarówno w literaturze obcojęzycznej, jak i polskiej. Abstrahując od kwestii definicyjnych tego pojęcia (materii dotyczącej sfer e-administracji), w kontekście dostępu do informacji publicznej należy skonstatować, że elektroniczna administracja publiczna realizuje się na etapie skierowanej do lub przychodzącej od administracji publicznej komunikacji za pomocą środków przekazu elektronicznego w wymiarach: udostępniania informacji, wykonywania praw i obowiązków, realizowania idei społeczeństwa partycypacyjnego.

Usługi publiczne, nazywane również często „e-usługami”, wiążą się bezpośrednio z zagadnieniem elektronicznego urzędu. Z punktu widzenia tzw. „klientów” administracji do najważniejszych składników e-urzędu należą: pełna integracja świadczeń dostępnych dla odbiorców w sposób

⁸² M. Maciejewski, *Prawo informacji – zagadnienia podstawowe*, [w:] W. Góralczyk (red.) *Prawo informacji. Prawo do informacji*, Warszawa 2006, s. 32-33.

⁸³ Szerzej na ten temat: J. Oleński, *Ekonomika informacji*, Warszawa 2000, s. 24.

intuicyjny oraz zapewnienie do nich dostępu za pomocą różnych środków komunikacji elektronicznej. Z punktu widzenia organu świadczącego usługi e-urząd to całokształt procesów składających się na relacje zewnętrzne z klientami administracji, przy właściwym wykorzystaniu teleinformatycznego zaplecza.

Zasadniczo można wyróżnić trzy sfery komunikacji elektronicznej nawiązywanej przez e-administrację: między organem a organem, organem a klientem administracji oraz w łonie samego organu. Tworzą one dwa typy stosunków administracyjnoprawnych (wewnętrzne oraz zewnętrzne), które mogą być zawiązywane za pośrednictwem sieci teleinformatycznych (usługa sieciowa, najczęściej stosowana metoda przez e-urzędy) lub za pomocą informatycznych nośników danych. Forma komunikacji każdorazowo przybiera postać elektroniczną, ściślej – cyfrową.

Dodatkowo można wskazać relacje zewnętrzne, jakie organ nawiązuje, świadcząc tzw. „usługi w ramach e-urzędu”. Przybierają one postać: informacyjną, interakcyjną (z ewentualnym wyróżnieniem interakcji dwukierunkowej) oraz transakcyjną. Wskazana kolejność nie jest przypadkowa i wiąże się ze stopniem zaawansowania świadczonej usługi. Informowanie przybiera bowiem charakter pasywny (zwłaszcza jeśli jest realizowany w trybie tzw. „bezwniioskowego” dostępu do informacji), natomiast interakcja związana jest z aktywnym komunikowaniem się z elektronicznym urzędem. Faza transakcyjna jest uwięzieniem koncepcji e-urzędu, gdyż najczęściej stanowi o możliwości załatwienia określonej sprawy w drodze komunikacji elektronicznej. Nie musi się zakończyć wydaniem aktu administracyjnego, lecz zawsze skutkuje nawiązaniem stosunku prawnego za pomocą środków komunikacji elektronicznej. Proces świadczenia konkretnej usługi przez e-urząd może obejmować kilka relacji, począwszy od informowania, przez nawiązanie interakcji, do fazy kończącej sprawę, czyli transakcji.

Częstokroć w publikacjach odnoszących się do zagadnienia elektronicznej administracji publicznej wskazywany jest obowiązek udostępnienia

informacji publicznej drogą komunikacji elektronicznej przez organ jako fundamentalny początek rozwoju samej e-administracji. Trudno bowiem wyobrazić sobie bardziej złożone relacje w płaszczyźnie organ administrujący a podmiot zainteresowany (najczęściej strona lub uczestnik postępowania), jeśli zasadniczy proces informowania o sprawach publicznych lub udostępniania dokumentów urzędowych za pośrednictwem Internetu nie będzie odbywał się sprawnie i bez ograniczeń w tej materii. Oczywiście zawężanie pojęcia elektronicznej administracji publicznej li tylko do sfery udostępnia informacji publicznej nie oddaje (definiuje) całego spektrum, jakie oferuje (lub bynajmniej teoretycznie powinna kreować) e-administracja. Nie można bowiem ograniczać ram e-administracji wyłącznie do problematyki dostępu obywateli do zasobów informacji publicznej w formie elektronicznej oraz uprawnień i obowiązków z niego wynikających⁸⁴.

W polskim porządku prawa publicznego (zwłaszcza administracyjnego) udostępnienie informacji publicznej zawartej w dokumentach urzędowych zawsze powinien poprzedzać proces analizy danych oraz informacji. Finalnym skutkiem owej analizy powinna być odpowiedź: jakie typy danych zawartych w dokumencie urzędowym przed jego udostępnieniem lub opublikowaniem powinny zostać usunięte tudzież trwale zmodyfikowane, aby skutecznie uniemożliwić dokonanie rozpoznania konkretnych faktów, podmiotów, okoliczności. W dużej mierze ów analityczny proces jest swoistym kompromisem między udostępnianiem informacji w celu ich upublicznienia a potrzebą przestrzegania obowiązujących norm prawnych gwarantujących ochronę określonych dóbr i wartości. Bogate spektrum normatywne kreuje bowiem szereg instytucji prawa, których zadaniem jest ochrona: tajemnic prawem chronionych, ochrona prawa do prywatności, danych osobowych czy ochrona informacji niejawnych. Czynności analityczne poprzedzające upublicznienie dokumentu (względnie jego wydanie wnioskodawcy) mają zatem spełniać

⁸⁴ Por. M. Kowalczyk, *E-urząd w komunikacji z obywatelem*, Warszawa 2009.

wymogi stawiane przez ustawodawcę w sferze powszechnego udostępnienia informacji publicznej i jednocześnie zagwarantować ochronę określonych dóbr i wartości prawem chronionych. Można przyjąć na potrzeby niniejszych rozważań, że powyższy proces będzie określony mianem anonimizacji, która stanowi swoistą próbę wyważenia interesów normatywnie równoległych, lecz konkurujących ze sobą. Obowiązek udostępnianiem informacji w celu jej upublicznienia zagwarantowana ustawowo jest bowiem normą prawną swoście „konkurującą” z potrzebą przestrzegania obowiązujących norm prawnych określających zakres podmiotowy i przedmiotowy informacji objętych ochroną.

Kluczowym zagadnieniem w przypadku ustawowo chronionych danych lub informacji jest kwestia obowiązku podmiotu do zachowania w tajemnicy określonych danych chronionych prawem. Stąd w większości przypadków ujawnienie w treści dokumentu urzędowego owych informacji skutkowałoby naruszeniem bądź niewypełnieniem tych obowiązków (wyrażonych w normach opisujących zachowanie należytej staranności przed bezprawnym ich ujawnieniem) podmiotu zobowiązanego. Jedynie w wyjątkowych przypadkach ujawnienie danych ustawowo chronionych nie będzie skutkowało naruszeniem obowiązku podmiotu zobowiązanego do zachowania określonej ustawowo tajemnicy. W takich przypadkach obowiązek zachowania tajemnicy przekształca się (w sferze podmiotowej) w uprawnienie takiego podmiotu.

Należy mieć na uwadze konieczność zdwojonej staranności przy tych typach danych objętych ustawową ochroną, które przez normę generalną kształtują obowiązek zachowania określonej tajemnicy, tzn. w której adresatem obowiązku zachowania tajemnicy jest „każdy”. W takich przypadkach prawdopodobieństwo wystąpienia danych ustawowo chronionych w dokumentach urzędowych jest zdecydowanie większe. Jednocześnie, prócz szerokiego wachlarza informacji chronionych

prawem⁸⁵, istnieje obszar – swego rodzaju subdziedzina – który został objęty ochroną szczególną z uwagi na typ danych oraz konieczność ich ochrony. Są to bowiem dane osobowe, których ochrona nabrała w ostatnim okresie istotnego znaczenia (choć nie tylko w sferze normatywnej). Regulacje krajowe oraz wspólnotowe nałożyły na państwo polskie w tej materii szereg nowych instytucji prawnych⁸⁶.

Prawo administracyjne w materii prawnej związanej z dostępem do informacji publicznej nie ogranicza się li tylko do sfery podmiotowej oraz przedmiotowej, ale obejmuje swym normatywnym zakresem również

⁸⁵ Jedynie analizując źródła prawa rangi ustawowej, można wskazać ponad pięćdziesiąt rodzajów informacji (tajemnic) objętych ochroną prawną. Tytułem przykładu można wskazać:

- a) tajemnicę informacji niejawnych określoną w ustawie z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2019 r. poz. 742 ze zm.);
- b) tajemnicę przedsiębiorstwa określoną w ustawie z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2020 r. poz. 1913 ze zm.); również tajemnicę przedsiębiorstwa określoną w ustawie z dnia 12 grudnia 2003 r. o ogólnym bezpieczeństwie produktów (t.j. Dz. U. z 2016 r. poz. 2047 ze zm.);
- c) tajemnicę przedsiębiorcy określoną w ustawie z dnia 25 sierpnia 2006 r. o bezpieczeństwie żywności i żywienia (t.j. Dz. U. z 2019 r. poz. 1252 ze zm.);
- d) tajemnicę biocy i dawcy organów do przeszczepu określoną w ustawie z dnia 1 lipca 2005 r. o pobieraniu, przechowywaniu i przeszczepianiu komórek, tkanek i narządów (t.j. Dz. U. z 2019 r. poz. 1405 ze zm.);
- e) tajemnicę statystyczną określoną w ustawie z dnia 29 czerwca 1995 r. o statystyce publicznej (t.j. Dz. U. z 2020 r. poz. 443 ze zm.);
- f) tajemnicę własności przemysłowej określoną w ustawie z dnia 30 czerwca 2000 r. – Prawo własności przemysłowej (t.j. Dz. U. z 2020 r., poz. 286 ze zm.);
- g) tajemnicę bankową określoną w ustawie z dnia 29 sierpnia 1997 r. – Prawo bankowe (t.j. Dz. U. z 2020 r. poz. 1896 ze zm.);
- h) tajemnicę dziennikarską określoną w ustawie z dnia 26 stycznia 1984 r. – Prawo prasowe (t.j. Dz. U. z 2018 r. poz. 1914 ze zm.).

Również na temat określonych typów tajemnic rozpatrywanych w kontekście prawa do prywatności wyrażonego w przepisach szczególnych A. Mednis, *Prawo do prywatności a interes publiczny*, Kraków 2006, s. 152-178.

⁸⁶ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119 z 4.05.2016 r., s. 1); tzw. ogólne rozporządzenie o ochronie danych, dalej jako: RODO; ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781, dalej jako: u.o.d.o.).

sferę technologiczną (informatyczną). Warto w tym miejscu zaakcentować, że w polskim porządku prawnym relatywnie od niedawna obowiązuje ustawa o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych⁸⁷. Ustawodawca prócz licznych aspektów natury technicznej zdefiniował m.in. takie pojęcia dotyczące stron internetowych i aplikacji mobilnych, jak: kompatybilność, postrzegalność, funkcjonalność czy zrozumiałość⁸⁸. Ujednolicenie w sensie technologicznym ma stanowić fundament pod likwidację barier (w tym przypadku cyfrowych) dla odbiorców informacji publicznej, zwiększając przy tym transparentność funkcjonowania sektora finansów publicznych⁸⁹ (poprzez większą i prostszą dostępność o działalności tych podmiotów w Internecie oraz aplikacjach), i jednocześnie stanowić kolejny etap szeroko rozumianego procesu interoperacyjności systemów teleinformatycznych tych podmiotów.

8. Anonimizacja oraz pseudonimizacja – definicje

Pojęcie anonimizacji ma swoje źródło w potocznym określeniu czynności związanych z potrzebą usunięcia danych osobowych w dokumentach urzędowych udostępnianych w trybie ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej⁹⁰. Zdumiewające, iż zarówno w samej u.d.i.p., jak i pozostałych aktach normatywnych rangi ustawowej ustawodawca nie stworzył legalnej definicji tego procesu. To właśnie czynności o charakterze materialno-technicznym sprowadzające się do udostępnienia informacji publicznej (czy to w ramach BIP, czy też zadość czyniąc żądaniom wnioskodawców) zdeterminowały konieczność

⁸⁷ Ustawa z dnia 4 kwietnia 2019 r., Dz. U. z 2019 r. poz. 848.

⁸⁸ Szerzej na ten temat: G. Szpor, [w:] G. Szpor, K. Czaplicki (red.), *Ustawa o dostępności stron internetowych i aplikacji mobilnych podmiotów publicznych, Komentarz*, Warszawa 2020, s. 53-65.

⁸⁹ W rozumieniu ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz. U. z 2020 r. poz. 1175).

⁹⁰ T.j. Dz. U. z 2019 r. poz. 1429 ze zm., dalej jako: u.d.i.p.

refleksji nad tym, w jaki sposób ową informację publiczną udostępnić, a co za tym następuje, czy wraz z udostępnieniem informacji publicznej nie zachodzi ryzyko (choćby potencjalne) naruszenia (lub kolizji) innych praw podmiotowych, względnie czy nie zachodzi proces interferencji określonych wartości prawem chronionych. Można skonstatować, że na długo przed pojawieniem się pierwszych przepisów, zaleceń czy też innych normatywnych odniesień do anonimizacji pojęcie to trwale wkomponowało się w mechanizmy związane z udostępnianiem informacji publicznej. W taki sposób określano czynności dotyczące usuwania określonych typów danych, w tym zwłaszcza danych osobowych. Taka zresztą interpretacja czynności związanych z anonimizacją była stosowana przez przedstawicieli sektora finansów publicznych oraz sędziów i pracowników administracyjnych wymiaru sprawiedliwości⁹¹. Koreluje ona zresztą z motywem 154 RODO, stanowiącym o tym, że: „[...] organ publiczny lub podmiot publiczny powinny móc publicznie ujawniać dane osobowe z dokumentów przez siebie przechowywanych, jeżeli takie ujawnienie jest przewidziane przepisami prawa Unii lub prawa państwa członkowskiego, któremu organ ten lub podmiot podlegają. Przepisy takie powinny godzić publiczny dostęp do dokumentów urzędowych i ponowne wykorzystywanie informacji sektora publicznego z prawem do ochrony danych osobowych, i dlatego mogą przewidywać niezbędne uwzględnienie prawa do ochrony danych osobowych na podstawie niniejszego rozporządzenia [...]”. Anonimizacja częstokroć jest zatem zrównana z depersonalizacją danych dotyczących osoby fizycznej⁹².

W taki też sposób określa anonimizację międzynarodowy standard normy technicznej (ISO/IEC 29100:201) zatytułowanej „Privacy framework”.

⁹¹ A. Gomułowicz, W. Sawczyn, *Jawność rozprawy a bezpieczeństwo prawne jednostki*, [w:] E. Bielak-Jomaa, U. Góral (red.), *Wdrożenie ogólnego rozporządzenia o ochronie danych osobowych. Aspekty proceduralne*, Warszawa 2018, s. 120.

⁹² Szerzej na ten temat: K. Wojsyk, *Przetwarzanie danych osobowych wrażliwych w systemach informatycznych ochrony zdrowia i ich anonimizacja*, [w:] G. Szpor, K. Czapliski (red.), *Przetwarzanie danych osobowych*, Warszawa 2019, s. 121-122.

Anonimizacja ma za zadanie „w sposób nieodwracalny zmienić informacje związane (powiązane) z osobą w sposób uniemożliwiający bezpośrednio lub pośrednio identyfikację podmiotu tej informacji przez administratora informacji działającego samodzielnie lub we współpracy z jakąkolwiek inną stroną”⁹³.

Pomimo braku definicji legalnej anonimizacji można przedstawić pewne odniesienia do tego pojęcia w przepisach prawa. Stąd:

- a) anonimizacja danych występowała już na gruncie ustawy o ochronie danych osobowych z 1997 r., gdzie w art. 2 ust. 3 wyartykułowana została obok czynności usunięcia danych⁹⁴. Na marginesie można jedynie dodać, że w doktrynie prawa powstał istotny dylemat dotyczący sposobu interpretacji obowiązków współistniejących z procesem anonimizacji, ujętych zaś we wskazanych przepisach już nieobowiązującej ustawy⁹⁵;
- b) wzmianka o anonimizacji jest też zawarta w ustawie o świadczeniu usług drogą elektroniczną⁹⁶ w art. 19 ust. 2 pkt 2 i ust. 4 w zw. z art. 18 ust. 4 oraz ust. 5, stanowiąc, że „[...] dla celów reklamy, badania rynku oraz zachowań i preferencji usługobiorców z przeznaczeniem wyników tych badań na potrzeby polepszenia jakości usług świadczonych przez usługodawcę, za zgodą usługobiorcy, dopuszcza się jedynie zestawianie danych dotyczących

⁹³ Anonymization – “process by which personally identifiable information (PII) is irreversibly altered in such a way that a PII principal can no longer be identified directly or indirectly, either by the PII controller alone or in collaboration with any other party”, <https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:en> [dostęp: 31.05.2022 r.].

⁹⁴ Termin ten nie został jednak w ustawie zdefiniowany, stanowił bowiem alternatywę wobec usuwania danych po ich wykorzystaniu ze zbiorów danych osobowych sporządzanych doraźnie, wyłącznie z względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922 ze zm.).

⁹⁵ Szerzej na ten temat: J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych, Komentarz*, Kraków 2007, s. 317-320.

⁹⁶ Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz. U. z 2020 r. poz. 344 ze zm.).

korzystania przez usługobiorcę z różnych usług świadczonych drogą elektroniczną, pod warunkiem usunięcia wszelkich oznaczeń identyfikujących usługobiorcę lub zakończenie sieci telekomunikacyjnej albo system teleinformatyczny, z którego korzystał (anonimizacja danych)”. Wskazane przepisy nie konstruują definicji, lecz wskazują jedynie rodzaje danych, które powinny zostać usunięte, a ściślej:

- 1) oznaczenia identyfikujące usługobiorcę nadawane na podstawie danych;
 - 2) oznaczenia identyfikujące zakończenie sieci telekomunikacyjnej lub system teleinformatyczny, z którego korzystał usługobiorca;
 - 3) informacje o rozpoczęciu, zakończeniu oraz zakresie każdorazowego korzystania z usługi świadczonej drogą elektroniczną;
 - 4) informacje o skorzystaniu przez usługobiorcę z usług świadczonych drogą elektroniczną;
 - 5) inne, które nie są niezbędne dla świadczenia usług, za zgodą usługobiorcy.
- c) Pojęcie anonimizacji można odnaleźć także w ustawie – prawo telekomunikacyjne⁹⁷, a ściślej w art. 166 w ust. 2 w zw. z ust. 1 stanowiącym, że: „W celu wykorzystania danych o lokalizacji dostawca publicznie dostępnych usług telekomunikacyjnych jest obowiązany:
- 1) uzyskać zgodę abonenta lub użytkownika końcowego na przetwarzanie danych o lokalizacji jego dotyczących, która, z zastrzeżeniem art. 174, może być wycofana okresowo lub w związku z konkretnym połączeniem, lub
 - 2) dokonać anonimizacji tych danych”.

⁹⁷ Ustawa z dnia 16 lipca 2004 r. – prawo telekomunikacyjne (t.j. Dz. U. z 2019 r. poz. 2460 ze zm.).

Jak wprost wynika w przytoczonych przepisów, ustawodawca w przepisach prawo telekomunikacyjne posługuje się terminem anonimizacji, bez dokładnego wyjaśnienia owego terminu (bez wskazania definicji legalnej), lecz wyłącznie jako przesłanki zwalniającej z obowiązku udzielenia zgody na przetwarzanie danych dotyczących lokalizacji podmiotów (abonentów czy tzw. użytkowników końcowych).

- d) anonimizacja jest również przez ustawodawcę wskazana w ustawie o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji⁹⁸. Występuje w kontekście nakładania kar pieniężnych, a następnie publikowania decyzji administracyjnych ostatecznych na łamach strony internetowej, zgodnie z procedurą ujętą w art. 339 ust. 3 tej ustawy, albowiem ustawodawca zawarł następujące zasady publikacji: „Odpowiednio Komisja Nadzoru Finansowego albo Fundusz dokonują publikacji informacji o nałożeniu kary, o której mowa w ust. 2, w formie zanonimizowanej, w przypadku gdy:
- 1) kara została nałożona na osobę fizyczną, a ujawnienie jej imienia i nazwiska byłoby środkiem niewspółmiernym do wagi dokonanego naruszenia;
 - 2) ujawnienie nazwy (firmy) podmiotu lub imienia i nazwiska osoby stanowiłoby zagrożenie dla stabilności rynków finansowych lub zagroziłoby prowadzonemu postępowaniu karnemu lub postępowaniu w sprawach o przestępstwa skarbowe;
 - 3) ujawnienie nazwy (firmy) podmiotu lub imienia i nazwiska osoby wyrządziłoby niewspółmierną szkodę tej osobie lub podmiotowi”⁹⁹.

⁹⁸ Ustawa z dnia 10 czerwca 2016 r. o Bankowym Funduszu Gwarancyjnym, systemie gwarantowania depozytów oraz przymusowej restrukturyzacji (t.j. Dz. U. z 2020 r. poz. 842 ze zm.).

⁹⁹ Analogicznie jak w wyżej wskazanych przykładach nie odnajdziemy definicji legalnej pojęcia anonimizacji. W analizowanym przypadku przepisy zawierają tylko przesłanki konieczne do rozważania w czynnościach poprzedzających publikację w Internecie, a zatem

Wydaje się, że każda próba zdefiniowania pojęcia anonimizacji powinna zostać poprzedzona analizą poszczególnych jej elementów, a ściślej:

- a) celu anonimizacji;
- b) granic (zakresu) anonimizacji;
- c) technik i sposobów jej realizacji;
- d) metodologii jej dokonania.

Znamienne jest przy tym nierozzerwalne skorelowanie wszystkich powyższych elementów składowych anonimizacji, na tyle trwałe i wzajemne, iż określenie jednego z nich pociąga automatycznie konieczność doszczegółowienia pozostałych (dla przykładu: definiując cel anonimizacji należy od razu wskazać metodę oraz granicę i sposób jej dokonania)¹⁰⁰.

Pseudonimizacja w przeciwieństwie do anonimizacji została zdefiniowana w prawie. Obecnie podstawową definicją legalną (z uwagi na zakres i częstotliwość jej zastosowania) jest definicja zawarta w art. 4 pkt 5 RODO, która stanowi, że pseudonimizacja oznacza przetwarzanie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Motyw 26 RODO rozwija kwestie dalej idące, a mianowicie zakres pseudonimizacji rozważany w kontekście prawdopodobieństwa zidentyfikowania owej osoby fizycznej na podstawie dodatkowych informacji z nią związanych. Warto w tym momencie przytoczyć dwie zasadnicze tezy ujęte w tym motywie:

upublicznienia pewnych informacji dotyczących podmiotów prawa. Wychodząc naprzeciw postulatowi kreowanemu przez przedstawicieli „sfery sektora publicznego” zobligowanych do udostępniania informacji publicznej, można skonstatować, że zasadniczym postulatem *de lege ferenda* jest zdefiniowanie pojęcia anonimizacji oraz procesu na niego się składającego w akcie prawnym rangi ustawowej.

¹⁰⁰ Por. uwagi w dalszej części artykułu.

- a) aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądne prawdopodobne sposoby, w stosunku do której istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej;
- b) aby zaś stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny.

Pseudonimizacja jest także procesem rekomendowanym jako rozwiązanie wspierające do celów badań naukowych lub historycznych, do celów statystycznych lub archiwalnych w interesie publicznym¹⁰¹. Jest ponadto dodatkowym zabezpieczeniem stosowanym w przypadku przetwarzania danych w celu innym niż cel, w którym dane osobowe zostały zebrane (zgodnie z art. 6 ust. 4 lit. e RODO).

Z przytoczonych przepisów wynika zatem zasadnicza cecha danych psseudonimizowanych, czyli ich odwracalny charakter. W przeciwieństwie do procesu anonimizacji dane osobowe poddane pseudonimizacji mogą zostać (jeśli zajdzie taka konieczność) poddane procesowi odwrotnemu, przywracającemu walor danych osobowych, oczywiście przy założeniu powtórnego powiązania uprzednio odseparowanych danych. Innymi słowy informacja poddana pseudonimizacji nie traci przez tę czynność waloru danych osobowych. Można wręcz skonstatować, że informacja psseudonimizowana jest etapem pośrednim, swoiście pojmowanym

¹⁰¹ Motyw 156 RODO oraz art. 89 ust. 1 RODO.

łącznikiem danych osobowych z danymi anonimowymi¹⁰². Różnic między analizowanymi procesami jest znacznie więcej¹⁰³.

9. Anonimizacja – techniki i sposoby jej realizacji

Problematykę poświęconą technikom realizacji anonimizacji można rozwarstwić na dwie płaszczyzny, a mianowicie badać ją w:

- a) ujęciu przedmiotowym;
- b) aspekcie podmiotowym.

Pierwsza z wymienionych dotyczy się aspektów *stricte* technologicznych. Innymi słowy jak można przeprowadzić proces anonimizacji w sensie instrumentalnym. Przesądzenie określonej metody (techniki) konstytuuje sposób, w jaki ostatecznie anonimizacja jest rekomendowana, czy też wdrożona w określoną procedurę, a następnie wprowadzona w życie określonym aktem normatywnym (np. w regulaminie, zarządzeniu *etc.*).

W dokumencie zatytułowanym: „Opinia 05/2014 w sprawie technik anonimizacji”, którego autorem są członkowie tzw. „Grupy Roboczej art. 29”, dokonano przeglądu wielu informatycznych metod dotyczących anonimizacji danych osobowych¹⁰⁴. Zasadniczo można wyodrębnić dwa zbiory technik anonimizacyjnych:

- a) oparte na randomizacji;
- b) oparte na uogólnianiu.

¹⁰² Por. P. Litwiński (red.), P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018, s. 207.

¹⁰³ Podsumowanie owych różnic między anonimizacją a pseudonimizacją znajduje się w dalszej części artykułu, w konkluzjach.

¹⁰⁴ Dokument jest dostępny m.in. pod następującym adresem internetowym: https://te-chinfo.uodo.gov.pl/wp-content/uploads/2018/10/Opinia-5_2014-w-sprawie-technik-anonimizacji-z-dnia-10-kwietnia-2014-r.-wersja-.pdf [dostęp: 31.05.2022 r.] pod sygnaturą: 0825/14/PL WP216; dalej jako: *Opinia Grupy Roboczej*.

Metodyka randomizacyjna tworzy rodzinę technik, która „[...] zmniejsza prawdziwość danych w celu wyeliminowania ścisłego związku między danymi a konkretną osobą fizyczną”¹⁰⁵. Wśród randomizacji można wymienić:

- a) technikę dodawania zakłóceń¹⁰⁶;
- b) permutację jako szczególną formę dodawania zakłóceń¹⁰⁷.
- c) prywatność różnicową¹⁰⁸.

Uogólnianie stanowi natomiast drugą rodzinę technik anonimizacji. Polega „[...] na uogólnianiu lub osłabianiu atrybutów osób, których dane dotyczą, poprzez modyfikowanie odpowiedniego zakresu lub rzędu wielkości (tj. raczej region, a nie miasto, raczej miesiąc, a nie tydzień)”¹⁰⁹. Podobnie jak randomizacja, uogólnianie może mieć swoje mutacje, wśród których najczęściej stosowane są:

- a) techniki agregacji i k-anonimizacji mające na celu uniemożliwienie wyodrębnienia osoby¹¹⁰;
- b) l-dywersyfikacja jest rozszerzeniem k-anonimizacji „[...] w celu zapewnienia, aby deterministyczne ataki oparte na wnioskowaniu nie były już możliwe poprzez zagwarantowanie, że w każdej klasie równoważności każdy atrybut ma co najmniej l różnych wartości”¹¹¹;
- c) t-bliskość „stanowi udoskonalenie l-dywersyfikacji pod tym względem, że ma na celu utworzenie równoważnych klas, które odzwierciedlają początkową dystrybucję atrybutów w tabeli”¹¹².

¹⁰⁵ *Opinia Grupy Roboczej*, s. 13.

¹⁰⁶ Szerzej na ten temat *ibidem*.

¹⁰⁷ *Ibidem*, s. 15.

¹⁰⁸ *Ibidem*, s. 16.

¹⁰⁹ *Ibidem*, s. 18.

¹¹⁰ Szerzej na ten temat *ibidem*.

¹¹¹ *Ibidem*, s. 20.

¹¹² *Ibidem*.

Abstrahując od aspektów technicznych możliwych do zastosowania podczas przeprowadzenia anonimizacji treści dokumentów, pozostaje jeszcze aspekt podmiotowy, to znaczy jaki podmiot (kto) ją przeprowadza. Zasadniczo odpowiedzialny za przeprowadzenie anonimizacji jest upoważniony pracownik podmiotu zobowiązanego do udostępnienia informacji publicznej. Niemniej wraz z postępem technologicznym coraz częściej mamy do czynienia z automatyzacją procesu anonimizacji, całkowitą lub jego częściową. Wówczas ów upoważniony pracownik (użytkownik) kontroluje jedynie wyniki pracy systemu przeprowadzającego anonimizację lub się nim wspomaga przy jej przeprowadzeniu. Można zatem wyróżnić trzy rodzaje (sposoby) przeprowadzenia anonimizacji:

- a) manualną (człowiek – pracownik przeprowadza w całości anonimizację);
- b) semi-automatyczną (człowiek – pracownik wspomaga się narzędziami informatycznymi w procesie anonimizacji);
- c) automatyczną (system – komputer w pełni dokonuje anonimizację, zaś człowiek – pracownik jedynie nadzoruje jego działanie oraz wyniki analizy treści).

Truizmem jest konstatacja o wypieraniu z procesu analizy treści danych ludzi i zastępowanie ich pracy pracą analityczną wykonywaną przez systemy, bazy danych czy sieci neuronowe bądź imitujące sztuczną inteligencję. Niemniej jednak, pomimo ogromnego postępu technologicznego, analiza semantyczna oraz gramatyczna języka polskiego zapewniająca odpowiednie rozpoznanie określonych typów danych, które docelowo powinny zostać poddane anonimizacji, nadal nastrocza wiele trudności. Nie można bowiem stracić z pola widzenia najważniejszego aspektu automatycznej anonimizacji, jakim jest wymóg prawidłowej anonimizacji, czyli konieczności bezbłędnej analizy morfologicznej treści dokumentu urzędowego.

Na tym tle trwa dyskurs nad zaletami oraz wadami zastosowania elektronicznych narzędzi wspierających tudzież zastępujących człowieka

w procesie anonimizacji. Niewątpliwie system elektronicznej anonimizacji w zestawieniu z tradycyjnym sposobem „ręcznej anonimizacji” posiada wiele zalet. Przede wszystkim wykonuje automatycznie wszelkie czynności związane z anonimizacją treści dokumentu, uzyskując nieporównywalnie większą efektywność procesu anonimizacji oraz eliminując błędy według opracowanego algorytmu. Z uwagi na różnorodne czynniki, takie jak zmęczenie czy też błędna interpretacja określonych typów danych wymagających anonimizacji, człowiek jest bardziej podatny na popełnianie błędów w toku niniejszego procesu aniżeli system dokonujący każdorazowo analizy treści na podstawie identycznego zestawu danych (reguł). Ważną cechą elektronicznego systemu anonimizacji jest również szybkość jego działania, która stwarza szersze możliwości jego wykorzystania, w tym do przetwarzania, udostępniania czy też publikowania informacji publicznej na zdecydowanie większą skalę, niż jest to czynione choćby dotychczas. Ponadto zważyć trzeba, że automatyczna anonimizacja wpływa istotnie na redukcję liczby powtarzalnych czynności wykonywanych przez człowieka, charakterystycznych dla anonimizacji nieautomatycznej. Wreszcie należy podnieść argument o jednolitej metodologii anonimizacji uzyskiwanej dzięki automatyzacji tego procesu¹¹³.

Waga zalet jest niekiedy zestawiana z wagą wad takich systemów. Podstawowym argumentem przemawiającym przeciwko zastosowaniu automatycznej anonimizacji jest pewne „ograniczenie analizy” treści dokumentów urzędowych, które sprowadza się do „nieinteligentnego” wykonywania algorytmu, co z kolei może prowadzić do błędów. Mowa o przypadkach, w których określony typ informacji (typ danych) powinien ze swojej istoty (jako typ danych chroniony normą prawną) zostać zanonimizowany, zaś pozostał w treści i nierzadko został ujawniony. Problem uwidacznia się przy analizie danych kontekstowych, które nie wprost dotyczą określonych danych (choćby osobowych). Ich powiązanie

¹¹³ Por. uwagi dotyczące reguł anonimizacji w dalszej części artykułu.

(dokonane przez odbiorcę) jest naturalnie niedopuszczalne i stanowi błąd anonimizacyjny. Niebawem trudnym zadaniem do wykonania jest opracowanie na tyle „inteligentnego” algorytmu, który będzie skutecznie mógł takie dane kontekstowe prawidłowo zinterpretować i w efekcie usunąć.

Kolejnym wyzwaniem systemów służących do automatycznej anonimizacji jest zjawisko tzw. „semantycznej interferencji danych”. W tych przypadkach następuje scalenie znaczeniowe określonych typów danych, które może wpłynąć na nieprawidłową analizę treści¹¹⁴.

Częstokroć przeciwnicy procesów zastosowania automatyzacji w procesie anonimizacji podnoszą jej „nadmierny charakter”, wskazując na zanonimizowanie treści dokumentów w sposób niepotrzebny. Zakres danych poddanych anonimizacji jest oczywiście uzależniony od reguł anonimizacyjnych, które to mogą z kolei wyznaczać różne granice anonimizacji. Innymi słowy określony system do automatycznej anonimizacji może usuwać określone dane w sposób nadmierny, co wynikać może z przyjętych granic owej anonimizacji, zaś wynikających z reguł kreujących ostateczny limit algorytmu odpowiedzialnego za anonimizację. Problem limitu algorytmu ma dwojaki podłoże:

- a) informatyczne;
- b) prakseologiczne.

Z jednej bowiem strony, twórcy takich systemów napotykają na ograniczenia o charakterze programistyczno-technologicznym, które uniemożliwiają stworzenie algorytmu bezbłędnie wykonującego proces anonimizacji, z drugiej zaś napotykają na ograniczenia natury koncepcyjnej. Te drugie odnoszą się do rozważań przedstawicieli doktryny prawa, uwag i komentarzy osób zajmujących się problematyką dostępu do informacji publicznej oraz doświadczeń osób wykonujących anonimizację manualną.

¹¹⁴ Typowym przykładem jest określenie odnoszące się do przedmiotu, które jednocześnie jest fragmentem nazwiska czy nazwy innego podmiotu (w fikcyjnym nazwisku Adam Koc-Kaprys system mógłby zakwalifikować te dane jako określenia niepoddane anonimizacji zamiast nazwiska osoby fizycznej).

Materia ociera się o wyznaczenie granic, swoiście pojmowanych zakresów, jakimi ma zostać ograniczona (lub zwiększona) anonimizacja. Problem zatem nie ma istic informatycznego charakteru, ale dotyczy też kwestii prakseologicznych¹¹⁵.

Rozważając sposoby realizacji anonimizacji, tym samym kładąc na szali wady i zalety obu metod, zdecydowanie zwycięża automatyczna, nawet jeśli jedynie wspomaga, a nie w pełni zastępuje pracę człowieka. Nie sposób bowiem przecenić korzyści płynących z wykorzystania elektronicznej anonimizacji w porównaniu z jej manualnym odpowiednikiem. Najważniejszą korzyścią jest jej masowe wykorzystanie w tworzeniu baz danych, zwłaszcza dostępnych publicznie i bezpłatnie¹¹⁶.

10. Anonimizacja – metodologia (reguły)

Anonimizacja jest niewątpliwie procesem – sekwencją pewnych czynności. Abstrahując od sposobu czy też od zastosowanej techniki jej przeprowadzenia, w każdym przypadku należy określić, według jakich zasad (rozpatrywanych merytorycznie) będzie dokonywana analiza treści, przesądzająca zarazem typy zanonimizowanych danych. Stąd każdy proces anonimizacji powinien zostać oparty na regułach (swoiście pojmowanych zasadach naczelnych), typizujących rodzaje danych poddanych anonimizacji. Abstrahując od przyjętego modelu anonimizacji, wyznaczającego jej granice (zakres), reguły muszą być jednorodne. Przez to pojęcie rozumiem ich niezmiennosć, swoistą „niepodatnosć” na liczne nowelizacje prawa polskiego bądź przyjęte praktyki osób odpowiedzialnych za anonimizację.

Reguły winny być ponadto uniwersalne, czyli wynikać z ich ogólnego charakteru, odbiegającego od nadmiernej kazuistyki, a także od

¹¹⁵ Por. uwagi w dalszej części artykułu.

¹¹⁶ Jedynie tytułem przykładu można wskazać Portal Orzeczeń Sądów Powszechnych, bazę ponad 380 000 orzeczeń, <https://orzeczenia.ms.gov.pl/> [dostęp: 31.05.2022 r.].

wyjątków stanowiących wyłom w przyjętych metodach interpretacji zbiorów danych, składających się na treść dokumentów urzędowych. Tylko wówczas ów uniwersalizm zapewni spełnienie zasadniczych funkcji udostępnienia informacji publicznej, przy jednoczesnym poszanowaniu wszelkich norm prawnych.

Reguły nie mogą wpływać na zniekształcenie walorów poznawczych udostępnianej informacji publicznej. Muszą zagwarantować taki mechanizm analizy danych (przeprowadzony przez człowieka lub maszynę), aby po ich zanonimizowaniu stworzyć użytkownikowi końcowemu, korzystającemu z udostępnionej informacji, wgląd w możliwie najszersze spektrum informacji dla niego istotnych.

Reguły nie mogą być niekonsekwentnie stosowane. Ze swoistą niekonsekwencją nie będziemy mieli nigdy do czynienia przy stosowaniu automatycznej anonimizacji, z uwagi na determinantę w postaci identycznego algorytmu odpowiedzialnego za jej przeprowadzenie. Niemniej pewne rozbieżności w interpretacji danych lub typów danych poddanych anonimizacji mamy do czynienia każdorazowo w przypadku anonimizacji manualnej¹¹⁷.

Kluczową cechą reguł powinna być ich walidacyjność, przez którą należy rozumieć, iż cały system reguł składający się na zasady anonimizacyjne rzeczywiście prowadzi do zaplanowanego wyniku, którym jest oczywiście bezbłędna analiza danych umożliwiająca prawidłową realizację obowiązku udostępnienia informacji publicznej.

¹¹⁷ Niekonsekwentne stosowanie reguł jest szczególnie widoczne w bazie orzeczeń sądów administracyjnych. Dla przykładu w treści sentencji orzeczenia jest zanonimizowany organ, zaś w uzasadnieniu jest podana pełna nazwa i właściwość miejscowa tego samego organu; lub w sposób odbiegający od przesłanek prawnych (np. imiona i nazwiska członków składu orzekającego nie są poddane anonimizacji, w przeciwieństwie do danych osobowych innych funkcjonariuszy publicznych).

11. Anonimizacja – orzecznictwo

Orzecznictwo sądowe, zwłaszcza sądów administracyjnych, wpłynęło oraz, co istotniejsze przy braku normatywnej definicji tego procesu, walnie wpływa na zrozumienie celu, zakresu oraz jego istoty. Wprawdzie nie udziela odpowiedzi na wszelkie nurtujące pytania związane z anonimizacją, lecz niewątpliwie przybliży wiele aspektów tego procesu. Zgodnie z przyjętym w orzecznictwie sądów administracyjnych „praktyka anonimizacyjna” polega na „zaczernianiu” lub „wybiałkowaniu” określonych fragmentów treści udostępnianie informacji publicznej zawierającej dane osobowe¹¹⁸. Wprawdzie owo usuwanie danych może być efektem zastosowania rozmaitych czynności, najważniejszy jest zaś efekt końcowy wyrażający się w wykluczeniu możliwości identyfikacji osoby fizycznej. Ochrona danych osobowych jest bowiem istotną przesłanką do ograniczenia prawa do informacji publicznej i zawsze powinna zostać zbadana przez pryzmat prywatności tejże osoby¹¹⁹. Można wywieść konkluzję, iż anonimizacja stanowi kompromis między prawem osób fizycznych do poszanowania ich danych osobowych i tym samym prawa do prywatności a koniecznością (obowiązkiem) udostępnienia informacji publicznej¹²⁰.

Anonimizacja jako czynność (względnie proces) nie jest traktowana jako czynność związana czy też towarzysząca przetworzeniu informacji zgodnie z u.d.i.p. Anonimizacja jest natomiast traktowana w charakterze czynności pomocniczej – technicznej (materialno-technicznej)¹²¹.

¹¹⁸ Por. wyrok Wojewódzkiego Sądu Administracyjnego we Wrocławiu z dnia 25 kwietnia 2017 r., IV SAB/Wr 34/17, CBOSA.

¹¹⁹ Por. wyrok Naczelnego Sądu Administracyjnego z dnia 14 marca 2013 r., I OSK 620/12, CBOSA; wyrok Wojewódzkiego Sądu Administracyjnego w Krakowie z dnia 13 maja 2019 r., II SA/Kr/19, Legalis nr 1951790.

¹²⁰ Por. wyrok Wojewódzkiego Sądu Administracyjnego w Gliwicach z dnia 12 marca 2013 r., IV SAB/Gl 115/12, Legalis nr 767644; wyrok Wojewódzkiego Sądu Administracyjnego w Gliwicach z dnia 31 lipca 2018 r., IV SAB/Gl 106/18, Legalis nr 1819490.

¹²¹ Por. wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 23 września 2009 r., II SA/Wa 978/09; wyrok Wojewódzkiego Sądu Administracyjnego we Wrocławiu z dnia 20 października 2004 r., IV SA/Wr 505/04, CBOSA.

Informacja prosta nie zmienia się bowiem w przetworzoną dzięki procesowi anonimizacji, ponieważ czynność ta polega jedynie na jej przekształceniu, a nie na jej przetworzeniu¹²². Powyższa praktyka orzecznicza jest zresztą zgodna z poglądami doktryny w tej materii¹²³. Należy jednak pamiętać, że w niektórych przypadkach wydanie wnioskowanego dokumentu wymagającego anonimizacji danych osobowych może być powiązane z koniecznością przeprowadzenia jeszcze innych czynności o charakterze analityczno-statystycznym, wówczas udostępnienie takiej informacji będzie stanowiło informację przetworzoną. W tym kontekście anonimizacja jest niejako podprocesem towarzyszącym i niezbędnym do wykonania procesu przetworzenia informacji publicznej¹²⁴.

W orzecznictwie utrwalony jest też pogląd, iż czynności związane z anonimizacją są zgodne z u.d.i.p., bowiem anonimizowane dane nie stanowią po jej dokonaniu kategorii informacji publicznej, natomiast przeprowadzenie tego procesu wymaga oczywiście podjęcia żadnego aktu administracyjnego¹²⁵. Brak konieczności wydania aktu administracyjnego koreluje zresztą z założeniem, że anonimizacja jest wyrazem

¹²² Por. wyrok Naczelnego Sądu Administracyjnego z dnia 9 sierpnia 2011 r., I OSK 792/11, CBOSA; wyrok Wojewódzkiego Sądu Administracyjnego we Wrocławiu z dnia 20 października 2004 r., IV SA/Wr 505/04; wyrok Wojewódzkiego Sądu Administracyjnego we Wrocławiu z dnia 19 grudnia 2005 r., IV SAB/Wr 47/05, CBOSA.

¹²³ Szerzej na ten temat: K. Kłosowska, *Czynności faktyczne jako prawna forma działania administracji*, Rzeszów 2009, s. 126-134 wraz ze wskazaną przez autorkę literaturą; M. Bernaczyk, M. Jabłoński, K. Wygoda, *Biuletyn Informacji Publicznej. Informatyzacja administracji*, Wrocław 2005, s. 87-94 wraz ze wskazaną przez autorów literaturą.

¹²⁴ Wyroki Naczelnego Sądu Administracyjnego: z dnia 19 grudnia 2017 r., I OSK 1362/17; z dnia 2 października 2014 r., I OSK 140/14; z dnia 21 września 2012 r., I OSK 1477/12; z dnia 9 sierpnia 2011 r., I OSK 792/11; z dnia 8 czerwca 2011 r., I OSK 426/11; z dnia 17 października 2006 r., I OSK 1347/05, CBOSA.

¹²⁵ Nie jest wymagane prawem wydanie w toku postępowania administracyjnego żadnego postanowienia lub decyzji w przedmiocie dokonania (lub odmowy przeprowadzenia) anonimizacji. Por. wyrok Naczelnego Sądu Administracyjnego z dnia 11 stycznia 2013 r., I OSK 2267/12, Legalis nr 594197; wyrok Wojewódzkiego Sądu Administracyjnego w Gliwicach z dnia 8 listopada 2018 r. IV SAB/Gl 193/18, Legalis nr 1847764.

innej formy działania administracji publicznej wyrażonej we wskazanych wyżej czynnościach faktycznych (materialno-technicznych).

Orzecznictwo sądów administracyjnych poświęcone problematyce anonimizacji obejmuje nie tylko zagadnienia związane z ochroną danych osobowych osób fizycznych. Obejmuje niekiedy inne typy danych (np. dane przedsiębiorców opublikowane w bazie orzeczeń sądowych czy przeniesione z wokandy sądowej do Internetu)¹²⁶. W tych przypadkach anonimizacja „wylewa” się na inne niż dane osobowe typy danych, zaś ich anonimizacja wynika z konieczności zachowania swoiście pojmowanej „poufności działalności gospodarczej”, uzasadniające przy tym konieczność zachowania takich informacji w tajemnicy. W innych orzeczeniach sąd dostrzega konieczność wykonania anonimizacji danych: „[...] prawem chronionych w dokumentach [...], uznając proces anonimizacji jako narzędzie gwarantujące właściwą realizację udostępnienia informacji publicznej, przy jednoczesnej ochronie innych praw podmiotowych”¹²⁷.

Poglądy wyrażone w przytoczonym orzecznictwie niejako *in statu nascendi* nie tylko odnoszą się do zagadnienia anonimizacji rozumianej instrumentalnie (jej zasadniczej funkcji), lecz dotyczą problemu bardziej złożonego, czyli granic (zakresów) możliwej, czy też prawidłowo przeprowadzonej anonimizacji. Zasadniczym postulatem jest, aby proces anonimizacji nie zniekształcał wartości informacyjnej upublicznianego dokumentu urzędowego. Granicą zatem anonimizacji jest zakres waloru

¹²⁶ Istotą rozstrzygnięcia był problem udostępnienia informacji publicznej widniejącej na sądowych wokandach, zaś dotyczących informacji o imieniu, nazwisku strony postępowania gospodarczego, jak również o toczącym się sporze z udziałem takich podmiotów. W ocenie sądu upublicznienie tych informacji, podobnie jak opublikowanie ich w internetowej bazie orzeczeń, może wiązać się z naruszeniem tajemnicy przedsiębiorstwa czy przedsiębiorcy, wymaga zatem anonimizacji. Por. wyrok Wojewódzkiego Sądu Administracyjnego w Szczecinie z dnia 29 maja 2013 r., II SA/SZ/331/13, Legalis nr 762346.

Analogiczny spór rozstrzygnął w identyczny sposób Wojewódzki Sąd Administracyjny w Gliwicach, por. wyrok z 17 maja 2013 r., IV SA/GL/328/13, Legalis nr 768226.

¹²⁷ Por. wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 21 sierpnia 2013 r., VIII SA/WA 386/13, Legalis nr 774229.

informacyjnego dokumentu¹²⁸. Należy przy tym pamiętać o wielowarstwowym aspekcie usuwania określonych typów danych z dokumentów urzędowych¹²⁹. Niemniej słuszny jest pogląd, który stanowi o konieczności zachowania walorów poznawczych udostępnianych treści. Często-kroć bowiem w wyniku dokonania anonimizacji dochodzi do usunięcia danych w sposób nadmierny, czyli wykraczający poza ramy normatywne, i który w efekcie niweczy istotę wyrażoną w dostępie do informacji publicznej, gdyż ta informacja staje się nieczytelna bądź niekompletna, przez co niezrozumiała dla jej odbiorcy¹³⁰.

12. Anonimizacja – granice (zakres)

Na podstawie przedstawionych wyżej argumentów należy postawić fundamentalne pytanie – czy anonimizacja powinna być zdeterminowana wyłącznie normami prawnymi, których istotą jest zapewnienie ochrony praw podmiotowych, czy też z uwagi na szerokie spektrum przedmiotowe definicji danych osobowych proces anonimizacji powinien wykraczać poza „sztywny gorset” regulacji normatywnych i uwzględniać także inne, pozaprawne „normy”, zwyczaje, względnie zasady (reguły) nakazujące anonimizację danych osobowych?

Ponadto czy anonimizacja (zgodnie zresztą z samym nazewnictwem odnoszącym się do podmiotów prawa, jakimi są „anonimowe” osoby fizyczne) może, czy też powinna obejmować inne typy danych poddanych anonimizacji aniżeli dane osobowe?

Aby udzielić odpowiedzi na wyżej postawione pytania – zasadnicze z punktu widzenia stosowania u.d.i.p. – należy niniejsze rozważania

¹²⁸ Por. wyrok Wojewódzkiego Sądu Administracyjnego w Olsztynie z dnia 21 listopada 2019 r., II SAB/OI 75/19, CBOSA.

¹²⁹ Por. uwagi w dalszej części artykułu.

¹³⁰ Por. wyrok Wojewódzkiego Sądu Administracyjnego w Krakowie z dnia 15 lipca 2014 r., II SAB/Kr 132/14, Legalis nr 1059666.

przenieść na grunt prakseologii, albowiem anonimizacja (towarzysząca jej czynności) nie stanowi istoty realizowanej przez organ administracyjny czynności. Stąd można przyjąć w sposób niewątpliwy, że:

- a) zasadniczym celem (sensem) anonimizacji jest udostępnienie informacji publicznej, przy jednoczesnym poszanowaniu innych uprawnień, dóbr czy wartości chronionych normami prawnymi;
- b) abstrahując od sposobów przeprowadzenia anonimizacji, ujawnienie danych wymagających ochrony zawsze stwarza określone skutki prawne, zaś nierzadko pociąga negatywne następstwa prawne, zarówno dla podmiotu upubliczniającego owe dane, jak i dla podmiotu, którego dane zostały ujawnione;
- c) wprost proporcjonalnie do ilości upublicznionych danych w następstwie anonimizacji rośnie ryzyko popełnienia błędu w tym procesie, co wiąże się z określonymi skutkami prawnymi (por. pkt b) wyżej);
- d) anonimizacja obejmująca określone typy danych, zaś wykraczająca poza ramy normatywne nie jest niezgodna z prawem, lecz wyrazem określonej „praktyki anonimizacyjnej” obranej w podmiocie udostępniającym informacje publiczne;
- e) usunięcie w wyniku anonimizacji danych, które mogłyby (potencjalnie) pozostać jawne w treści dokumentu urzędowego przy jednoczesnym wyodrębnieniu i zastosowaniu jednorodnych zasad interpretacyjnych tworzących logiczne oraz czytelne granice (reguły) tejże anonimizacji, nie musi być adekwatne z pozbawieniem waloru informacyjnego udostępnianej informacji publicznej;
- f) dla podmiotów zainteresowanych treścią określonych dokumentów urzędowych, zaś przede wszystkim dla tych podmiotów nieposiadających interesu prawnego w uzyskaniu do nich dostępu, nie powinny mieć znaczenia szczegółowe dane (np. osobowe funkcjonariuszy publicznych);

- g) sfera podmiotowości prawno-administracyjnej jest w polskim systemie prawa administracyjnego złożona, bowiem nie każdy organ administrujący jest organem administracyjnym (dotyczy to m.in. niepublicznych podmiotów administrujących wykonujących zadania administracji publicznej powierzone im w drodze umowy, koncesji, zezwolenia, wpisu do rejestru czy ewidencji)¹³¹. W tym kontekście mogłoby nastąpić naruszenie praw podmiotowych (np. upublicznienie danych osobowych wolontariusza – osoby fizycznej jednocześnie wykonującej określone zadania publiczne, zaś niebędącej funkcjonariuszem publicznym oraz niepełniącej funkcji publicznej).

Z prakseologicznego punktu widzenia wydaje się, że anonimizacja nie musi (być może nawet nie powinna) ograniczać się do wyłącznie do granic wyznaczonych normami prawa. W dobie społeczeństwa informacyjnego oraz Internetu rekomendowane jest przyjęcie innych paradygmatów udostępniania informacji, w tym informacji publicznej. Chodzi bowiem o to, aby raz ujawniona w sieci informacja (stająca się jednocześnie informacją publicznie dostępną w globalnym medium) nie stanowiła aktu naruszenia czyichś dóbr, prywatności, praw, albo by nie powodowała szkód czy też negatywnych następstw prawnych (np. kar administracyjnych). Słowem, anonimizacja z definicji swojego celu ma czynić zadość potrzebie uzyskania dostępu do informacji publicznych przy jednoczesnym zabezpieczeniu (zminimalizowaniu) ewentualnych negatywnych skutków prawnych dla podmiotu ujawniającego ową informację czy dla podmiotu, którego dane zostały bezprawnie ujawniane (lub upublicznione w Internecie). Wydaje się, że zastosowanie modelu łączącego wymogi prawa z wymogami oraz realiami technicznymi, personalnymi i organizacyjnymi może uczynić proces anonimizacji zdecydowanie bardziej szczelnym

¹³¹ Szerzej na ten temat: M. Stahl, *Niepubliczne podmioty administrujące*, [w:] R. Hauser, Z. Niewiadomski, A. Wróbel (red.), *System Prawa Administracyjnego*, t. 6. *Podmioty administrujące*, Warszawa 2011, s. 529-551.

i mniej narażonym na błędy, skutkujące ujawnieniem niepożądanych informacji.

13. Anonimizacja oraz pseudonimizacja – konkluzje

Podjmując wyzwanie dookreślenia pojęcia (procesu) anonimizacji, starając się wykreować jej zręby definicyjne, można przyjąć następujące założenia (w pewnym stopniu w opozycji do pojęcia pseudonimizacji):

- I. Anonimizacja nie powinna być pojmowana w sposób derywacyjny, czyli odłączony od istoty jej dokonania, która wyraża się w realizacji prawa dostępu do informacji publicznej. Jest etapem pośrednim, poprzedzającym oraz jednocześnie urealniającym uprawnienie do dostępu informacji publicznej. Pseudonimizacja zaś nie posiada takiego waloru, nie jest bowiem żadnym etapem w procesie wykonywania praw podmiotowych, gdyż stanowi jedną z metod wpływających na zwiększenie bezpieczeństwa przetwarzanych danych osobowych, nie musi być zatem wykonywana (stanowi alternatywę wobec innych metod zabezpieczania danych osobowych).
- II. Anonimizacja nie musi (*de facto* nie powinna) ograniczać się jedynie do danych osobowych; pseudonimizacja dotyczy wyłącznie danych osobowych.
- III. Anonimizację cechuje działanie jednokierunkowe; pseudonimizacja jest procesem z definicji odwracalnym. Tym samym nieuprawnione odwrócenie pseudonimizacji może doprowadzić do ujawnienia danych osobowych. Tymczasem anonimizacji z definicji nie można odwrócić, stanowi zatem pewniejszy sposób ochrony danych.
- IV. Dane zanonimizowane tracą walor danych osobowych; pseudonimizacja nie pozbawia danych osobowych ich zasadniczych cech.
- V. Anonimizacja podobnie jak pseudonimizacja jest procesem, lecz w przypadku anonimizacji może być wykonywana manualnie lub

semi-automatycznie. Pseudonimizacja z uwagi na swój charakter i cechy (choćby możliwość przywrócenie stanu pierwotnego) musi być realizowana automatycznie.

- VI. Anonimizacja powinna być (lecz nie musi, jeśli nie jest wykonywana automatycznie) oparta na kanwie reguł anonimizacyjnych (istotnie wpływających na poprawę całego procesu). Pseudonimizacja działa z zasady według określonych reguł (algorytmu).
- VII. Anonimizacja jest pojęciem szerszym – w pewnym sensie „konsuuje” proces pseudonimizacji. Podobnie jak pseudonimizacja jest metodą zwiększającą bezpieczeństwo danych, ale również wpływającą na zwiększenie transparentności funkcjonowania podmiotów publicznych (np. przez tworzenie baz dokumentów urzędowych), czy też dostępności do danych (np. przez upublicznienie w Internecie baz zanonimizowanych orzeczeń sądowych).
- VIII. Anonimizację cechuje różnorodność jej form (technik) przeprowadzenia; pseudonimizacja opiera się na jednej (zasadniczej) metodzie.
- IX. Pojęcie anonimizacji w przeciwieństwie do pojęcia pseudonimizacji nie zostało zdefiniowane w prawie (brak bowiem jej definicji legalnej).

Kończąc rozważania dotyczące owych zagadnień, wypada wskazać, że wyjątkową alternatywą procesu anonimizacji jest zastosowanie tzw. „danych syntetycznych”. Można rzec, że koncepcja danych syntetycznych stanowi „odłam” koncepcji anonimizacji danych, z tym jednak zastrzeżeniem, że dane syntetyczne nie prezentują faktycznych (rzeczywistych) informacji umożliwiających identyfikację podmiotów prawa (nie tylko osób fizycznych) oraz nie muszą prezentować rzeczywistych sytuacji (okoliczności) będących podstawą badań¹³².

¹³² Szerzej na ten temat: M. Kiedrowicz, *Zastąpienie anonimizacji danych danymi syntetycznymi*, [w:] G. Szpor, K. Czaplicki (red.), *Przetwarzanie danych osobowych...*, s. 230 i n.

Bibliografia

- Adamski A., *Prawo karne komputerowe*, Warszawa 2000.
- Barrow G.M., *Chemia fizyczna*, przeł. J. Kuryłowicz, Warszawa 1978.
- Bursa S., *Chemia fizyczna*, Warszawa 1979.
- Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Kraków 2007.
- Barta P., Kawecki M., [w:] P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018.
- Bazewicz M., Collen A., *Methodological Foundations of Human Activity Systems and Informatics*, Wrocław 1995.
- Bazewicz M., *Wizja społeczeństwa ery komunikacji, informacji i wiedzy XXI wieku*, Wrocław 2000.
- Bell D., *The Coming of Post-industrial Society*, New York 1973.
- Benkler Y., *Bogactwo sieci. Jak produkcja społeczne zmienia rynki i wolność*, przeł. R. Próchniak, Warszawa 2008.
- Bernaczyk M., Jabłoński M., Wygoda K., *Biuletyn Informacji Publicznej. Informatyzacja administracji*, Wrocław 2005.
- Biernat J., *Architektura komputerów*, Wrocław 2002.
- Błaś A., [w:] J. Boć (red.), *Prawo administracyjne*, Wrocław 2007.
- Boć J., (red.), *Prawo administracyjne*, Wrocław 2007.
- Brillouin L., *Nauka a teoria informacji*, przeł. S. Mazurek, J. Szklanny, Warszawa 1969.
- Castells M., *The information Age: Economy, Society and Culture*, Oxford 2000.
- Castells M., *The Rise of the Network Society*, Oxford 1996.
- Cellary W., *Techniki internetowe*, Poznań 2005.
- Chyrowicz B. (red.), *Spółeczeństwo informatyczne: szansa czy zagrożenie?*, Lublin 2003.
- Davis P., *Bóg i nowa fizyka*, przeł. P. Amsterdamski, Warszawa 1996.
- Dobrzeńiecki K., *Prawo a etos cyberprzestrzeni*, Toruń 2004.

- Durka P.J., *Komputer. Internet. Cyfrowa rewolucja*, Warszawa 2000.
- Ekel J., *Decyzyjnoinformacyjny model czynności ludzkich*, [w:] J. Koziński (red.), *Problemy psychologii matematycznej*, Warszawa 1971.
- Fukuyama F., *Wielki wstrząs. Natura ludzka a odbudowa porządku społecznego*, przeł. H. Komorowska, Warszawa 2000.
- Gees F.W., *From sectoral systems of innovation to socio-technical systems: Insights about dynamics and change from sociology and institutional theory*, "Research Policy", Vol. 33, Iss. 6-7, September 2004.
- Gill-Tarnowska D., *Dobra i usługi informacyjne – informacja jako towar*, [w:] A. Szewczyk (red.), *Informacja – dobra lub zła nowina*, Szczecin 2004.
- Gliński W. (red.), *Spółczesność informacyjna i jej technologie*, Warszawa 2004.
- Głocki W., *Układy cyfrowe*, Warszawa 1996.
- Goban-Klas T., Sienkiewicz P., *Spółczesność informacyjna: szanse, zagrożenia*, wyzwania, Kraków 1999.
- Goban-Klas T., *Uniwersytet a mass media*, „Forum Akademickie” 1996, nr 2.
- Gołaczyński J. (red.), *Prawne i ekonomiczne aspekty komunikacji elektronicznej*, Warszawa 2003.
- Gomułowicz A., Sawczyn W., *Jawność rozprawy a bezpieczeństwo prawne jednostki*, [w:] Bielak-Jomaa E., Góral U. (red.), *Wdrożenie ogólnego rozporządzenia o ochronie danych osobowych. Aspekty proceduralne*, Warszawa 2018.
- Góralczyk W. (red.), *Prawo informacji. Prawo do informacji*, Warszawa 2006.
- Greniewski H., *Cybernetyka niematematyczna*, Warszawa 1969.
- Greniewski H., Kempisty M., *Cybernetyka z lotu ptaka*, Warszawa 1963.
- Haber L.H. (red.), *Polskie doświadczenia w kształtowaniu społeczeństwa informacyjnego: dylematy cywilizacyjno-kulturowe (materiały ogólnopolskiej konferencji naukowej, Kraków, 28 września 2001 r.)*, Kraków 2002.
- Harmon G., *The measurement of information*, „Information Processing and Management” 1984, nr 1-2.
- Hetmański M., *Internet jako maszyna cybernetyczna*, [w:] R. Skubisz (red.), *Internet 2000*, Lublin 2000.

- Hetmański M., *Spoleczny charakter informacji*, [w:] B. Chyrowicz (red.), *Spoleczeństwo informatyczne: szansa czy zagrożenie?*, Lublin 2003.
- Kerckhove D. de, *Inteligencja otwarta*, przeł. A. Hildebrandt, Warszawa 2001.
- Kilian W., *Wprowadzenie*, [w:] J. Gołaczyński (red.), *Prawne i ekonomiczne aspekty komunikacji elektronicznej*, Warszawa 2003.
- Kłosowska K., *Czynności faktyczne jako prawna forma działania administracji*, Rzeszów 2009.
- Kossecki J., *Cybernetyka społeczna*, Warszawa 1981.
- Kościański A.J., *Spoleczeństwo informacyjne: propozycje konceptualizacji*, „Kultura i Spoleczeństwo” 1999, nr 3 (lipiec–wrzesień).
- Kowalczyk M., *E-urząd w komunikacji z obywatelem*, Warszawa 2009.
- Kropiwnicki J., *Budowa cywilizacji informacyjnej jako filar długookresowej strategii dla Polski do roku 2025*, [w:] T. Zasępa (red.), *Internet – fenomen społeczeństwa informacyjnego*, Częstochowa 2001.
- Kulikowski L., *Informacja i świat, w którym żyjemy*, Warszawa 1978.
- Kuriata E., *Wirusy komputerowe. Mechanizmy infekcji i środki ochrony*, Wrocław 1999.
- Lach A., *Dowody elektroniczne w procesie karnym*, Toruń 2004.
- Lang W., Mrózek A., *Proces stosowania prawa jako proces przetwarzania informacji*, „Państwo i Prawo” 1970, nr 7.
- Lekka-Kowalik A., *Demokracja i autonomia jednostki w globalnej infrastrukturze informacyjnej*, „Nauka” 1999, nr 1.
- Lekka-Kowalik A., *Ukryte założenia społeczeństwa informacyjnego*, [w:] T. Zasępa (red.), *Internet – fenomen społeczeństwa informacyjnego*, Częstochowa 2001.
- Litwiński P. (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018.
- Maciejewski M., *Prawo informacji – zagadnienia podstawowe*, [w:] W. Góralczyk (red.) *Prawo informacji. Prawo do informacji*, Warszawa 2006.
- Madej D., Marasek K., Kuryłowicz K., *Komputery osobiste*, Warszawa 1987.
- Malinowski A., *Wstęp do badań cybernetycznych w prawoznawstwie*, Warszawa 1977.

- Mazur M., *Cybernetyczna teoria układów samodzielnych*, Warszawa 1966.
- Mednis A., *Prawo do prywatności a interes publiczny*, Kraków 2006.
- Negroponte N., *Cyfrowe życie. Jak się odnaleźć w świecie komputerów*, Warszawa 1997.
- Newcomb T., Turner R.H., Converse P.E., *Psychologia społeczna*, przeł. H. Muszyński [et al.], Warszawa 1970.
- Niedzielska E., *Próba systematyzacji procesów rozwoju systemów informacyjnych*, „Wiadomości Statystyczne” 1986, nr 4.
- Nowakowski J., W. Sobczak, *Teoria informacji*, Warszawa 1978.
- Piróg W., *Zagadnienia informacji i dokumentacji naukowej*, Warszawa 1978.
- Ober J., *Etyka w rozwoju informatyki*, „Nauka” 1999, nr 1.
- Oleński J., *Ekonomika informacji*, t. 1, Warszawa 2001.
- Oleński J., *Ekonomika informacji*, Warszawa 2000.
- Oleński J., *Ekonomika informacji. Metody*, Warszawa 2003.
- Pettersson R., *What is Information Design?*, Pittsburgh, PA 1998.
- Petzel J., *Informatyka prawnicza: zagadnienia teorii i praktyki*, Warszawa 1999.
- Płoski Z., *Słownik encyklopedyczny. Informatyka*, Wrocław 1999.
- Pomykański A., *Informacja na potrzeby innowacji*, Warszawa 1976.
- Przybylska B., *Informacja jako towar*, [w:] A. Szewczyk (red.), *Informacja – dobra lub zła nowina*, Szczecin 2004.
- Rot H., *Podstawy cybernetyki i informatyki prawniczej*, Wrocław 1983.
- Rothert A., *Między porządkiem a chaosem*, Warszawa 2006.
- Shannon C.E., *A Mathematical Theory of Communication*, http://free.art.pl/fotografie/teoria_obrazu/shannon.pdf.
- Shapiro C., Varian H., *Information Rules: A Strategic Guide to the Network Economy*, Cambridge 1998.
- Sibiga G., *Stosowanie technik informatycznych w postępowaniu administracyjnym ogólnym*, Warszawa 2019.
- Sobczak W., Malina W., *Metody selekcji informacji*, Warszawa 1978.
- Sosińska-Kalata B., *Czym jest dziś nauka o informacji?*, [w:] B. Sosińska-Kalata, K. Materska, W. Gliński (red.), *Spółczesność informacyjna i jej technologie*, Warszawa 2004.

- Stefanowicz B., *Informacja*, Warszawa 2004.
- Stoll C., *Krzemowe remedium*, przeł. T. Hornowski, Poznań 2000.
- Szewczyk A. (red.), *Informacja – dobra lub zła nowina*, Szczecin 2004.
- Szpor G., [w:] G. Szpor, K. Czaplicki (red.), *Ustawa o dostępności stron internetowych i aplikacji mobilnych podmiotów publicznych. Komentarz*, Warszawa 2020.
- Szpor G., Czaplicki K. (red.), *Przetwarzanie danych osobowych*, Warszawa 2019.
- Szpor G., Czaplicki K. (red.), *Ustawa o dostępności stron internetowych i aplikacji mobilnych podmiotów publicznych. Komentarz*, Warszawa 2020.
- Szpor G., *Informacja w zagospodarowaniu przestrzennym. Zagadnienia administracyjno-prawne*, Katowice 1998.
- Szymczak M. (red.), *Słownik języka polskiego PWN*, t. I, Warszawa 1996.
- Szymona J.J., *Wolność i własność w Internecie*, [w:] R. Skubisz (red.), *Internet – problemy prawne*, Lublin 1999.
- Tadeusiewicz R., *Spółeczność Internetu*, Warszawa 2002.
- Taras W., *Informowanie obywateli przez administrację*, Wrocław-Warszawa-Kraków 1992.
- Toffler A., *Trzecia fala*, przeł. M. Kłobukowski, Warszawa 2001.
- Topolewski Z., *Komputerowe zabezpieczenie poufności informacji w zarządzaniu*, Wrocław 2002.
- Traczyk W., *Układy cyfrowe. Podstawy teoretyczne i metody syntezy*, Warszawa 1982.
- Vinck D., *Sociologie des sciences*, Paris 1995, za: J. Kulpińska, *Od społeczeństwa postindustrialnego do społeczeństwa informacyjnego – koncepcje i dyskusje*, [w:] L.H. Haber (red.), *Polskie doświadczenia w kształtowaniu społeczeństwa informacyjnego: dylematy cywilizacyjno-kulturowe (materiały ogólnopolskiej konferencji naukowej, Kraków, 28 września 2001 r.)*, Kraków 2002.
- Watson A., Hill A., *Dictionary of Communication and Media Studies*, London 1991, za: S. Juszczak, *Komunikacja człowieka z mediami*, Katowice 1998.

- Wiener N., *Cybernetyka a społeczeństwo*, przeł. O. Wojtasiewicz, Warszawa 1961.
- Wiener N., *Cybernetyka czyli sterowanie i komunikacja w zwierzęciu i maszynie*, przeł. J. Mieścicki, Warszawa 1971.
- Wilk A.M., *Polska wobec wyzwań społeczeństwa informacyjnego*, [w:] R. Skubisz (red.), *Internet 2000*, Lublin 2000.
- Wojsyk K., *Przetwarzanie danych osobowych wrażliwych w systemach informatycznych ochrony zdrowia i ich anonimizacja*, [w:] G. Szpor, K. Czapliski (red.), *Przetwarzanie danych osobowych*, Warszawa 2019.
- Zasępa T. (red.), *Internet – fenomen społeczeństwa informacyjnego*, Częstochowa 2001.

Wybrane aspekty prawne scrapowania ze szczególnym uwzględnieniem informacji i danych publicznych

Selected legal aspects of web-scraping with special regard to public sector data and information scraping

Streszczenie: Autorka omawia prawne aspekty scrapowania. W opracowaniu przeanalizowano stopniowe zmiany w zakresie ram prawnych w UE i w Polsce dotyczące pozyskiwania danych z internetu. Odrębna część opracowania została poświęcona zagadnieniu ekstrakcji ze źródeł dostępnych w internecie szczególnego rodzaju treści w postaci danych i informacji publicznych. Autorka wskazuje na pewne odrębności w odniesieniu do legalności ich pozyskiwania. Zwraca ponadto uwagę na niedawno przyjęte przepisy regulujące eksplorację tekstów i danych oraz zagadnienie *re-use*.

Słowa kluczowe: scrapowanie, dane, pozyskiwanie danych, ekstrakcja danych, agregacja danych, eksploracja tekstów i danych, bazy danych, ochrona baz danych, prawo autorskie, prawo do informacji publicznej, informacja publiczna, otwarte dane, ponowne wykorzystywanie informacji sektora publicznego, prawo UE

Abstract: The Author presents legal aspects of web-scraping. The paper discusses the gradual development of a legal framework regarding internet data mining in the EU and in Poland. Specific attention is paid to scraping of public sector data and information. The Author indicates why different approach should be adopted for data made available through electronic means by the 'public sector body' and 'body governed by public law'. Furthermore, it is explained how the latest legislation on text and data mining and re-use.

Keywords: Web-scraping, data, data extraction, data collection, data aggregation, data mining, text and data mining, databases, databases protection, copyrights law, re-use of public sector information, open data, public sector data, EU law

¹ Radca prawny, specjalista w zakresie prawa własności intelektualnej, prawa nowych technologii i ochrony danych osobowych (kontakt: tel. 881 790 719, adres email: ewa.wojnarska-krajewska@wp.pl).

Wstęp

Niniejsze opracowanie poświęcone jest zagadnieniu automatycznego pobierania danych z internetu. Szczególna uwaga została w nim poświęcona tym danym i informacjom, które zostały udostępnione na stronach internetowych przez podmioty zobowiązane do udostępniania informacji publicznej i informacji do ponownego wykorzystywania.

Dla jasności wywodu należy odwołać się do pojęć z zakresu terminologii informatycznej, które mają kluczowe znaczenie dla zrozumienia prawnych aspektów zagadnienia będącego przedmiotem niniejszej analizy.

Współczesna gospodarka w coraz większym stopniu oparta jest na przetwarzaniu wielkich zbiorów danych. Dla ich określenia używa się pojęcia *big data*. Odnosi się ono do dużej ilości danych, nieustrukturyzowanych, o dużej różnorodności², których rozmiary i szybkość napływu wymagają posłużenia się szczególnymi narzędziami do ich gromadzenia, przechowywania, agregowania, czyli analizowania i zestawiania, a w efekcie do ich przekształcania w nową wartość³.

Narzędziem, które umożliwia ekstrakcję istotnych dla określonego celu danych z wielkich zbiorów i dokonania ich analizy, jest *data mining*, a szerzej *text and data mining* (czyli „eksploracja tekstów i danych”). W efekcie jego zastosowania z dotychczas dostępnych danych można wygenerować nowe informacje lub dokonać prognoz⁴. Dzięki temu mogą powstawać innowacyjne rozwiązania w nauce i gospodarce. Klasycznym przykładem mogą być dane z badań medycznych. Zestawione z dużej

² A. Heiss, *Big Data Challenges in Big Science, Computing and Software for Big Science*, „Computing and Software for Big Science” 2019, <https://link.springer.com/content/pdf/10.1007%2Fs41781-019-0030-7.pdf> [dostęp: 23.08.2020].

³ Zob. A. De Mauro, A.M. Greco, M. Grimaldi, *A formal definition of Big data based on its essential features*, „Library Review” 2016, Vol. 3, s. 122-135.

⁴ S. Selamat, S. Prakoonwit, W. Khan, *A review of data mining in knowledge management: applications/findings for transportation of small and medium enterprises*, „SN Applied Sciences” 2020, <https://link.springer.com/content/pdf/10.1007%2Fs42452-020-2589-3.pdf> [dostęp: 23.08.2020].

liczby baz i przeanalizowane prowadzą do nowych wniosków na temat chorób, uwidaczniają określone tendencje lub pozwalają przewidzieć ryzyka.

Pozyskiwanie danych z wielkich baz odbywa się automatycznie za pomocą techniki, którą określa się mianem *scraping* (*web scraping*, *screen scraping*). *Scraping*, zwany również „scrapowaniem”, polega na ekstrakcji dużych ilości informacji ze stron internetowych za pomocą automatycznych narzędzi – internetowych botów – programów komputerowych, których zadaniem jest systematyczne przeszukiwanie internetu w celu pobrania z nich wyselekcjonowanych informacji według zadanych kryteriów, może iść w parze z indeksowaniem treści⁵.

Scrapowanie dotyczy wszelkiego rodzaju danych dostępnych w internecie. Aktywność ta jest od dawna przedmiotem obaw wielu przedsiębiorców, którzy upubliczniają swoje bazy danych i jednocześnie dążą do zapewnienia im jak najszerzej ochrony. Z drugiej strony – na podstawie dostępnych danych powstają przedsięwzięcia, które opierają się na kreatywnym ich przekształcaniu w produkty o nowym znaczeniu i nowej wartości dla odbiorców.

Szczególne miejsce wśród dostępnych danych zajmują te wytworzone przez podmioty funkcjonujące w sferze publicznej albo przez takie, które mają prawny obowiązek udostępniania określonych informacji. Mają one z mocy prawa inny status niż dane udostępniane przez prywatne podmioty. Szczegółowe regulacje poświęcone zarówno ogólnym zasadom scrapowania i wykorzystywania tak pozyskanych danych, jak i dokonywania tych czynności w odniesieniu do danych i informacji publicznych, zostały omówione w dalszej części pracy.

⁵ A. Zamora, *Making Room For Big Data: Web Scraping and an Affirmative Right to Access Publicly Available Information Online*, “The Journal of Business, Entrepreneurship & the Law” 2019, Vol. 12, s. 203-228; E. Wojnarska-Krajewska, *Crawlowanie – legalne czy nie*, <https://wpprawoautorskie.wordpress.com/2014/04/17/crawlowanie-crawler-roboty-txt/> [dostęp: 24.08.2021].

1. Scrapowanie w świetle strategicznych założeń Unii Europejskiej w zakresie otwierania dostępu do danych sektora publicznego

Przepisy Unii Europejskiej odnoszą się do scrapowania w sposób bezpośredni, jednak tylko w określonym zakresie. Scrapowanie podlega przede wszystkim ograniczeniom prawnym w odniesieniu do chronionych baz danych. Producentów bazy danych, którzy ponieśli istotne nakłady inwestycyjne na ich stworzenie, chronią przepisy dyrektywy 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r. w sprawie ochrony prawnej baz danych⁶. Jest to o tyle istotna regulacja, że znacząca część stron internetowych opiera się na bazach danych. Za takie bowiem uznać można na przykład zbiory danych o produktach podlegających sprzedaży, dane podmiotów fizycznych udostępniane w ramach serwisów społecznościowych, informacje o filmach, zdjęcia i recenzje dostępne na stronach serwisów VOD i wiele innych.

Zakres tych ograniczeń określa art. 5 dyrektywy, zgodnie z którym producentowi bazy danych przysługuje wyłączne prawo do czasowego lub trwałego zwielokrotniania, w jakikolwiek sposób lub w jakiegokolwiek formie, w całości lub w części bazy danych (art. 5 lit. a) oraz do dokonywania w odniesieniu do niej wszelkich innych czynności określonych w art. 5 lit. b-e oraz art. 7 ust. 1, zgodnie z którym producentowi przysługuje prawo do ochrony przed pobieraniem danych i/lub wtórnym ich wykorzystaniem w całości lub w istotnej części, co do jakości i/lub ilości. Art. 7 ust. 5 dyrektywy stanowi, iż: „niedozwolone jest powtarzające się i systematyczne pobieranie danych i/lub wtórne ich wykorzystanie w nieistotnej części, jeśli czynności te są sprzeczne z normalnym korzystaniem z tej bazy danych lub w sposób nieuzasadniony naruszają słusze interesy producenta bazy danych”. W tym zakresie zatem, w odniesieniu do

⁶ Dz. Urz. UE L 77 z 27.03.1996 r., s. 20.

baz danych chronionych prawem *sui generis*, scrapowanie zostało wprost ograniczone.

Istotne przepisy regulujące pobieranie treści z internetu zostały wprowadzone również na mocy dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE⁷. Przywołana dyrektywa uregulowała kwestię eksploracji tekstów i danych, czyli posługiwania się narzędziami umożliwiającymi przetwarzanie dużych ilości informacji w celu uzyskania nowej wiedzy i odkrycia nowych tendencji. W niektórych przypadkach eksploracja tekstów i danych może obejmować czynności chronione prawem autorskim lub prawem do bazy danych *sui generis*, w szczególności zwielokrotnianie utworów lub innych przedmiotów objętych ochroną lub pobieranie treści z bazy danych. W tym zakresie dyrektywa przewiduje wprowadzenie wyjątków, a poza ich zakresem – konieczność uzyskania zezwolenia od podmiotów uprawnionych.

Ponieważ niniejsze opracowanie poświęcone jest scrapowaniu szczególnego rodzaju danych, a mianowicie tych udostępnianych przez podmioty zaliczane do sektora publicznego, należy zwrócić uwagę na wyjątkowe podejście unijnego prawodawcy do tej kategorii danych. Informacje sektora publicznego odnoszą się do wszystkich informacji, które podmioty publiczne wytwarzają, zbierają lub za które płacą. Przykładami są informacje geograficzne, statystyki, dane pogodowe, dane z projektów badawczych finansowanych ze środków publicznych i zdigitalizowane książki z bibliotek. Polityka Unii Europejskiej zmierza do jak najszerzego otwarcia tych zasobów w celu tworzenia wartości dla gospodarki i społeczeństwa poprzez ponowne wykorzystywanie zawartych w nich danych⁸.

⁷ Dz. Urz. UE L 130 z 17.05.2019 r., s. 92.

⁸ Zob. Komisja Europejska, *Shaping Europe's digital future, Open Data*, <https://ec.europa.eu/digital-single-market/en/open-data> [dostęp: 28.08.2021].

Wyżej wskazane podejście znalazło swój wyraz w wielu europejskich strategicznych dokumentach i inicjatywach, ostatnio w Europejskiej Strategii w zakresie danych przyjętej przez Komisję Europejską w dniu 19 lutego 2020 r., zgodnie z którą: „Obywateli należy wyposażać w odpowiednie narzędzia umożliwiające im podejmowanie lepszych decyzji w oparciu o doświadczenia uzyskane w obszarze danych nieosobowych. Dane te powinny natomiast być dostępne dla wszystkich [...]. Dzięki temu społeczeństwo będzie w stanie czerpać jak największe korzyści z innowacji i konkurencji”.

Realizacja tych założeń opiera się na kilku filarach. Po pierwsze transparentność procesu decyzyjnego oraz dostęp do dokumentów urzędowych stanowią współcześnie istotną gwarancję jasności i przejrzystości funkcjonowania samych struktur UE⁹. W Traktacie o funkcjonowaniu Unii Europejskiej w art. 15 ust. 1 zapisano, iż w celu wspierania dobrych rządów i zapewnienia uczestnictwa społeczeństwa obywatelskiego, instytucje, organy i jednostki organizacyjne UE działają z jak największym poszanowaniem zasady otwartości. W wykonaniu delegacji określonej w Traktacie przyjęto rozporządzenie 1049/2001/WE w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji.

Przepisy unijne wprowadziły ponadto ramy prawne dla szerokiego dostępu do informacji i danych wytwarzanych przez sektor publiczny w krajach członkowskich oraz do ich ponownego wykorzystywania. Odpowiednie przepisy zostały zawarte w dyrektywie Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (dalej jako: dyrektywa *re-use*)¹⁰, która zastąpiła wcześniejsze unijne regulacje w tym

⁹ B. Opaliński, *Dostęp do informacji publicznej w prawie międzynarodowym i prawie Unii Europejskiej*, [w:] P. Szustakiewicz (red.), *Dostęp do informacji publicznej*, Warszawa 2014, s. 7.

¹⁰ Dz. Urz. UE L 172 z 26.06.2019 r., s. 56.

zakresie. W ramach realizacji unijnej polityki otwartych danych od 2015 r. działa także Europejski Portal Danych, ogólnoeuropejskie repozytorium informacji sektora publicznego, które można ponownie wykorzystać¹¹. Portal oferuje zbiory danych z Komisji Europejskiej, a także innych instytucji i agencji UE, gromadzi także metadane na temat informacji o sektorze publicznym dostępnych w witrynach z publicznymi danymi krajów członkowskich.

2. Scrapowanie a wykorzystywanie treści pobranych ze stron internetowych

Ocena prawna działań podmiotów scrapujących dane z internetu opiera się na dwóch płaszczyznach: przeszukiwania zasobów internetu i pobierania danych z cudzych stron internetowych oraz wykorzystywania pobranych danych, które to sfery w coraz większym stopniu się przenikają i uzupełniają. Problematyka korzystania z udostępnionych publicznie dóbr i treści od dawna była przedmiotem regulacji prawnych. Scrapowanie natomiast jest zagadnieniem stosunkowo nowym, które jednak już znajduje odzwierciedlenie w rosnącej liczbie regulacji.

W zależności od charakteru udostępnionych w internecie treści zakres ich ochrony i dopuszczalnego legalnego ich wykorzystywania regulują przepisy o prawie autorskim i prawach pokrewnych lub inne szczególne regulacje, np. dotyczące ochrony znaków towarowych.

Stosunkowo nowsze są przepisy dotyczące ograniczeń w korzystaniu z samych danych. Jeśli mają one charakter prostych informacji o faktach, same w sobie nie podlegają ochronie autorskoprawnej, nawet jeśli zostały wyodrębnione z chronionego utworu. Nie oznacza to jednak, że mogą być dowolnie wykorzystywane. Szczególną, rozszerzaną na przestrzeni ostatnich

¹¹ Europejski Portal Danych dostępny pod adresem: <https://www.europeandataportal.eu/pl>.

lat ochroną zostały objęte dane osobowe. Zakres ich wykorzystywania określony został w rozporządzeniu 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/WE¹², które jest aktem obowiązującym we wszystkich krajach unijnych, a zatem i w Polsce – bezpośrednio. Problematykę ochrony danych osobowych uzupełnia w Polsce ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (dalej jako: u.o.d.o.)¹³. Ponieważ za przetwarzanie danych osobowych uznaje się wszelkie czynności dokonywane na danych włącznie z ich zbieraniem, utrwalaniem i przechowywaniem, należy uznać, że ich scrapowanie musi znajdować legalną podstawę prawną w obowiązujących przepisach o ochronie danych osobowych. Jest to wymóg niezależny od regulacji omawianych w dalszej części opracowania.

Inne dane, które w oderwaniu od siebie nie byłyby chronione, mogą podlegać ochronie zestawione w ramach bazy danych. Strony internetowe zawierają często, oprócz innych elementów, również bazy danych (nieraz bardzo rozbudowane), wśród których można wymienić:

- 1) bazy danych, które nie podlegają ochronie prawnej (np. zawierające zestawienia wyników meczów piłkarskich);
- 2) bazy danych chronione na podstawie przepisów ustawy z dnia 27 lipca 2001 r. o ochronie baz danych (dalej jako: u.o.b.d.)¹⁴, (tzw. ochrona *sui generis*).

Przez bazę danych podlegającą ochronie *sui generis* (samoistnej) należy rozumieć: „zbiór danych lub jakichkolwiek innych materiałów i elementów zgromadzonych według określonej metody lub systematyki, indywidualnie dostępnych w jakikolwiek sposób, w tym środkami elektronicznymi, wymagający istotnego co do jakości lub ilości nakładu inwestycyjnego, w celu sporządzenia, weryfikacji lub prezentacji

¹² Dz. Urz. UE L 119 z 4.05.2016 r., s. 1.

¹³ T.j. Dz. U. z 2019 r. poz. 1781.

¹⁴ T.j. Dz. U. z 2021 r. poz. 386.

zawartości” (art. 2 ust. 1 pkt 1 u.o.b.d.). Przez wykorzystywanie bazy danych należy rozumieć zgodnie z art. 2 ust. 1 pkt 3 u.o.b.d. wszystkie postaci publicznego udostępniania jej zawartości. Dopuszczalność takich działań regulują przepisy art. 7 i 8 u.o.b.d.

- 3) bazy danych chronione przez ustawę z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (dalej jako: u.p.a.p.p.)¹⁵, przy czym aby baza mogła podlegać przepisom prawa autorskiego, musi posiadać cechy oryginalne i twórcze.

Powyżej nakreślono w skrócie złożoność problematyki wykorzystania danych przez inne podmioty niż ich pierwotny dysponent. Temat ten nie zostanie szerzej omówiony, jako że niniejsze opracowanie jest poświęcone zagadnieniu scrapowania, które zasadniczo służy późniejszemu wtórnemu wykorzystywaniu pozyskanych treści. Zauważyć natomiast należy, że sfery pobierania i korzystania z danych w coraz większym stopniu się przenikają. Tak jak już wskazano, na przykład dyrektywa o ochronie danych osobowych obejmuje swym zakresem każdą operację na danych, a zatem i ich ekstrakcję ze stron internetowych. Podobnie przepisy o ochronie praw autorskich i praw pokrewnych, w świetle których już sama eksploracja utworów może być rozumiana jako wkroczenie w monopol twórcy. Jednak ograniczenia na etapie scrapowania danych często mają swój specyficzny charakter i różnią się od tych obowiązujących na dalszych etapach korzystania z pozyskanych danych.

W kolejnych rozdziałach omówione zostały przepisy, które regulują tematykę pozyskiwania upublicznianych w internecie treści w drodze scrapowania. Wywód został uzupełniony odpowiednim orzecznictwem i wypowiedziami doktryny. Ogólne regulacje w omawianym zakresie znajdują zastosowanie również do informacji publicznych i informacji udostępnianych przez podmioty sektora publicznego do ponownego wykorzystywania. Szczególny jednak status powyższych treści prowadzi do

¹⁵ T.j. Dz. U. z 2021 r. poz. 1062.

niewielkiego odmiennego podejścia również w odniesieniu do ich scrapowania, co zostanie opisane w dalszej części opracowania.

3. Scrapowanie w świetle przepisów o ochronie baz danych

3.1. Przesłanki ochrony *sui generis* baz danych

Jak zostało wskazane wcześniej, najdalej idące ograniczenia w zakresie scrapowania zostały określone przez przepisy regulujące ochronę baz danych, dlatego zostaną tu one szerzej omówione. Prawo *sui generis* do bazy danych, wynikające z przepisów ustawy o ochronie baz danych (art. 6 w zw. z art. 2 ust. 1 pkt 1 u.o.b.d.), przysługuje jej producentowi, jeśli poniósł istotny nakład inwestycyjny na jej sporządzenie, weryfikację lub prezentację. Inwestycja taka może polegać na zaangażowaniu zasobów ludzkich, środków technicznych i finansowych. Powinna być też istotna z punktu widzenia ilościowego lub jakościowego. Ocena pod względem ilościowym odnosi się przy tym do środków dających się wyrazić liczbowo, a ocena jakościowa – do nakładów, których wysokości nie da się ustalić, takich jak wkład pracy intelektualnej lub wydatkowanie energii (wynika to z motywów 7, 39 i 40 dyrektywy o ochronie baz danych, która stanowi podstawę polskich przepisów i w świetle której muszą być one interpretowane).

Do pojęcia „inwestycji” ponoszonej przez producenta bazy danych odniósł się Trybunał Sprawiedliwości Unii Europejskiej¹⁶, uznając, że pojęcie to obejmuje środki poświęcone na poszukiwanie już istniejących materiałów i ich gromadzenie w bazie danych, nie obejmuje natomiast środków użytych w celu stworzenia materiałów składających się na zawartość bazy danych. W kontekście rozstrzyganej sprawy, która dotyczyła

¹⁶ Zob. wyrok TSUE z dnia 9 listopada 2004 r. w sprawie C-444/02 *Fixtures Marketing Ltd. przeciwko Organismos Prognostiken Agnon Podosfairou AE*.

terminarza spotkań w celu organizacji mistrzostw w piłce nożnej, Trybunał uznał, że pojęcie „inwestycji” nie obejmuje środków poświęconych na wyznaczenie dat, godzin i ustalenie doboru w pary drużyn odnoszących się do poszczególnych spotkań w ramach tych mistrzostw. W konsekwencji bazę danych z terminarzem spotkań piłkarskich TSUE uznał za niepodlegającą ochronie.

W Polsce oceny inwestycji w kontekście baz danych dokonał Sąd Apelacyjny w Szczecinie w wyroku z dnia 2 maja 2012 r. (I ACa 105/12)¹⁷, które to rozstrzygnięcie zostało podtrzymane w wyroku Sądu Najwyższego z dnia 9 maja 2013 r. (II CSK 466/12)¹⁸. W przywołanym wyroku Sąd Apelacyjny uznał, że właściciel portalu motoryzacyjnego nie poniósł istotnej ilościowo ani jakościowo inwestycji w pozyskiwanie danych do portalu ani w ich weryfikowanie, jako że sami użytkownicy zamieszczali ogłoszenia, które nie były poddawane procedurze weryfikacji. Odmienienie natomiast Sąd ocenił nakład poniesiony przez producenta bazy na stworzenie całego systemu ogłoszeń.

Jeżeli baza danych podlega ochronie na podstawie przepisów o bazach danych, nie tylko jej wykorzystywanie lub wykorzystywanie jej części podlega ograniczeniom, ale również pobieranie z niej danych. U.o.b.d. odnosi się bezpośrednio do czynności, które polegają na przeszukiwaniu baz danych i ekstrakcji jej treści.

3.2. Dopuszczalny prawnie zakres pobierania danych z chronionych baz danych

Pobieranie danych oznacza, zgodnie z art. 2 ust. 1 pkt 2 u.o.b.d., przejęcie lub przeniesienie ich na inny nośnik, przy czym przepis odnosi się zarówno do nieograniczonego w czasie przejęcia i przeniesienia, jak i do tego typu czynności dokonanych tylko na pewien czas. Pojęcie pobierania obejmuje swym zakresem każdy sposób i formę przejęcia lub

¹⁷ Zob. uzasadnienie wyroku opubl. w OSASz 2012/4/56-86.

¹⁸ Opubl. w OSNC-ZD 2014/3/46.

przeniesienia. Przeniesienie zakłada umieszczenie danych na nowym nośniku z jednoczesnym ich usunięciem z dotychczasowego nośnika, a przejście to umieszczenie na nowym nośniku bez usunięcia z poprzedniego¹⁹. Do pojęcia „pobierania” danych odniósł się też TSUE, uznając, że należy je rozumieć szeroko jako odnoszące się do każdej czynności dokonanej bez upoważnienia i polegającej na przywłaszczeniu całości lub części zawartości bazy danych, niezależnie od charakteru czy formy zastosowanej w tym kontekście metody²⁰. Za pobieranie należy uznać też przejście elementów chronionej bazy danych do innej bazy, które wskutek jego powtarzalnego i systematycznego charakteru mogło doprowadzić do przeniesienia istotnej części jej zawartości²¹. Należy uznać, że w ramach definicji „pobierania” mieści się scrapowanie, które w części polega na ekstrakcji danych ze stron internetowych za pomocą automatycznych narzędzi.

Przepisami, które bezpośrednio regulują zakres dozwolonego pobierania treści z chronionych prawnie baz danych, są art. 7 oraz art. 8 ust. 2 u.o.b.d. Zgodnie z art. 7 ust. 1 ustawy u.o.b.d. producent bazy danych udostępnionej publicznie nie może zabronić korzystającemu z niej użytkownikowi nie tylko jej wtórnego wykorzystania (o czym była już mowa), ale również pobierania w jakimkolwiek celu nieistotnej, co do jakości lub ilości, części jej zawartości. Przepis odpowiednio odnosi się do części bazy danych (art. 7 ust. 2 u.o.b.d.). Postanowienia umowne sprzeczne z przywołaną regulacją są nieważne (art. 7 ust. 4 u.o.b.d.). Zgodnie z art. 8 ust. 2 u.o.b.d. z kolei: „nie jest dozwolone powtarzające się i systematyczne pobieranie lub wtórne wykorzystanie sprzeczne z normalnym korzystaniem i powodujące nieusprawiedliwione naruszenie słusznych interesów producenta”.

¹⁹ Zob. uzasadnienie wyroku Sądu Apelacyjnego w Szczecinie z dnia 2 maja 2012 r., I ACa 105/12.

²⁰ Zob. wyrok TSUE z dnia 9 listopada 2004 r. w sprawie C-203/02 *The British Horseracing Board Limited przeciwko William Hill*, EU:C:2004:695.

²¹ Zob. wyrok TSUE z dnia 9 października 2008 r. w sprawie C-304/07 *Directmedia Publishing przeciwko Albert-Ludwigs-Universität Freiburg*, EU:C:2008:552.

Z przywołanych regulacji wynikają następujące wnioski:

- 1) zabronione jest pobieranie istotnej części bazy danych podlegającej ochronie *sui generis*;
- 2) producent takiej bazy danych nie może sprzeciwić się pobieraniu nieistotnej, co do jakości lub ilości, części jej zawartości;
- 3) jeżeli pobieranie nieistotnej części bazy danych ma charakter powtarzający się i systematyczny, a ponadto jest sprzeczne z normalnym korzystaniem z tej bazy danych i narusza w sposób nieuzasadniony słusne interesy producenta – jest sprzeczne z prawem.

Jeżeli baza danych nie jest pobierana w całości, lecz jedynie w części, aby ocenić legalność takiego działania, należy w każdym konkretnym przypadku przeanalizować wszystkie przesłanki określone w art. 8 ust. 2 u.o.b.d. oraz wziąć pod uwagę całość przepisów ustawy w kontekście regulacji dyrektywy o ochronie baz danych, co uczyniono poniżej.

Do określenia zakresu zastosowania przepisu art. 8 ust. 2 u.o.b.d. konieczne jest też wyjaśnienie znaczenia określeń: „powtarzający się” i „systematyczny” odnoszących się do zakazów pobierania objętych analizowaną regulacją. Przede wszystkim wskazać należy, że dla zastosowania regulacji wyżej wskazanego art. 8 ust. 2 niezbędne jest, by pobieranie lub wtórne wykorzystanie nieistotnej części bazy danych miało charakter zarówno powtarzający się, jak i systematyczny, a zatem przesłanki te muszą zostać spełnione łącznie²². Wobec braku definicji tych pojęć w zakresie wykładni literalnej stwierdzić można, zestawiając słownikowe znaczenie powołanych pojęć, że nie wystarczy, by pobieranie czy wtórne wykorzystywanie nastąpiło ponownie więcej niż jeden raz, ale także musi być metodyczne, regularne, ewentualnie również zachodzące od pewnego czasu²³.

²² R. Stötzel, S. Wille, *Der Urheberrechtsschutz sui generis für Datenbanken*, “Europäisches Wirtschafts- und Steuerrecht” 2004, H. 11, s. 493.

²³ S. Dubisz (red.), *Uniwersalny słownik języka polskiego*, Warszawa 2003, t. 3, s. 476 i 1480.

Systematyczne i powtarzające się pobieranie stanowi zasadniczo istotę scrapowania, zatem podmioty podejmujące tego typu czynności zawsze rozważyć muszą ich zgodność z regulacją art. 8 ust. 2 u.o.b.d.²⁴

Kolejną przesłanką, którą należy rozważyć przy ocenie legalności scrapowania chronionych baz danych, jest rozmiar i istotność pobranych elementów. Nie wynika ona bezpośrednio z art. 8 ust. 2 u.o.b.d., który stanowi w tym zakresie nieprawidłową implementację dyrektywy o ochronie baz danych, ale z całościowej analizy regulacji dokonanej w świetle celów dyrektywy. Dyrektywa w art. 7 ust. 5 stanowi, iż: „niedozwolone jest powtarzające się i systematyczne pobieranie danych i/lub wtórne ich wykorzystanie w nieistotnej części, jeśli czynności te są sprzeczne z normalnym korzystaniem z tej bazy danych lub w sposób nieuzasadniony naruszają słuszne interesy producenta bazy danych”.

Pojęcie „istotnej pod względem ilościowym” części zawartości bazy danych odnosi się do pobranej ilości danych i należy je oceniać w stosunku do całkowitej ilości danych zawartych w tej bazie. Pojęcie „istotnej pod względem jakościowym” części zawartości bazy danych z kolei odnosi się do rozmiaru inwestycji związanej z uzyskaniem, weryfikacją i prezentacją tej zawartości, która została pobrana lub wtórnie wykorzystana, niezależnie od tego, czy pobrana lub wtórnie wykorzystana zawartość bazy stanowi istotną pod względem ilościowym część całkowitej zawartości chronionej bazy danych. Pojęcie „nieistotnej” części bazy danych obejmuje każdą część, która ani pod względem ilościowym, ani jakościowym nie wchodzi w zakres pojęcia „istotnej” części²⁵.

²⁴ Za spełniające warunki „systematycznego” i „powtarzającego się” pobierania uznano między innymi działanie metapoziomowej wyszukiwarki umożliwiającej publicznie kręgowi odbiorców na wyszukiwanie w ramach całości lub istotnej części zawartości udostępnionej online bazy danych „w czasie rzeczywistym”, zob.: wyrok TSUE z dnia 19 grudnia 2013 r. w sprawie C-202/12 *Innoweb BV przeciwko Wegener ICT Media BV i Wegener Mediaventions BV*, EU:C:2013:850.

²⁵ Zob. wyrok TSUE z dnia 9 listopada 2004 r. w sprawie C-203/02 *The British Horseracing Board Limited przeciwko William Hill*, EU:C:2004:695.

W sprawie, która była podstawą powyższych wniosków TSUE, ostatecznie sąd w Wielkiej Brytanii uznał, że działanie pozwanego polegające na ściąganiu z internetowej bazy danych i wykorzystywania danych z serwisu powoda w postaci informacji o lekarzach, które pozwany zestawiał w swoim serwisie z informacjami zagregowanych z innych serwisów, było nielegalne. Pozwany korzystał z ok. 4300 rekordów z serwisu powoda, co stanowił 10-11% całości. Sąd jednak uznał, że – mimo że nie była to istotna ilościowa część pobranej bazy danych – była istotna jakościowo, a zatem podlegała ochronie.

W doktrynie podkreśla się, że badając „istotność” części bazy danych, należy brać pod uwagę wartość gospodarczą (handlową) tej części, jej rodzaj oraz zakres. Za istotne należy uważać te części, które same „jako takie” mogłyby stanowić przedmiot ochrony *sui generis*. Podobnie należy oceniać te części bazy danych, które faktycznie mogą zastąpić korzystanie z całości bazy danych z punktu widzenia potrzeb określonych użytkowników. W tym kontekście należy badać, czy przejęcie części zawartości bazy otwiera możliwość wytworzenia konkurencyjnego produktu, który byłby w stanie zastępować produkt pierwotny. Przy ustalaniu „istotnej części” bazy danych istotne jest także, czy eksploatacja bazy danych obejmuje jej najbardziej wartościowe elementy²⁶.

Nawet jeżeli pobieranie danych z cudzej bazy danych zostanie dokonane w „nieistotnej” części, może wciąż stanowić naruszenie przepisów prawa. Stanie się tak w sytuacji, gdy będzie sprzeczne z normalnym korzystaniem z tej bazy danych i w sposób nieuzasadniony naruszy słuszne interesy producenta. Należy zwrócić uwagę, że omawiana polska regulacja jest istotnie niezgodna z dyrektywą o ochronie baz danych w zakresie konstrukcji przesłanek zastosowania przepisu art. 8 ust. 2 u.o.b.d. Art. 7 ust. 5 dyrektywy o ochronie baz danych stanowi bowiem, iż aby uznać, że pobieranie danych jest nielegalne, wystarczy, że spełnia jeden

²⁶ Zob. J. Barta, R. Markiewicz, *Ustawa o ochronie baz danych. Komentarz*, Warszawa 2002, s. 117.

z warunków: jest sprzeczne z normalnym korzystaniem z bazy danych lub powoduje nieusprawiedliwione naruszenie słuszych interesów producenta. Polski ustawodawca zamiast łącznika „lub” posłużył się łącznikiem „i”, w związku z czym dla zaktualizowania się uprawnień ochronnych producenta bazy danych przesłanki sprzeczności z normalnym korzystaniem i naruszenia interesów producenta muszą być spełnione łącznie.

Pojęciem wymagającym wyjaśnienia w kontekście omawianego zagadnienia jest „normalne korzystanie”. W doktrynie przyjmuje się, że obejmuje ono czynności, których wykonywania w normalnych, zwykłych warunkach można się spodziewać, zwłaszcza w powiązaniu z poczynioną przez uprawnionego inwestycją i oczekiwaniem dochodu z niej uzyskiwanego. *A contrario*, naruszające normalne korzystanie będą zatem takie formy eksploatacji, które godzą w inwestycję producenta, ograniczając albo wykluczając realizację praw producenta bazy danych lub wykorzystanie przez niego lub z jego upoważnienia bazy danych w oczekiwanym w normalnych warunkach zakresie²⁷.

W rozstrzyganej w Polsce sprawie z tego zakresu Sąd Apelacyjny w Szczecinie w przywołanym już wcześniej wyroku I ACa 105/12 uznał, że usługi świadczone przez serwis internetowy polegające na „przeglądaniu” w wersji on-line ofert pod kątem zleceń klientów i udostępnianiu im oferty w wersji całościowej z pominięciem strony głównej serwisu, z którego oferta ta pochodziła, nie przekraczało granic normalnego korzystania. Normalne korzystanie z bazy danych powódki bowiem polegało nie na wejściu użytkownika na stronę główną serwisu, ale na dotarciu do konkretnej oferty, co ostatecznie następowało.

Wydaje się, że działaniem zakłócającym „normalne korzystanie” z bazy danych są takie działania automatów do przeszukiwania treści strony, które zakłócają jej normalne funkcjonowanie. Ideą działania

²⁷ Zob. E. Traple, [w:] J. Barta, R. Markiewicz (red.), *Prawo autorskie i prawa pokrewne. Komentarz*, Kraków 2005, s. 372-373; zob. także S. Ciupa, *Dozwolony użytek w ustawie o ochronie baz danych*, „Monitor Prawniczy” 2003, nr 12, s. 550.

botów jest jak najszybsze otwieranie kolejnych znalezionych linków, a to powoduje ryzyko wystąpienia różnego rodzaju problemów technicznych, szczególnie wzrostu obciążenia serwera.

W odniesieniu do pojęcia „słuszne interesy producenta bazy danych” w literaturze prezentowane jest stanowisko, że miarą, którą należy mierzyć ograniczenie dla słusznych interesów producenta bazy danych, są interesy użytkowników tej bazy. Równowaga, do której należy dążyć, ma zapewnić wyważenie z jednej strony ekonomicznych interesów producentów związanych z poczynioną inwestycją, a z drugiej strony – interesów użytkowników w zakresie dostępu do informacji inkorporowanych w bazach danych. Szeroka wykładnia „słusznych interesów producenta bazy danych” nie jest zatem dopuszczalna, prowadzi bowiem *de facto* przez ochronę prawem *sui generis* do monopolizacji informacji, tworząc samoistną podstawę ochrony treści, co wprost wykluczono w motywie 46 dyrektywy o ochronie baz danych²⁸.

W istotnym rozstrzygnięciu TSUE z tego zakresu z dnia 19 grudnia 2013 r. w sprawie C202/12 *Innoweb BV przeciwko Wegener ICT Media BV, Wegener Mediaventions BV* Trybunał uznał, iż serwis internetowy pobierający oferty sprzedaży używanych samochodów z różnych platform zajmujących się pośrednictwem przy ich sprzedaży narusza słuszne interesy producentów tych serwisów. Wynika to z faktu, że klient może dokonać zakupu, posiłkując się jedynie danymi z serwisu agregującego oferty bez konieczności wchodzenia do serwisu, który ofertę oryginalnie wystawił, może znaleźć samochód w konkurencyjnej cenie na innej platformie i skorzystać z tej oferty zamiast z oferty skarżącego producenta, co godzi w jego interesy. Ponadto właściciel oryginalnej witryny ponosi koszty jej utrzymania i aktualizowania ofert, a z uwagi na możliwe

²⁸ Por. E. Traple, [w:] J. Barta, R. Markiewicz (red.), *Prawo autorskie...*, s. 372-373; D. Lubasz, M. Namysłowska (red.), *Ustawa o ochronie baz danych. Komentarz*, Warszawa 2013, LEX.

zmniejszenie liczby użytkowników w wyniku działań pozwanego grozi mu utrata wpływów związanych z reklamami umieszczanymi na stronie.

Jak już wcześniej wspomniano, w związku z błędną implementacją dyrektywy o ochronie baz danych do polskiego porządku prawnego warunki sprzeczności z normalnym korzystaniem i ze słusznym interesem producenta muszą być spełnione łącznie. Takie rozumienie polskich przepisów uznał w przywoływanym już wcześniej wyroku I ACa 105/12 Sąd Apelacyjny w Szczecinie, co wydaje się stać w sprzeczności z prounijną wykładnią polskich przepisów prawa (w wyroku kasacyjnym do tego orzeczenia o sygn. II CSK 466/12 Sąd Najwyższy przywołał zarówno przepisy polskie, jak i unijne).

4. Scrapowanie w świetle prawa autorskiego; eksploracja tekstów i danych

Przepisy prawa autorskiego, które należy wziąć pod uwagę przy omawianiu zagadnienia legalności scrapowania, dotyczą ochrony baz danych i pól eksploatacji utworu. Niezwykle istotne regulacje zagadnienia eksploracji tekstów i danych (*text and data mining*) zostały zawarte w dyrektywie w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym, która nie została jeszcze zaimplementowana do polskiego porządku prawnego mimo upływu terminu na to wyznaczonego. Oznacza to, że obowiązujące obecnie w Polsce przepisy prawa powinny być interpretowane w zgodzie z wprowadzonymi przez dyrektywę zasadami mimo braku nowej krajowej regulacji prawnoautorskiej.

Ochronie prawnoautorskiej podlegają zarówno strony internetowe, jeśli mają oryginalny charakter, twórcze elementy stron, jak i bazy danych o cechach utworu, które są częściami takich stron. Zgodnie z art. 3 u.p.a.p.p.: „bazy danych spełniające cechy utworu są przedmiotem prawa autorskiego, nawet jeżeli zawierają niechronione materiały, o ile przyjęty w nich

dobór, układ lub zestawienie ma twórczy charakter, bez uszczerbku dla praw do wykorzystanych utworów”.

W obowiązującym stanie prawnym ochrona *sui generis* w odniesieniu do baz danych uznawana jest zasadniczo za silniejszą od ochrony wynikającej z prawa autorskiego. Jak wskazuje się w literaturze, ustawa o prawie autorskim zapewnia ochronę tylko w tym zakresie, w jakim jego utwór ma twórczy i indywidualny charakter, pozostałe składniki utworu nie są przedmiotem wyłączności i mogą być dowolnie wykorzystywane w innych wytworach niematerialnych (w tym bazach danych). Natomiast ochrona *sui generis* baz danych rozciąga się także na ich zawartość²⁹.

Podkreślić należy, że przedmiotem regulacji prawa autorskiego jest generalnie eksploatacja utworów. Przedmiotem dyskusji zatem było rozstrzygnięcie, czy same czynności, jakim poddawany jest utwór, a więc na przykład jego przeszukiwanie czy ekstrakcja czystych danych niemających cech twórczych z utworu bądź bazy danych o takich cechach, podlegają regulacjom prawnoautorskim, a jeżeli tak – to jak trzeba czynności takie kwalifikować. Należy tu przywołać stanowisko wskazujące, że o ile informacje i dane nie są objęte monopolem prawnoautorskim, to nie jest to równoznaczne ze stwierdzeniem, że żadna z czynności, którym jest poddawany utwór w celu uzyskania informacji i danych, nie wkracza w monopol uprawnionego. Wskazano przy tym, że niezależnie od przyjętego modelu teoretycznego faz analizy danych co najmniej część takich działań jest nierozdzielnie powiązana z reprodukcją co najmniej kilku fragmentów utworów. Co więcej, czynności takie mogą być powtarzane w kolejnych etapach eksploracji danych³⁰. Prowadzi to do uznania, że w określonych okolicznościach podmiot dokonujący czynności scrapowania treści objętych ochroną prawnoautorską samą tą czynnością może

²⁹ Por. J. Barta, R. Markiewicz, *Prawo autorskie. Komentarz*, Warszawa 2013, s. 315.

³⁰ K. Gienas, *Data mining jako problem prawa autorskiego*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego” 2017, z. 1, s. 26.

naruszyć monopol twórcy. Stanowisko takie legło u podstaw skonstruowania przepisów regulujących eksplorację tekstów i danych.

Regulacja zagadnienia eksploracji tekstów i danych (*text and data mining*) jest nową konstrukcją prawną przyjętą w dyrektywie w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym. Odnosi się do wszystkich efektów twórczej działalności chronionych na podstawie przepisów o prawie autorskim, ale swoim zakresem wykracza poza regulacje *stricte* prawnoautorskie. Ponieważ eksploracja tekstów i danych dotyczy wprost zagadnienia scrapowania, omówienie tego zagadnienia jest istotne dla niniejszej pracy.

Pojęcie „eksploracji tekstów i danych” zostało wyjaśnione w motywie 8 preambuły dyrektywy, zgodnie z którym: „Nowe technologie umożliwiają automatyczną matematyczną analizę informacji w postaci cyfrowej, takich jak teksty, dźwięki, obrazy lub dane, powszechnie określaną jako eksploracja tekstów i danych. Eksploracja tekstów i danych umożliwia przetwarzanie dużych ilości informacji w celu uzyskania nowej wiedzy i odkrycia nowych tendencji [...]. W niektórych przypadkach eksploracja tekstów i danych może obejmować czynności chronione prawem autorskim lub prawem do bazy danych *sui generis*, w szczególności zwielokrotnianie utworów lub innych przedmiotów objętych ochroną lub pobieranie treści z bazy danych, co ma miejsce na przykład w przypadku normalizacji danych podczas eksploracji tekstów i danych. Jeżeli nie znajduje zastosowanie wyjątek lub ograniczenie, konieczne jest uzyskanie zezwolenia na dokonanie takich czynności od podmiotów uprawnionych”.

Jak wynika z powyższego, zagadnienie eksploracji tekstów i danych ma tak szeroki charakter, że wykracza poza ramy regulacji przedmiotu ochrony prawa autorskiego i wkracza nawet w zakres ochrony *sui generis* baz danych. Implementacja dyrektywy oznaczać zatem będzie zmiany w zakresie dotychczasowych zasad scrapowania na różnych poziomach.

W literaturze przyjmuje się, że nowy sposób korzystania stanowi nowe pole eksploatacji³¹ i jako taki wymaga odrębnej zgody podmiotu uprawnionego. W motywie 9 wyjaśniono jednocześnie, iż eksploracja tekstów i danych może być również dokonywana w odniesieniu do samych faktów lub danych, które nie są chronione prawem autorskim, i w takich przypadkach nie jest wymagane zezwolenie na podstawie prawa autorskiego, podobnie jak w odniesieniu do eksploracji tekstów i danych, w których nie dokonuje się czynności zwielokrotniania.

Dyrektywa wprowadza kilka szczegółowych wyjątków w zakresie eksploracji tekstów i danych odnoszących się do eksploracji na potrzeby badań naukowych, dydaktyki czy w celu zachowania dziedzictwa kulturowego. Ponadto na mocy art. 4 nakłada na państwa członkowskie obowiązek wprowadzenia wyjątku lub ograniczenia odnoszącego się generalnie do eksploracji tekstów i danych, bez wskazania kontekstu. W takim przypadku wyjątek lub ograniczenie mają zastosowanie pod warunkiem, że korzystanie z utworów i innych przedmiotów objętych ochroną nie zostało wyraźnie zastrzeżone w odpowiedni sposób przez podmioty uprawnione. Przepis ten oznacza zmianę w stosunku do obecnie obowiązujących regulacji, jako że dotyczy nie tylko eksploracji treści poddanych ochronie prawnoautorskiej, ale również przewiduje, że wyjątek ma być wprowadzony w odniesieniu do art. 5 lit. a) i art. 7 ust. 1 dyrektywy o ochronie baz danych. Jego potencjał został znacznie ograniczony zastrzeżeniem, że podmiot uprawniony będzie mógł zastrzec brak zgody na eksplorację tekstów i danych. W odniesieniu do przedsiębiorców zarządzających serwisami internetowymi może to zatem w praktyce nie mieć większego znaczenia. W odniesieniu jednak do informacji i danych publicznych może oznaczać ułatwienia w dostępie.

³¹ K. Gliściński, *Komentarz do art. 50 ustawy o prawie autorskim i prawach pokrewnych*, [w:] A. Michalak (red.), *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, Warszawa 2019, s. 390.

5. Scrapowanie informacji publicznych oraz informacji i danych sektora publicznego

5.1. Prawo do informacji publicznej

W Polsce prawo obywatela do uzyskiwania informacji od organów władzy publicznej i osób pełniących funkcje publiczne jest prawem konstytucyjnym. Art. 61 Konstytucji określa je szeroko, obejmując jego zakresem również uzyskiwanie informacji o działalności organów samorządu gospodarczego i zawodowego, a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub mieniem Skarbu Państwa.

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (dalej jako: u.d.i.p.)³² jako informację publiczną definiuje każdą informację o sprawach publicznych (art. 1 ust. 1 u.d.i.p.), a art. 6 ustawy zawiera otwarty katalog informacji podlegających udostępnieniu. Podmioty zobowiązane do udostępniania informacji publicznych zostały wymienione w art. 4 ustawy, przy czym katalog ten nie jest zamknięty:

„Art. 4. 1. Obowiązane do udostępniania informacji publicznej są władze publiczne oraz inne podmioty wykonujące zadania publiczne, w szczególności:

- 1) organy władzy publicznej;
- 2) organy samorządów gospodarczych i zawodowych;
- 3) podmioty reprezentujące zgodnie z odrębnymi przepisami Skarb Państwa;
- 4) podmioty reprezentujące państwowe osoby prawne albo osoby prawne samorządu terytorialnego oraz podmioty reprezentujące inne państwowe jednostki organizacyjne albo jednostki organizacyjne samorządu terytorialnego;

³² T.j. Dz. U. z 2020 r. poz. 2176 ze zm.

5) podmioty reprezentujące inne osoby lub jednostki organizacyjne, które wykonują zadania publiczne lub dysponują majątkiem publicznym, oraz osoby prawne, w których Skarb Państwa, jednostki samorządu terytorialnego lub samorządu gospodarczego albo zawodowego mają pozycję dominującą w rozumieniu przepisów o ochronie konkurencji i konsumentów.

2. Obowiązane do udostępnienia informacji publicznej są organizacje związkowe i pracodawców, reprezentatywne w rozumieniu ustawy z dnia 24 lipca 2015 r. o Radzie Dialogu Społecznego i innych instytucjach dialogu społecznego (Dz. U. z 2018 r. poz. 2232), oraz partie polityczne.

3. Obowiązane do udostępniania informacji publicznej są podmioty, o których mowa w ust. 1 i 2, będące w posiadaniu takich informacji”.

W judykaturze i doktrynie utrwalił się pogląd, że informacją publiczną będzie każda wiadomość wytworzona lub odnosząca się do władz publicznych, a także odnosząca się do innych podmiotów wykonujących funkcje publiczne w zakresie wykonywania przez nie zadań w zakresie władzy publicznej³³.

O uznaniu, że określona informacja jest informacją publiczną, decydują więc dwa elementy łącznie:

- 1) podmiotowy: dany podmiot zaliczony jest do zbioru władz publicznych lub w imieniu państwa wykonuje zadania publiczne;
- 2) przedmiotowy: informacja dotyczy spraw związanych z wykonywaniem przez ten podmiot zadań publicznych.

5.2. Scrapowanie stron internetowych podmiotów zobowiązanych do udostępniania informacji publicznych

Informacje publiczne mogą być udostępniane bądź przez internet (w ramach Biuletynu Informacji Publicznej prowadzonego przez podmioty

³³ Zob. wyrok NSA z dnia 27 czerwca 2013 r., I OSK 513/13, CBOSA; podobnie wyrok NSA z dnia 10 stycznia 2014 r., I OSK 1966/13, CBOSA.

zobowiązane do jej udostępniania, ale również poza nim), bądź na wniosek. W niniejszym opracowaniu ze względu na charakter scrapowania skoncentrowano się jedynie na trybie bezwnioskowym.

Na stronach internetowych podmiotów zobowiązanych do udostępniania informacji publicznej możemy znaleźć treści, które stanowią taką informację, i takie, które nie mają charakteru informacji publicznej. Jest to szczególnie istotne w odniesieniu do podmiotów, które nie są instytucjami publicznymi, takich jak spółki z udziałem Skarbu Państwa, jednostki organizacyjne wykonujące zadania publiczne czy organy samorządu zawodowego lub gospodarczego. Zasady scrapowania treści niemających charakteru informacji publicznej w niczym nie odbiegają od omówionych we wcześniejszej części opracowania. Typ podmiotu, który je udostępnia w internecie, nie ma przy tym znaczenia. Co do zasady również w odniesieniu do treści, które mają charakter informacji publicznych, znajdują zastosowanie regulacje ogólne. Ustawodawca nie wprowadził wyjątku w odniesieniu do pobierania danych udostępnianych przez podmioty zobowiązane do tego na mocy u.d.i.p. Niemniej szczególny charakter takich treści prowadzi do nieco odmiennej interpretacji ogólnych przepisów dotyczących ich automatycznego pobierania z internetu.

Jak wskazano, omawiając przepisy dotyczące baz danych chronionych prawem *sui generis*, producentowi bazy przysługuje wyłączne prawo do wtórnego pobierania lub wykorzystywania jej istotnej części. Producent może jednak udzielić zgody na takie działania innym podmiotom. Niedozwolone jest ponadto powtarzające się i systematyczne pobieranie nieistotnej części bazy danych producenta przez podmiot trzeci. Aby podejmowane przez użytkowników czynności w odniesieniu do baz danych mogły być uznane za niezgodne z przepisami, muszą być sprzeczne z normalnym korzystaniem i powodować nieusprawiedliwione naruszenie interesów producenta.

Jeżeli użytkownik dokonuje scrapowania strony internetowej podmiotu zobowiązanego do udostępniania informacji publicznej, jego

działania podlegają takiej samej ocenie jak w odniesieniu do każdego innego rodzaju witryny internetowej. Jeżeli zatem jego aktywność dotyczy korzystania z chronionej bazy danych w dozwolonym zakresie, nie może naruszać normalnego z niej korzystania. Za naruszające „normalne korzystanie” uznane będą takie formy eksploatacji, które godzą w inwestycję producenta, ograniczając albo wykluczając realizację jego praw. Powinno się do nich zaliczać również te, które zakłócają korzystanie ze strony internetowej. Podmiot dokonujący scrapowania może też naruszyć „słuszne interesy producenta” w różny sposób, ale w szczególności jeżeli jego działania naruszają ekonomiczne interesy producenta związane z poczynioną inwestycją.

Gdy scrapowanie dotyczy informacji publicznych udostępnionych przez podmioty, które są organami państwowymi albo samorządowymi, ale również państwowych czy samorządowych osób prawnych lub jednostek organizacyjnych czy też podmiotów reprezentujących Skarb Państwa, ryzyko naruszenia normalnego korzystania z udostępnionej przez nie bazy danych czy słusznych interesów takich podmiotów jest ograniczone. Wynika to z faktu, że w pełni państwowe czy samorządowe podmioty z założenia nie udostępniają informacji publicznej w ramach komercyjnych serwisów, a ich celem nie jest osiąganie zysków ani pozyskiwanie jak największej liczby odbiorców treści o charakterze informacji publicznych. Działalność tych podmiotów nie ma na celu osiągnięcia zysku, a zatem nie można zagrozić ich ekonomicznym interesom. Natomiast już aktywność programów komputerowych przeszukujących zasoby stron takich podmiotów i zakłócających ich działanie może zostać uznana za sprzeczne z normalnym z niej korzystaniem.

W odniesieniu do omawianej kategorii podmiotów należy również zwrócić uwagę na przepisy dyrektywy w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym. Nakazuje ona państwom członkowskim, o czym była mowa wcześniej, wprowadzenie wyjątku w zakresie eksploracji tekstów i danych. Określa jednocześnie prawo

dysponentów praw autorskich i praw pokrewnych oraz producentów baz danych do zastrzeżenia niedopuszczalności jej dokonywania. Należy jednak uznać, że podmioty, o których mowa w niniejszej części opracowania, są tymi, które zastrzeżeń w zakresie eksploracji tekstów i danych nie powinny zgłaszać w odniesieniu do informacji, co do których prawami dysponują. Wynika to zarówno z charakteru tych podmiotów, jak i ze specyfiki udostępnianych przez nie treści.

Odmiennej charakter mają inne niż wymienione wyżej podmioty zobowiązane do udostępniania informacji publicznej, np. spółki z udziałem Skarbu Państwa. Ich podstawowa działalność może mieć komercyjny charakter, mogą również tworzyć bazy danych, które wymagają znacznych inwestycji niepublicznych środków, ich celem może być osiągnięcie jak największej liczby odwiedzin na swojej stronie. Wszystkie te interesy mogą być chronione przed nielegalnym scrapowaniem na zasadach ogólnych.

5.3. Ponowne wykorzystywanie informacji sektora publicznego i otwarte dane publiczne

Od prawa dostępu do informacji publicznej należy odróżnić prawo do ponownego wykorzystywania informacji sektora publicznego (*re-use*), które znalazło wyraz w odrębnej regulacji, a mianowicie w przepisach ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (dalej jako: u.o.d.p.w.i.s.p)³⁴. Ustawa stanowi implementację dyrektywy 2019/1024/UE i zastępuje obowiązującą uprzednio ustawę z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego³⁵.

Prawo do informacji publicznej i prawo do ponownego wykorzystywania informacji sektora publicznego mają odmienny charakter i służą realizacji innych celów. Pierwsze z nich, określone w ustawie o dostępie

³⁴ Dz. U. z 2021 r. poz. 1641, dalej jako u.o.d.p.w.i.s.p

³⁵ T.j. Dz. U. z 2019 r. poz. 1446.

do informacji publicznej, stanowi implementację zasady jawności wyrażonej w art. 61 Konstytucji i realizuje prawo do informacji, które uważane jest za jedno z podstawowych praw człowieka. Prawo do ponownego wykorzystywania informacji sektora publicznego natomiast ma przede wszystkim wymiar ekonomiczny i pozwala podmiotom zainteresowanym osiągać korzyści związane z możliwością dalszego wykorzystywania (przetwarzania) udostępnionej informacji. Celem zasadniczym przyjęcia regulacji w zakresie udostępniania informacji sektora publicznego do ponownego wykorzystywania było zwiększenie podaży otwartych danych, w tym zasobów informacji o istotnej wartości i potencjale do tworzenia nowych usług i produktów, a także stworzenie optymalnego otoczenia regulacyjnego dla efektywnego wykorzystywania informacji sektora publicznego w Polsce³⁶.

Zdefiniowane w art. 2 pkt 8 u.o.d.p.w.i.s.p pojęcie informacji sektora publicznego jest szersze niż pojęcie informacji publicznej. Przez informację sektora publicznego należy rozumieć bowiem „każdą treść lub jej część, niezależnie od sposobu utrwalenia, w szczególności w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej, będącą w posiadaniu podmiotu zobowiązanego”.

Za podmioty zobowiązane do udostępniania lub przekazywania informacji sektora publicznego w celu ponownego wykorzystywania zostały uznane, zgodnie z art. 3 u.o.d.p.w.i.s.p, analogiczne jednostki jak w ustawie z 2016 r., a mianowicie:

- 1) jednostki sektora finansów publicznych w rozumieniu przepisów ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych;
- 2) inne państwowe jednostki organizacyjne nieposiadające osobowości prawnej niebędące jednostkami sektora finansów publicznych;

³⁶ Zob. *Uzasadnienie do projektu ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego*, Druk nr 1338, Internetowy System Aktów Prawnych [dostęp: 24.09.2021].

3) osoby prawne niebędące jednostkami sektora finansów publicznych, utworzone w szczególnym celu zaspokajania potrzeb o charakterze powszechnym, niemających charakteru przemysłowego ani handlowego, jeżeli jednostki o których mowa w tym przepisie, jednostki sektora finansów publicznych oraz inne państwowe jednostki organizacyjne nieposiadające osobowości prawnej, pojedynczo lub wspólnie, bezpośrednio albo pośrednio przez inny podmiot: finansują je w ponad 50% lub posiadają ponad połowę udziałów albo akcji, lub sprawują nadzór nad organem zarządzającym, lub mają prawo do powoływania ponad połowy składu organu nadzorczego lub zarządzającego;

4) związki podmiotów, o których mowa wyżej;

oraz dotatkowo podmioty mieszczące się zakresie definicji „przedsiębiorstwa publicznego” w rozumieniu art. 2 pkt 3 dyrektywy 2019/1024/UE.

Podmioty zobowiązane w celu ponownego wykorzystania udostępniają informacje sektora publicznego:

- 1) w Biuletynie Informacji Publicznej (dotyczy wyłącznie informacji publicznej);
- 2) w Portalu Danych: danepubliczne.gov.pl;
- 3) w inny sposób (np. w innym systemie teleinformatycznym);
- 4) przekazują je również na wniosek (przy czym ten sposób nie ma znaczenia w kontekście zagadnienia będącego przedmiotem niniejszego opracowania).

Ustawa przewiduje podstawę prawną do dobrowolnego udostępniania informacji sektora publicznego za pośrednictwem prowadzonego przez ministra właściwego do spraw informatyzacji portalu dane.gov.pl. Co więcej, polska ustawa w tym zakresie wykracza poza ramy wyznaczone przez dyrektywę 2019/1024/UE, wprowadzając możliwość także dla podmiotów sektora prywatnego dobrowolnego udostępniania w portalu dane.gov.pl zasobów informacji będących w ich posiadaniu. Portal ten w założeniu zatem powinien więc być źródłem bogatego zasobu danych,

z których wszystkie zainteresowane osoby czy podmioty będą mogły wtórnie korzystać.

U.o.d.p.w.i.s.p kompleksowo realizuje zamysł jak najszerszego otwarcia publicznych zasobów. Jednym z elementów jego realizacji jest wprowadzenie nowych, istotnych rozwiązań wynikających z wymogów dyrektywy 2019/1024/UE. W tym celu do ustawy wprowadzono kategorie danych o wysokiej wartości i danych dynamicznych oraz objęto jej zakresem dane badawcze.

Dane o wysokiej wartości zdefiniowane zostały w art. 2 pkt 4 u.o.d.p.w.i.s.p jako „informacje sektora publicznego, których ponowne wykorzystywanie wiąże się z istotnymi korzyściami dla społeczeństwa, środowiska i gospodarki, w szczególności ze względu na ich przydatność do tworzenia produktów, usług i zastosowań opartych na wykorzystywaniu tych danych”. Podmioty zobowiązane mają obowiązek udostępniania takich danych do ponownego wykorzystywania co do zasady bezpłatnie, w formie nadającym się do odczytu maszynowego, za pośrednictwem interfejsu programistycznego aplikacji (API), oraz, w odpowiednich przypadkach, do zbiorczego pobrania.

Dane dynamiczne zostały zdefiniowane w art. 4 pkt 3 u.o.d.p.w.i.s.p jako „informacje sektora publicznego utrwalone w postaci elektronicznej podlegające częstym aktualizacjom lub aktualizacjom w czasie rzeczywistym, w tym ze względu na ich zmienność lub szybką dezaktualizację, w szczególności dane wygenerowane przez czujniki”. Podmioty zobowiązane są zobligowane do ich udostępniania do ponownego wykorzystywania natychmiast po ich zgromadzeniu, za pośrednictwem interfejsu programistycznego aplikacji (API), oraz, w odpowiednich przypadkach, do zbiorczego pobrania.

Ustawa objęła swym zakresem również dane badawcze, które zostały zdefiniowane w art. 2 pkt 2 u.o.d.p.w.i.s.p jako „informacje sektora publicznego utrwalone w postaci elektronicznej, inne niż publikacje naukowe, które zostały wytworzone lub zgromadzone w ramach działalności

naukowej i są wykorzystywane jako dowody w procesie badawczym lub służą do weryfikacji poprawności ustaleń i wyników badań”.

W ramach kompleksowego podejścia do otwierania danych w przepisie art. 10 ust. 1 u.o.d.p.w.i.s.p sformułowano zasadę, zgodnie z którą podmioty zobowiązane, o ile to możliwe, powinny udostępniać lub przekazywać informacje sektora publicznego w celu ponownego wykorzystywania, jako otwarte dane.

Samego pojęcia danych ustawa nie definiuje, jednak, w jaki sposób je rozumieć, wskazuje rządowy dokument wprowadzający Program Otwierania Danych. Zgodnie z jego brzmieniem pod pojęciem danych publicznych należy rozumieć „liczby i pojedyncze wydarzenia lub obiekty na możliwie najniższym poziomie agregacji, które nie zostały poddane przez administrację publiczną przetworzeniu do postaci raportów, wykresów, itp. oraz nie został im nadany odpowiedni kontekst lub interpretacja”³⁷.

U.o.d.p.w.i.s.p definiuje natomiast pojęcie otwartych danych, które zgodnie z jej art. 2 ust. 11 są informacjami sektora publicznego udostępnianymi lub przekazywanymi w postaci elektronicznej, bezwarunkowo lub z uwzględnieniem warunków i które to dane są: kompletne, aktualne, w wersji źródłowej, w otwartym i niezastrzeżonym formacie przeznaczonym do odczytu maszynowego oraz są przeznaczone do bezpłatnego ponownego wykorzystywania na tych samych zasadach dla każdego użytkownika, bez konieczności potwierdzania przez niego tożsamości.

Zgodnie z wytycznymi UE Polska prowadzi program otwierania danych publicznych. Jego założenia zostały określone w Programie Otwierania Danych Publicznych na lata 2021-2027. Otwarte dane w rozumieniu ustawowym powinny spełniać w filary otwartości zdefiniowane w tym Programie. Otwarte dane powinny być również zgodne ze Standardami Otwartości Danych. Zostały one przygotowane przez Ministerstwo

³⁷ Zob. uchwała Rady Ministrów nr 28 z dnia 18 lutego 2021 r. w sprawie Programu Otwierania Danych Publicznych na lata 2021-2027, M. P. z 2021 r. poz. 290, s. 6.

Cyfryzacji i obejmują wytyczne dotyczące: regulacji prawnych, zapewnienia bezpieczeństwa i ochrony prywatności danych, technicznych aspektów ich udostępniania oraz dostępu do baz danych przez API (interfejs programistyczny aplikacji). W 2020 r. opublikowana została nowa wersja dokumentów, zmienionych w trakcie wcześniejszych konsultacji³⁸.

W u.o.d.p.w.i.s.p wprowadzono ograniczenia dotyczące zakresu jej obowiązywania, jak również zasady, tryb oraz warunki udostępniania i ponownego wykorzystywania informacji sektora publicznego. Ograniczenia te, jako mające istotny wpływ na dopuszczalność dokonywania scrapowania danych publicznych, zostaną omówione w dalszej części opracowania.

5.4. Scrapowanie informacji i danych sektora publicznego podlegających ponownemu wykorzystaniu

Omówione wyżej regulacje opierają się na założeniach jak najszerzego otwarcia danych sektora publicznego i umożliwienia wykorzystywania ich przez wszystkie zainteresowane osoby i podmioty. Służyć to ma wspieraniu innowacyjności europejskich gospodarek. W tym zatem kontekście należy interpretować regulacje polskiej u.o.d.p.w.i.s.p. Zasady te znalazły też swój wyraz w Planie Otwierania Danych na lata 2021-2027 i w Standardach Otwartości Danych, które wśród filarów otwartości wymieniają „dostępność” danych, rozumiejąc przez to wprost możliwość ich pobierania, indeksowania i przeszukiwania zasobów. Jak najszerzej dostępności danych służą też regulacje nakładające na podmioty udostępniające niektóre rodzaje informacji do ponownego wykorzystywania stosowanie formatów nadających się do maszynowego odczytu czy udostępniania danych do zbiorczego pobrania. Działania takie stanowią wprost przygotowanie do tego, aby aplikacje komputerowe mogły łatwo zidentyfikować, rozpoznać i uzyskać określone dane, w tym poszczególne

³⁸ Standardy Otwartości Danych dostępne pod adresem: <https://dane.gov.pl/pl/knowledgebase/useful-materials/standardy-otwartosci-danych> [dostęp: 23.09.2021].

stwierdzenia faktów, i ich wewnętrzną strukturę³⁹. U.o.d.p.w.i.s.p nie wprowadza jednak wyraźnego wyjątku w zakresie prawa do scrapowania.

Prawo do ponownego wykorzystywania podlega ograniczeniom, które określone zostały w art. 6 u.o.d.p.w.i.s.p. Dla niniejszego opracowania szczególne znaczenie ma przepis art. 6 ust. 4 pkt 4 tej ustawy, zgodnie z którym prawo do ponownego wykorzystywania podlega ograniczeniu w zakresie informacji sektora publicznego, do których prawa autorskie i prawa pokrewne oraz prawa do baz danych przysługują podmiotom innym niż podmioty zobowiązane. Przywołany art. 6 wprowadza jednak i inne znaczące ograniczenia w zakresie możliwości ponownego wykorzystywania informacji sektora publicznego, np. w odniesieniu do informacji, których wytwarzanie przez podmioty zobowiązane nie należy do zakresu ich zadań publicznych określonych prawem czy w odniesieniu do części materiałów archiwalnych. Tym samym do dopuszczalności scrapowania takich informacji zastosowanie znajdą zasady szczegółowo omówione w poprzednich rozdziałach.

W odniesieniu natomiast do informacji sektora publicznego nie podlegających ograniczeniom, o których mowa w poprzednim akapicie, zastosowanie znajdzie zasada określona w art. 14 ust. u.o.d.p.w.i.s.p, zgodnie z którą informacje sektora publicznego udostępnia się lub przekazuje w celu ponownego wykorzystywania bezwarunkowo, z wyjątkiem przypadków określonych w ustawie.

Podmiot zobowiązany określa, na podstawie art. 14 ust. 2 u.o.d.p.w.i.s.p, warunki ponownego wykorzystywania informacji sektora publicznego mających cechy utworu lub przedmiotu praw pokrewnych lub stanowiących bazę danych w rozumieniu przepisów ustawy o ochronie baz danych, do których przysługują mu prawa. W art. 15 u.o.d.p.w.i.s.p określono z kolei katalog fakultatywnych warunków ponownego wykorzystywania informacji sektora publicznego, jakie podmiot zobowiązany może ustanowić,

³⁹ Zob. Pogram Otwierania Danych Publicznych..., s. 6.

udostępniając lub przekazując informacje sektora publicznego do ponownego wykorzystywania, przy czym podmiot zobowiązany może jedynie zdecydować o tym, czy zastosuje dodatkowe warunki, sama ich treść natomiast ustalona jest przez ustawodawcę⁴⁰. W odniesieniu do udostępniania szczególnego rodzaju danych, jakimi są dane badawcze, podstawę prawną dla określenia warunków ich wykorzystywania stanowi art. 22 u.o.d.p.w.i.s.p.

Nie ma podstaw prawnych do wprowadzania innych niż opisane powyżej ograniczeń w odniesieniu do informacji sektora publicznego udostępnianej w celu ponownego jej wykorzystywania.

Czynności, które składają się na scrapowanie danych w postaci eksploracji danych, ich pobierania czy agregowania, należy uznać za mieszczące się w ramach pojęcia ponownego wykorzystywania informacji sektora publicznego, które zostało zdefiniowane w art. 2 pkt 12 u.o.d.p.w.i.s.p. jako „wykorzystywanie przez użytkowników informacji sektora publicznego w jakimkolwiek celu”. Tym samym w określonym zakresie podmiot zobowiązany może wprowadzić pewne ograniczenia również na tym etapie korzystania przez użytkownika z informacji.

Dla pełnego obrazu sytuacji prawnej podmiotu zobowiązanego do udostępniania informacji sektora publicznego do ponownego wykorzystywania należy jeszcze przywołać przepisy omawianej już wcześniej dyrektywy 2019/790/UE w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym, która nakłada na państwa członkowskie obowiązek wprowadzenia ograniczeń uprawnień dysponentów praw autorskich i praw pokrewnych oraz producentów chronionych baz danych w zakresie eksploracji tekstów i danych (jeśli nie zastrzegą inaczej).

⁴⁰ W omawianym zakresie art. 15 ustawy jest co do zasady tożsamy z art. 14 ustawy z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego, a zatem odpowiednie zastosowanie znajdują uwagi zawarte w: B. Fischer, A. Piskorz-Ryń, M. Sakowska-Baryła, J. Wyporska-Frankiewicz, *Ustawa o ponownym wykorzystywaniu informacji sektora publicznego. Komentarz*, wyd. 2, Warszawa 2019, s. 307.

Z powyższego wynika wniosek, że podmiot zobowiązany w rozumieniu u.o.d.p.w.i.s.p powinien co do zasady udostępniać dane będące w jego posiadaniu w sposób otwarty i bezwarunkowy. Nie oznacza to jednak możliwości w pełni swobodnego scrapowania takich danych w każdym przypadku. Podmiot zobowiązany może bowiem określić pewne ograniczenia w tym zakresie, jeśli są one uzasadnione na przykład z uwagi na ochronę baz danych lub gdy udostępniane informacje albo bazy danych są objęte prawem autorskim, a on jest ich dysponentem. Należy uznać jednak, że ograniczenia w zakresie scrapowania danych, jeśli w ogóle zostaną przez podmiot zobowiązany określone, powinny mieć wyjątkowy i wąski charakter (np. dotyczyć tylko zapewnienia sprawnego działania strony internetowej). Wynika to zarówno z celu, jakiemu mają służyć przepisy o otwieraniu danych i umożliwieniu ich ponownego wykorzystywania, jak i z zasady jak najszerzego udostępniania danych (również na etapie przeszukiwania zasobów podmiotów sektora publicznego, pobierania czy indeksowania danych) oraz z przepisów, które wprost regulują kwestię udostępniania części danych do maszynowego odczytu czy zbiorczego pobierania. Jeżeli warunki w odniesieniu do scrapowania nie zostały przez podmiot zobowiązany określone, należy uznać, że jest ono prawnie dopuszczalne.

Zakończenie

Narzędziem, które służy do pozyskiwania danych z internetu, jest scrapowanie. Regulacje dotyczące tego zagadnienia są stosunkowo nowe, wywodzone z różnych aktów prawnych i niejednoznaczne. Sytuacja ta stopniowo ulega zmianie. Przepisy o eksploracji tekstów i danych, przyjęte w niewdrożonej jeszcze do polskiego systemu prawnego dyrektywie w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym, wspólnie z obowiązującymi

przepisami o ochronie baz danych stanowią ramy dla scrapowania danych z internetu. Dla omawianego zagadnienia mają również znaczenie regulacje dotyczące poszczególnych kategorii scrapowanych danych, takie jak przepisy prawnoautorskie czy przepisy o ochronie danych osobowych.

W odniesieniu do części podmiotów obowiązanych do udostępniania informacji publicznych, w szczególności takich jak organy państwowe i samorządowe, państwowe czy samorządowe osoby prawne lub jednostki organizacyjne czy podmioty reprezentujące Skarb Państwa, zasadą powinno być niewprowadzanie przez nie ograniczeń w scrapowaniu informacji publicznych, chyba że podmioty te nie dysponują pełnią praw do udostępnianej informacji bądź gdy scrapowanie powoduje ryzyko naruszenia normalnego korzystania z udostępnianych przez nie baz danych.

Podobnie oceniać również należy scrapowanie informacji sektora publicznego, o ile prawami do nich dysponują podmioty zobowiązane do ich udostępnienia w celu ponownego wykorzystywania. W tym przypadku jednak wprost określono zasadę, że przy braku określenia warunków ponownego wykorzystywania informacji sektora publicznego podlega ona wykorzystaniu bezwarunkowo. Jednostki sektora publicznego działające w interesie publicznym i dzięki funduszom pochodzącym od podatników powinny jak najszerszej udostępniać dane i informacje, które wytwarzają lub nabywają w ramach swojej publicznej działalności. Służą to nie tylko wykonywaniu funkcji kontrolnej przez obywateli, ale i pozytywnej stymulacji gospodarki, która dzięki tak dostępnym danym może wytwarzać nowe produkty i usługi. W związku z powyższym należy uznać, iż pomimo możliwości wprowadzenia ograniczeń w korzystaniu z danych sektora publicznego podmioty udostępniające informacje do ponownego wykorzystywania powinny zapewnić jak najszerszą możliwość ich scrapowania. Za uzasadnione można uznać ewentualne określenie warunków, które prowadzą do ograniczenia scrapowania baz danych w sposób zakłócający normalne z nich korzystanie.

Bibliografia

- Barta J., Markiewicz R., *Prawo autorskie, Komentarz*, Warszawa 2013.
- Barta J., Markiewicz R., *Ustawa o ochronie baz danych. Komentarz*, Warszawa 2002.
- Ciupa S., *Dozwolony użytek w ustawie o ochronie baz danych*, „Monitor Prawniczy” 2003, nr 12.
- Fischer B., Piskorz-Ryń A., Sakowska-Baryła M., Wyporska-Frankiewicz J., *Ustawa o ponownym wykorzystywaniu informacji sektora publicznego. Komentarz*, wyd. 2, Warszawa 2019.
- De Mauro A., Greco A.M., Grimaldi M., *A Formal definition of Big data based on its essential features*, “Library Review” 2016, Vol. 3.
- Dubisz S. (red.), *Uniwersalny słownik języka polskiego*, t. 3, Warszawa 2003.
- Europejski Portal Danych, <https://www.europeandataportal.eu/pl>.
- Gienas K., *Data mining jako problem prawa autorskiego*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego” 2017, z. 1.
- Gliściński K., *Komentarz do art. 50 ustawy o prawie autorskim i prawach pokrewnych*, [w:] A. Michalak (red.), *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, Warszawa 2019.
- Heiss A., *Big Data Challenges in Big Science, Computing and Software for Big Science*, “Computing and Software for Big Science” 2019, <https://link.springer.com/content/pdf/10.1007%2Fs41781-019-0030-7.pdf>.
- Komisja Europejska, *Shaping Europe’s digital future. Open Data*, <https://ec.europa.eu/digital-single-market/en/open-data>.
- Lubasz D., Namysłowska M. (red.), *Ustawa o ochronie baz danych. Komentarz*, Warszawa 2013, LEX.
- Opaliński B., *Dostęp do informacji publicznej w prawie międzynarodowym i prawie Unii Europejskiej*, [w:] P. Szustakiewicz (red.), *Dostęp do informacji publicznej*, Warszawa 2014.
- Selamat S., Prakoonwit S., Khan W., *A review of data mining in knowledge management: applications/findings for transportation of small and medium enterprises*, “SN Applied Sciences” 2020, <https://link.springer.com/content/pdf/10.1007%2Fs42452-020-2589-3.pdf>.

Standardy Otwartości Danych, <https://dane.gov.pl/pl/knowledgebase/usefu-materials/standardy-otwartosci-danych>.

Stötzel R., Wille S., *Der Urheberschutz sui generis für Datenbanken*, "Europäisches Wirtschafts- und Steuerrecht" 2004, H. 11.

Traple E., [w:] J. Barta, R. Markiewicz (red.), *Prawo autorskie i prawa pokrewne. Komentarz*, Kraków 2005.

Wojnarska-Krajewska E., *Crawlowanie – legalne czy nie*, <https://wpprawoautorskie.wordpress.com/2014/04/17/crawlowanie-crawler-roboty-txt/>.

Zamora A., *Making Room for Big Data: Web Scraping and an Affirmative Right to Access Publicly Available Information Online*, "The Journal of Business, Entrepreneurship & the Law" 2019, Nr 12.

Uzasadnienie do projektu ustawy o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego.

**Publikacje z dyscypliny nauki prawne – prawo konstytucyjne,
które ukazały się w e-Wydawnictwie WPAE UWr**

Justyna Węgrzyn, *Prawo konsumenta do informacji w Konstytucji RP i w prawie unijnym*, Wrocław 2013.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/40651>

Współczesne koncepcje ochrony wolności i praw podstawowych, red. Andrzej Bator, Mariusz Jabłoński, Marek Maciejewski, Krzysztof Wójtowicz, Wrocław 2013.

Dostęp online: <http://bibliotekacyfrowa.pl/publication/42456>

Małgorzata Masternak-Kubiak, *Odesłania do prawa międzynarodowego w Konstytucji RP*, Wrocław 2013.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/41352>

Realizacja i ochrona konstytucyjnych wolności i praw jednostki w polskim porządku prawnym, red. Mariusz Jabłoński, Wrocław 2014.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/51986>

Aktualne wyzwania ochrony wolności i praw jednostki. Prace uczniów i współpracowników dedykowane Profesorowi Bogusławowi Banaszakowi, red. Mariusz Jabłoński i Sylwia Jarosz-Żukowska, Wrocław 2014.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/56032>

Krzysztof Wójtowicz, *Constitutional Courts and European Union Law*, Wrocław 2014.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/54527>

Zasada pierwszeństwa prawa Unii Europejskiej w praktyce działania organów władzy publicznej RP, red. Mariusz Jabłoński, Sylwia Jarosz-Żukowska, Wrocław 2015.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/64552>

Artur Ławniczak, *Geneza Konstytucji*, Wrocław 2015.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/65468>

Teoretyczne i praktyczne aspekty realizacji prawa petycji, red. Ryszard Balicki i Mariusz Jabłoński, Wrocław 2015.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/66901>

Ewolucja państwowości w Brazylii, Polsce i Eurazji. Evolução do estado no Brasil, Polônia e Eurásia, red. Marcos A. Maliska, Krystian Complak, Wrocław 2015.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/64761>

Międzynarodowa ochrona praw człowieka – współczesne problemy na świecie, red. Mariusz Jabłoński, Tomasz Jurczyk, Patryk Gutierrez, Wrocław 2015.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/67621>

Identyfikacja granic wolności i praw jednostki. Prawnoporównawcza analiza tożsamego przypadku pod kątem praktyki stosowania prawa amerykańskiego i polskiego, red. Mariusz Jabłoński, Wrocław 2016.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/79781>

Instytucje demokracji bezpośredniej w praktyce, red. Olga Hałub, Mariusz Jabłoński, Mateusz Radajewski, Wrocław 2016.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/80567>

Aktualne problemy ochrony wolności i praw mniejszości w Polsce i na świecie, red. Joanna Beata Banach-Gutierrez, Mariusz Jabłoński, Wrocław 2017.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/84127>

Współczesne polityczno-prawne systemy państw Europy, Azji i Ameryki Łacińskiej, red. Krystian Complak, Patryk Gutierrez, Jolanta Rosiak, Wrocław 2017.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/84639>

Reforma ochrony danych osobowych a jawność Dostępu do informacji sądowej – aspekty proceduralne, red. Mariusz Jabłoński, Kinga Flaga-Gieruszyńska, Krzysztof Wygoda, Wrocław 2017.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/92803>

Magdalena Bainczyk, *Polski i niemiecki Trybunał Konstytucyjny wobec członkostwa państwa w Unii Europejskiej*, Wrocław 2017.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/84085>

Dookoła Wojtek... Księga pamiątkowa poświęcona Doktorowi Arturovi Wojciechowi Preisnerowi, red. Ryszard Balicki, Mariusz Jabłoński, Wrocław 2018.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/95368>

Ryszard Balicki, *Funkcja europejska Sejmu RP*, Wrocław 2019.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/101626>

Specyfika organizacji i funkcjonowania organów władzy publicznej. Analiza porządków prawnych państw współczesnych, red. Mariusz Jabłoński, Magdalena Abu Gholeh, Wrocław 2019.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/101490>

Anna Śledzińska-Simon, *Analiza proporcjonalności ograniczeń konstytucyjnych praw i wolności. Teoria i praktyka*, Wrocław 2019.

Dostęp online: <http://www.bibliotekacyfrowa.pl/publication/102713>

Olga Hałub-Kowalczyk, Mariusz Jabłoński, Mateusz Radajewski, *Identyfikacja treści prawa do sądu – wybrane zagadnienia*, Wrocław 2019.

Dostęp online: <https://www.bibliotekacyfrowa.pl/publication/104603>

Osobowość prawna jako przesłanka wykonywania konstytucyjnych wolności i praw, red. Michał Bernaczyk, Mariusz Jabłoński, Wrocław 2019.

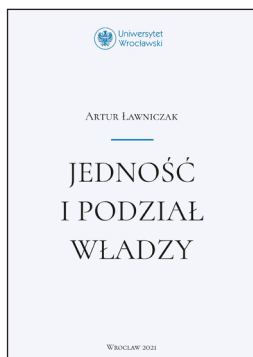
Dostęp online: <https://www.bibliotekacyfrowa.pl/publication/108539>

Magdalena Abu Gholeh, Dominka Kuźnicka-Błaszowska, *Ochrona danych osobowych w wybranych państwach Azji*, Wrocław 2019.

Dostęp online: <https://www.bibliotekacyfrowa.pl/publication/112255>

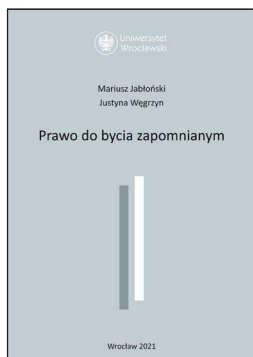
Między konstytucjonalizmem polskim a latynoamerykańskim. Wybór prac z okresu 47-lecia twórczości naukowej Profesora Krystiana Complaka, red. Marta Kłopocka-Jasińska, Wrocław 2020.

Dostęp online: <https://www.bibliotekacyfrowa.pl/publication/115875>



Artur Ławniczak, *Jedność i podział władzy*, Wrocław 2021.

Dostęp online: <https://bibliotekacyfrowa.pl/publication/143474>



Mariusz Jabłoński, Justyna Węgrzyn, *Prawo do bycia zapomnianym*, Wrocław 2021.

Dostęp online: <https://bibliotekacyfrowa.pl/publication/142660>

Niniejsza publikacja wyjaśnia znaczenie kluczowych pojęć związanych z otwartością danych, które powinny być uwzględniane przy wykładni i rewizji ustawowych norm (materialnych i proceduralnych) przyznających uprawnienie do ponownego wykorzystywania informacji i danych. Okazją do tej analizy stało się uchwalenie ustawy z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego oraz redukowaniu znaczenia ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. Uprawnienia informacyjne ewoluują pod hasłem innowacyjności gospodarki i rozwoju cyfrowych usług publicznych, niekoniecznie zaś przejrzystości władz publicznych czy wzmocnienia politycznych praw jednostki. Jednakże nowe cele stawiane dostępowi do informacji ukrywają stare dylematy: jak zapewnić jakość i interoperacyjność danych w administracji publicznej? Czy dane publiczne są ekskluzywną własnością publiczną i gdzie leżą prawne granice ich przetwarzania przez podmioty prywatne? Gdzie jest granica pomiędzy informacją a danymi jako przedmiotem roszczenia informacyjnego jednostki? Jakie jest konstytucyjne i ponadnarodowe uzasadnienie dostępu do otwartych danych? Niniejsza książka niewątpliwie przybliży nas do odpowiedzi na te pytania.

ISBN 978-83-66601-81-9 (druk)

ISBN 978-83-66601-82-6 (online)