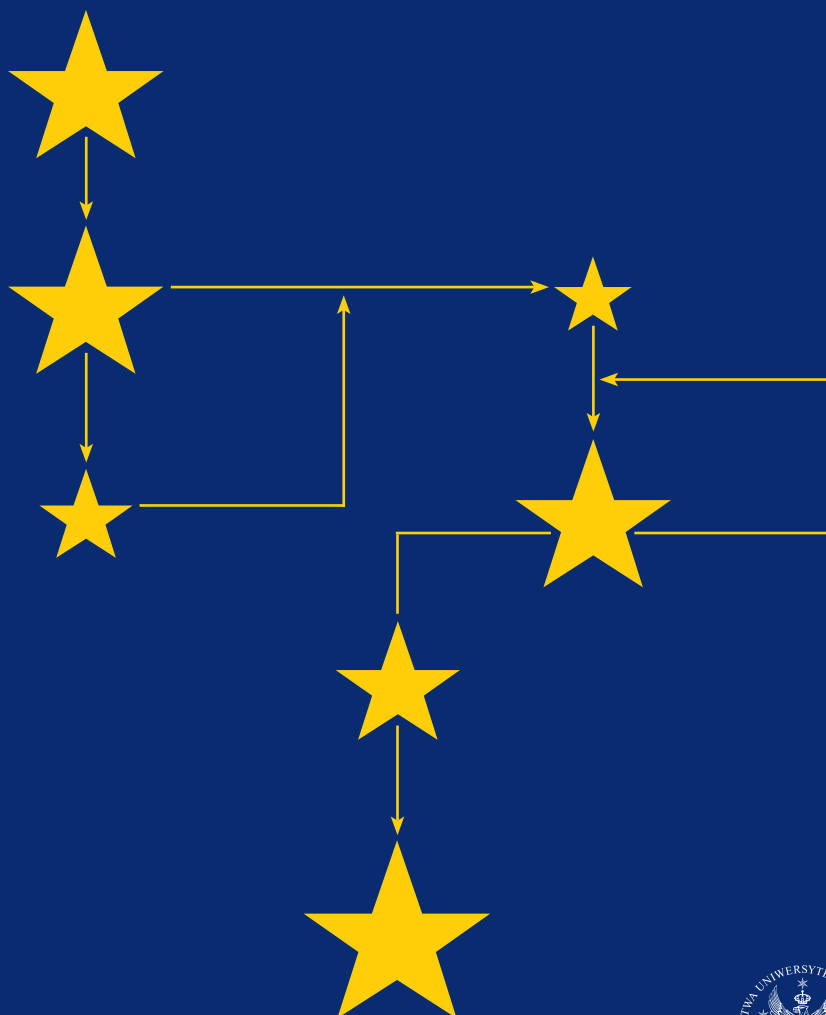


Joanna Mazur

Algorytm

jako informacja publiczna
w prawie europejskim



Algorytm

jako informacja publiczna
w prawie europejskim

Joanna Mazur

Algorytm

jako informacja publiczna
w prawie europejskim



Recenzenci
Agnieszka Grzelak
Monika Namysłowska

Redaktor prowadzący
Małgorzata M. Przybyszewska

Redakcja
Jadwiga Witecka

Korekta
Małgorzata Nowak

Projekt okładki i stron tytułowych
Anna Gogolewska

Skład i łamanie
Pracownia DTP Aneta Osipiak-Wypiór

Publikacja dofinansowana przez Uniwersytet Warszawski

© Copyright by Wydawnictwa Uniwersytetu Warszawskiego, Warszawa 2021

Joanna Mazur ORCID 0000-0002-0417-5743 Uniwersytet Warszawski

ISBN 978-83-235-5135-5 (pdf online)

Wydawnictwa Uniwersytetu Warszawskiego
00-838 Warszawa, ul. Prosta 69
e-mail: wuw@uw.edu.pl
księgarnia internetowa: www.wuw.pl

Wydanie 1, Warszawa 2021

Druk i oprawa
POZKAL

Spis treści

Wykaz skrótów i skrótowców	9
Wstęp	15
1. Zakres badań, hipoteza i pytania badawcze	21
2. Metody i materiał badawczy	25
3. Streszczenie rozdziałów	26
4. Terminologia	28
4.1. Zautomatyzowane podejmowanie decyzji i profilowanie	29
4.2. Algorytm, kod i program komputerowy	34
4.3. Sztuczna inteligencja	36
Rozdział pierwszy	
Ramy teoretyczne prawnego wymiaru zautomatyzowanego	
podejmowania decyzji	41
1.1. Teoretyczne konceptualizacje relacji między kodem komputerowym a prawem	41
1.1.1. Kod jako prawo	41
1.1.2. Granice algorytmizacji prawa a zautomatyzowane podejmowanie decyzji	45
1.1.3. Kod zastępujący przepisy i akty prawne	48
1.2. Wyzwania tworzone przez zautomatyzowane podejmowanie decyzji w świetle prawa europejskiego	52
1.2.1. Stronniczość zautomatyzowanego podejmowania decyzji	53
1.2.2. Bariery dla przejrzystości zautomatyzowanego podejmowania decyzji	56
1.2.3. Nieprzejrzyste zautomatyzowane podejmowanie decyzji w świetle zakazu dyskryminacji na gruncie prawa UE	61
1.2.4. Nieprzejrzyste zautomatyzowane podejmowanie decyzji w świetle zakazu dyskryminacji na gruncie prawa Rady Europy	73
1.3. Kolektywny wymiar dyskryminacji w ramach zautomatyzowanego podejmowania decyzji	75
1.4. Podsumowanie	80
Rozdział drugi	
Zautomatyzowane podejmowanie decyzji z perspektywy ochrony danych osobowych w prawie europejskim	83
2.1. Zautomatyzowane podejmowanie decyzji w prawie Unii Europejskiej: od dyrektywy 95/46/WE do RODO	83
2.1.1. Zakaz zautomatyzowanego podejmowania decyzji w art. 22 RODO	88
2.1.2. Wyjątki od zakazu zautomatyzowanego podejmowania decyzji w art. 22 RODO	94
2.1.3. Obowiązki informacyjne i prawo dostępu: kontrowersje wokół „prawa do wyjaśnienia”	99

2.1.4. Zakaz podejmowania zautomatyzowanych decyzji i prawo do wyjaśnienia: podsumowanie ustaleń	106
2.1.5. Prawo do usunięcia danych i prawo do przenoszenia danych a problem zautomatyzowanego podejmowania decyzji	111
2.1.6. Systemowe ujęcie problematyki zautomatyzowanego podejmowania decyzji w RODO: ocena skutków dla ochrony danych i wiążące reguły korporacyjne	115
2.1.7. Kolektywny wymiar zautomatyzowanego podejmowania decyzji a RODO	121
2.2. Zautomatyzowane podejmowanie decyzji w prawie Rady Europy.....	123
2.3. Podsumowanie	128

Rozdział trzeci

Algorytmy stosowane w zautomatyzowanym podejmowaniu decyzji

a dostęp do informacji w prawie Rady Europy.....	131
3.1. Treść artykułu 10 EKPCz w świetle działalności ONZ w zakresie wolności informacji	131
3.2. Prawo dostępu do informacji w działalności Rady Europy	137
3.3. Prawo dostępu do informacji w orzecznictwie ETPCz.....	142
3.3.1. Wypracowywanie spójnego podejścia do prawa dostępu do informacji w orzecznictwie ETPCz.....	147
3.3.2. Systematyzacja podejścia do prawa dostępu do informacji w orzecznictwie ETPCz.....	152
3.4. Warunki powoływania się na prawo dostępu do informacji.....	156
3.5. Warunki powoływania się przez państwa na ograniczenia prawa dostępu do informacji	160
3.6. Możliwość stosowania prawa dostępu do informacji w stosunku do systemów zautomatyzowanego podejmowania decyzji	165
3.6.1. Artykuł 10 jako podstawa żądania dostępu do algorytmów służących do zautomatyzowanego podejmowania decyzji	166
3.6.2. Prawo dostępu do informacji jako narzędzie do korzystania z innych praw	171
3.6.3. Prawo dostępu do informacji w świetle zakazu dyskryminacji.....	176
3.7. Podsumowanie.....	178

Rozdział czwarty

Dostęp do dokumentów i informacji w odniesieniu do algorytmów

stosowanych do zautomatyzowanego podejmowania decyzji w prawie UE	181
4.1. Od prawa dostępu do informacji na temat jednostki do prawa dostępu do dokumentów unijnych	181
4.1.1. Ramy prawne dotyczące prawa dostępu do dokumentów unijnych	184
4.1.2. Prawo dostępu do dokumentów unijnych jako narzędzie służące demokratyzacji	188
4.1.3. W poszukiwaniu charakteru prawa dostępu do dokumentów w prawie UE.....	192
4.1.4. Zbieżność aksjologiczna między prawem dostępu do dokumentów a zasadami prawa ochrony danych osobowych	194
4.2. Treść prawa dostępu do dokumentów unijnych w prawie UE	195
4.2.1. Konceptualizacja relacji prawa dostępu do dokumentów unijnych i prawa dostępu do informacji w UE	195
4.2.2. Relacja między prawem dostępu do dokumentów w prawie UE a prawem dostępu do informacji w orzecznictwie ETPCz – nieobecny art. 11 KPP	200
4.2.3. Algorytm jako dokument w prawie UE w świetle koncepcji <i>kodu jako prawa</i>	207
4.3. Wyjątki od prawa dostępu do dokumentów unijnych w prawie UE	214
4.3.1. Wyjątki obligatoryjne	217
4.3.2. Wyjątki fakultatywne.....	221
4.3.3. Wyjątki od prawa dostępu do dokumentów w odniesieniu do problematyki zautomatyzowanego podejmowania decyzji	222

4.3.4. Porównanie konstrukcji wyjątków od prawa dostępu do dokumentów unijnych w prawie UE z konstrukcją wyjątków od prawa do informacji w orzecznictwie ETPCz.....	226
4.4. Dostęp do dokumentów i informacji w prawie UE w świetle zautomatyzowanego podejmowania decyzji w państwach członkowskich	228
4.4.1. <i>Dyrektywa 2019/1024</i> w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego a zautomatyzowane podejmowanie decyzji	229
4.4.2. Prawa podstawowe a dostęp do informacji o zautomatyzowanym podejmowaniu decyzji	231
4.4.3. Dostęp do dokumentów jako element wartości unijnych	233
4.5. Podsumowanie	235
Wnioski końcowe	239
1. Prawo ochrony danych osobowych jako niewystarczający instrument do ochrony przed brakiem przejrzystości zautomatyzowanego podejmowania decyzji	239
2. Algorytmy stosowane w zautomatyzowanym podejmowaniu decyzji jako informacja publiczna w świetle orzecznictwa ETPCz i TSUE	241
3. Rola przejrzystego zautomatyzowanego podejmowania decyzji w gwarantowaniu zgodności działań państw członkowskich z wartościami UE	243
4. Neutralność technologiczna i dynamiczna wykładnia vs postulatory <i>de lege ferenda</i>	244
5. Komplementarność rozwiązań regulacyjnych dotyczących dostępu do informacji na temat zautomatyzowanego podejmowania decyzji.....	247
Bibliografia	249
Literatura	249
Akty prawne	261
Orzecznictwo TSUE	263
Opinie rzeczników generalnych.....	266
Orzecznictwo ETPCz	266
Orzecznictwo i decyzje innych sądów.....	267
Dokumenty, raporty i publikacje organizacji międzynarodowych oraz innych instytucji	267
Źródła internetowe	270
Summary	271
Podziękowania	273

Wykaz skrótów i skrótowców

AI – *Artificial Intelligence*

Akt w sprawie SI – Wniosek: Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące Sztucznej Inteligencji (Akt w sprawie Sztucznej Inteligencji) i zmieniające niektóre akty ustawodawcze Unii Europejskiej

BCR – wiążące reguły korporacyjne (*binding corporate rules*)

COMPAS – *Correctional Offender Management Profiling for Alternative Sanctions*

decyzja 2004/258/WE – Decyzja Europejskiego Banku Centralnego z dnia 4 marca 2004 r. w sprawie publicznego dostępu do dokumentów Europejskiego Banku Centralnego

deklaracja nr 17 – Deklaracja nr 17 dotycząca prawa dostępu do informacji

DESI – *Digital Economy and Society Index*

DPIA – ocena skutków dla ochrony danych (*data protection impact assessment*)

DRM – *Digital Rights Management*

dyrektywa 95/45/WE – Dyrektywa 95/45/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych

dyrektywa 96/9/WE – Dyrektywa 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r. w sprawie ochrony prawnej baz danych

dyrektywa 2006/54/WE – Dyrektywa 2006/54/WE Parlamentu Europejskiego i Rady z dnia 5 lipca 2006 r. w sprawie wprowadzenia w życie zasady równości szans oraz równego traktowania kobiet i mężczyzn w dziedzinie zatrudnienia i pracy

dyrektywa 2009/24/WE – Dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE z dnia 23 kwietnia 2009 r. w sprawie ochrony prawnej programów komputerowych

dyrektywa 2016/680 – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW

dyrektywa 2016/943 – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem

- dyrektywa 2019/1024 – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego
- dyrektywa Rady 2000/43/WE – Dyrektywa Rady 2000/43/WE z dnia 29 czerwca 2000 r. wprowadzająca w życie zasadę równego traktowania osób bez względu na pochodzenie rasowe lub etniczne
- dyrektywa Rady 2000/78/WE – Dyrektywa Rady 2000/78/WE z dnia 27 listopada 2000 r. ustanawiająca ogólne warunki ramowe równego traktowania w zakresie zatrudnienia i pracy
- dyrektywa Rady 2004/113/WE – Dyrektywa Rady 2004/113/WE z dnia 13 grudnia 2004 r. wprowadzająca w życie zasadę równego traktowania mężczyzn i kobiet w zakresie dostępu do towarów i usług oraz dostarczania towarów i usług
- EBC – Europejski Bank Centralny
- EKPCz – Konwencja o ochronie praw człowieka i podstawowych wolności
- EOG – Europejski Obszar Gospodarczy
- EROD – Europejska Rada Ochrony Danych
- ETPCz – Europejski Trybunał Praw Człowieka
- Grupa Robocza Art. 29 – Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych
- HRIA – ocena skutków z punktu widzenia ochrony praw człowieka (*human rights impact assessment*)
- KDOD – Konwencja Rady Europy o dostępie do oficjalnych dokumentów
- Kodeks – Kodeks postępowania dotyczącego publicznego dostępu do dokumentów Rady i Komisji
- Konwencja 108 – Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych
- Konwencja 108+ – Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, tekst zmieniony protokołem CETS Nr 223
- KPP – Karta praw podstawowych Unii Europejskiej
- KRS – Krajowa Rada Sądownictwa
- MPPOiP – Międzynarodowy pakt praw obywatelskich i politycznych
- OBWE – Organizacja Bezpieczeństwa i Współpracy w Europie
- OECD – Organizacja Współpracy Gospodarczej i Rozwoju
- ONZ – Organizacja Narodów Zjednoczonych
- OPA – Organizacja Państw Amerykańskich
- PDPC – Powszechna deklaracja praw człowieka i obywatela
- RODO – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
- rozporządzenie 1049/2001 – Rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji
- rozporządzenie 2018/1725 – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE

rozporządzenie 2018/302 – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/302 z dnia 28 lutego 2018 r. w sprawie nieuzasadnionego blokowania geograficznego oraz innych form dyskryminacji klientów ze względu na przynależność państwową, miejsce zamieszkania lub miejsce prowadzenia działalności na rynku wewnętrznym oraz w sprawie zmiany rozporządzeń (WE) nr 2006/2004 oraz (UE) 2017/2394 i dyrektywy 2009/22/WE

SI – sztuczna inteligencja

SLPS – system losowego przydzielania spraw

STEM – *Science, Technology, Engineering, Mathematics*

TFUE – Traktat o funkcjonowaniu Unii Europejskiej

TSUE – Trybunał Sprawiedliwości Unii Europejskiej

TUE – Traktat o Unii Europejskiej

UE – Unia Europejska

UODO – Urząd Ochrony Danych Osobowych

„W słynnej powieści 1984 George Orwell pomylił się w jednej kwestii. Wielki Brat nie obserwuje ciebie, on obserwuje nas. Większość ludzi staje się przedmiotem cyfrowego dochodzenia jako członkowie grup społecznych, nie jako jednostki. Osoby o niebiałym kolorze skóry, migranci, mniejszościowe grupy religijne, mniejszości seksualne, biedni oraz inne opresjonowane i wyzyskiwane społeczności ponoszą dużo większy ciężar monitorowania i śledzenia niż grupy uprzywilejowane”.

Virginia Eubanks, *Automating Inequality*¹

¹ V. Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, St Martin's Press, Nowy Jork 2018 [edycja epub]. Ponadto warto podkreślić, że o zagrożeniach związanych z wykorzystywaniem analizy danych w stosunku do grup wrażliwych pisano już ok. 20 lat temu, zob. np. *Surveillance as Social Sorting Privacy, Risk, and Digital Discrimination*, red. D. Lyon, Routledge, Londyn–Nowy Jork 2003. Wszystkie tłumaczenia, o ile nie zaznaczono inaczej, wykonane zostały przeze mnie. Kluczowe frazy czy wyrazy zdecydowałam się przytaczać w treści pracy w nawiasach.

Wstęp

Chociaż rozwiązania wykorzystujące algorytmy w ramach zautomatyzowanego podejmowania decyzji obecne są w sferze zarówno usług publicznych, jak i tych świadczonych przez sektor prywatny od dekad², ich regulacja nadal powoduje wiele wątpliwości. Rozwiązania legislacyjne dotyczące zautomatyzowanego podejmowania decyzji są relatywnie nowe w prawie Unii Europejskiej (UE) i Rady Europy, a ich rzeczywisty wpływ na stosowanie takich metod podejmowania decyzji pozostaje dyskusyjny. Tymczasem używanie zautomatyzowanego podejmowania decyzji staje się coraz bardziej powszechne zarówno w sektorze prywatnym, jak i publicznym. W sektorze prywatnym przykładem zastosowania zautomatyzowanego podejmowania decyzji jest ocena zdolności kredytowej³ dokonywana z wykorzystaniem zautomatyzowanej analizy danych czy profilowany przekaz marketingowy, którego treść jest personalizowana w zależności od tego, do jakiej grupy została przyporządkowana jednostka, do której dana reklama ma być skierowana⁴. Z kolei obszary wykorzystywania systemów zautomatyzowanego

² Na przykład już w latach 70. XX w. w Norwegii system informatyczny był używany do decydowania, czy danej jednostce przysługuje prawo do wsparcia w postaci dodatku mieszkaniowego. System wykorzystywał wprowadzony przez daną osobę numer identyfikacyjny do połączenia z innymi bazami danych i na podstawie dostępnych w nich informacji wydawał decyzje, czy należy przyznać danej osobie zasiłek, zob. J. Bing, *Code, Access and Control*, [w:] *Human Rights in the Digital Age*, red. A. Murray, M. Klang, Routledge-Cavendish, Londyn–Sydney–Portland 2005, s. 204.

³ Omówienie problemu, zob. K. Johnson, F. Pasquale, J. Chapman, *Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation*, „Fordham Law Review” 2019, t. 88, nr 2, s. 499–530.

⁴ Badanie empiryczne na ten temat, zob. A. Datta, M.C. Tschantz, A. Datta, *Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination*, „Proceedings on Privacy Enhancing Technologies” 2015, nr 1, s. 92–112.

podejmowania decyzji w sektorze publicznym obejmują np. działania mające na celu prewencję przestępczości, czyli sytuacje, w których analiza danych stanowi podstawę prowadzenia działań przez policję w określonych dzielnicach lub wobec danych jednostek⁵, wydawanie decyzji w zakresie przysługującej jednostkom pomocy społecznej⁶, zarządzanie mobilnością nauczycieli, czyli przyporządkowywanie przez algorytm przyszłego miejsca pracy do danej osoby⁷, a także przydzielanie spraw sędziom⁸ czy zapewnianie dzieciom miejsc w żłobkach⁹ przy użyciu decyzji wydawanych za pośrednictwem analizy dokonanej przez system informatyczny.

Rozdźwięk między rosnącym znaczeniem społecznym zautomatyzowanego podejmowania decyzji i jego coraz powszechniejszym stosowaniem a brakiem jasności w zakresie dotyczących go rozwiązań regulacyjnych stanowił główne źródło motywacji do przeprowadzania badań w tym zakresie. W książce stawiam hipotezę, że możliwe jest postrzeganie algorytmów używanych w ramach systemów zautomatyzowanego podejmowania decyzji jako informacji podlegającej prawu dostępu do informacji lub do dokumentów urzędowych w świetle prawa europejskiego¹⁰. Dlatego przedmiotem zainteresowania mojej analizy są algorytmy stosowane w systemach zautomatyzowanego podejmowania decyzji wykorzystywanego w sektorze publicznym.

Przez pojęcie systemów zautomatyzowanego podejmowania decyzji rozumie się programy komputerowe używane do wspierania lub zastępowania procesów podejmowania decyzji wykonywanych przez człowieka rozwiązaniami zautomatyzowanymi, niezależnie od tego, jak duży jest udział rozwiązań cyfrowych w tym procesie¹¹. Samo zautomatyzowane podejmowanie

⁵ AlgorithmWatch, Bertelsmann Stiftung, Open Society Foundations, *Automating Society. Taking Stock of Automated Decision-Making in the EU*, 2019, s. 44, 52, 90–91, 100. https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/001-148_AW_EU-ADMreport_2801_2.pdf, dostęp: 1.04.2021.

⁶ *Ibidem*, s. 101, 130–131.

⁷ *Ibidem*, s. 88.

⁸ Zob. Fundacja ePaństwo, *alGOVrithms. STATE of PLAY. Report on Algorithms Usage in Government-Citizens Relations in Czechia, Georgia, Hungary, Poland, Serbia and Slovakia*, 2019, s. 15–32. <https://epf.org.pl/en/wp-content/uploads/sites/3/2019/05/alGOVrithms-State-of-Play-Report.pdf>, dostęp: 1.04.2021.

⁹ Zob. Centrum Cyfrowe, Klub Jagielloński, *AlgoPolska. Zautomatyzowane podejmowanie decyzji w służbie społeczeństwu*, 2019, s. 25. <https://centrumcyfrowe.pl/wp-content/uploads/sites/16/2019/12/AlgoPolska-raport.pdf>, dostęp: 1.04.2021.

¹⁰ Na temat różnicy między pojęciami informacji i dokumentów urzędowych – zob. rozdział trzeci i czwarty.

¹¹ Definicja jest zbliżona do tych proponowanych w: AlgorithmWatch, Bertelsmann Stiftung and Open Society Foundations, *op. cit.*, s. 9 i Algo:aware, *State-of-the-Art Report. Algorithmic decision-making*, 2018, s. II. <https://platformobservatory.eu/app/uploads/2019/06/AlgoAware-State-of-the-Art-Report.pdf>, dostęp: 1.04.2021.

decyzji to proces, w którym jest stosowany system zautomatyzowanego podejmowania decyzji rozumiany jako rozwiązanie technologiczne, u którego podstaw stoi algorytm. Bez algorytmu nie jest możliwe wprowadzenie zautomatyzowanego podejmowania decyzji. Dlatego za każdym razem, kiedy w książce posługuję się pojęciem zautomatyzowanego podejmowania decyzji, w jego ramach mieści się stosowany w nim algorytm. Przyjmuję przy tym perspektywę neutralną technologicznie, czyli niezależną od tego, jaka konkretna metoda czy technologia jest stosowana w ramach danego systemu zautomatyzowanego podejmowania decyzji.

Aby odnieść tę definicję do konkretnych przykładów, można się posłużyć algorytmem, który był używany do profilowania osób bezrobotnych w Polsce. Na podstawie sumy punktów, przyznanych za odpowiedzi na pytania sformułowane w kwestionariuszu, osoba bezrobotna była kwalifikowana do jednego z trzech profili. Teoretycznie urzędnik miał możliwość dokonania zmiany w stosunku do profilu zaproponowanego przez system, jednak sytuacja taka występowała w mniej niż 1% przypadków profilowania¹². Chociaż rozwiązanie technologiczne nie zastępowało człowieka całkowicie, w praktyce jego wpływ na podejmowane decyzje był ogromny. Ponadto przykład ten pokazuje, że stosowane rozwiązania mogą nie być zbyt wysublimowane technologicznie – algorytm nie „uczył się” na analizowanych danych, nie doskonalił metod dopasowywania pomocy do konkretnych jednostek. Odmianą sytuację ilustruje sprawa programu SyRI, który był używany w Holandii w celu identyfikacji oszustw związanych z korzystaniem z pomocy socjalnej. System mógł wykorzystywać technologie uczenia maszynowego i na podstawie analizy danych pochodzących z wielu różnych baz przewidywać ryzyko zachowań niepożądanych z punktu widzenia państwa¹³. W świetle przyjętej przeze mnie definicji oba te przykłady są objęte zakresem znaczenia terminu „system zautomatyzowanego podejmowania decyzji”.

Taki sposób zdefiniowania zautomatyzowanego podejmowania decyzji pozwala ponadto zauważyć, że na implementację rozwiązań służących

¹² Zob. Fundacja Panoptykon (J. Niklas, K. Sztandar-Sztanderska, K. Szymielewicz), *Profiling the Unemployed in Poland: Social and Political Implications of Algorithmic Decision Making*, Warszawa 2015, s. 17. https://panoptykon.org/sites/default/files/leadimage-biblioteka/panoptykon_profiling_report_final.pdf, dostęp: 1.04.2021; M. Kuziemski, G. Misuraca, *AI Governance in the Public Sector: Three Tales from the Frontiers of Automated Decision-Making in Democratic Settings*, „Telecommunications Policy” 2020, t. 44, nr 6, artykuł nr 101976.

¹³ System omówiony np. w: Agencja Praw Podstawowych Unii Europejskiej, *Artificial Intelligence, Big Data and Fundamental Rights Country Research Netherlands 2020 Report provided to FRA under contract D-SE-19-T021*, 2020, s. 28–31. https://fra.europa.eu/sites/default/files/fra_uploads/fra-ai-project-netherlands-country-research_en.pdf, dostęp: 1.04.2021.

takiemu podejmowaniu decyzji można spojrzeć z jednej strony z perspektywy skoncentrowanej na technologii, z drugiej zaś strony – z perspektywy kładącej nacisk na zmiany zachodzące w samych procesach podejmowania decyzji i relacji między człowiekiem a maszyną¹⁴. Szczególnie rozwój uczących się algorytmów stanowi pokusę do zwiększenia efektywności podejmowanych na masową skalę decyzji, np. przez administrację publiczną. Możliwość zastąpienia żmudnych i pracochłonnych analiz dokumentów dokonywanych przez urzędników zunifikowanym kwestionariuszem, którego analizę przeprowadza maszyna i sugeruje decyzję, może istotnie przyspieszyć wiele procesów. W sytuacji, w której maszyna ta jest na dodatek zdolna – na podstawie analizy zbiorów danych dotyczących kolejnych przeprowadzanych przez nią spraw – coraz lepiej rozpoznawać, jakiego rodzaju rozwiązanie wydaje się najkorzystniejsze, zautomatyzowane podejmowanie decyzji może być postrzegane jako ergonomiczna utopia.

Wystarczy jedynie nieco przesunąć akcenty w takiej narracji, skupionej na efektywności i szybkości zautomatyzowanego podejmowania decyzji, aby okazało się, że równie blisko jej do dystopii. Podstawowym problemem związanym z zautomatyzowanym podejmowaniem decyzji są wątpliwości co do tego, na ile jest ono bezstronne. Badanie nad stosowanym w Stanach Zjednoczonych programem COMPAS, który jest używany do oceny prawdopodobieństwa, z jakim dana jednostka popełni ponownie przestępstwo, wykazało, że stosowanie programu prowadzi do wyników powielających niekorzystną sytuację osób o innym niż biały kolorze skóry, a także sugeruje surowsze traktowanie kobiet niż mężczyzn¹⁵. Podobnie konkluzje badania nad wynikami stosowania systemu PredPol, służącego do wspierania procesów decyzyjnych dotyczących patrolowania danych dzielnic, wskazują na nieproporcjonalną koncentrację na dzielnicach zamieszkałych głównie przez osoby czarnoskóre¹⁶. Chociaż istnieją badania wykazujące, że stosowanie algorytmów w miejsce ludzi może mieć pozytywne skutki w odniesieniu do traktowania osób narażonych na dyskryminację¹⁷, problem możliwej dyskry-

¹⁴ Zob. konkluzje analizy J. Zerilli, A. Knott, J. Maclaurin, C. Gavaghan, *Algorithmic Decision-Making and the Control Problem*, „Minds and Machines” 2019, nr 29, s. 575.

¹⁵ J. Angwin, J. Larsona, S. Mattu, L. Kirchner, *Machine Bias. There's Software Used across the Country to Predict Future Criminals. And It's Biased against Blacks*, „ProPublica” 2016. <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>, dostęp: 1.04.2021.

¹⁶ K. Lum, W. Isaac, *To Predict and Serve?*, „Significance” 2016, t. 13, nr 5, s. 14–19.

¹⁷ Prowadzone w tym kontekście badania dotyczące dostępu do pożyczek udzielanych przy wykorzystaniu zautomatyzowanego podejmowania decyzji, zob. R. Bartlett, A. Morse, R. Stanton, N. Wallace, *Consumer-Lending Discrimination in the FinTech Era*, „NBER Working Paper” 2019, nr 25943, a także analiza B. Lepri, N. Oliver, E. Letouzé, A. Pentland, P. Vinck, *Fair, Transparent, and Accountable Algorithmic Decision-making*

minacji wynikającej ze stosowania systemów zautomatyzowanego podejmowania decyzji pozostaje aktualny.

Ponadto zautomatyzowane podejmowanie decyzji może oznaczać zastępowanie przez rozwiązania technologiczne procesów rządzących się do tej pory normami zawartymi w aktach prawnych lub mogących podlegać kontroli pod względem ich zgodności z normami prawnymi (np. wydawanie decyzji co do pomocy społecznej przysługującej jednostce). Można postawić pytanie o słuszność cedowania na algorytmy i ich twórców możliwości ustalenia, kto na jakie traktowanie zasługuje. Technologie tworzą konkretne osoby, np. programiści i programistki, inżynierowie i inżynierki. W przeciwieństwie do ustawodawców, osoby tworzące algorytmy nie są wybierane w demokratycznych wyborach. Mimo to, wraz z rozpowszechnianiem się zautomatyzowanego podejmowania decyzji, rośnie ich wpływ na tworzenie zasad rządzących życiem społecznym. Nawet w sytuacji, w której stworzone zostają wytyczne dotyczące kryteriów, jakimi mają się kierować twórcy algorytmów, efekt przekładania wytycznych na ostatecznie podejmowane decyzje zostaje ukryty w czarnej skrzynce¹⁸ technologii. Brak demokratycznej kontroli nad oprogramowaniem, które zaczyna pełnić funkcje prawa, może zatem niepokoić.

Brak przejrzystości wprowadzanych rozwiązań sprawia, że na uwagę zasługuje pytanie o to, czy i w jaki sposób prawo może chronić jednostki przed potencjalnie dyskryminacyjnym traktowaniem wynikającym z zautomatyzowanego przetwarzania danych. To właśnie brak dostępu do informacji na temat tego, jak dany system zautomatyzowanego podejmowania decyzji działa, często uniemożliwia jednoznaczne stwierdzenie, czy prowadzi ono, czy też nie, do dyskryminacyjnego traktowania. W analizie nie kwestionuję tego, że możliwe jest tworzenie zautomatyzowanego podejmowania decyzji, którego wyniki będą mniej dyskryminujące niż te osiągnięte w wyniku działań człowieka¹⁹. Twierdzą natomiast, że ich rozwój może być inspirowany rozwiązaniami instytucjonalno-prawnymi, które będą gwarantować przejrzystość w zakresie wdrażanych zautomatyzowanych rozwiązań i tym samym tworzyć możliwość weryfikacji, czy dany algorytm prowadzi do dyskryminacyjnego traktowania. Jak okazało się w czasie przeprowadzonych przeze mnie badań, sama informacja na temat działania danego systemu zautomatyzowanego

Processes. The Premise, the Proposed Solutions, and the Open Challenges, „Philosophy and Technology” 2018, t. 31, s. 611–627.

¹⁸ Metafora, która weszła do dyskursu na temat nowych technologii w związku z publikacją F. Pasquale, *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge–Londyn 2015.

¹⁹ Przedstawienie takiej perspektywy, zob. J. Kleinberg, J. Ludwig, S. Mullainathan, C.R. Sunstein, *Discrimination in the Age of Algorithms*, „Journal of Legal Analysis” 2018, t. 10, s. 113–174.

podejmowania decyzji jest kluczowa dla możliwości oceny jego funkcjonowania w świetle zakazu dyskryminacji w prawie europejskim, czyli prawie UE oraz Rady Europy²⁰.

Dlatego też założeniem stojącym u podstaw przeprowadzonej analizy jest przekonanie o konieczności „odczarowania” istniejących i potencjalnych „czarnych skrzynek” technologii przy wykorzystaniu narzędzi oferowanych przez prawo europejskie. Możliwe jest, że w przyszłości prawo ulegnie daleko idącym przemianom, np. pod wpływem rozwoju tzw. uczenia maszynowego, rejestrów rozproszonych czy inteligentnych kontraktów. Wtedy rozbieżności między technologią i regulującymi ją ramami prawnymi mogą utrudniać podporządkowywanie nowych rozwiązań technologicznych istniejącym ramom prawnym. Punktem wyjścia analizy jest założenie, że dopóki innowacje technologiczne funkcjonują w ramach istniejącego obecnie porządku prawnego, konieczne są próby osadzenia ich w obowiązujących normach prawnych.

Moją intencją jest przeprowadzenie analizy zautomatyzowanego podejmowania decyzji w szerszym świetle pytań o europejską aksjologię. Przede wszystkim mierzę się z zagadnieniem relacji zachodzącej między zakazem dyskryminacji a zautomatyzowanym podejmowaniem decyzji zarówno w odniesieniu do prawa UE, jak i Rady Europy. Ponadto stawiam pytanie o związek między nieprzejrzystym charakterem zautomatyzowanych rozwiązań a wartościami chronionymi przez art. 2 TUE²¹, w tym szczególnie demokracją i państwem prawnym²². Wartości UE mogą stanowić istotną wskazówkę, w jaki sposób myśleć o regulacji nowych technologii, a przede wszystkim o wymogach dotyczących ich przejrzystości. Po skandalu związanym z Cambridge Analytyką²³ i z rolą, jaką nowe technologie odegrały w kampaniach

²⁰ Posługuję się pojęciem „prawo europejskie”, kiedy odnoszę się do prawa UE i Rady Europy łącznie. Kiedy pisze tylko o prawie UE lub tylko o prawie Rady Europy, używam odpowiednio tych terminów precyzyjnie odnoszących się jedynie do danej organizacji. Ze względu na tak zarysowany zakres pracy nie zajmuję się analizą prawa krajowego. W zakresie polskich publikacji dotyczących jawności należy wskazać wielotomowe wydanie *Jawność i jej ograniczenia*, red. G. Szpor, C.H. Beck, Warszawa 2013–2016. Tom XI serii, zatytułowany *Standardy europejskie*, red. C. Mik, C.H. Beck, Warszawa 2016, najbliższy jest tematowi analizy i odsyłam do niego w odpowiednich miejscach.

²¹ *Traktat o Unii Europejskiej* (TUE), Dz.Urz. EU 2012 C 326, s. 13–46.

²² W odniesieniu do UE analizuję również zagadnienie dostępu do zasad stojących za systemami zautomatyzowanego podejmowania decyzji w świetle „otwartości” przywoływanej w art. 15, *Traktat o funkcjonowaniu Unii Europejskiej* (TFUE), Dz.Urz. EU 2012 C 326, s. 47–390.

²³ Skandal dotyczył problemu targetowanych reklam i ich wpływu na wyniki wyborcze. Dane pozyskane w celu analizy profili psychologicznych jednostek zostały w dużym stopniu pobrane bez wiedzy i zgody osób, których dotyczyły, ponieważ osoby wypełniające test stanowiący jedno z ich źródeł udostępniły jednocześnie informa-

wyborczych i referendalnych ostatnich lat, trudno kwestionować, że tworzą one poważne wyzwanie dla demokracji i praworządności.

Przy pisaniu towarzyszyło mi przekonanie, że wydarzenia te wymuszają próbę odejścia od indywidualistycznej perspektywy skupionej na pojedynczym podmiocie i zwrócenia się ku instytucjom, normom i środkom prawnym stawiającym w centrum zbiorowość i jej interes. Jak wskazuje motto książki, zautomatyzowane podejmowanie decyzji nie jest problemem dotyczącym wyłącznie jednostki – jest ono zjawiskiem dotyczącym poszczególne osoby, ale jako członków konkretnych grup społecznych lub przedstawicieli algorytmicznie wygenerowanej zbiorowości. Dlatego też odpowiedzi na wyzwania tworzone przez zautomatyzowane podejmowanie decyzji powinny uwzględniać ten kolektywny wymiar stosowanych w tym zakresie mechanizmów.

1. Zakres badań, hipoteza i pytania badawcze

Celem analizy jest weryfikacja hipotezy mówiącej, że możliwe jest postrzeganie algorytmów używanych w zautomatyzowanym podejmowaniu decyzji jako informacji publicznej lub dokumentów urzędowych²⁴. Rozwiązanie takie pojawia się wśród propozycji, które są formułowane jako narzędzia mające na celu zwiększenie poziomu przejrzystości zautomatyzowanego podejmowania decyzji²⁵. Analiza takiej możliwości została już przeprowadzona dla ram prawnych dotyczących dostępu do informacji w Stanach

cję na temat swoich znajomych na Facebooku. Artykuły prasowe na temat skandalu, zob. Z. Kleinman, *Cambridge Analytica: The story so far*, BBC, 21 marca 2018 r. <https://www.bbc.co.uk/news/technology-43465968>, dostęp: 1.04.2021 czy J.C. Wong, *The Cambridge Analytica Scandal Changed the World – But It Didn't Change Facebook*, „The Guardian”, 18 marca 2019 r. <https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>, dostęp: 1.04.2021.

²⁴ Używam zamiennie terminów „prawo dostępu do informacji” i „prawo dostępu do informacji publicznej” ze względu na fakt, że zarówno ETPCz, jak i TSUE często ogranicza się do mówienia właśnie o „dostępie do informacji”, pomijając przymiotnik „publicznej”. Podobnie zamiennie używam terminów „prawo dostępu do dokumentów” i „prawo dostępu do dokumentów urzędowych” dla większej przejrzystości. Natomiast w zakresie różnic między znaczeniem pojęcia „dokument” i „informacja” przeprowadzam analizę dotyczącą ich znaczenia w prawie Rady Europy i prawie UE odpowiednio w trzecim i czwartym rozdziale.

²⁵ Dostęp do kodu źródłowego jako jeden ze sposobów przeciwdziałania niejawności zautomatyzowanego podejmowania decyzji pojawia się np. w raporcie Omidyar Network, Upturn, *Public Scrutiny of Automated Decisions: Early Lessons and Emerging Methods An Upturn and Omidyar Network Report*, 2018, s. 19. <https://omidyar.com/wp-content/uploads/2020/09/Public-Scrutiny-of-Automated-Decisions.pdf>, dostęp: 1.04.2021.

Zjednoczonych²⁶ oraz Australii²⁷. Poniższa analiza ma natomiast na celu sprawdzenie, czy takie podejście do zautomatyzowanego podejmowania decyzji jest uprawnione w świetle prawa UE oraz prawa Rady Europy – a jeżeli tak, to w jakim zakresie.

Analiza jest motywowana wątpliwościami, które zautomatyzowane podejmowanie decyzji może budzić w zakresie zgodności stosowanych w nim rozwiązań z zakazem dyskryminacji w prawie europejskim. W książce skupiam się na zautomatyzowanym podejmowaniu decyzji w stosunku do jednostek w obszarach zadań publicznych wykonywanych przez państwo lub podmioty upoważnione przez państwo²⁸. Przykładami takich sytuacji są podejmowanie decyzji dotyczącej wymiaru pomocy udzielonej osobie bezrobotnej, wdrażanie systemu zautomatyzowanego przydzielania spraw sędziom czy wykorzystywanie systemów sugerujących odpowiedni wymiar czy typ kary sędziom wydającym wyroki. Zakres badań obejmuje zatem jedynie część sytuacji, w których zautomatyzowane podejmowanie decyzji znajduje zastosowanie²⁹.

Próba analizy algorytmów, jako informacji podlegającej prawu dostępu do informacji publicznej lub dokumentów urzędowych, wynika ze spostrzeżenia, że w demokratycznym społeczeństwie jest nie do przyjęcia, aby nieprzejrzysta technologia pełniła funkcję organu administracyjnego lub prawodawcy. Szczególnie jeśli istnieją wątpliwości co do zgodności jej stosowania z zakazem dyskryminacji. W związku z tym w celu weryfikacji głównej hipotezy niezbędne jest poszukanie odpowiedzi na wymienione poniżej pytania badawcze.

²⁶ Zob. H. Bloch-Wehba, *Access to Algorithms*, „Fordham Law Review” 2020, t. 88, s. 1265–1314. Analiza Bloch-Wehby oparta jest m.in. na orzecznictwie amerykańskich sądów i ukazuje brak jednolitego podejścia do kwestii umożliwiania dostępu do algorytmów jako informacji publicznej. Tekst zamyka podkreślenie konieczności wprowadzania nowych rozwiązań prawnych, które stanowiłyby bardziej adekwatną odpowiedź na wyzwania tworzone przez zautomatyzowane podejmowanie decyzji.

²⁷ Zob. A. Ray, B. Adams, D. Thampapillai, *Access to Algorithms Post-Robodebt: Do Freedom of Information Laws Extend to Automated Systems?*, „Alternative Law Journal” 2021 (online first). <https://doi.org/10.1177/1037969X211029434>, dostęp: 18.07.2021. Konkluzją autorów jest niejasny status systemów zautomatyzowanego podejmowania decyzji z punktu widzenia prawa dostępu do informacji. Wskazują oni jednak, że wydaje się możliwe traktowanie jako informacji publicznej przynajmniej części takich systemów.

²⁸ Wybór taki w żaden sposób nie powinien być odczytywany jako próba umniejszania konieczności gwarantowania ochrony praw jednostki w odniesieniu do stosowania zautomatyzowanego podejmowania decyzji w ramach sektora prywatnego. Jest on związany z charakterem prawa dostępu do informacji i do dokumentów urzędowych, których potencjał w odniesieniu do uzyskiwania dostępu do kodu komputerowego używanego w ramach zautomatyzowanego podejmowania decyzji jest przedmiotem przedstawionego badania.

²⁹ W związku z tak określonym zakresem tematycznym nie uwzględniam w książce szczegółowych rozważań doktrynalnych dotyczących części używanych przeze mnie pojęć i poruszanych zagadnień.

Po pierwsze, konieczne jest wykazanie, czy rozwój systemów zautomatyzowanego podejmowania decyzji i rozpowszechnianie ich stosowania w ramach sektora publicznego mogą być postrzegane jako procesy zmieniające prawo i zastępujące normy prawne kodem komputerowym. Część analizy poświęcona tym zagadnieniom jest osadzona w nurcie teorii przedstawiającej kod komputerowy jako prawa, a rozwijanej przez m.in. Lawrence'a Lessiga i Mireille Hildebrandt.

Po drugie, niezbędne jest przedstawienie przyczyn, w związku z którymi przejrzystość algorytmów jest istotnym zagadnieniem badawczym w odniesieniu do prawa europejskiego. Wśród nich kluczowe jest wskazanie na zagrożenia związane z brakiem przejrzystości oraz z dyskryminacyjnym traktowaniem jednostek w obszarach objętych prawem UE i w odniesieniu do praw i wolności chronionych przez EKPCz³⁰ w związku z wdrażaniem systemów zautomatyzowanego podejmowania decyzji. Na uwagę zasługuje analiza mechanizmów prowadzących do częściowego lub całkowitego zastępowania regulacji prawnych rozwiązaniami technologicznymi, czyli zautomatyzowanym podejmowaniem decyzji, które oparte są na klasyfikowaniu jednostek do grup, w stosunku do których podejmowane są dane typy decyzji. Scharakteryzowanie wyzwań tworzonych przez takie mechanizmy dla zakazu dyskryminacji oraz dla przejrzystości – która determinuje możliwość rozpoznania dyskryminacyjnego charakteru stosowanych rozwiązań – pozwala uzasadnić konieczność poszukiwania rozwiązań prawnych dotyczących nie tylko jednostkowych decyzji wydawanych z użyciem zautomatyzowanego podejmowania decyzji (obecnych w prawie ochrony danych osobowych), lecz także algorytmów używanych do ich wydawania.

Po trzecie, istotne jest sprawdzenie, czy ramy regulacyjne stworzone przez Ogólne rozporządzenie o ochronie danych (RODO)³¹ oraz działania podejmowane przez Radę Europy w obszarze zautomatyzowanego podejmowania decyzji odnoszą się w adekwatny sposób do zagrożeń związanych z brakiem przejrzystości zautomatyzowanego podejmowania decyzji. Kryterium, które jest istotne do dokonania takiej oceny, jest m.in. precyzja przyjętych przepisów. Interesuje mnie również, na ile odnoszą się one do decyzji podejmowanych wobec danej jednostki, a na ile pozwalają ocenić system zautomatyzowanego podejmowania decyzji sam w sobie. Odpowiedź na te

³⁰ *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 (EKPCz)*, Dz.U. 1993 nr 61 poz. 284.

³¹ *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG) (RODO)*, Dz.Urz. UE 2016 L 119, s. 1–88.

pytania pozwala skonfrontować rozwiązania problemów związanych z zautomatyzowanym podejmowaniem decyzji przyjmowane w obszarze ochrony danych osobowych z kolektywnym wymiarem używania zautomatyzowanych metod podejmowania decyzji.

Po czwarte, należy wskazać, czy RODO pozostawia część zagadnień związanych z możliwością ochrony jednostki przed nieprzejrzystym i potencjalnie dyskryminacyjnym charakterem zautomatyzowanego podejmowania decyzji w zakresie ustawodawstwa państw. Dyskrecjonalność przyjmowanych środków ochrony praw jednostek może prowadzić do efektu sprzecznego z celem przyjęcia rozporządzenia, czyli tworzeniem różnych standardów ochrony w ramach UE w odniesieniu do zautomatyzowanego podejmowania decyzji. Luki w istniejących ramach prawnych, dotyczących ochrony praw jednostki w odniesieniu do używania przez państwa zautomatyzowanych systemów podejmowania decyzji, stanowiły dla mnie motywację do poszukiwania innych perspektyw pozwalających zmierzyć się z problemami wynikającymi z ich stosowania.

Po piąte, konieczne jest dokonanie analizy warunków, pod którymi możliwe jest korzystanie z prawa dostępu do informacji zgodnie z wykładnią EKPCz. Przedstawienie testu umożliwiającego sprawdzenie, czy w danej sytuacji dostęp do informacji objęty jest prawem dostępu do informacji, pozwala stwierdzić, czy istnieją przypadki, w których zasady działania systemów służących do zautomatyzowanego podejmowania decyzji w postaci kodu komputerowego mogłyby być postrzegane jako informacja publiczna w świetle orzecznictwa ETPCz.

Po szóste, niezbędne jest zestawienie podejścia prezentowanego przez ETPCz z wykładnią odnoszącą się do prawa dostępu do informacji dokonywaną przez TSUE. W tym celu konieczne jest przedstawienie kształtowania się prawa dostępu do dokumentów urzędowych w prawie UE oraz orzecznictwa TSUE dotyczącego tej kwestii. Wskazanie rozbieżności między perspektywą prezentowaną w orzecznictwie ETPCz a podejściem przyjętym przez TSUE pozwala wykazać ograniczenia unijnych regulacji dotyczących dostępu do dokumentów urzędowych oraz prawa dostępu do informacji, a także ich konsekwencje dla przejrzystości zautomatyzowanego podejmowania decyzji.

Ponadto prezentowane przez TSUE podejście do zagadnienia prawa dostępu do informacji oraz prawa dostępu do dokumentów urzędowych rodzi pytania o relację między tymi prawami a wartościami stojącymi u podstaw UE, dlatego staram się zbadać związek między „demokratyzacją”, której służyć miało m.in. wprowadzenie prawa dostępu do dokumentów urzędowych UE, a „demokracją” jako wartością wymienianą w art. 2 TUE. W efekcie stawiam pytanie, czy narzędzie mające w zamyśle służyć demokratyzacji UE może być postrzegane jako element niezbędny dla zgodności z zasadą demokracji i praworządności porządków prawnych państw członkowskich?

Czy możliwe jest wymaganie od państw członkowskich, aby działały one w zgodzie z zasadą przejrzystości postrzeganej jako niezbędny element demokracji? Próba odpowiedzi osadza pracę w szerszym kontekście pytań o specyfikę europejskiego podejścia do regulacji nowych technologii i jego związku z wartościami chronionymi przez prawo europejskie.

2. Metody i materiał badawczy

Analiza została przeprowadzona z wykorzystaniem metody formalno-dogmatycznej oraz komparatystycznej³². Pomocniczo, przede wszystkim w odniesieniu do historii rozwoju wykładni prawa dostępu do informacji, stosowana jest metodologia historyczno-prawna. Materiał, na którym opierają się badania, obejmuje akty prawne UE i Rady Europy dotyczące ochrony danych osobowych oraz dostępu do dokumentów urzędowych i dostępu do informacji, a także relewantne dla tematu orzecznictwo TSUE i ETPCz. Wykorzystuję również dokumenty i raporty przygotowane przez UE i Radę Europy oraz na ich zlecenie. Kluczowym punktem odniesienia dla analizy są ustalenia na temat zautomatyzowanego podejmowania decyzji prezentowane przez badaczy, a więc sfera doktrynalna. Książka opiera się głównie na analizie przeprowadzonej w latach 2017–2020. W lipcu 2021 r. została ona uzupełniona o informacje o najnowszych dokumentach, orzecznictwie i literaturze, istotnych z punktu widzenia jej tematu.

Wśród źródeł, z których korzystam pomocniczo, znajdują się raporty i artykuły prasowe przygotowywane przez rozmaite fundacje, stowarzyszenia, oddolne inicjatywy pozarządowe czy dziennikarzy na temat algorytmów i zautomatyzowanego podejmowania decyzji. Powodem wykorzystywania tych publikacji jest z jednej strony ich interdyscyplinarność, która pozwala spojrzeć na badane przeze mnie zagadnienia z szerszej perspektywy – niezbędnej w świetle tematu badania, z drugiej zaś strony – powolne tempo publikacji w czasopiśmie naukowych. Rozwój technologiczny sprawia, że badane przeze mnie zagadnienia podlegają niezwykle dynamicznym zmianom i dyskusje na ich temat odbywają się niekiedy poza obiegiem naukowym zależnym od powolnego procesu wydawniczego. Źródła te są użyteczne ze względu na to, że zawierają np. przystępnie opisane przykłady problemów związanych z zautomatyzowanym podejmowaniem decyzji, czyli sferę faktów dotyczących analizowanej technologii.

³² W zakresie, w jakim rozwiązania przyjęte w ramach UE są porównywane z tymi, które pojawiają się w ramach działalności Rady Europy i w wyniku wykładni EKPCz.

3. Streszczenie rozdziałów

Na książkę składają się cztery rozdziały. W rozdziale pierwszym, po pierwsze, dokonuję przeglądu teoretycznych conceptualizacji znaczenia rozwoju zautomatyzowanego przetwarzania danych. Przedstawione są w nim wyzwania związane z intensyfikacją interakcji między prawem i technologią oraz wynikające z nich zagrożenia dla przejrzystości i – szerzej – demokratycznych procedur stanowienia i stosowania prawa. Po drugie, wykazuję źródła braku przejrzystości zautomatyzowanego podejmowania decyzji oraz dyskryminacji algorytmicznej. Przedstawiony wywód ma za zadanie udzielenie odpowiedzi, czy przejawy dyskryminującego potencjału zautomatyzowanego podejmowania decyzji mogą dotyczyć obszarów objętych prawem europejskim i w rezultacie prowadzić do tworzenia zagrożeń dla zgodności z zakazem dyskryminacji. Po trzecie, przedstawiam przyjęte przeze mnie ramy teoretyczne. Kładę nacisk na konieczność postrzegania zagrożeń związanych z rozwojem zautomatyzowanego podejmowania decyzji w odniesieniu do zakazu dyskryminacji, jako problemu dotyczącego całych grup i wynikającego z samych systemów zautomatyzowanego podejmowania decyzji. Dążenie do zwiększenia ich przejrzystości jest krokiem w stronę zagwarantowania możliwości sprawdzenia, czy nie naruszają one zakazu dyskryminacji.

Aby ocenić, czy konieczne jest poszukiwanie nowych rozwiązań problemów pojawiających się w odniesieniu do relacji między zautomatyzowanym podejmowaniem decyzji a zakazem dyskryminacji, niezbędne jest przedstawienie relewantnych rozwiązań regulacyjnych wypracowanych do tej pory, czemu służy rozdział drugi. Po pierwsze, odpowiada on na pytanie badawcze dotyczące tego, w jakim stopniu ramy regulacyjne stworzone przez prawo ochrony danych osobowych odpowiadają na zagrożenia związane z potencjałem dyskryminacyjnym zautomatyzowanego podejmowania decyzji. Odpowiedź na to pytanie jest udzielona przede wszystkim na podstawie analizy przepisów RODO, w tym zwłaszcza art. 13–15 oraz art. 22. Ponadto przedstawiam analizę innych praw podmiotów danych oraz rozwiązań odnoszących się do systemowego wymiaru zautomatyzowanego podejmowania decyzji (ocena skutków dla ochrony danych – DPIA i wiążące reguły korporacyjne – BCR) w RODO. Ponieważ wciąż nie ma orzecznictwa relewantnego dla zagadnienia, ogromną rolę dla prowadzonej analizy odgrywają debata akademicka tocząca się na temat zautomatyzowanego podejmowania decyzji i jego regulacji w RODO, jak również wskazówki wypracowane w tym zakresie przez Grupę Roboczą Art. 29 i EROD³³. Po drugie, przedstawiam działania podjęte przez Radę Europy w obszarze zautomatyzowanego podejmowania

³³ Grupa Robocza Art. 29 została zastąpiona w związku z reformą unijnego prawa ochrony danych osobowych przez EROD.

decyzji, czyli propozycje zmian w treści *Konwencji 108*³⁴ (tzw. *Konwencja 108+*³⁵). Jednym z nowych praw sformułowanych w protokole zmieniającym *Konwencję 108* jest prawo do niepodlegania decyzji opartej na zautomatyzowanym przetwarzaniu danych. Analiza wzajemnego oddziaływania rozwiązań z prawa unijnego i tych przyjmowanych w ramach działalności Rady Europy pozwala zarysować pełny obraz stanu prawnego dotyczącego zautomatyzowanego podejmowania decyzji w prawie europejskim.

Celem rozdziału trzeciego jest częściowa weryfikacja głównej hipotezy. Poświęcony jest on próbie zbadania i wykazania, czy prawo dostępu do informacji może stanowić narzędzie prowadzące do zwiększania poziomu przejrzystości algorytmów, a jeśli tak, to pod jakimi warunkami. Rozdział poświęcony jest analizie charakteru prawa dostępu do informacji w ramach działalności Rady Europy. Rozpoczyna go krótkie wprowadzenie dotyczące roli odgrywanej przez prawo dostępu do informacji w historii rozwoju międzynarodowych umów dotyczących praw człowieka oraz w działalności Rady Europy. Analiza art. 10 EKPCz wymaga sięgnięcia do historii międzynarodowych inicjatyw wiążących się z wolnością informacji, ponieważ to dyskusje na jej temat i negocjacje międzynarodowych umów dotyczących praw człowieka stanowiły inspirację dla treści EKPCz. Dlatego w rozdziale została zarysowana historia udziału ONZ w kształtowaniu standardów dotyczących dostępu do informacji, a na jej tle przedstawiono kontrowersje związane z art. 10 EKPCz i prawem dostępu do informacji. Ze względu na wagę perspektywy porównawczej w odniesieniu do zrozumienia wątpliwości wiążących się z obecnością prawa dostępu do informacji w art. 10 EKPCz w tym fragmencie analizy została zastosowana metoda komparatystyczna oraz do pewnego stopnia historyczno-prawna. Obecność tego podrozdziału znajduje uzasadnienie m.in. w argumentacji przytoczanej przez ETPCz w orzecznictwie odnoszącym się do prawa do informacji. W związku z wagą wyroków ETPCz dla tej kwestii, kluczową częścią rozdziału trzeciego jest analiza orzecznictwa dotyczącego prawa dostępu do informacji. Zostały w niej przedstawione zarówno warunki, których spełnienie determinuje możliwość powołania się na prawo do informacji jako część dorobku europejskiego systemu ochrony praw człowieka, jak i możliwe ograniczenia tego prawa. Uwzględniona została również możliwość traktowania prawa dostępu do informacji jako narzędzia służącego realizacji innych praw gwarantowanych w EKPCz. Rozdział przedstawia również analizę przeprowadzoną ściśle w odniesieniu do

³⁴ Polska wersja językowa: *Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r.* (Konwencja 108), Dz.U. 2003 nr 3 poz. 25 (*Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, ETS No. 108).

³⁵ *Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (Konwencja 108+), CETS 223.

zautomatyzowanego podejmowania decyzji: ma ona pomóc w dokładnym przedstawieniu możliwych zastosowań prawa dostępu do informacji do algorytmów i tym samym doprowadzić do weryfikacji głównej hipotezy w zakresie dotyczącym działalności Rady Europy.

Pierwsza część rozdziału czwartego przedstawia kolejno zarys historyczny rozwoju prawa dostępu do dokumentów w UE oraz szerszy kontekst reform instytucjonalnych UE i ewolucji horyzontów aksjologicznych integracji europejskiej w zakresie istotnym dla wykazania ich znaczenia dla prawa dostępu do dokumentów. Taka struktura podrozdziału jest podyktowana chęcią skupienia się na tych elementach prawa dostępu do dokumentów w prawie UE, które są istotne z punktu widzenia analizy, w odniesieniu zaś do innych zagadnień ogranicza się do odsyłania do literatury przedmiotu. Drugą część rozdziału otwiera analiza *dyrektywy 2019/1024*³⁶. Jest ona poświęcona dostępowi do dokumentów i informacji w prawie UE w świetle zautomatyzowanego podejmowania decyzji wprowadzanego przez państwa członkowskie. Znajduje się w niej również analiza osadzona na szerszym tle zagadnienia zakresu ochrony praw podstawowych w UE oraz związku między wartościami z art. 2 TUE a prawem dostępu do dokumentów i prawem dostępu do informacji.

Każdy z rozdziałów zamyka krótkie podsumowanie opisanych w nim zagadnień, natomiast książkę wieńczy zakończenie stanowiące zestawienie wniosków wynikających z weryfikacji głównej hipotezy i odpowiedzi na stawiane pytania badawcze.

4. Terminologia

Przedmiotem zainteresowania analizy są algorytmy służące do zautomatyzowanego podejmowania decyzji (*automated decision-making*). Z perspektywy istniejących regulacji należy odnotować, że pojęcie zautomatyzowanego podejmowania decyzji jest terminem używanym w prawie ochrony danych osobowych, które reguluje wybrane sytuacje posługiwania się takimi rozwiązaniami. W świetle hipotezy weryfikowanej w tej książce niezbędne jest jednak nie tylko zarysowanie znaczenia tego terminu zgodnie z jego charakterystyką zawartą w RODO, lecz również uzupełnienie go o definicję pojęć takich jak algorytm i sztuczna inteligencja. Przyjrzenie się temu, czym są algorytmy, czyli rozwiązania stojące za systemami zautomatyzowanego podejmowania decyzji, dostarcza argumentów za możliwością postrzegania zautomatyzowanego podejmowania decyzji jako narzędzia mogącego kształtować

³⁶ *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego* (dyrektywa 2019/1024), Dz.Urz. EU 2019 L 172, s. 56–83.

sytuację prawną jednostki i w związku z tym zmieniającego rozumienie, czym jest prawo.

4.1. Zautomatyzowane podejmowanie decyzji i profilowanie

W związku z brakiem definicji legalnej terminu „zautomatyzowane podejmowanie decyzji” punktem wyjścia do analizy jest definicja, którą można wywodzić z treści art. 22 RODO zatytułowanego „Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie”³⁷. Stwierdza on, że osoba, której dane dotyczą, ma prawo nie podlegać decyzji opierającej się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołującej wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływającej. Taki sposób patrzenia na zautomatyzowane podejmowanie decyzji jest neutralny technologicznie: obejmuje on zarówno prosty algorytm, jak i zaawansowany technologicznie system wykorzystujący uczenie maszynowe, jak długo decyzja wydawana z jego użyciem spełnia warunki wymienione w art. 22 RODO.

W związku z niejasnym znaczeniem określeń użytych w art. 22, takich jak „całkowicie zautomatyzowany” oraz „decyzja wywołująca skutki prawne”, należy odwołać się do wytycznych na temat zautomatyzowanego podejmowania decyzji przygotowanych przez Grupę Roboczą Art. 29³⁸. Wytyczne Grupy Roboczej Art. 29 nie mają co prawda mocy prawnie

³⁷ Art. 22, RODO. Przepis ten analizuję szczegółowo w rozdziale drugim, tutaj jedynie zaznaczam kluczowe elementy definicyjne niezbędne do określenia zakresu analizy. Rozwiązania dotyczące zautomatyzowanego podejmowania decyzji wprowadzone w RODO zostały powtórzone w art. 24, *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Tekst mający znaczenie dla EOG)* (rozporządzenie 2018/1725), Dz.Urz. UE 2018 L 295, s. 39–98. W nieco odmienny sposób są one regulowane w art. 11, *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW* (dyrektywa 2016/680), Dz.Urz. UE 2016 L 119, s. 89–131. Na problemy związane z taką strategią regulacji ochrony danych osobowych zwracała uwagę już na etapie prac nad projektami tych aktów prawnych A. Grzelak, *Projekt reformy ochrony danych osobowych – czy rzeczywiście powstanie jednolity i spójny system?*, „Kwartalnik Kolegium Ekonomiczno-Społecznego. Studia i Prace” 2014, nr 4, s. 93–125.

³⁸ Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE*, 3 października 2017 r., ostatnio zmienione i przyjęte 6 lutego 2018 r., 17/PL WP 251 rev.01. Rozważania doktryny na temat art. 22 przedstawiam w rozdziale drugim.

wiążącej, stanowią natomiast istotną wskazówkę dla wykładni pojęć pojawiających się w RODO. Zgodnie z wytycznymi Grupy Roboczej Art. 29, aby przetwarzanie danych nie zostało uznane za całkowicie zautomatyzowane, to interwencja ludzka musi pozwalać na istotny nadzór nad podejmowaniem decyzji. Ponadto działanie musi być podejmowane przez osobę, która ma uprawnienia i kompetencje do zmiany decyzji, i musi uwzględniać wszystkie dane istotne dla danego podejmowania decyzji³⁹. Pozorny udział człowieka w podejmowaniu decyzji, polegający np. jedynie na zatwierdzeniu decyzji wskazywanej przez algorytm, nie będzie zatem stanowić przesłanki do wyłączenia danego podejmowania decyzji z zakresu zastosowania zakazu z art. 22 RODO.

Wytyczne pozwalają ponadto uniknąć interpretacji problematycznego pojęcia decyzji, przez uwzględnienie całych fraz użytych w RODO, czyli „decyzja wywołująca skutki prawne” lub „podobny istotny wpływ”. Za decyzję taką należy uznać dokonanie wyboru, który „ma [...] wpływ na prawa danej osoby przewidziane w przepisach, takie jak wolność do zrzeszania się, głosowania w wyborach lub wystąpienia na drogę sądową” lub „na status prawny danej osoby lub na prawa przysługujące jej na mocy umowy”⁴⁰. Proponowany przez Grupę Roboczą Art. 29 zakres znaczenia zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach jest zatem bardzo szeroki. Zdaniem Grupy Roboczej Art. 29 zakaz z art. 22 powinien odnosić się do wszelkich praw jednostki, które są zagwarantowane w przepisach⁴¹.

Zakres sytuacji objętych zakazem z art. 22 poszerza dodatkowo uwzględnienie kategorii decyzji, które na sytuację jednostki mają „podobnie istotny wpływ”. Przykłady takich sytuacji pojawiają się w motywie 71 RODO (automatyczne odrzucenie elektronicznego wniosku kredytowego, elektroniczne

³⁹ Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji...*, *op. cit.*, s. 23.

⁴⁰ *Ibidem*, s. 24.

⁴¹ Przykładami są np. kwestie udzielania świadczeń społecznych czy mechanizmy rekrutacyjne zdefiniowane przepisami prawa. W podobnym duchu, zob. G. Malgieri, G. Comandé, *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, „International Data Privacy Law” 2017, t. 7, nr 4, s. 252. To, co pozostaje niejasne, to kwestia, czy te elementy praw jednostki zagwarantowanych w przepisach, które nie są w przepisach zdefiniowane, mogą być również objęte zakresem stosowania art. 22 RODO. Jeśli np. system zautomatyzowanego podejmowania decyzji jest używany do określania dzielnic będących priorytetem dla kontroli policji opartej na kryteriach dyskryminacyjnych, to czy można uznać, że stanowi on naruszenie jakiegoś prawa jednostki gwarantowanego przepisami prawa, mimo że to konkretne, dane zagadnienie nie jest regulowane w przepisach? W świetle RODO sytuacje takie powinny być prawdopodobnie uznane za mające „podobnie istotny wpływ” na jednostkę.

metody rekrutacji bez interwencji ludzkiej⁴²). Wytyczne Grupy Roboczej Art. 29 sugerują konieczność szerokiej interpretacji tej kategorii jako uwzględniającej sytuację, w których decyzja stwarza ryzyko „wywarcia istotnego wpływu na sytuację danej osoby, jej zachowanie lub podejmowane przez nią wybory, wywarcia długotrwałego lub trwałego wpływu na osobę, której dane dotyczą lub w najbardziej ekstremalnym przypadku, doprowadzenia do wykluczenia lub dyskryminacji osób fizycznych”⁴³. W ich obrębie mogą znaleźć się nawet decyzje dotyczące marketingu *online*, w sytuacji, w której będą one prowadzić do istotnego wpływu na jednostkę, np. w odniesieniu do jej sytuacji finansowej⁴⁴.

Należy podkreślić, że w art. 22 RODO została uwzględniona również szczególna kategoria zautomatyzowanego podejmowania decyzji, czyli zautomatyzowane podejmowanie decyzji oparte na profilowaniu⁴⁵. Termin „profilowanie”, zdefiniowany w art. 4 RODO, oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej⁴⁶. Definicja profilowania z art. 4 nie pokrywa się całkowicie z zakresem sytuacji, do których odnosi się art. 22. Nie jest to dostrzegane przez część polskich autorów komentujących RODO, np. Marcin Zadrożny nie do końca trafnie określa prawa jednostki zdefiniowane w art. 22 RODO jako „prawa związane z profilowaniem”⁴⁷. Podobnie Witold Chomiczewski odwołuje się również do pojęcia profilowania, referując przepisy dotyczące zautomatyzowanego podejmowania decyzji⁴⁸. Natomiast różnicę między zakresem znaczeniowym tych pojęć odnotowuje np. Arwid Mednis, który zauważa, że „[...] profilowanie i podejmowanie zautomatyzowanych decyzji to dwie

⁴² Motyw 71, RODO.

⁴³ Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji...*, *op. cit.*, s. 24.

⁴⁴ Taki sposób rozumienia sytuacji używania zautomatyzowanego podejmowania decyzji podlegających regulacji RODO stanowi również argument za przyjęciem perspektywy szerokiej, w której są analizowane możliwości otrzymania dostępu do algorytmów oparte na prawie dostępu do informacji lub prawie dostępu do dokumentów urzędowych i którą przyjmuję – jak zauważyłam powyżej – w książce.

⁴⁵ Przykładem analizy wychodzącej od pojęcia profilowania i charakteryzującej ramy prawne dotyczącego tego zagadnienia w obszarze prawa ochrony danych osobowych jest: M. Ciechomska, *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych*, „Europejski Przegląd Sądowy” 2017, nr 5, s. 37–42.

⁴⁶ Art. 4 ust. 4, RODO.

⁴⁷ A. Dmochowska, M. Zadrożny, *Unijna reforma ochrony danych osobowych. Analiza zmian*, C.H. Beck, Warszawa 2016, s. 49–52.

⁴⁸ W. Chomiczewski w *Profilowanie w ogólnym rozporządzeniu o ochronie danych*, [w:] *Polska i Europejska Reforma Ochrony Danych Osobowych*, red. E. Bielak-Jomaa, D. Lubasz, Wolters Kluwer Polska, Warszawa 2016, s. 127–138.

różne czynności, które mogą być ze sobą powiązane, ale mogą też występować niezależnie od siebie”⁴⁹.

Zakres sytuacji objętych treścią art. 22 RODO obejmuje np. profilowanie oparte całkowicie na zautomatyzowanym podejmowaniu decyzji. Natomiast zgodnie z definicją profilowania z art. 4 „musi [ono] obejmować pewną formę zautomatyzowanego przetwarzania – interwencja ludzka nie musi jednak powodować, że dane działanie wykracza poza definicję profilowania”⁵⁰. Znacząca interwencja człowieka w podejmowanie decyzji będzie natomiast sprawiała, że dana sytuacja nie będzie objęta zakazem zautomatyzowanego podejmowania decyzji sformułowanym w art. 22. Grupa Robocza Art. 29 podsumowała zagadnienie relacji między zautomatyzowanym podejmowaniem decyzji i profilowaniem:

Zautomatyzowane podejmowanie decyzji ma inny zakres niż profilowanie, może jednak częściowo pokrywać się z profilowaniem lub z niego wynikać. [...] Zautomatyzowane podejmowanie decyzji może, ale nie musi, obejmować profilowanie, z kolei profilowanie może zachodzić bez podejmowania zautomatyzowanych decyzji. Profilowanie i zautomatyzowane podejmowanie decyzji nie muszą jednak stanowić odrębnych działań. Bywa, że działanie, które początkowo stanowi zwykły proces zautomatyzowanego podejmowania decyzji, może przekształcić się w działanie oparte na profilowaniu, co będzie zależeć od sposobu wykorzystania danych⁵¹.

Należy zauważyć, że zautomatyzowane podejmowanie decyzji i profilowanie zostało uregulowane – poza RODO – w *dyrektywie 2016/680* oraz w *rozporządzeniu 2018/1725*. *Dyrektywa 2016/680* dotyczy ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar. Przepisy *dyrektywy 2016/680* zawierają rozwiązanie dotyczące zautomatyzowanego podejmowania decyzji nieopierającego się na szczególnych kategoriach danych. Z zasady są one zakazane, z wyjątkiem sytuacji, w której dopuszcza je prawo Unii lub państwa członkowskiego, któremu podlega administrator oraz które przewiduje odpowiednie zabezpieczenia praw i wolności osoby, której dane dotyczą, a przynajmniej prawo do uzyskania interwencji ludzkiej ze strony administratora (art. 11 ust. 1). Definicja profilowania została natomiast ujęta art. 3 ust. 4 *dyrektywy 2016/680* i stanowi

⁴⁹ A. Mednis, *Prawo ochrony danych osobowych wobec profilowania osób fizycznych*, PRESSCOM, Warszawa 2019, s. 179.

⁵⁰ Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji...*, *op. cit.*, s. 7.

⁵¹ *Ibidem*, s. 8–9.

powtórzenie definicji profilowania sformułowanej w RODO. W art. 11 ust. 3 *dyrektywy 2016/680* zabronione zostało profilowanie skutkujące dyskryminacją osób fizycznych na podstawie danych osobowych szczególnych kategorii⁵². *Rozporządzenie 2018/1725* natomiast powtarza przepisy dotyczące zautomatyzowanego podejmowania decyzji pojawiające się w RODO⁵³, dotyczy ono jednak przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne UE. Z perspektywy ściśle definicyjnej te akty prawne nie tworzą zatem dodatkowych wyzwań interpretacyjnych⁵⁴.

Problemy prawne związane ze sposobem sformułowania zakazu zautomatyzowanego podejmowania decyzji w RODO obejmują bardzo różnorodne kwestie, począwszy od wspomnianej niejasności pojęć użytych w RODO, dla których rozumienia wytyczne Grupy Roboczej Art. 29 stanowią jedynie wskazówkę, nie zaś wiążącą ich wykładnię, przez to jak dopuszczone w treści rozporządzenia wyjątki ograniczają rzeczywisty zakres zastosowania zakazu, po trudności związane z uwzględnieniem kolektywnego wymiaru wpływu zautomatyzowanego podejmowania decyzji. Perspektywa opierająca się na prawie ochrony danych osobowych sprawia, że z dwóch elementów niezbędnych do zautomatyzowanego podejmowania decyzji, czyli danych, na podstawie których decyzja jest podejmowana, oraz algorytmu wykorzystywanego do jej podjęcia, uwaga unijnego ustawodawcy skupia się na danych. Z wyjątkiem „prawa do wyjaśnienia”⁵⁵ prawa podmiotu danych dotyczą danych osobowych i dostępu do nich. Natomiast w analizie koncentruję się na algorytmach używanych do podejmowania zautomatyzowanych decyzji oraz prawie dostępu do informacji. Stąd też definicja, którą przedstawiłam na początku wstępu, nie jest identyczna z tym, jak może być rozumiane zautomatyzowane podejmowanie decyzji na tle przepisów RODO.

⁵² Zgodnie z art. 10 *dyrektywy 2016/680* są to: „dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe lub przynależność do związków zawodowych oraz przetwarzanie danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia lub danych dotyczących seksualności i orientacji seksualnej osoby fizycznej”.

⁵³ Art. 24 *rozporządzenia 2018/1725* jest odpowiednikiem art. 22 RODO, profilowanie zdefiniowane jest natomiast w art. 3 ust. 5 *rozporządzenia 2018/1725*.

⁵⁴ Nieco inaczej kwestia przedstawia się w odniesieniu do materialnej treści przepisów *dyrektywy 2016/680*. Jest ona jednak przedmiotem zainteresowania analizy jedynie w zakresie, w jakim może stanowić wskazówkę interpretacyjną dotyczącą niejasności pojawiających się w związku z wykładnią przepisów RODO (w rozdziale drugim).

⁵⁵ Również analizowanym w rozdziale drugim.

4.2. Algorytm, kod i program komputerowy

Przez pojęcie algorytmu określa się łańcuch poleceń, których wykonanie ma prowadzić do „osiągnięcia danego celu pod danymi warunkami”⁵⁶. Definicja taka jest neutralna technologicznie – „algorytm nie musi być oprogramowaniem: w szerokim sensie są to zakodowane procedury służące zmianie danych wprowadzanych w pożądaną formę, w oparciu o sprecyzowane wyliczenia”⁵⁷. Z tej perspektywy przez pojęcie algorytmu można rozumieć zarówno schemat blokowy zapisany na kartce, jak i algorytm determinujący treść facebookowego *newsfeeda*. Taki sposób myślenia o algorytmach jest coraz rzadszy w związku z upowszechnieniem rozumienia algorytmów jako immanentnie związanych z cyfrowością. W dyskursie publicznym algorytmy wiążą się z oprogramowaniem, systemami informacyjnymi, aplikacjami⁵⁸. To semantyczne przesunięcie jest widoczne również w definicjach stworzonych przez organizacje międzynarodowe:

Każdy zestaw zasad dotyczący zmiany cyfrowego wkładu w cyfrowy wynik jest „algorytmem”. Algorytm to oprogramowanie służące do podejmowania decyzji. Jak w przypadku innych typów podejmowania decyzji, jakość decyzji – wynik – zależy od tego, jakiego rodzaju dane zostały wprowadzone do algorytmu oraz od jakości algorytmu⁵⁹.

Definicja ta stanowi przykład dualnej struktury zautomatyzowanego podejmowania decyzji i ilustruje, czym jest w nim algorytm: działanie algorytmu jest zależne od danych przez niego używanych, ale i sam algorytm determinuje sposób, w jaki dane te są używane.

Fakt, że zgodnie z definicją zautomatyzowanego podejmowania decyzji z RODO musi się ono odbywać wyłącznie automatycznie, sprawia, że algorytm używany do takiego podejmowania decyzji musi mieć formę cyfrową. Nie zmienia to jednak faktu, że pozostaje on „zestawem zasad”, jak np. zgodnie z definicją Solona Barocasa i Andrew D. Selbsta, którzy określają algorytm jako „formalnie sprecyzowaną sekwencję operacji logicznych, która

⁵⁶ R.K. Hill, *What an Algorithm Is*, „Philosophy & Technology” 2016, nr 29, s. 47. Przegląd literatury dotyczącej definicji algorytmu, zob. M. Kullmann, *Platform Work, Algorithmic Decision-Making, and EU Gender Equality Law*, „International Journal of Comparative Labour Law and Industrial Relations” 2018, t. 34, nr 1, s. 6.

⁵⁷ T. Gillespie, *The Relevance of Algorithms*, [w:] T. Gillespie, P. Boczkowski, K. Foot, *Media Technologies, Essays on Communication, Materiality, and Society*, MIT Press, Cambridge–Londyn 2014, s. 167.

⁵⁸ Zob. B.D. Mittelstadt, P. Allo, M. Taddeo, S. Wachter, L. Floridi, *The ethics of algorithms: Mapping the debate*, „Big Data & Society” 2016, t. 3, nr 2, s. 2.

⁵⁹ OECD (Directorate for Financial and Enterprise Affairs Competition Committee), *Algorithms and Collusion – Note from the European Union*, DAF/COMP/WD (2017) 12, s. 2.

dostarcza komputerowi instrukcji w kolejnych krokach, w celu dokonywania operacji na danych i w związku z tym automatyzacji decyzji”⁶⁰. Cyfrowa forma algorytmów używanych do zautomatyzowanego podejmowania decyzji sprawia z kolei, że zaciera się różnica między tym, jak rozumiany jest algorytm, a tym, czym jest program komputerowy, czego świadectwem jest przykładowa definicja programu komputerowego:

Powszechnie za program komputerowy uważa się zbiór instrukcji (rozkazów, poleceń), wyrażonych w postaci zrozumiałej dla komputera (słowami, symbolami matematycznymi, znakami graficznymi) i mający na celu wywołanie zamierzonych przez twórcę programu działań komputera, prowadzących do osiągnięcia określonego rezultatu⁶¹.

Bliski związek pojęć algorytmu i programu lub kodu komputerowego w przypadku systemów zautomatyzowanego podejmowania decyzji pozwala traktować je – dla celów analizy⁶² – jako do pewnego stopnia tożsame. Zautomatyzowane podejmowanie decyzji zakłada używanie programu komputerowego, czyli wymusza zapis procedur rozwiązywania danego problemu (algorytmu) w formie cyfrowej (kodu komputerowego). Ze względu na to, że algorytmy w ramach systemów zautomatyzowanego podejmowania decyzji muszą być sformułowane w postaci kodu komputerowego, żądanie dostępu do nich jako do informacji publicznej lub dokumentów urzędowych może oznaczać żądanie dostępu do kodu, w postaci którego zostały one ujęte. Nie wyklucza to oczywiście wnioskowania o inne, bardziej abstrakcyjne formy zapisu stosowanych algorytmów (np. dokumenty opisujące je w formie tekstu pisanego językiem naturalnym lub formułami matematycznymi). Jak wyjaśniam w rozdziałach trzecim i czwartym pracy, zaletą podejścia koncentrującego się na zapisie algorytmów w formie kodu komputerowego jest konieczność istnienia zapisu stosowanych w zautomatyzowanym podejmowaniu decyzji algorytmów w formie kodu komputerowego – bez niego nie byłoby bowiem możliwe stosowanie takich rozwiązań. Z tych powodów używam zamiennie pojęć algorytm, kod komputerowy i program komputerowy,

⁶⁰ S. Barocas, A.D. Selbst, *Big Data's Disparate Impact*, „California Law Review” 2016, t. 104, s. 674.

⁶¹ F. Rodaniewicz, *Ochrona programów komputerowych w prawie UE (cz. I)*, „Europejski Przegląd Sądowy” 2009, nr 3, s. 24.

⁶² Chociaż należy odnotować inne interpretacje relacji między programem komputerowym a algorytmem obecne w literaturze, np.: „uwzględniając poglądy zgłaszane w literaturze przedmiotu, poza zakresem ochrony prawnoautorskiej należałoby w typowej sytuacji pozostawić algorytm, rozumiany jako pewien abstrakcyjny sposób rozwiązania problemu”. *Prawo Internetu*, red. P. Podrecki, Z. Okoń, P. Litwiński, M. Świerczyński, T. Targosz, M. Smycz, D. Kasprzycki, wyd. 2, Lexis Nexis, Warszawa 2007, s. 440. Więcej na ten temat piszę w sekcji poświęconej problemom z przejrzystością algorytmów.

najchętniej posługując się jednak terminem „algorytm”, ponieważ ma on najszersze znaczenie i najbardziej pozwala podkreślić fakt, że mamy do czynienia z zapisem (w wypadku zautomatyzowanego podejmowania decyzji: w formie cyfrowej) pewnych procedur⁶³.

Perspektywa, która stoi u podstaw głównej hipotezy, opiera się bowiem na spojrzeniu na algorytm z punktu widzenia neutralności technologicznej. Niezależnie od tego, czy jest on wyrażony w zapisie cyfrowym, czy na papierze, powinien być postrzegany jako zestaw zasad. Klasycznym przykładem przypominającym o tej neutralności technologicznej może być zdjęcie przedstawiające Margaret Hamilton, która stoi obok równie wysokiej jak ona góry papieru. Na papierze znajduje się kod, dzięki któremu możliwe stało się wysłanie człowieka na księżyc⁶⁴. Perspektywa taka – odrywająca algorytmy od postrzegania technologii jako tajemniczej czarnej skrzynki – umożliwia analizę prawną algorytmu jako informacji lub dokumentu, który w określonych przypadkach powinien podlegać prawu dostępu do informacji lub dokumentów. Zważywszy na odnotowany powyżej wpływ zarówno algorytmu, jak i danych na jakość podejmowanej w sposób zautomatyzowany decyzji, stawiana hipoteza, skupiona na samych algorytmach, nie stanowi uniwersalnej i wyczerpującej odpowiedzi na problemy związane z rozwijanymi w tym obszarze technologiami. Jest ona raczej poszukiwaniem uzupełnienia rozwiązań wprowadzonych w RODO. Stawiam w jej centrum zainteresowania drugi, obok danych, ale również niezbędny, element zautomatyzowanego podejmowania decyzji.

4.3. Sztuczna inteligencja

Temat analizy jest częściowo związany z zagadnieniem sztucznej inteligencji i jej wpływu na prawo. W książce unikam jednak posługiwania się terminem SI (AI), stąd też istnieje konieczność podania przyczyn stojących za takim wyborem terminologicznym, który mógłby się wydawać konieczny dla przedstawionej analizy. Definicje słownikowe⁶⁵ wskazują, że SI jest pojęciem opisującym dwa typy fenomenów. Po pierwsze, odnosi się ono do dziedziny wiedzy i nauki⁶⁶. Po drugie, opisuje ono programy lub systemy komputerowe, które

⁶³ Za wskazanie konieczności bardziej szczegółowego opisu tego zagadnienia dziękuję dr hab. prof. UŁ Monice Namysłowskiej.

⁶⁴ Zdjęcie dostępne w Wikipedii: [https://en.wikipedia.org/wiki/Margaret_Hamilton_\(scientist\)#/media/File:Margaret_Hamilton_-_restoration.jpg](https://en.wikipedia.org/wiki/Margaret_Hamilton_(scientist)#/media/File:Margaret_Hamilton_-_restoration.jpg), dostęp: 1.04.2021.

⁶⁵ *Oxford Dictionary*: https://en.oxforddictionaries.com/definition/artificial_intelligence, dostęp: 1.04.2021; *Słownik języka polskiego*: <https://sjp.pwn.pl/sjp/sztuczna-inteligencja;2466532.html>, dostęp: 1.04.2021.

⁶⁶ W definicji podanej w *Słowniku języka polskiego* jest postrzegana ściśle jako „dział informatyki”, co w świetle interdyscyplinarności badań prowadzonych nad sztuczną inteligencją jest dość kontrowersyjnym stwierdzeniem i przykładem traktowania technologii

mają na celu wykonywanie różnego typu zadań „normalnie wymagających inteligencji ludzkiej”⁶⁷, takich jak np. rozpoznawanie mowy, tłumaczenie czy podejmowanie decyzji. Możliwość wykonywania przez SI tych zadań wiąże się z pewnym stopniem autonomii i zdolnością do uczenia się, która charakteryzuje algorytmy wykorzystujące np. uczenie maszynowe. Jednocześnie drugi obszar znaczeniowy tego pojęcia wskazuje na wiele problemów związanych z wyborem precyzyjnej definicji SI: czym jest sama inteligencja?⁶⁸ Jaki jest poziom zadań, które wymagają inteligencji ludzkiej? Jak traktować to kryterium w świetle rozwoju technologicznego?

Z perspektywy prawnej pojawia się szersze pytanie: czy istnieje możliwość lub konieczność objęcia SI regulacjami? Dyskusje prowadzone w zakresie tej kwestii już w drugiej połowie XX stulecia⁶⁹ koncentrują się z jednej strony na określeniu relacji między sztuczną inteligencją a ciałami fizycznymi, które dzięki niej nabyć mogą pewien stopień autonomii (np. roboty), z drugiej zaś na rozwiązaniach technologicznych wykorzystujących sztuczną inteligencję, które nie wiążą się z przybieraniem przez dane wynalazki formy fizycznej wykazującej się pewną autonomią. Dwoistość ta uwidoczniła została w definicji SI, która pojawia się w komunikacie Komisji Europejskiej „Sztuczna inteligencja dla Europy”:

Termin sztuczna inteligencja odnosi się do systemów, które wykazują inteligentne zachowanie dzięki analizie otoczenia i podejmowaniu działań – do pewnego stopnia autonomicznie – w celu osiągnięcia konkretnych celów. Systemy SI mogą być oparte na oprogramowaniu, działając w świecie wirtualnym (np. asystenci głosowi, oprogramowanie do analizy obrazu, wyszukiwarki, systemy rozpoznawania mowy i twarzy), lub mogą być wbudowane w urządzenia (np. zaawansowane roboty, samochody autonomiczne, drony lub aplikacje internetu rzeczy)⁷⁰.

W związku z brakiem przyjętej definicji legalnej SI to właśnie komunikaty i wnioski legislacyjne Komisji Europejskiej stanowią główne źródło

informatycznych jako osobnej rzeczywistości, nie zaś – czym w rzeczywistości one są – elementu współkształtującego również świat fizyczny.

⁶⁷ Oxford Dictionary: https://en.oxforddictionaries.com/definition/artificial_intelligence, dostęp: 1.04.2021.

⁶⁸ Kompleksowy przegląd definicji „inteligencji”: S. Legg, M. Hutter, *A Collection of Definitions of Intelligence*, [w:] B. Goertzel, P. Wang, *Frontiers in Artificial Intelligence and Applications: Volume 157: Advances in Artificial General Intelligence: Concepts, Architectures and Algorithms*, IOS Press, Amsterdam 2007, s. 17–24.

⁶⁹ Zob. S.N. Lehman-Wilzig, *Frankenstein Unbound: Towards a Legal Definition of Artificial Intelligence*, „Futures” 1981, t. 13, nr 6, s. 442–457.

⁷⁰ Komisja, *Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Sztuczna inteligencja dla Europy*, COM (2018) 237 final, s. 1.

informacji dotyczących tego, co przez to pojęcie jest określone przez instytucje unijne⁷¹. Należy również odnotować prowadzenie prac przez Grupę ekspertów wysokiego szczebla ds. sztucznej inteligencji powołaną przez Komisję Europejską, która w kwietniu 2019 r. opublikowała raport na temat etycznego wymiaru rozwoju SI⁷². Definicja proponowana przez ekspertów z jednej strony przypomina tę sformułowaną przez Komisję przez określenie SI jako systemów charakteryzujących się pewnymi cechami, z drugiej jednak uwzględnia tradycyjne rozumienie SI jako obszaru wiedzy i zbioru rozwiązań programistycznych. Pojawia się w niej również techniczny wymiar rozwoju SI⁷³.

Jego obecność w pracach Grupy ekspertów wysokiego szczebla ds. sztucznej inteligencji mogła mieć wpływ na uwzględnienie technicznych aspektów definicji SI w opublikowanej w kwietniu 2021 r. propozycji wniosku legislacyjnego *Aktu w sprawie SI*⁷⁴. Wniosek legislacyjny zawiera propozycję definicji legalnej SI, która opiera się na wymienieniu w Załączniku I technik i podejść, które miałyby być traktowane jako SI, np. mechanizmy uczenia maszynowego, w tym uczenie nadzorowane, uczenie się maszyn bez nadzoru i uczenie przez wzmacnianie, z wykorzystaniem szerokiej gamy metod, w tym uczenia głębokiego⁷⁵. Zgodnie z wnioskiem *Aktu w sprawie SI* przez pojęcie systemu sztucznej inteligencji należy rozumieć oprogramowanie opracowane przy użyciu co najmniej jednej spośród technik i podejść wymienionych w Załączniku I do rozporządzenia, które może:

⁷¹ Pierwsze zdanie definicji przedstawionej w komunikacie „Sztuczna inteligencja dla Europy” zostało powtórzone w komunikacie „Skoordynowany plan wobec sztucznej inteligencji” (‘Coordinated Plan on Artificial Intelligence’): Komisja, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Coordinated Plan on Artificial Intelligence*, COM (2018) 795 final, s. 1.

⁷² Grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji, *Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji*, Bruksela 2019 – oparte na szkicu: The European Commission’s High-Level Expert Group on Artificial Intelligence, *Draft Ethics Guidelines For Trustworthy AI. Working Document for stakeholders’ consultation*, Bruksela 2018.

⁷³ Zob. Grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji, *Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji*, *op. cit.*, s. 36. Dodatkowo Grupa przygotowała dokument: Grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji, *Definicja SI: główne funkcje i dyscypliny naukowe*, Bruksela 2019.

⁷⁴ Komisja, *Wniosek: Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące Sztucznej Inteligencji (Akt w sprawie Sztucznej Inteligencji) i zmieniające niektóre akty ustawodawcze Unii*, COM/2021/206 final. *Pre-print kompleksowego artykułu omawiającego Akt w sprawie SI*: M. Veale, F. Zuiderveen Borgesius, *Demystifying the Draft EU Artificial Intelligence Act*, SocArXiv 2021. <https://doi.org/10.31235/osf.io/38p5f>, dostęp: 18.07.2021.

⁷⁵ Zob. Załącznik I do *Aktu w sprawie SI*.

[...] dla danego zestawu celów określonych przez człowieka – generować wyniki, takie jak treści, przewidywania, zalecenia lub decyzje wpływające na środowiska, z którymi wchodzi w interakcję⁷⁶.

Taka strategia definicyjna stanowi nowe podejście do problemu określenia, czym jest SI w świetle prawa UE. Nie jest jednak oczywiste, że proponowana przez Komisję definicja znajdzie się w ostatecznej formie rozporządzenia. W momencie przygotowywania książki do druku dyskusja nad *Aktem w sprawie SI* dopiero się rozpoczyna, doświadczenia zaś z prac nad RODO podpowiadają, że będzie ona długa i obfitująca w niespodzianki.

Brak konsensu w odniesieniu do znaczenia terminu SI, kontrowersje wokół znaczenia pojedynczych elementów proponowanych definicji, brak wiążących prawnie aktów w prawie europejskim, które odnosiłyby się bezpośrednio do tego zagadnienia, a przede wszystkim brak obowiązującej w czasie przygotowywania tej książki definicji legalnej SI w prawie europejskim sprawiają, że posługiwanie się tym pojęciem może generować niejasności terminologiczne. Próby określenia, czym z perspektywy prawnej jest SI, stanowią osobny przedmiot badań, pozostający poza zakresem zainteresowania tej pracy⁷⁷. Tymczasem zjawisko zautomatyzowanego podejmowania decyzji w rozumieniu zgodnym z RODO jest czymś niezależnym od SI, jednocześnie obejmującym część sytuacji, w których SI znajduje lub może znaleźć zastosowanie. Systemy zautomatyzowanego podejmowania decyzji nie muszą – chociaż mogą – charakteryzować się zdolnością do uczenia się i autonomii. Biorąc pod uwagę zasadę neutralności technologicznej⁷⁸ wyrażoną w RODO⁷⁹, fakt używania lub nieużywania technologii określanych terminem SI w zakresie zautomatyzowanego podejmowania decyzji ma

⁷⁶ Art. 3 ust. 1, *Akt w sprawie SI*.

⁷⁷ Przegląd definicji oraz zagadnień dotyczących podmiotowości prawnej SI, zob. M. Jankowska, *Podmiotowość prawna sztucznej inteligencji?*, [w:] *O czym mówią prawnicy, mówiąc o podmiotowości*, red. A. Bielska-Brodziak, Uniwersytet Śląski, Katowice 2015, s. 171–196; A. Chłopecki, *Sztuczna inteligencja – szkice prawnicze i futurologiczne*, C.H. Beck, Warszawa 2018, s. 1–6.

⁷⁸ Zasada neutralności technologicznej zgodnie z definicją M. Hildebrandt: „Prawo neutralne technologicznie to zasadniczo apel normatywny, aby tworzyć prawo, które nie faworyzuje żadnej technologii, bo to szkodzi innowacyjności, lub aby powstrzymać się od przyjmowania prawa, które odnosi się tylko do konkretnych technologii, jako że to czyni prawo mniej możliwym do egzekwowania na dłuższą metę, lub też jako apel, aby brać pod uwagę to, jak dane technologie wpływają na zmniejszenie efektywności danych praw podstawowych, poprzez kompensację tych efektów środkami prawnymi”. M. Hildebrandt, *Smart Technologies and the End(s) of Law. Novel Entanglements of Law and Technology*, Edward Elgar Publishing, Cheltenham 2015, s. 174.

⁷⁹ Art. 2 ust. 1 oraz wprost: motywy 15, RODO.

ograniczony wpływ na stosowanie rozporządzenia wobec zautomatyzowanego podejmowania decyzji⁸⁰. Jak już wcześniej podkreśliłam, kryteria definicyjne zautomatyzowanego podejmowania decyzji nie odnoszą się do rodzajów technologii zastosowanych do ich stworzenia. Z tych powodów to przede wszystkim algorytmy i zautomatyzowane podejmowanie decyzji są terminami, którymi posługuję się w analizie.

⁸⁰ Problem ten omawiam w rozdziale drugim.

Ramy teoretyczne prawnego wymiaru zautomatyzowanego podejmowania decyzji

1.1. Teoretyczne konceptualizacje relacji między kodem komputerowym a prawem

Inspiracją teoretyczną do analizy są koncepcje, które postulują postrzeganie kodu komputerowego jako prawa⁸¹. Pytania rozważane w ich ramach nabierają coraz większego znaczenia w świetle rozwoju technologii zautomatyzowanego podejmowania decyzji. Prawo zaczyna być zastępowane przez kod komputerowy, czego przykładem są próby „przekładania” istniejących przepisów i norm prawnych na kod komputerowy, np. w celu usprawnienia wydawania decyzji czy egzekwowania ochrony praw autorskich przez blokowanie danych treści. Innym mechanizmem jest przechodzenie od regulacji danych zagadnień przepisami do regulacji za pośrednictwem systemów informatycznych, np. przez odwołanie do systemu informatycznego w miejsce regulowania kolejności przydzielania sędziom spraw w akcie prawnym. Obecność mechanizmów pozwalających na kształtowanie rzeczywistości za pomocą kodu komputerowego pokazuje, że konieczne jest przyjrzenie się temu, jak ich działanie wpływa na prawo i funkcjonowanie jednostek nie tylko w przestrzeni cyfrowej.

1.1.1. Kod jako prawo

Początki konceptualizacji kodu jako prawa⁸² sięgają połowy lat 90. poprzedniego stulecia⁸³. W opublikowanej w 1995 r. pracy *City of Bits Space, Place,*

⁸¹ Posługuję się w tym miejscu pojęciem „prawa” ze względu na fakt, że różne sposoby wdrażania zautomatyzowanego podejmowania decyzji w obszarach objętych regulacjami mogą mieć charakter zastępowania konkretnych przepisów, ale i zastępowania norm prawnych. Ponadto użycie wyrażenia „prawo” znajduje uzasadnienie w przedstawionych niżej koncepcjach teoretycznych.

⁸² Szeroki wykaz literatury relewantnej dla tego tematu, zob. E. Bayamlioglu, R. Leenes, *The ‘Rule of Law’ Implications of Data-driven Decision-Making: a Techno-Regulatory Perspective*, „Law, Innovation and Technology” 2018, t. 10, nr 2, s. 297.

⁸³ Nie oznacza to, że wcześniej nie istniały koncepcje dotyczące mechanizacji prawa, próby związania go z matematyką – tropy takie śledzi np. A. Supiot, *Governance by*

and the Infobahn Williama J. Mitchella można odnaleźć następujące wyjaśnienie sformułowania „kod jako prawo” (*code as law*, zawierające nieprzetłumaczalną grę słów, w której *code* to zarówno kod, np. komputerowy, jak i kodeks):

Tam, na cyfrowej granicy, kod jest prawem. Reguły rządzące jakimkolwiek mikroświatem komputerowo-skonstruowanej gry wideo, pulpit twojego osobistego komputera, okno edytora tekstu, bankomat, czat w sieci – są precyzyjnie i rygorystycznie określone w tekście programu, który odpowiada za to, co jest widoczne na twoim monitorze⁸⁴.

Chociaż Mitchell zajmował się designem i architekturą, jego refleksja na temat roli kodu jako prawa wyprzedziła prace prawnicze na ten temat, a także zainspirowała prawników do jej rozwoju. Na podstawie jego sformułowania powstała najbardziej znana praca dotycząca tej teorii, czyli *Code and Other Laws of Cyberspace*⁸⁵ Lawrence’a Lessiga⁸⁶. W celu ukazania normatywnej roli odgrywanej przez kod komputerowy Lessig porównuje go do aktów prawnych regulujących przestrzeń realną⁸⁷. To konstytucje, statuty, ustawy czy umowy międzynarodowe wyznaczają w niej ramy działania państw i jednostek, decydują o uznaniu danego zachowania za zgodne lub niezgodne z prawem. W przestrzeni cyfrowej granice możliwości naszych zachowań są wyznaczane przez kod komputerowy: bez ingerencji w kod nie jest możliwe obejście oferowanych przez niego możliwości. Przykładem zasad narzucanych przez kod jest brak możliwości wyjścia poza zaprogramowane

Numbers. The Making of a Legal Model of Allegiance, tłum. S. Brown, Hart Publishing, Oxford 2017.

⁸⁴ W.J. Mitchell, *City of Bits Space, Place, and the Infobahn*, MIT Press, Cambridge –Londyn 1996, s. 111.

⁸⁵ Zob. L. Lessig, *Code and Other Laws of Cyberspace*, Basic Books, Nowy Jork 1999. W książce posługuję się wydaniem drugim, czyli: L. Lessig, *Code. Version 2.0*, Basic Books, Nowy Jork 2006.

⁸⁶ W podobnym nurcie, ukazującym kod jako prawo, funkcjonuje pojęcie *lex informatica*, ukute przez Joela R. Reidenberga. Definiuje on *lex informatica* jako: „zestaw zasad dla przepływu informacji, który narzuca technologia i sieci komunikacyjne”. J.R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, „Texas Law Review” 1997–1998, t. 76, s. 555. Ze względu na bardziej krytyczne podejście do roli kodu jako prawa reprezentowane przez Lessiga oraz szerszą rozpoznawalność zastosowanego przez niego terminu zdecydowałam się zrezygnować ze sformułowania *lex informatica* na rzecz „kodu jako prawa”.

⁸⁷ Zob. „W przestrzeni realnej rozpoznajemy to jak prawo ją reguluje – przez konstytucje, statuty i inne prawne kodeksy. W przestrzeni cyfrowej musimy zrozumieć jak regulują ją różne «kody» – jak software i hardware (tzn. «kod» przestrzeni cyfrowej), które czynią z przestrzeni cyfrowej to czym ona jest, również regulują to jaka ona jest”. L. Lessig, *op. cit.*, s. 5.

ramy gry komputerowej czy wybrania z rozwijalnego pola możliwości, która nie została w nim uwzględniona. Kod komputerowy, tak jak prawo, tworzy zespół reguł obowiązujących jego użytkowników.

Możliwości te mogą się wydawać użytkownikom dane z góry. Koncepcja, zgodnie z którą przestrzeń cyfrowa jest regulowana przez kod, nie jest jednak deterministyczna. Kod jest tworzony, jest wypadkową pewnych wyborów⁸⁸. Twórcy kodu mają wpływ na to, na jakich zasadach opiera się tworzony przez nich element cyfrowej rzeczywistości. Jak podkreśla Lessig, egzekwowanie tych zasad nie jest weryfikowane przez państwo, lecz właśnie przez twórców kodu. Oznacza to, że elementy przestrzeni cyfrowej mogą się różnić tym, w jaki sposób są regulowane, w zależności od tego, jak jest ukształtowany kod, który je opisuje i tworzy⁸⁹, ten z kolei może być różny w zależności od tego, kto go pisał.

Podobnie jak w wypadku aktów prawnych, których treść jest różna w zależności np. od tego, czy są wydawane dla ochrony czy promowania pewnych wartości, także możliwości oferowane przez kod komputerowy mogą być odzwierciedleniem wyborów o charakterze aksjologicznym. Przykładem przytaczanym przez Lessiga jest problem potwierdzania tożsamości w internecie, który stanowił barierę rozwoju handlu elektronicznego we wczesnych latach 90. XX w. Wprowadzenie technologicznego rozwiązania w postaci ciasteczek (*cookies*), polegającego na pozostawianiu elementów kodu i sprawdzaniu przeglądarki użytkownika, umożliwiło komunikację między komputerem a serwerem, a tym samym automatyzację rozpoznawania „z kim ma się do czynienia”⁹⁰. Jak podkreśla Lessig, zmiana ta, mająca ogromny wpływ na ochronę – a właściwie jej ograniczenie – prywatności w sieci, nie była efektem zmian prawnych. Stanowiła ona efekt działań podjętych w ramach płaszczyzny technologicznej, które miały z kolei wpływ na prawa jednostek.

Przykład ten pokazuje dwoistość możliwej relacji między kodem jako prawem a prawem w jego tradycyjnym rozumieniu. Z jednej strony, kod może stanowić narzędzie umożliwiające automatyzację egzekwowania istniejących regulacji, czego przykładem są systemy zarządzania prawami cyfrowymi (DRM), czyli narzędzia używane w celu ograniczania możliwości używania utworów chronionych prawami autorskimi do opcji zgodnych z regulacjami dotyczącymi tej kwestii. Z drugiej strony, sposób wprowadzenia norm prawnych do kodu komputerowego może wpływać na to, jak stosowane są wdrażane przez niego przepisy, np. obostrzenia nakładane przez DRM są

⁸⁸ Zob. L. Lessig, *op. cit.*, s. 318.

⁸⁹ *Ibidem*, s. 24.

⁹⁰ L. Lessig, *Law Regulating Code Regulating Law*, „Loyola University Chicago Law Journal” 2003, t. 35, s. 5.

niekiedy bardziej surowe niż obowiązujące prawo⁹¹. Algorytmy nie stanowią dokładnego tłumaczenia norm prawnych na kod komputerowy. Tym samym kod w rzeczywistości tworzy nowe normy, które determinują możliwości podejmowania danych działań w sieci i poza nią. Zagadnienie tej ambiwalencji relacji między prawem a kodem jako prawem ukazuje ścieżkę rozwoju teorii kodu jako prawa: skodyfikowane normy prawne oraz kod komputerowy zaczynają wchodzić w interakcję.

Warto w tym miejscu odwołać się do propozycji podziału odnoszącej się do faz, które można zaobserwować w odniesieniu do tej interakcji⁹². Pierwsza z nich to digitalizacja informacji, czyli – w odniesieniu do prawa – systemy takie jak np. EUR-Lex. Faza druga to wprowadzenie automatyzacji do procesu podejmowania decyzji, których przykładem są wspomniane powyżej systemy DRM. Faza trzecia dodaje do drugiej wyższy stopień interakcji między prawem a kodem. Z jednej strony prawo zaczyna regulować kod, jak np. przepisy RODO dotyczące ochrony danych w fazie projektowania i domyślna ochrona danych (art. 25, *data protection by design* i *by default*), czy normy techniczne, które mogą tworzyć standardy odnoszące się do stosowanych rozwiązań technologicznych⁹³. Wymogi takie dotyczą warunków, które spełniać ma kod komputerowy. Z drugiej strony pojawiają się elementy regulacji za sprawą kodu. Zgodnie z tą kwalifikacją

⁹¹ „Nie ulega wątpliwości, że im bardziej skomplikowane mechanizmy technologiczne, tym większa ingerencja w formę dozwolonego użytku, odsłaniająca coraz to nowe pola konfliktu między ochroną zabezpieczeń technicznych utworów a ograniczeniami praw wyłącznych twórców”. K. Gienas, *Zabezpieczenia techniczne utworów a dozwolony użytek na tle prawa wspólnotowego i polskiego*, „Europejski Przegląd Sądowy” 2009, nr 12, s. 14. Innym przykładem są rozwiązania oparte na sieciach *peer-to-peer*, w których technologia może np. ułatwiać obchodzenie prawa, zob. T. Wu, *When Code Isn't Law*, „Virginia Law Review” 2003, t. 89, nr 4, s. 679–751, przykłady innych sposobów użycia technologii do obchodzenia prawa: s. 707–709.

⁹² Klasyfikację oraz część przykładów przedstawiam za: P. De Filippi, S. Hassan, *Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code*, „First Monday” 2016, t. 21, nr 12. https://www.researchgate.net/publication/311447869_Blockchain_Technology_as_a_Regulatory_Technology_From_Code_is_Law_to_Law_is_Code, dostęp: 1.04.2021.

⁹³ Myśl dotyczącą związku między kodem a normami technicznymi zawdzięczam recenzentce mojej pracy doktorskiej, dr hab. prof. UJ Ninie Półtorak. W świetle moich przemyśleń normy techniczne wydają się jednak raczej przykładem sytuacji, w której to prawo próbuje regulować technologię, nie zaś sytuacji, w której technologia służy do zapisania prawa. Ponadto perspektywa, którą staram się przedstawiać, kładzie nacisk na daleko idące skutki stosowania zautomatyzowanego podejmowania decyzji w zakresie ingerencji w proces stosowania, a nawet tworzenia prawa. Stąd też bronię stanowiska, zgodnie z którym zastępowanie przepisów odwołaniem do technologii i wprowadzanie rozwiązań technologicznych w celu stosowania prawa wykracza poza „techniczne” aspekty regulacji danych zagadnień.

dopuszczanie zautomatyzowanego podejmowania decyzji, jako narzędzia używanego w postępowaniach mających wpływ na uprawnienia jednostki, stanowi przykład takiej sytuacji. Większość z mechanizmów wdrażanych systemów zautomatyzowanego podejmowania decyzji obecnie można by zakwalifikować jako należące do fazy trzeciej. Faza czwarta to *kod-yfikacja* prawa (*code-ification of law*): kod staje się „współtwórcą” regulacji, nie zaś jedynie narzędziem niezbędnym do ich egzekwowania. Przykładem takiej sytuacji byłoby wdrażanie mechanizmów opartych na maszynowym uczeniu do systemów zautomatyzowanego podejmowania decyzji. W ramach fazy czwartej używany kod komputerowy zaczyna mieć zdolność do samodoskonalenia, np. przez wykrywanie nowych typów potencjalnych naruszeń i blokowanie ich prób na podstawie analizy dotychczasowych danych.

Klasyfikacja ta ukazuje przede wszystkim rosnący poziom skomplikowania zjawisk zachodzących na styku prawa i technologii, kodeksów i kodu. Kod komputerowy, jako forma zapisu algorytmów, staje się nie tylko mechanizmem rządzącym i tworzącym reguły działania w przestrzeni cyfrowej. Ma on rosnące znaczenie dla świata fizycznego, m.in. w związku z legitymizowaniem stosowania go przez akty prawne. Wagi w związku z tym nabiera pytanie o granice możliwej algorytmizacji prawa, czyli przekładania treści norm prawnych na kod komputerowy. Przykładem mechanizmu, w którym są podejmowane takie próby, jest zautomatyzowane podejmowanie decyzji wykorzystywane w sektorze publicznym. Wdrażanie zautomatyzowanych rozwiązań wiąże się z wiarą, że algorytm jest w stanie odtworzyć proces decyzyjny człowieka lub nawet go udoskonalić, i tym samym przyspieszyć wydawanie decyzji w danych sprawach. Poczynione powyżej uwagi ukazują, że myślenie takie nie uwzględnia dwustronności relacji między kodem i prawem. Próba zapisu cyfrowego regulacji prawnych może prowadzić do problemów, takich jak np. konieczność przełożenia na wartości matematyczne wagi danych kryteriów oceny jednostki czy kwantyfikacji pojęć o charakterze abstrakcyjnym. Tym samym kod, mający wspomóc proces stosowania prawa, będzie je w rzeczywistości zmieniał.

1.1.2. Granice algorytmizacji prawa a zautomatyzowane podejmowanie decyzji

Badania zestawiające zautomatyzowane podejmowanie decyzji oraz regulacje prawne stojące u jego podstaw były podejmowane już na początku lat 90. poprzedniego wieku. Ich wyniki wskazywały na zasadnicze problemy wiążące się z próbą przetłumaczenia prawa na kod komputerowy: brak wdrażania poprawek do danych aktów prawnych do kodu komputerowego, interpretację prawa przez kod komputerowy, która nie jest poprawna, czy problemy wynikające z niemożności przetłumaczenia na kod

przepisów zbyt abstrakcyjnych lub niejasnych⁹⁴. Osoby odpowiedzialne za przygotowanie danego kodu komputerowego stają się władne dokonywać jego wykładni: „w sytuacji, w której możliwa jest więcej niż jedna prawidłowa wykładnia regulacji, to programista musi dokonać wyboru”⁹⁵. Problemy te są relewantne dla prób wdrażania systemów komputerowych opartych na wysokim poziomie interakcji między kodem komputerowym i prawem⁹⁶. W sytuacji, w której systemy zautomatyzowanego podejmowania decyzji obejmują zagadnienia regulowane przez prawo, np. dostęp do zasiłków, dostęp do edukacji czy kwestie związane z prawem do sądu, niepoprawne czy niedokładne przełożenie norm prawnych na kod komputerowy ma bezpośredni wpływ na możliwości korzystania z danych praw przez jednostkę.

Można wskazać trzy obszary, w których przede wszystkim mogą wystąpić poważne ograniczenia zabiegów mających na celu przełożenie norm prawnych na kod komputerowy, czyli algorytmizacji prawa. Po pierwsze, są to wyzwania dla prawa jako przedsięwzięcia normatywnego, po drugie, wyzwania dla prawa jako przedsięwzięcia przyczynowego, oraz po trzecie, upadek prawa jako przedsięwzięcia moralnego⁹⁷.

W odniesieniu do związku między zautomatyzowanym podejmowaniem decyzji a prawem, jako przedsięwzięciem normatywnym, należy zwrócić uwagę na wyzwania wynikające ze zmiany sposobu ewolucji wykładni: „Zmieniające się wiedza, opinie, interesy itp., mogą wymagać ponownej debaty i w związku z tym kontestowania norm jako kluczowego mechanizmu umożliwiającego ewolucję prawa i społeczeństwa”⁹⁸. Odwołując się do metod wykładni stosowanych w prawie europejskim, jest raczej niemożliwe, aby zautomatyzowane podejmowanie decyzji pozwalało na stosowanie wykładni EKPCz traktującej ją jako żyjący instrument, którego wykładnia pozwala uwzględnić zmieniające się realia społeczne. Chociaż zautomatyzowane podejmowanie decyzji może prowadzić do ewolucji wykładni danych

⁹⁴ Przykłady podają za: J. Bing, *Code, Access and Control*, *op. cit.*, s. 204–205. Autorską koncepcję argumentów przeciwko zautomatyzowanemu podejmowaniu decyzji przedstawia G. Noto La Diega, *Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information*, „Journal of Intellectual Property, Information Technology and Electronic Commerce Law” 2018, t. 9, nr 3, s. 5–11.

⁹⁵ J. Bing, *op. cit.*, s. 205.

⁹⁶ *De facto* od fazy drugiej do fazy czwartej z opisywanej powyżej kwalifikacji, przy czym im wyższy poziom interakcji między kodem komputerowym i normami prawnymi, tym problemy stają się bardziej znaczące w świetle np. coraz mniejszej możliwości weryfikacji, jak właściwie interakcja między prawem a kodem przebiega.

⁹⁷ Zob. E. Bayamlioglu, R. Leenes, *op. cit.*, s. 305–311.

⁹⁸ *Ibidem*, s. 305.

norm⁹⁹, nie wydaje się, aby mogła być ona wynikiem głębszego namysłu nad zachodzącymi w świecie realnym zmianami. Jak podkreślają twórcy charakteryzowanej systematyki, Emre Bayamlioglu i Ronald Leenes, dynamika rozwiązań proponowanych przez algorytmy może wynikać raczej z danych, które są wykorzystywane do analizy w danym systemie¹⁰⁰. Tym samym problem ten wiąże się ze stronniczością (*bias*)¹⁰¹, która może się pojawić w danych. Jej efektem zaś może być – teoretycznie – dynamiczne rozumienie norm przez zautomatyzowany system. Dynamika ta jednak może nie być zgodna z intencją prawodawcy. Ponadto w związku z brakiem przejrzystości w zakresie zasad, które stoją za zautomatyzowanym podejmowaniem decyzji, podstawa dokonania danego wyboru staje się niezrozumiała. Rezultatem tych mechanizmów może być rosnący rozdźwięk między decyzjami proponowanymi przez systemy zautomatyzowanego podejmowania decyzji a normami prawnymi, które miały one za zadanie wdrażać.

Drugim problemem jest mechanizm stojący u podstaw zautomatyzowanego podejmowania decyzji, czyli oparcie ich na korelacji, nie zaś na związkach przyczynowych. W przeciwieństwie do mechanizmów, na których opierają się stosowanie i wykładnia prawa, systemy zautomatyzowanego podejmowania decyzji opierają się na statystycznych kalkulacjach biorących pod uwagę współwystępowanie pewnych cech czy zjawisk. Spostrzeżenie to łączy się, w odniesieniu do zautomatyzowanego podejmowania decyzji, z konstruowaniem przez te systemy tzw. nierozdzielczych (*non-distributive*) profili grupowych¹⁰². W przypadku tworzenia rozdzielnych profili grupowych cecha, której obecność jest sprawdzana, odnosi się do wszystkich członków danej grupy, np. odsetek prawdopodobieństwa, że mężczyzna w Stanach Zjednoczonych spędzi pewien okres swojego życia w więzieniu. Jednak w przypadku nierozdzielczego profilu grupowego perspektywa zostaje odwrócona: pod uwagę brane jest prawdopodobieństwo, z jakim dany, konkretny mężczyzna znajdzie się w więzieniu. Oparcie takiego profilu na samej płci nie pozwoli osiągnąć dokładnych wyników, ponieważ są one zależne od innych zmiennych. Jednocześnie nawet uwzględnienie tych zmiennych – czyli opracowanie modelu pozwalającego na dokładniejszą korelację – nie pozwoli ocenić kwestii związanych z przyczynowością. Problemy te wskazują

⁹⁹ Szczególnie w ramach opisywanej powyżej fazy czwartej interakcji między kodem komputerowym i prawem.

¹⁰⁰ E. Bayamlioglu, R. Leenes, *op. cit.*, s. 306.

¹⁰¹ Zjawisko stronniczości w kontekście zautomatyzowanego podejmowania decyzji opisuję dalej w rozdziale.

¹⁰² Zob. M. Hildebrandt, *Smart Technologies and the End(s) of Law...*, *op. cit.*, s. 66 oraz M. Hildebrandt, *Profiling: From Data to Knowledge The challenges of a crucial technology*, „Datenschutz und Datensicherheit” 2006, t. 30, nr 9, s. 549.

na prostą myśl, że sam fakt posłużenia się metodami ilościowymi w ocenie danego zjawiska nie powinien prowadzić do postrzegania tej oceny jako prawidłowej.

Problem ten prowadzi do trzeciego obszaru wyzwań związanych z interakcją między prawem a zautomatyzowanym podejmowaniem decyzji, czyli obszaru moralności. Spostrzeżenie takie jest krokiem dalej w stosunku do stwierdzenia, że technologia nie jest neutralna pod względem normatywności. Chociaż immanentnie nie jest ona dobra lub zła, to sposób, w jaki działa, ma przełożenie na możliwości zachowania zgodnie lub niezgodnie z normami, jak również na sposób kształtowania norm samych w sobie¹⁰³. Przykładem ponownie może być korzystanie z utworów chronionych prawami autorskimi. Internet nie jest narzędziem, które jednoznacznie pozytywnie lub negatywnie wpływa na możliwości dystrybucji i korzystania z utworów – bez wątpienia nie jest on jednak neutralny dla tego obszaru. Ma on wpływ na możliwości zachowania użytkowników, np. korzystających z nieautoryzowanego dostępu, na decyzje producentów i dystrybutorów o tworzeniu autoryzowanych kanałów umożliwiających korzystanie z utworów, a także na samo stosowanie i tworzenie norm prawnych dotyczących praw autorskich.

Należy postawić pytanie, czy rozwiązania technologiczne wdrażane w celu kształtowania wpływu nowych technologii na przestrzeganie prawa budowane są na podstawie wartości, które prawo to ma za zadanie chronić. Przykładem z obszaru praw autorskich jest problematyka filtrowania treści naruszających prawo autorskie. W związku z ich stronniczością, która prowadzi do nadgorliwego identyfikowania treści jako naruszających prawo autorskie¹⁰⁴, ich użycie może stanowić naruszenie wolności wyrazu. Są one jednocześnie narzędziem pozwalającym chronić własność. Tym samym technologia staje się nośnikiem wartości moralnych i zestawem narzędzi wymuszających dokonanie wyboru między dwiema wartościami.

1.1.3. Kod zastępujący przepisy i akty prawne

Obszarem konfliktów między zautomatyzowanym podejmowaniem decyzji a prawem, niewymienianych wprost przez Bayamlioglu i Leenesa, a który zasługuje na podkreślenie, jest wymiar proceduralny. W państwach demokratycznych akty prawne są przyjmowane zgodnie z ustaloną procedurą. Użycie algorytmów, pełniących *de facto* funkcję prawa, może zostać legitymizowane aktem prawnym. Przykładem jest wprowadzenie przez *Rozporządzenie Ministra Sprawiedliwości z dnia 28 grudnia 2017 r. zmieniające rozporządzenie*

¹⁰³ Zob. M. Hildebrandt, *Smart Technologies and the End(s) of Law...*, *op. cit.*, s. 162.

¹⁰⁴ Podnosiła to np. J. Reda, *When filters fail: These cases show we can't trust algorithms to clean up the internet*, 28 września 2017 r. <https://juliareda.eu/2017/09/when-filters-fail/>, dostęp: 1.04.2021.

– *Regulamin urzędowania sądów powszechnych* przepisów dotyczących losowania spraw¹⁰⁵. Zgodnie z wprowadzanym przez ten akt prawny § 43 ust. 1: „Sprawy są przydzielane referentom (sędziom i asesorum sądowym) losowo, zgodnie z ustalonym podziałem czynności, przez narzędzie informatyczne działające w oparciu o generator liczb losowych [...]”¹⁰⁶. Tym samym w akcie prawnym wprowadzono obowiązek korzystania z zautomatyzowanego podejmowania decyzji. Opis zasad określających przydział spraw, który znajdował się w akcie prawnym, został zastąpiony odesłaniem do „narzędzia informatycznego” i „generatora liczb losowych”, których zasady działania nie zostały opisane w rozporządzeniu w szczegółowy sposób.

Takie rozwiązanie nie uwzględnia możliwości demokratycznej kontroli nad tworzeniem prawa czy jego modyfikacją, która staje się zależna od systemów zautomatyzowanego podejmowania decyzji. Brak dostępu do informacji na temat działania narzędzia informatycznego wymienionego w przepisie, w tym np. kodu źródłowego programu używanego do losowania, uniemożliwia weryfikację jego sposobu działania – a tym samym *de facto* weryfikację treści przyjętego aktu prawnego. „Narzędzie informatyczne” staje się w rzeczywistości zestawieniem norm regulujących aspekty dotychczas regulowane w rozporządzeniu. Kod komputerowy z kolei jest zapisem kodyfikującym normy określające sposób postępowania dotychczas charakteryzowany przez przepisy rozporządzenia. Można postrzegać go zatem jako przepisy, chociaż nie jest identyfikowany formalnie jako akt prawny.

Z realistyczno-prawnego punktu widzenia kod komputerowy i używane w nim algorytmy mogą być potraktowane jako akt prawny, który został zapisany w formie cyfrowej. W rzeczywistości pełni on taką samą funkcję: jego zapis określa pewne normy, a także idzie o krok dalej, ponieważ automatyzuje proces gwarantowania ich przestrzegania. Dlatego też możliwe jest rozważenie podejścia odchodzącego od abstrakcyjnego sposobu postrzegania kodu jako prawa, a zbliżającego się do dosłownego rozumienia algorytmu czy kodu komputerowego jako aktu prawnego. Interpretacja taka możliwa

¹⁰⁵ Uchylone i zastąpione przez *Rozporządzenie Ministra Sprawiedliwości z dnia 18 czerwca 2019 r. – Regulamin urzędowania sądów powszechnych*, Dz.U. 2019 poz. 1141. Odwołuję się do rozporządzenia z 2017 r., ponieważ to ono wprowadziło rozwiązanie mówiące o narzędziu informatycznym.

¹⁰⁶ Pełna treść przepisu brzmiała: „Sprawy są przydzielane referentom (sędziom i asesorum sądowym) losowo, zgodnie z ustalonym podziałem czynności, przez narzędzie informatyczne działające w oparciu o generator liczb losowych, oddzielnie dla każdego repertorium, wykazu lub innego urzędzenia ewidencyjnego, chyba że przepisy niniejszego rozporządzenia przewidują inne zasady przydziału”. *Rozporządzenie Ministra Sprawiedliwości z dnia 28 grudnia 2017 r. zmieniające rozporządzenie – Regulamin urzędowania sądów powszechnych*, Dz.U. 2017 poz. 2481. Na marginesie należy zauważyć, że algorytm używany w SLPS został uznany przez NSA za możliwy do rozważania jako informacja publiczna, zob. Wyrok NSA, III OSK 836/21, 19 kwietnia 2021 r.

jest np. w sytuacji, w której obszar objęty uprzednio regulacjami prawnymi zostaje objęty regulacją za sprawą technologii (np. zautomatyzowanego podejmowania decyzji).

Zwykle transformacja ta jest postrzegana jako zachodząca właśnie w tym kierunku: od wersji analogowej zapisu aktu prawnego do cyfrowej wersji umożliwiającej jego automatyczne stosowanie¹⁰⁷. Główna hipoteza tej książki opiera się na próbie odwrócenia kierunku patrzenia na tę transformację: co, jeśli fakt, że regulacja odbywa się za sprawą algorytmów, powinien być interpretowany jako sygnał, iż algorytm należy traktować jako *de facto* akt prawny? Skoro w rzeczywistości to kod komputerowy wyznacza sposób traktowania danej jednostki w obszarach teoretycznie regulowanych aktami prawnymi, to jest uzasadnione traktowanie samego kodu komputerowego jako *de facto* aktu prawnego. Jak wskazuję w analizie powyżej: próba zapisania norm prawnych w formie kodu może prowadzić np. do konieczności przyjęcia danego sposobu wykładni tych norm lub zmian w ich stosowaniu. Kod komputerowy nie jest neutralnym narzędziem, ponieważ staje się częścią procesu tworzenia i stosowania prawa.

Skupienie się wyłącznie na kodzie komputerowym jako akcie prawnym ograniczałoby jednak zakres analizy do sytuacji ściśle regulowanych uprzednio aktem prawnym. Przykładem takiej sytuacji może być opisane powyżej zastąpienie norm prawnych dotyczących przydziału spraw sędziom odwołaniem do narzędzia cyfrowego. Tymczasem w niektórych przypadkach zautomatyzowane podejmowanie decyzji jest wdrażane w zakresie procesów, które nie są ściśle regulowane aktem prawnym, np. w odniesieniu do tego, jakie dzielnice powinna patrolować policja czy szczegółowych zasad rządzących procesami rekrutacyjnymi. Sposób działania zautomatyzowanego podejmowania decyzji w tych obszarach może być jednak niezgodny z obowiązującymi regulacjami. Dlatego też zamiast do kategorii aktu prawnego, odwołuję się do pojęcia informacji i prawa dostępu do niej. Perspektywa taka pozwala uchwycić szerszy zakres zastosowań zautomatyzowanego podejmowania decyzji i skupić się na pytaniu o rolę przejrzystości w odniesieniu do możliwości weryfikacji zgodności używanego zautomatyzowanego podejmowania decyzji z istniejącymi regulacjami.

¹⁰⁷ Stąd też w literaturze jest podkreślony aspekt rewolucjonizujący sposób, w który działa prawo, zwłaszcza w świetle rozwoju technologii uczenia maszynowego: „Prawo dotyczy tekstu, czy może powinniśmy przyznać – precyzując – prawo istnieje jako tekst? Jeśli to ostatnie jest prawdą, czy powinniśmy podejrzewać, że sztuczna inteligencja – jako technologia – podda transformacji sposób, w który funkcjonuje prawo?”. M. Hildebrandt, *Smart Technologies and the End(s) of Law...*, *op. cit.*, s. 161; szerzej na temat tej transformacji: M. Hildebrandt, *A Vision of Ambient Law*, [w:] *Regulating Technologies Legal Futures, Regulatory Frames and Technological Fixes*, red. R. Brownsword, K. Yeung, Hart Publishing, Oxford–Portland 2008, s. 181–185.

Postrzeganie algorytmu jako aktu prawnego powinno być traktowane w moim przekonaniu jako szczególny przypadek, w którym argumenty przemawiające za koniecznością zagwarantowania przejrzystości zautomatyzowanego podejmowania decyzji nabierają szczególnej wagi. Z jednej strony, w świetle konieczności publikacji aktu prawnego w dzienniku urzędowym dla uznania jego autentyczności¹⁰⁸ zauważenie, że kod komputerowy zastępuje treść aktów prawnych, może rodzić wątpliwości co do tego, czy może być on kwestionowany jako niespełniający tego warunku. Z drugiej strony, można twierdzić, że nie może być on uznany za akt prawny właśnie dlatego, że nie jest opublikowany, będąc jednocześnie formą *de facto* norm prawnych, które określają warunki postępowania¹⁰⁹. Analiza redefinicji tworzenia i ogłaszania aktów prawnych w związku z używaniem w tych procesach rozwiązań takich jak zautomatyzowane podejmowanie decyzji przekracza ramy przedstawionych w książce rozważań. Jak zaznaczyłam powyżej, ze względu na różne sposoby włączania korzystania z zautomatyzowanego podejmowania decyzji w zadania wykonywane w ramach sektora publicznego, zdecydowałam się skoncentrować na kwestii samego braku dostępu do informacji na temat tego, czy i jakie rozwiązania technologiczne są przez sektor publiczny wykorzystywane, niezależnie od tego, czy korzystanie z nich jest przewidziane w akcie prawnym czy nie. Stąd też analiza dotyczy przede wszystkim dostępu do algorytmów opartego na prawie dostępu do informacji i prawie dostępu do aktów urzędowych, nie zaś pytania o ewentualny obowiązek publikacji algorytmów jako aktów prawnych.

Ogólną konstatacją wynikającą z opisanego powyżej ujęcia interakcji między prawem a nowymi technologiami wykorzystywanymi w zautomatyzowanym podejmowaniu decyzji jest konieczność odejścia od perspektywy skupionej na jednostce i konkretnej decyzji podjętej w stosunku do niej w zautomatyzowany sposób na rzecz koncentracji na samym modelu determinującym podejmowanie decyzji oraz całych grup, których te decyzje dotyczą. Z tego powodu wśród postulatów dotyczących zasad, które powinny być uwzględniane podczas oceny technologii związanych z kwestiami regulowanymi prawnie, pojawiają się propozycje promujące zaangażowanie różnych grup interesów w proces regulowania technologii, większą przejrzystość, badanie innych możliwości czy instrumenty prawne

¹⁰⁸ Zob. G. Wierczyński, *Udostępnianie informacji o prawie jako warunek skutecznej działalności prawotwórczej*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2015, s. 208. W książce, zgodnie z przedstawionymi powyżej zastrzeżeniami, traktuję takie rozważania uzupełniająco w stosunku do głównego przedmiotu analizy, czyli możliwości traktowania algorytmów jako informacji publicznej lub dokumentu urzędowego.

¹⁰⁹ Odnośnie do pojawiających się w tym fragmencie pojęć (norma prawna i przepis), zob. G. Wierczyński, *Udostępnianie informacji o prawie...*, *op. cit.*, s. 16–18.

zwiększające rozliczalność zautomatyzowanego podejmowania decyzji¹¹⁰. Ich wspólną cechą jest oparcie na przekonaniu, że zautomatyzowane podejmowanie decyzji nie zastępuje jedynie urzędnika w danej konkretnej sprawie. Systemy zautomatyzowanego podejmowania decyzji wpływają również na generalne i abstrakcyjne normy prawne kształtujące sytuację prawną całych społeczeństw. Dlatego położenie nacisku na kolektywny wymiar zautomatyzowanego podejmowania decyzji stanowi jedno z uzasadnień poszukiwania rozwiązań problemów z nim związanych nie tylko w ramach reżimu ochrony danych osobowych.

1.2. Wyzwania tworzone przez zautomatyzowane podejmowanie decyzji w świetle prawa europejskiego

Refleksja nad algorytmami jako źródłem potencjalnego dyskryminacyjnego traktowania oraz ich nieprzejrzystości staje się coraz bardziej obecna w dyskursie publicznym, czego przykładem są raporty organizacji pozarządowych¹¹¹, popularno-naukowe publikacje badaczy i badaczek¹¹², a także aktywność zarówno UE¹¹³, jak i Rady Europy w tym obszarze¹¹⁴. Publikacje te skupiają się na wyzwaniach stworzonych przez brak przejrzystości automatyzacji procesów podejmowania decyzji i powielania przez nie dyskryminacyjnych mechanizmów. Prowadzone są również badania empiryczne skupione m.in. na ocenie zróżnicowania ze względu na płeć wyświetlania użytkownikom

¹¹⁰ B.-J. Koops, *Criteria for Normative Technology: The Acceptability of 'Code as law' in Light of Democratic and Constitutional Values*, [w:] *Regulating Technologies Legal Futures...*, *op. cit.*, s. 168; R.H. Weber, *Socio-Ethical Values and Legal Rules on Automated Platforms: The Quest for a Symbiotic Relationship*, „Computer Law & Security Review” 2020, t. 36, s. 6–7.

¹¹¹ Na przykład AlgorithmWatch, Bertelsmann Stiftung, Open Society Foundations, *op. cit.*; Fundacja ePaństwo, *op. cit.*; Centrum Cyfrowe, Klub Jagielloński, *op. cit.*

¹¹² C. O’Neil, *Broń matematycznej zagłady. Jak algorytmy zwiększają nierówność i zagrażają demokracji*, tłum. M. Zieliński, Wydawnictwo Naukowe PWN, Warszawa 2017; V. Eubanks, *Automating Inequality...*, *op. cit.*

¹¹³ Agencja Praw Podstawowych Unii Europejskiej, *#BigData: Discrimination in Data-Supported Decision Making*, Wiedeń 2018.

¹¹⁴ Raport wydany przez Radę Europy wskazuje np. na co najmniej sześć powodów, w związku z którymi algorytmy mogą być dyskryminujące, takich jak: sposób definiowania zmiennej docelowej (*target variable*) i opisów klas (*class labels*), określanie danych używanych do trenowania algorytmu, zbieranie i trenowanie danych, wybieranie istotnych cech, tworzenie połączeń między danymi a kategoriami oraz celowe tworzenie dyskryminacyjnych algorytmów. Zob. F. Zuiderveen Borgesius, *Discrimination, Artificial Intelligence, and Algorithmic Decision-Making*, Strasburg 2018, s. 10, oraz 10–14 charakterystyka tych przyczyn. Pierwsze pięć wymienionych przyczyn opiera się na klasyfikacji autorstwa Barocas i Selbst, zob. S. Barocas, A.D. Selbst, *op. cit.*

mediów społecznościowych ofert pracy w obszarze STEM¹¹⁵, jak również ofert edukacji w obszarze STEM dla nastolatków¹¹⁶ czy różnicowanie decyzji zarówno ze względu na płeć, jak i na etniczność w ocenie prawdopodobieństwa recydywy ocenianym przez system COMPAS¹¹⁷. Ich wyniki wskazują na fakt, że kryterium, zgodnie z którym dochodzi do nierównego traktowania, może należeć do cech, ze względu na które dyskryminacja jest zakazana w prawie europejskim. Stąd też należy bliżej przyjrzeć się specyfice potencjału dyskryminacyjnego zautomatyzowanego podejmowania decyzji¹¹⁸ oraz barierom dla jego większej przejrzystości.

1.2.1. Stronniczość zautomatyzowanego podejmowania decyzji

Problemy pojawiające się w związku z rozwojem zautomatyzowanych rozwiązań i koniecznością stosowania w nich uogólnień były odnotowane już w latach 80. ubiegłego wieku¹¹⁹. Pewien stopień generalizacji był wtedy postrzegany jako niezbędny dla rozwoju technologii, takich jak uczenie maszynowe (*machine learning*). Jednocześnie już wówczas zjawisko stronniczości algorytmicznej (*algorithmic bias*, również *machine bias*), polegające na reprodukowaniu istniejących nierówności lub nawet wzmacnianiu ich przez zastosowanie algorytmizowanych procedur, budziło niepokój badaczy. Ze względu na brak odpowiedniego polskiego słowa, oddającego pełnię znaczenia terminu *bias*, posługuję się słowem „stronniczość”, jednocześnie jednak starając się umieszczać angielskie pierwowzory pojawiających się wyrażen, ze względu na niedoskonałość polskiej terminologii.

Za źródła stronniczości algorytmicznej mogą zostać uznane dwa elementy, czyli dane wykorzystywane przez algorytm oraz sam algorytm¹²⁰. Ze względu na to, że algorytmy są trenowane na historycznych danych, wyniki uzyskane przez ich stosowanie mogą replikować i odzwierciedlać stan z momentu

¹¹⁵ A. Lambrecht, C. Tucker, *Algorithmic Bias? An Empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads*, 2018. <https://ssrn.com/abstract=2852260>, dostęp: 1.04.2021.

¹¹⁶ G. Cecere, C. Jean, F. Le Guel, M. Manant, *STEM and Teens: An Algorithm Bias on a Social Media*, 2018. <https://ssrn.com/abstract=3176168>, dostęp: 1.04.2021.

¹¹⁷ J. Angwin, J. Larsona, S. Mattu, L. Kirchner, *op. cit.*

¹¹⁸ Pogłębiony przegląd literatury na temat zagadnienia zautomatyzowanego podejmowania decyzji i stronniczości, zob. np. R. Binns, *Algorithmic Accountability and Public Reason*, „Philosophy & Technology” 2018, t. 31, nr 4, s. 547.

¹¹⁹ T. Mitchell, *The Need for Biases in Learning Generalizations*, „Techreport” 1980. <https://www.semanticscholar.org/paper/The-Need-for-Biases-in-Learning-Generalizations-Mitchell/6cf35ec34efa592f83e3a1b748aea14957fc784a>, dostęp: 1.04.2021.

¹²⁰ Zob. J. Weizenbaum, *Computer Power and Human Reason: From Judgment to Calculation*, W.H. Freeman and Company, San Francisco 1976.

pozyskania danych użytych do trenowania algorytmu (*training data bias*¹²¹). Jako przykład może posłużyć algorytm stosowany w latach 80. w procesie rekrutacji do St. George's Hospital Medical School w Londynie. W związku z tym, że historycznie patrząc, studenci przyjmowani do szkoły byli białymi mężczyznami, po kilku latach stosowania algorytmu okazało się, że replikuje on taki stan rzeczy, automatycznie obniżając punktację osób, których nazwisko lub miejsce urodzenia wskazuje na niekawkaską etniczność¹²². Z kolei sposób, w jaki algorytm jest napisany, może prowadzić np. do nadawania większej wagi przez jego twórców zmiennym ściśle związanym z etnicznością (np. kod pocztowy jako wskaźnik pozwalający ocenić etniczność i status materialny danej osoby czy – w USA – informacja na temat tego, czy doświadczyło się postrzelenia kogoś w swoim sąsiedztwie lub rodzinie), przez co wyniki danej grupy etnicznej z założenia mogą się różnić od innych, jedynie w związku z potraktowaniem danej zmiennej jako kluczowej (*algorithmic focus bias*¹²³). W ramach rodzajów stronniczości algorytmu można ponadto wskazać na te związane z przetwarzaniem danych (*algorithmic processing bias*), czyli np. w wyniku grupowania danych w określony sposób.

Dodatkowo należy zwrócić uwagę na dwa kolejne typy stronniczości algorytmu, które wiążą się z otoczeniem, w którym jest on używany. Po pierwsze, jest to stronniczość związana ze zmianą kontekstu (*transfer context bias*). Wynika ona ze stworzenia i rozwijania algorytmu w danych warunkach. Przykładem może być oparcie algorytmu mającego wspierać diagnozę danej choroby skóry jedynie na białych pacjentach. Próba zastosowania go wobec osób o innym kolorze skóry może wykazać, że algorytm ma mniejszą skuteczność. Po drugie zaś, jest to stronniczość interpretacyjna (*interpretation bias*). Może ona wynikać zarówno z ludzkich działań podjętych w ramach interpretacji rezultatów proponowanych przez algorytm, jak i w wyniku interpretacji rezultatów podawanych przez algorytm przez inne algorytmy wchodzące w ramy tego samego zautomatyzowanego systemu¹²⁴. Problemy wiążące się z interpretacją wyników zautomatyzowanego podejmowania decyzji wynikają m.in. z wiary w obiektywizm technologii¹²⁵. Tymczasem

¹²¹ D. Danks, A.J. London, *Algorithmic Bias in Autonomous Systems*, „Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI-17)” 2017, s. 4692. https://www.researchgate.net/profile/Alex_London/publication/318830422_Algorithmic_Bias_in_Autonomous_Systems/links/5a4bb017aca2729b7c893d1b/Algorithmic-Bias-in-Autonomous-Systems.pdf, dostęp: 1.04.2021.

¹²² O. Schwartz, *Untold History of AI: Algorithmic Bias Was Born in the 1980s*, „IEEE Spectrum” 2019. <https://spectrum.ieee.org/tech-talk/tech-history/dawn-of-electronics/untold-history-of-ai-the-birth-of-machine-bias>, dostęp: 17.04.2019.

¹²³ D. Danks, A.J. London, *op. cit.*, s. 4693.

¹²⁴ *Ibidem*, s. 4694.

¹²⁵ V. Eubanks, *Automating Inequality...*, *op. cit.*

wskazane powyżej przyczyny sprawiają, że w rzeczywistości nie jest trudno zakwestionować ów domniemany obiektywizm technologii.

Należy podkreślić, że stronniczość, która może występować w ramach zautomatyzowanego podejmowania decyzji, nie musi mieć charakteru dyskryminacyjnego. Istnieją badania wykazujące, że zastosowanie zautomatyzowanego podejmowania decyzji może mieć pozytywny wpływ na niedoreprezentowane grupy¹²⁶. Jednocześnie część badaczy twierdzi, że zautomatyzowane podejmowanie decyzji ma inherentnie dyskryminujący charakter. Ich zdaniem pogląd ten znajduje uzasadnienie w samej strukturze mechanizmów pozwalających na zautomatyzowane podejmowanie decyzji, czyli w podejmowaniu decyzji w stosunku do jednostek na podstawie wpisania ich do danej grupy¹²⁷.

Tak radykalna perspektywa nie jest jednak prezentowana w tej analizie. Stoję na stanowisku, zgodnie z którym zautomatyzowane podejmowanie decyzji może kamuflować dyskryminacyjne mechanizmy wpisane w kod komputerowy. Obecność tych dyskryminujących mechanizmów tworzy problemy na tle zakazu dyskryminacji w prawie europejskim. Dlatego konieczne jest dążenie do większej przejrzystości w zakresie informacji na temat stosowania zautomatyzowanego podejmowania decyzji¹²⁸. Jednym z elementów takiego ostrożnego podejścia do zautomatyzowanego podejmowania decyzji powinno być dbanie o przejrzystość algorytmów. To przejrzystość stanowi

¹²⁶ Zob. B. Cowgill, C. Tucker, *Algorithmic Bias: A Counterfactual Perspective*, „Working Paper: NSF Trustworthy Algorithms” 2017, s. 2. <https://bitlab.cas.msu.edu/trustworthy-algorithms/whitepapers/Bo%20Cowgill.pdf>, dostęp: 1.04.2021.

¹²⁷ „Użycie zaalgorytmizowanego profilowania dla alokacji zasobów jest, w pewnym sensie, inherentnie dyskryminacyjne. Profilowanie ma miejsce, kiedy podmioty danych są grupowane w kategorie w zależności od różnych zmiennych, a decyzje podejmowane są w oparciu o to, że podmioty danych pasują do zdefiniowanych w ten sposób grup”. B. Goodman, S. Flaxman, *European Union Regulations on Algorithmic Decision-Making and a “Right to Explanation”*, „2016 ICML Workshop on Human Interpretability in Machine Learning (WHI 2016)” 2016, s. 4. <https://arxiv.org/abs/1606.08813>, dostęp: 1.04.2021.

¹²⁸ O poczuciu, że używanie części technologicznych nowinek powinno być traktowane z dużą dozą ostrożności świadczy również propozycja Komisji, która sugeruje wydzielenie sektorów szczególnego ryzyka, w których wdrażanie technologii wykorzystujących SI miałyby być obwarowane zestawieniem wymogów dotyczących m.in. jakości danych używanych do rozwijania systemów, zob. Komisja, *Biała księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania*, COM (2020) 65 final. Dokument ten omawiam w artykule J. Mazur, *Unia Europejska wobec rozwoju sztucznej inteligencji: proponowane strategie regulacyjne a budowanie jednolitego rynku cyfrowego*, „Europejski Przegląd Sądowy” 2020, nr 9, s. 13–18. Propozycja ta w odniesieniu do poszczególnych zastosowań SI w ramach danych sektorów została podtrzymana w propozycji wniosku legislacyjnego Komisji dotyczącego regulacji SI, zob. *Akt w sprawie SI* (w tym zwłaszcza art. 6 oraz załącznik II i III), w którym jednocześnie została sformułowana propozycja wydzielenia zastosowań SI, które łączą się z ryzykiem niemożliwym do zaakceptowania i dlatego powinny być zakazane.

jeden z warunków umożliwiających wykrywanie dyskryminacyjnych mechanizmów i dążenie do ich eliminacji.

1.2.2. Bariery dla przejrzystości zautomatyzowanego podejmowania decyzji

Źródła trudności w zakresie zwiększenia przejrzystości algorytmów są zróżnicowane i obejmują nie tylko bariery prawne. Poniższy opis opiera się na klasyfikacji wypracowanej przez Jennę Burrell¹²⁹. Wskazuje ona trzy grupy przeszkód w zakresie przejrzystości algorytmów: brak przejrzystości jako celowe utajnienie informacji ze strony korporacji lub państwa¹³⁰, brak przejrzystości jako wynik braku kompetencji cyfrowych i brak przejrzystości jako sposób funkcjonowania algorytmów w związku ze skalą ich stosowania.

Celowym działaniem podejmowanym przez państwo i zmniejszającym poziom przejrzystości systemów zautomatyzowanego podejmowania decyzji może być również uznanie danego algorytmu za informację niejawną. Sytuacja taka może mieć szczególne znaczenie dla algorytmów używanych w dziedzinach związanych z bezpieczeństwem publicznym i porządkiem publicznym. Jednocześnie jednak przykład wyroku holenderskiego sądu dotyczącego systemu SyRI używanego w Królestwie Niderlandów do oceny zagrożenia stwarzanego przez jednostkę w zakresie np. oszustw dotyczących korzystania z pomocy państwa ukazuje, że nawet zautomatyzowane rozwiązania używane w celu ochrony interesów państwa mogą być ocenione jako naruszające prawa jednostki¹³¹. Niejawny charakter tego typu rozwiązań może znacznie utrudniać pozyskiwanie dostępu do informacji na temat ich działania. Powinien on jednocześnie być przedmiotem debaty publicznej i kontroli sądowej w celu rozważenia możliwości balansowania między różnymi wartościami zagrożonymi przez niejawność bądź nadmierną przejrzystość zautomatyzowanego podejmowania decyzji.

¹²⁹ J. Burrell, *How the machine "thinks": Understanding opacity in machine learning algorithms*, „Big Data and Society” 2016, t. 3, nr 1, s. 1–12. Inny przegląd barier dla przejrzystości algorytmów przedstawia: M. Temme, *Algorithms and Transparency in View of the New General Data Protection Regulation*, „European Data Protection Law Review” 2017, t. 3, nr 4, s. 476–480, w którym zwraca uwagę m.in. na barierę dla przejrzystości w postaci samouczących się algorytmów.

¹³⁰ Omówienie tych zagadnień jako przeszkody do tworzenia wyjaśnień decyzji podejmowanych w sposób zautomatyzowany, zob. M. Brkan, G. Bonnet, *Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas*, „European Journal of Risk Regulation” 2020, t. 11, nr 1, s. 39–46.

¹³¹ Zob. Rechtbank Den Haag, SyRI, 5.2.2020, C-09-550982 HA ZA 18- 388, ECLI:NL:RBDHA:2020:865. <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2020:865>, dostęp: 1.04.2021.

Brak przejrzystości, jako celowe utajnienie informacji ze strony korporacji lub państwa, jest związany również m.in. z ochroną programów komputerowych jako własności intelektualnej oraz tajemnic handlowych. W państwach członkowskich UE ochrona programów komputerowych została uregulowana *dyrektywą Rady 91/250/EWG z 14.05.1991 r. w sprawie ochrony prawnej programów komputerowych*¹³², zmienioną następnie *dyrektywą 2009/24/WE*¹³³. Ponadto w sytuacji, w której mamy do czynienia z wynalazkiem realizowanym dzięki wykorzystaniu programu komputerowego, możliwe staje się również uzyskanie ochrony patentowej¹³⁴. Program komputerowy zawiera algorytm wyrażony w formie cyfrowej. Tym samym algorytm utrwalony jako program komputerowy wykorzystywany w systemie zautomatyzowanego podejmowania decyzji może być objęty ochroną prawnoautorską (choć sam algorytm, jako abstrakcyjny sposób rozwiązania danego problemu, nie może jej podlegać). Trudniejsze do wyobrażenia jest zastosowanie wynalazku realizowanego dzięki wykorzystaniu programu komputerowego do zautomatyzowanego podejmowania decyzji. Dlatego też ochrona patentowa w tym przypadku ma mniejsze znaczenie.

Objęcie programów komputerowych ochroną prawnoautorską nie jest tożsame z utrudnieniem dostępu do ich treści, lecz stanowi barierę w zakresie możliwości podejmowania działań mających na celu eksperymentowanie z nimi, np. w celu dekompilacji (używanej jako metoda służąca *reversed engineering*). Dekompilacja oznacza „czynność polegającą na przekształceniu wersji wynikowej programu komputerowego do wersji źródłowej”¹³⁵ programu. Stanowi ona narzędzie umożliwiające np. próbę oceny, jakiego typu zmienne brane są pod uwagę podczas determinowania wyniku zastosowania algorytmu. Na podstawie art. 6 *dyrektywy 2009/24/WE*¹³⁶ oraz dotychczasowego orzecznictwa TSUE¹³⁷ można stwierdzić, że dekompilacja jest do pewnego stopnia dozwolona w ramach istniejącego w UE reżimu ochrony

¹³² *Dyrektywa Rady z dnia 14 maja 1991 r. w sprawie ochrony prawnej programów komputerowych*, Dz.Urz. WE 1991 L 122, s. 42–46. Zob. F. Rodaniewicz, *Ochrona programów komputerowych w prawie UE (cz. I)*..., op. cit., s. 22–29.

¹³³ *Dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE z dnia 23 kwietnia 2009 r. w sprawie ochrony prawnej programów komputerowych (Wersja skodyfikowana) (Tekst mający znaczenie dla EOG)* (dyrektywa 2009/24/WE), Dz.Urz. UE 2009 L 111, s. 16–22.

¹³⁴ A. Grabowski, *Kumulacja ochrony programu komputerowego prawem autorskim i patentowym, w przypadku udzielenia skutecznego w Polsce patentu europejskiego na wynalazek realizowany przy użyciu programu komputerowego – część I*, „Studia Prawnicze i Administracyjne” 2013, nr 2, s. 51–57.

¹³⁵ F. Rodaniewicz, *Ochrona programów komputerowych w prawie UE (cz. II)*, „Europejski Przegląd Sądowy” 2009, nr 5, s. 28.

¹³⁶ *Ibidem*, s. 28.

¹³⁷ Zob. Wyrok Trybunału z dnia 2 maja 2012 r. w sprawie C-406/10, *SAS Institute Inc. przeciwko World Programming Ltd.*, ECLI:EU:C:2012:259 oraz P. Ciancarini, D. Russo,

programów komputerowych. Celem, który umożliwia legalną dekompilację, jest osiągnięcie interoperacyjności¹³⁸. Ten warunek nie pozwala jednak uzasadnić przeprowadzenia legalnej dekompilacji w celu np. próby określenia, czy dany algorytm ma potencjał dyskryminacyjny czy go nie ma. Tym samym należy stwierdzić, że istnieją elementy prawnoautorskiej ochrony programów komputerowych, które w świetle zautomatyzowanego podejmowania decyzji mogą stanowić przeszkodę do osiągnięcia większego stopnia ich przejrzystości.

Innym elementem z zakresu ochrony prawnoautorskiej, który może wpływać na przejrzystość stosowanych rozwiązań, są postanowienia umów licencyjnych zawieranych w sytuacji korzystania z oprogramowania danego przedsiębiorstwa przez np. administrację publiczną. Jak stwierdza Ryszard Markiewicz:

Ograniczenia w eksploatacji programu źródłowego przez podmiot praw autorskich lub licencjobiorcę uprawnionego do wprowadzania zmian do programu mogą mieć swą podstawę tylko w zobowiązaniach umownych co do niekorzystania z programu źródłowego w oznaczonym zakresie lub mogą powstać w sytuacji, gdy wejście w posiadanie tej wersji programu doszło w warunkach czynu z art. 11 ustawy o zwalczaniu nieuczciwej konkurencji¹³⁹.

Tym samym prawdopodobna jest sytuacja, w której postanowienia umowy będą prowadzić do braku dostępu podmiotu korzystającego z oprogramowania np. na zasadach „oprogramowanie jako usługa” (*Software as a Service*) do kodu źródłowego oprogramowania.

Ponadto – na co wskazuje cytowana uwaga Markiewicza – przeszkodę dla dostępu do algorytmów stanowi ochrona danych rozwiązań jako tajemnicy przedsiębiorstwa. W UE kwestie dotyczące tajemnic przedsiębiorstwa zostały zharmonizowane *dyrektywą 2016/943*¹⁴⁰. Ochrona tajemnicy przed-

A. Sillitti, G. Succi, *Reverse engineering: a European IPR perspective*, „SAC ‘16 Proceedings of the 31st Annual ACM Symposium on Applied Computing” 2016, s. 1498–1503.

¹³⁸ „[...] jest niezbędne do otrzymania informacji koniecznych do osiągnięcia interoperacyjności niezależnie stworzonego programu komputerowego z innymi programami”. Art. 6, *dyrektywa 2009/24/WE*.

¹³⁹ R. Markiewicz, *Kłopoty z programem źródłowym*, „Zagadnienia Naukoznawstwa” 2015, nr 3(205), s. 316.

¹⁴⁰ *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem (Tekst mający znaczenie dla EOG)* (dyrektywa 2016/943), Dz.Urz. UE 2016 L 157, s. 1–18. Porównawcza analiza europejskiego podejścia i ram prawnych dotyczących napięcia między ochroną tajemnic przedsiębiorstwa i prawem dostępu do informacji, zob. S.K. Sandeen, U.-M. Mylly, *Trade Secrets and the Right to Information: A Comparative Analysis of E.U. and U.S. Approaches to Freedom of Expression and Whistleblowing*, „North Carolina Journal of Law & Technology” 2020, t. 21, nr 3, s. 1–61.

siębiorstwa jest typowym przykładem celowej tajności stosowanej przez dane przedsiębiorstwo, która ma na celu zagwarantowanie sobie przewagi opartej na posiadaniu unikatowej technologii. Chociaż mogą istnieć przyczyny uzasadniające utajnianie technologicznych rozwiązań używanych w ramach zautomatyzowanego podejmowania decyzji¹⁴¹, rozwiązania takie są wdrażane kosztem przejrzystości i możliwości kontrolowania zasad działania technologii. Ochrona własności i przedsiębiorczości – w razie objęcia algorytmów używanych w ramach zautomatyzowanego podejmowania decyzji tajemnicą przedsiębiorstwa – stają się wartościami, których wagę trzeba zestawiać z ochroną jednostek oraz grup przed potencjalną dyskryminacją wynikającą ze stosowania zautomatyzowanego podejmowania decyzji. Warto przy tym zwrócić uwagę na przepis art. 1 ust. 2 lit. b *dyrektywy 2016/943*, zgodnie z którym możliwe jest:

[...] stosowanie przepisów unijnych lub krajowych wymagających od posiadaczy tajemnicy przedsiębiorstwa ujawnienia – z uwagi na interes publiczny – informacji, w tym tajemnic przedsiębiorstwa, organom publicznym, administracyjnym lub sądowym w celu wykonywania obowiązków tych organów¹⁴².

W odniesieniu do algorytmów rozwijanych przez prywatne przedsiębiorstwa i używanych przez publiczne instytucje lub w celu świadczenia usług publicznych można postawić pytanie, czy powołany przepis nie pozwala – przynajmniej organom publicznym – na pozyskanie informacji dotyczących stosowanego algorytmu, nawet jeśli jest on chroniony jako tajemnica przedsiębiorstwa. Wyjątek ten nie rozwiązuje jednak całokształtu problemów związanych z brakiem kontroli nad zautomatyzowanym podejmowaniem decyzji i brakiem informacji dotyczących zasad, na jakich się ono odbywa.

Ponadto w odniesieniu do systemów zautomatyzowanego podejmowania decyzji stosowanego w sektorze publicznym jawność mogą ograniczać również przepisy dotyczące ochrony informacji niejawnych¹⁴³. W związku z faktem, że zagadnienia te regulowane są na poziomie państw członkowskich, nie zajmuję się nimi w rozprawie jako osobnym problemem badawczym.

¹⁴¹ „Istnieją ważne przyczyny, w związku z którymi polityka utajniania informacji w odniesieniu do zautomatyzowanego podejmowania decyzji jest uzasadniona. Ujawnianie kodu źródłowego oraz danych wykorzystywanych do analizy może prowadzić do wyjawienia tajemnicy przedsiębiorstwa, naruszeń prywatności, utrudnień w egzekwowaniu prawa i prowadzić do igrania procesami podejmowania decyzji”. J.A. Kroll, J. Huey, S. Barocas, E.W. Felten, J.R. Reidenberg, D.G. Robinson, H. Yu, *Accountable Algorithms*, „University of Pennsylvania Law Review” 2017, t. 165, s. 705.

¹⁴² Art. 1 ust. 2 lit. b, *dyrektywa 2016/943*.

¹⁴³ W Polsce regulowane przez *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*, Dz.U. 2010 nr 182 poz. 1228. Za wskazanie tego problemu dziękuję recenzentowi mojej rozprawy doktorskiej, dr. hab. prof. UG Grzegorzowi Wierczyńskiemu.

Ze względu na fakt, że możliwość zastrzeżenia przez państwa tajności pewnych informacji jest przewidziana w EKPCz, przedstawiam analizę warunków, które muszą spełnić państwa, aby powoływać się na wyjątki od prawa dostępu do informacji zgodnie z wykładnią ETPCz. Warto jednak w tym odniesieniu do możliwości ograniczania dostępu do algorytmów stosowanych w ramach zautomatyzowanego podejmowania decyzji jako informacji niejawniej wskazać na fakt, że samo uznanie algorytmu za informację niejawną stanowiłoby potwierdzenie, iż może być on postrzegany jako informacja.

Druga grupa przesłanek utrudniających osiągnięcie wyższego stopnia przejrzystości algorytmów wskazywana przez Burrell odnosi się do bardziej socjologicznego wymiaru. Zważywszy na wysoki poziom skomplikowania algorytmów używanych we współczesnej gospodarce, jest oczywiste, że brak kompetencji cyfrowych stanowi poważną barierę w zakresie zrozumienia zarówno sposobu działania, jak i potencjalnych konsekwencji wiążących się z zautomatyzowanym podejmowaniem decyzji. Problemem jest również brak kompetencji wśród polityków odpowiedzialnych za umożliwianie wykorzystania tego typu rozwiązań i ich brak wiedzy na temat tego, jak w rzeczywistości one działają. Podobnie problematyczny jest poziom zrozumienia narzędzi zautomatyzowanego podejmowania decyzji przez samych urzędników czy sędziów, którzy mają korzystać z ich wsparcia.

Trzecia grupa przyczyn wskazywanych przez Burrell to brak przejrzystości wynikający ze sposobu funkcjonowania algorytmów, w szczególności w związku ze skalą ich stosowania. Z jednej strony wiąże się ona z poziomem skomplikowania używanych współcześnie programów komputerowych, z drugiej zaś może być powiązana z technologiami używanymi do ich tworzenia i udoskonalania (czyli np. wspomnianymi powyżej narzędziami określanymi mianem SI: uczeniem maszynowym). W związku z tym algorytmy mogą być nie tylko trudne do wyjaśnienia szerszemu gronu odbiorców, ale i niekiedy niezrozumiałe dla ich twórców. Wśród innych wskazywanych przez badaczy barier przejrzystości algorytmów – wiążących się z tą kategorią – można wymienić konieczność ich utajnienia w celu zagwarantowania braku manipulacji sposobem ich działania przez zewnętrznych aktorów (np. uniknięcia prób zmiany wyników wyszukiwania, które mogłyby pojawić się w momencie, w którym algorytm byłby całkowicie jawny)¹⁴⁴. Ogrom skali zastosowania niektórych algorytmów sprawia, że ich nadmierna przejrzystość jest postrzegana jako zagrożenie.

Nieprzejrzystość algorytmów jest wypadkową wymienionych przyczyn. Środki prawne przyjmowane w celu złagodzenia skutków nieprzejrzystości odnoszą się w różnym stopniu do jej różnych źródeł, np. „prawo do

¹⁴⁴ A. Chander, *The Racist Algorithm*, „Michigan Law Review” 2017, t. 115, s. 1040.

wyjaśnienia” oraz inne rozwiązania dotyczące zautomatyzowanego podejmowania decyzji przyjęte na gruncie RODO nie zwiększają przejrzystości dotyczącej samych algorytmów, chociaż mogą ją zwiększyć w odniesieniu do konkretnych użytkowników, np. przez konieczność wyjaśnienia im logiki stojącej za daną decyzją. Złożoność problematyki przeszkód dla większej przejrzystości zautomatyzowanego podejmowania decyzji powoduje, że trudne jest zaproponowanie uniwersalnego rozwiązania. Analiza ma na celu eksplorację jednej ze ścieżek, którymi mogłaby podążać wykładnia istniejących przepisów dotyczących dostępu do informacji i dokumentów urzędowych. Przyświeca jej cel w postaci ochrony jednostki przed potencjalną dyskryminacją, która może być wynikiem stosowania mechanizmów zautomatyzowanego podejmowania decyzji, a która stoi w sprzeczności z zakazem dyskryminacji na gruncie prawa europejskiego.

1.2.3. Nieprzejrzyste zautomatyzowane podejmowanie decyzji w świetle zakazu dyskryminacji na gruncie prawa UE

Tytułem ogólnego wprowadzenia należy podkreślić, że w prawie UE zakaz dyskryminacji bywa postrzegany jako szczególny wyraz zasady ogólnej w postaci równego traktowania¹⁴⁵. Podczas gdy posługiwanie się pojęciem równości prowadzi do kładzenia nacisku na pozytywne działania mające na celu niwelowanie istniejących różnic w traktowaniu, to pojęcie niedyskryminacji¹⁴⁶ odsyła raczej do negatywnego charakteru obowiązków danych podmiotów, czyli zakazu dyskryminacyjnego traktowania¹⁴⁷. Jak zauważa Andrzej Wróbel,

¹⁴⁵ Zob. „Zasada równego traktowania stanowi zasadę ogólną prawa Unii, wyrażoną w art. 20 karty, której szczególnym wyrazem jest zasada niedyskryminacji ujęta w art. 21 ust. 1 karty”. Wyrok Trybunału z dnia 22 maja 2014 r. w sprawie C-356/12, *Wolfgang Glatzel przeciwko Freistaat Bayern*, ECLI:EU:C:2014:350, pkt 43. Zakaz dyskryminacji, jak pokazuje ten cytat, jest określany również jako zasada niedyskryminacji. Ze względu na przyjętą w analizie optykę, która kładzie nacisk na charakter zakazu dyskryminacji jako obowiązku danych podmiotów i wiążącego się z nim prawa jednostek, unikam posługiwania się pojęciem zasady.

¹⁴⁶ Sama zasada niedyskryminacji w prawie unijnym jest definiowana jako „jeden z wyrazów zasady równości w znaczeniu formalnym, odpowiadający zakazowi niekorzystnego traktowania podmiotów wyróżnionych na podstawie pewnej relewantnej cechy charakterystycznej, będącej niedozwolonym kryterium różnicującym”. A. Zawidzka-Łojek, *Źródła prawa antydyskryminacyjnego Unii Europejskiej*, [w:] *Prawo antydyskryminacyjne Unii Europejskiej*, red. A. Zawidzka-Łojek, A. Szczerba-Zawada, Instytut Wydawniczy EuroPrawo, Warszawa 2015, s. 57. Publikacja zawiera również odesłania do publikacji relewantnych dla poszczególnych aspektów tematu.

¹⁴⁷ Zob. również: „Równość od niedyskryminacji odróżnia charakter obowiązków spoczywających na władzy publicznej. W pierwszym wypadku mają one charakter pozytywny i polegają na podjęciu określonych działań na rzecz równości (np. uprzywilejowania pewnej grupy społecznej). W drugim – obowiązki mają charakter negatywny i polegają na powstrzymaniu się od pewnych działań, które naruszają zasadę równego traktowania”.

TSUE posługuje się pojęciami równości i niedyskryminacji naprzemiennie „w zależności od tego, czy chce zwrócić uwagę na aspekt pozytywny, czy też negatywny”¹⁴⁸ tego zagadnienia. Dlatego też uzasadnione jest traktowanie tych terminów jako odnoszących się do tych samych problemów, chociaż opisujących je z różnych perspektyw.

W książce zdecydowałam się posługiwać sformułowaniem „zakaz dyskryminacji” jako terminem najściślej ujmującym sposób określenia normy prawnej dotyczącej niedyskryminacji w art. 21 KPP. „Zakaz dyskryminacji” oznacza zakaz nierównego traktowania podmiotów w oparciu o daną przesłankę, np. narodowość, rasę czy płeć. Zakazowi temu odpowiada z kolei prawo do bycia traktowanym w sposób niedyskryminacyjny: „zakaz dyskryminacyjnego traktowania rodzi dla adresatów tego zakazu, zwłaszcza Unii i państw członkowskich, obowiązek niedyskryminacyjnego traktowania «każdego», któremu odpowiada podmiotowe prawo «każdego» żądania od podmiotów zobowiązanych takiego działania lub zaniechania”¹⁴⁹. Dlatego też przez pojęcie zakazu dyskryminacji rozumiem w analizie obowiązek odpowiednich podmiotów i odpowiadające mu prawo jednostek do niedyskryminacyjnego traktowania¹⁵⁰.

Wybór sformułowania „zakaz dyskryminacji” jako najtrafniejszego z punktu widzenia tematu wynika również ze specyfiki zautomatyzowanego podejmowania decyzji. Zautomatyzowane podejmowanie decyzji musi opierać się na przydziale jednostek do grup i różnicowaniu podejmowanych w stosunku do nich decyzji na podstawie określonych kryteriów¹⁵¹. Stąd też

A. Śledzińska-Simon, *Zasada równości i zasada niedyskryminacji w prawie Unii Europejskiej*, „Studia BAS” 2011, nr 2(26), s. 42.

¹⁴⁸ *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, red. A. Wróbel, C.H. Beck, Warszawa 2019, s. 4 (do art. 20).

¹⁴⁹ *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, op. cit., s. 4 (do art. 21).

¹⁵⁰ Jak wspomniałam powyżej, unikam natomiast perspektywy, w której niedyskryminacja postrzegana jest jako zasada. Stanowisko takie opieram na ustaleniach doktrynalnych Andrzeja Wróbla, które kładą nacisk na konieczność odczytywania art. 21 ust. 1 KPP właśnie jako prawa. Stanowisko takie nie jest do końca zgodne z orzecznictwem TSUE, w którym obecne są zarówno sformułowania świadczące o postrzeganiu zakazu dyskryminacji jako prawa, jak i jako zasady ogólnej niedyskryminacji, zob. „W orzecznictwie TS nadal konkurują ze sobą dwa odmienne podejścia do prawnego charakteru art. 21 ust. 1 Karty, a mianowicie stanowisko w sprawach *Egenberger* i *Cresco*, które uznaje ten przepis za bezwzględnie wiążący i samoistnie przyznający jednostkom egzekwowalne sądowo prawo podmiotowe, oraz w sprawach *ASM* i *IR*, które kwalifikuje art. 21 ust. 1 jako zawierający lub potwierdzający zasadę ogólną niedyskryminacji, która przyznaje jednostkom sądowo egzekwowalne prawo”. *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, op. cit., s. 5 (do art. 21). Ponieważ skutek przyjmowania obu perspektyw jest podobny, a znaczenie tej kwestii dla analizy jest znikome, pozostaję przy odesłaniach do odpowiedniej literatury rozwijającej ten wątek rozważań doktrynalnych.

¹⁵¹ M. Hildebrandt, *Profiling: From Data to Knowledge...*, op. cit., s. 548–552.

nacisk należy położyć raczej na kryteria, które są uznane za istotne w zakresie podejmowania danych decyzji, i postawienie pytania, czy są one dyskryminacyjne w świetle przesłanek, że względu na które jest zakazana dyskryminacja w prawie UE. Tą drogą możliwe jest stwierdzenie, czy zautomatyzowane podejmowanie decyzji – w zależności od tego, czy opiera się ono na kryteriach dyskryminacyjnych, czy nie – jest zgodne z zakazem dyskryminacji. Można wyobrazić sobie dążenie do tworzenia systemów zautomatyzowanego podejmowania decyzji, które miałyby za zadanie podejmowanie działań pozytywnych w celu realizacji zasady równego traktowania. Jednak skupienie się na takim scenariuszu oddaliłoby analizę od kluczowego dla tematu problemu, który widoczny jest już dzisiaj. Opisana stronniczość prowadzi do rozwoju rozwiązań technologicznych, które mogą być postrzegane jako oparte na dyskryminacyjnych mechanizmach. Właśnie te mechanizmy rodzą wątpliwości w świetle europejskich regulacji dotyczących zakazu dyskryminacji i stanowią motywację do poszukiwania możliwości zwiększenia poziomu przejrzystości zautomatyzowanego podejmowania decyzji.

W unijnym prawie pierwotnym jako pierwszy został uwzględniony zakaz dyskryminacji ze względu na przynależność państwową, stanowiący podstawę międzypaństwowej integracji gospodarczej oraz mający zastosowanie w zakresie zastosowania traktatów stanowiących UE (art. 18 TFUE). Można zastanawiać się, czy sam w sobie szeroki zakres zakazu dyskryminacji ze względu na przynależność państwową nie powinien być traktowany jako argument przemawiający za koniecznością gwarantowania wysokiego stopnia przejrzystości rozwiązań wykorzystujących zautomatyzowane podejmowanie decyzji. W sytuacji, w której kryteria podejmowania decyzji w zautomatyzowany sposób są nieznane, może się okazać, że stosowane są rozwiązania w sposób bezpośredni lub pośredni dyskryminujące poddane im jednostki ze względu na przynależność państwową. Przykładem prób podejmowanych w celu zapobieżenia takim sytuacjom jest regulacja nieuzasadnionego geoblokowania, czyli mechanizmu opartego na różnicowaniu np. cen lub warunków sprzedaży na podstawie lokalizacji geograficznej konsumenta, z której próbuje on uzyskać dostęp do danej oferty¹⁵². Zauważenie tego problemu w prawie UE świadczy o wadze zagwarantowania niedyskryminacyjnych rozwiązań w zakresie np. zautomatyzowanego kierowania do konsumentów ofert opartych na ocenie ich lokalizacji dla funkcjonowania rynku wewnętrznego w przestrzeni cyfrowej.

¹⁵² Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/302 z dnia 28 lutego 2018 r. w sprawie nieuzasadnionego blokowania geograficznego oraz innych form dyskryminacji klientów ze względu na przynależność państwową, miejsce zamieszkania lub miejsce prowadzenia działalności na rynku wewnętrznym oraz w sprawie zmiany rozporządzeń (WE) nr 2006/2004 oraz (UE) 2017/2394 i dyrektywy 2009/22/WE (Tekst mający znaczenie dla EOG) (rozporządzenie 2018/302), Dz.Urz. UE 2018 L 601, s. 1–15.

Wraz z rozwojem prawa unijnego wagi nabrała również kwestia regulacji dyskryminacji ze względu na inne przesłanki. W świetle art. 10 TFUE dążenie do zwalczania wszelkiej dyskryminacji ze względu na płeć, rasę lub pochodzenie etniczne, religię lub światopogląd, niepełnosprawność, wiek lub orientację seksualną przy określaniu i realizacji polityk i działań powinno stanowić podstawę aktywności UE. Przepis ten – w obliczu rozwoju technologii wykorzystujących zautomatyzowane podejmowanie decyzji – mógłby stać się inspiracją do poszukiwania niedyskryminacyjnych rozwiązań i podejmowania aktywnych działań w celu ich wdrażania. Jednocześnie art. 10 TFUE nie jest bezpośrednio skuteczny, dlatego też jego wpływ mógłby być jedynie zapośredniczony jako podstawa wydawania odpowiednich aktów prawa pochodnego.

Ponadto w związku z nadaniem KPP mocy wiążącej oraz rangi równej traktatom zakaz dyskryminacji stał się częścią prawa pierwotnego w zakresie określonym przez wspomniany powyżej art. 21 ust. 1 KPP¹⁵³. Zakaz dyskryminacji w tym artykule obejmuje takie przesłanki, jak: płeć, rasa, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religia lub przekonania, poglądy polityczne lub wszelkie inne poglądy, przynależność do mniejszości narodowej, majątek, urodzenie, niepełnosprawność, wiek i orientacja seksualna¹⁵⁴. Katalog ten ma charakter otwarty¹⁵⁵. Zakaz dyskryminacji w KPP, w przeciwieństwie do jego ujęcia w EKPCz, ma charakter autonomiczny, czyli dyskryminacja nie musi się wiązać z naruszeniem innego prawa gwarantowanego w KPP. Jednocześnie jego samodzielne stosowanie może występować „wyłącznie w sytuacjach podlegających prawu Unii, w odniesieniu do których Traktat nie zawiera szczególnych przepisów o zakazie dyskryminacji ze względu na przynależność państwową”¹⁵⁶.

Sam fakt uwzględnienia zakazu dyskryminacji w KPP jest jednocześnie świadectwem postrzegania tego zagadnienia nie tylko jako przeszkody do budowania rynku wewnętrznego (jak zakaz dyskryminacji ze względu na przynależność państwową), lecz także jako jednego z praw podstawowych

¹⁵³ *Karta praw podstawowych Unii Europejskiej*, Dz.Urz. UE 2012 C 326, s. 391–407.

¹⁵⁴ Analiza porównawcza zakazu dyskryminacji ze względu na przesłanki pojawiające się w KPP i ze względu na typy danych osobowych wymienianych w RODO jako szczególne kategorie danych, zob. J. Niklas, *Problem dyskryminacji automatycznej – uwagi na tle ogólnego rozporządzenia o ochronie danych osobowych*, „Europejski Przegląd Sądowy” 2019, nr 7, s. 4–9.

¹⁵⁵ Zob. J. Maliszewska-Nienartowicz, *Rozdział I. Pojęcie i źródła europejskiego prawa antydyskryminacyjnego*, [w:] *Prawo antydyskryminacyjne. System prawa Unii Europejskiej*, t. 6, red. J. Maliszewska-Nienartowicz, C.H. Beck, Warszawa 2020, s. 12. O tej cesze art. 21 KPP jako możliwej ścieżce gwarantującej jego skuteczność w odniesieniu do zalgorytmizowanej dyskryminacji, zob. R. Xenidis, *Tuning EU Equality Law to Algorithmic Discrimination: Three Pathways to Resilience*, „Maastricht Journal of European and Comparative Law” 2020, t. 27, nr 6, s. 736–758.

¹⁵⁶ *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, op. cit., s. 23 (do art. 21).

zasługujących na ochronę w obszarach objętych prawem UE. O wzmocnieniu znaczenia niedyskryminacji w prawie UE świadczy również fakt, że w treści art. 2 TUE znalazła się niedyskryminacja jako jedna z podstaw, na których oparte jest społeczeństwo i równość, oraz fundamentalnych zasad, na których powinna się opierać organizacja społeczeństw państw członkowskich oraz UE. Ukazuje to wagę zakazu dyskryminacji w ramach aksjologicznego wymiaru integracji europejskiej.

Mimo rosnącego znaczenia zakazu dyskryminacji w prawie UE problemem, który ma szczególną wagę dla ukazania jego praktycznego znaczenia, jest zakres stosowania przepisów go dotyczących. W przeciwieństwie do szerokiego zakresu zakazu dyskryminacji ze względu na przynależność państwową, który obowiązuje w „zakresie zastosowania Traktatów”, zakres obowiązywania zakazu dyskryminacji ze względu na inne przesłanki może rodzić wątpliwości. Zakaz dyskryminacji zawarty w KPP powinien być odczytywany jako obowiązujący w zakresie zastosowania KPP¹⁵⁷. Zgodnie z art. 51 ust. 1 KPP oznacza to, że ma on zastosowanie do instytucji, organów i jednostek organizacyjnych Unii przy poszanowaniu zasady pomocniczości oraz do państw członkowskich wyłącznie w zakresie, w jakim stosują one prawo Unii¹⁵⁸.

¹⁵⁷ Z kolei w odniesieniu do zakazu dyskryminacji z art. 21 KPP ust. 2 tego artykułu brzmi: „W zakresie zastosowania Traktatów i bez uszczerbku dla ich postanowień szczególnych zakazana jest wszelka dyskryminacja ze względu na przynależność państwową”, art. 21 ust. 2 KPP. Tym samym można by postawić pytanie o zakres znaczeniowy sformułowania „stosowanie prawa unijnego” (art. 51 ust. 1 KPP) i „zakres zastosowania Traktatów” (art. 21 ust. 2 KPP). TSUE wydaje się jednak niekonsekwentnie posługiwać tymi terminami (zob. E. François, *Zakres zastosowania Karty Praw Podstawowych UE*, „Europejski Przegląd Sądowy” 2016, nr 8, s. 19–20), w związku z czym – na potrzeby poniższej analizy – nie wydaje się uzasadnione zagłębianie się w ten temat.

¹⁵⁸ W świetle najnowszego orzecznictwa TSUE należy jednak odnotować możliwość szerszej wykładni zakresu zastosowania KPP, w tym szczególnie zakazu dyskryminacji. W sprawie *Vera Egenberger przeciwko Evangelisches Werk für Diakonie und Entwicklung eV*. TSUE przedstawił wykładnię KPP, zgodnie z którą zakaz dyskryminacji ze względu na religię i przekonania jest normą o charakterze bezwzględnie wiążącym. Dlatego też w formie uwzględnionej w art. 21 ust. 1 KPP zakaz ten „samoistnie przyznaje jednostkom prawo, na które mogą się one bezpośrednio powoływać w sporze dotyczącym jednej z dziedzin objętych prawem Unii”, w tym również w sporach między jednostkami. Wyrok Trybunału z dnia 17 kwietnia 2018 r. w sprawie C-414/16, *Vera Egenberger przeciwko Evangelisches Werk für Diakonie und Entwicklung eV*, ECLI:EU:C:2018:257, pkt 76; potwierdzone w odniesieniu do treści art. 21 ust. 1 w Wyrok Trybunału z dnia 6 listopada 2018 r. w sprawach połączonych C-569/16 i C-570/16, *Stadt Wuppertal przeciwko Marii Elisabeth Bauer i Volker Willmeroth przeciwko Martinie Broßonn*, ECLI:EU:C:2018:871, pkt 89. W orzeczeniu w sprawie *Bauer* TSUE potwierdził, że art. 21 ust. 1 KPP samoistnie przyznaje jednostkom prawo, na które mogą się one bezpośrednio powoływać w sporze z inną jednostką: „Jeśli chodzi o skutek art. 31 ust. 2 karty w odniesieniu do prywatnych pracodawców, należy zauważyć, że o ile art. 51 ust. 1 Karty stanowi, że jej postanowienia

Zakres zastosowania KPP prowadzi do konieczności zagwarantowania niedyskryminacyjnego charakteru systemów zautomatyzowanego podejmowania decyzji wdrażanych przez instytucje, organy i jednostki organizacyjne Unii (art. 21 ust. 1 w związku z art. 51 ust. 1 KPP). Zgodnie z treścią KPP w tych wypadkach należałoby rozważyć, czy zautomatyzowane rozwiązania nie dyskryminują na podstawie przesłanek zawartych w art. 21 KPP. W odniesieniu do państw członkowskich jest natomiast konieczne, aby w zakresie stosowania prawa unijnego zakaz dyskryminacji z art. 21 KPP był przez nie uwzględniany w razie wdrażania rozwiązań wykorzystujących zautomatyzowane podejmowanie decyzji. Tym samym możliwość odwołania do zakazu dyskryminacji przewidzianego w KPP w odniesieniu do zautomatyzowanego podejmowania decyzji wdrażanego w sektorze publicznym zależna jest od tego, w jaki sposób rozumiane jest pojęcie stosowania prawa

mają zastosowanie do instytucji, organów i jednostek organizacyjnych Unii, zgodnie z zasadą pomocniczości, oraz do państw członkowskich tylko wtedy, gdy wdrażają one prawo Unii, o tyle omawiany art. 51 ust. 1 nie odnosi się do kwestii, czy takie osoby mogą, w stosownych przypadkach, być bezpośrednio związane niektórymi postanowieniami wspomnianej karty, a zatem nie można go interpretować w ten sposób, że systematycznie wyklucza taką ewentualność”. Wyrok Trybunału z dnia 6 listopada 2018 r. w sprawach połączonych C-569/16 i C-570/16, *Stadt Wuppertal przeciwko Marii Elisabeth Bauer i Volker Willmeroth przeciwko Martinie Broßonn*, ECLI:EU:C:2018:871, pkt 67. Również wyrok TSUE w sprawie *Stadt Wuppertal przeciwko Marii Elisabeth Bauer i Volker Willmeroth przeciwko Martinie Broßonn* zasugerował wykładnię, zgodnie z którą istnieje możliwość wywierania przez przepisy zawarte w KPP skutku bezpośredniego w relacjach horyzontalnych. Argumentacja TSUE oparta została na braku wykluczenia takiej możliwości w treści art. 51 ust. 1 KPP. Zob. również Wyrok Trybunału z dnia 22 stycznia 2019 r. w sprawie C-193/17, *Cresco Investigation GmbH przeciwko Markusowi Achatziemmu*, ECLI:EU:C:2019:43 oraz komentarz do zagadnienia: J. Maliszewska-Nienartowicz, *Rozdział I. Pojęcie i źródła europejskiego prawa antydyskryminacyjnego*, [w:] *Prawo antydyskryminacyjne. System..., op. cit.*, s. 13–14. Tym samym orzecznictwo TSUE zdaje się iść w kierunku szerokiego postrzegania zakazu dyskryminacji przewidzianego w KPP jako obowiązującego zarówno w relacjach wertykalnych, jak i horyzontalnych. Podejście takie może być próbą przeciwdziałania skomplikowanemu i eklektycznemu stanowi prawnemu wynikającemu z przyjęcia opisanych poniżej aktów prawa wtórnego. Stworzony na ich podstawie system ochrony przed dyskryminacją w bardzo konkretnych obszarach i ze względu na wyselekcjonowane przesłanki jest niekompatybilny z tym, w jak szerokiej formie zakaz dyskryminacji przyjęty został w KPP. Stąd też mogą wynikać próby TSUE, który dąży do wykładni art. 21 KPP w sposób podkreślający konieczność postrzegania zakazu dyskryminacji, jako jednej z podstawowych norm dla unijnego porządku prawnego. Dopiero nadchodzące lata w pełni pozwolą ocenić, jaki kształt przybierze możliwość powoływania się na KPP, zwłaszcza zaś na art. 21 ust. 1, również w odniesieniu do relacji horyzontalnych. Wiele rozwiązań stosujących zautomatyzowane podejmowanie decyzji jest rozwijane i stosowane w sektorze prywatnym, dlatego też wykładnia zakresu zastosowania zakazu dyskryminacji może okazać się istotna dla spraw dotyczących tej kwestii. Jednocześnie horyzontalne stosowanie KPP nie jest istotne z punktu widzenia poniższej analizy, ze względu na jej koncentrację na zautomatyzowanym podejmowaniu decyzji wdrażanym w sektorze publicznym.

unijnego. Kwestia ta budzi kontrowersje wśród badaczy¹⁵⁹. Z orzecznictwa TSUE wynika, że nie jest możliwe powoływanie się na KPP jako samodzielną podstawę do twierdzenia, że prawo UE znajduje zastosowanie w danej sprawie. Niezbędne jest istnienie innego łącznika, takiego jak np. stosowanie przepisów krajowych będących transpozycją dyrektywy, element transgraniczny w danej sprawie, stosowanie przepisów prawa UE wywołujących skutek bezpośredni czy też rozporządzeń jako bezpośrednio stosowanych aktów prawa unijnego¹⁶⁰. W sytuacji, w której istniałby odpowiedni łącznik między stosowaniem systemu zautomatyzowanego podejmowania decyzji wdrażanego przez państwo a prawem unijnym, wydaje się konieczne, aby system ten był zgodny również z zakazem dyskryminacji, jako jednym z praw podstawowych gwarantowanych przez KPP.

Zagadnienie zakazu dyskryminacji w UE wymaga również odniesienia się do kwestii dotyczących dyskryminacji, które stały się przedmiotem regulacji w ramach prawa wtórnego. Ich przyjęcie wiąże się m.in. z uwzględnieniem w Traktacie z Amsterdamu (obecnie art. 19 TFUE¹⁶¹) normy kompetencyjnej,

¹⁵⁹ Zob. N. Półtorak, *Zakres związania państw członkowskich Kartą Praw Podstawowych Unii Europejskiej*, „Europejski Przegląd Sądowy” 2014, nr 9, s. 17–28; M. Szpunar, *Kilka uwag systematyzujących na temat zakresu zastosowania Karty Praw Podstawowych UE*, „Europejski Przegląd Sądowy” 2015, nr 10, s. 4–10; E. François, *op. cit.* Ponadto wątpliwości co do wykładni TSUE dotyczącej zakresu, w którym zakaz dyskryminacji powinien mieć zastosowanie, wiążą się m.in. z przywołanymi powyżej wątpliwościami co do jego charakteru. W sytuacjach, w których zakaz dyskryminacji jest przedstawiany jako zasada ogólna wynikająca z tradycji konstytucyjnych państw członkowskich oraz EKPCz, jego bezwzględnie wiążący w zakresie stosowania prawa UE charakter może być uzasadniany właśnie przez odwołanie do niego jako zasady ogólnej. Zob. J. Maliszewska-Nienartowicz, *Rozdział III: Konstrukcja prawna zakazu dyskryminacji oraz prawa do niedyskryminacyjnego traktowania*, [w:] *Prawo antydyskryminacyjne. System...*, *op. cit.*, s. 32–33.

¹⁶⁰ Jak podsumowuje to zagadnienie Emmanuel François: „Po pierwsze, Trybunał Sprawiedliwości nie odróżnia wyraźnie pojęć stosowania prawa unijnego, zakresu zastosowania, ram prawa unijnego czy elementów powiązania z tym prawem. Po drugie, wyłączone jest powoływanie się na postanowienia Karty w celu uzasadnienia ich zastosowania (wyklucza się błędne koło w rozumowaniu). Po trzecie, możliwość zastosowania *in abstracto* prawa UE nie jest wystarczająca, aby «uruchomić» stosowanie KPP. Po czwarte, postanowienia Karty mogą zostać zastosowane jedynie w odniesieniu do sytuacji podlegających prawu unijnemu. Innymi słowy, nie ma stanów faktycznych podlegających prawu unijnemu, w których nie można by uczynić użytku z przepisów Karty. Po piąte wreszcie, okoliczność, że uregulowanie krajowe dotyczy dziedziny podlegającej kompetencji Unii, nie wystarczy sama w sobie, aby skorzystać z postanowień Karty”. E. François, *op. cit.*, s. 20.

¹⁶¹ Zgodnie z art. 19 ust. 1 TFUE: „Bez uszczerbku dla innych postanowień Traktatów i w granicach kompetencji, które Traktaty powierzają Unii, Rada, stanowiąc jednomyślnie zgodnie ze specjalną procedurą ustawodawczą i po uzyskaniu zgody Parlamentu Europejskiego, może podjąć środki niezbędne w celu zwalczania wszelkiej dyskryminacji ze względu na płeć, rasę lub pochodzenie etniczne, religię lub światopogląd, niepełnosprawność, wiek lub orientację seksualną”.

która umożliwi UE przyjmowanie aktów prawnych dotyczących zwalczania wszelkiej dyskryminacji ze względu na płeć, rasę lub pochodzenie etniczne, religię lub światopogląd, niepełnosprawność, wiek lub orientację seksualną. Przyjęte dyrektywy w różnym zakresie regulują zagadnienia związane z dyskryminacją, w zależności od tego, na których przesłankach się ona opiera¹⁶². W literaturze odnotowuje się, że prowadzi to do wysokiego stopnia zróżnicowania zakresu przepisów antydyskryminacyjnych¹⁶³. Wynika to z potraktowania zagadnienia dyskryminacji ze względu na różne przesłanki i w różnych obszarach jako przedmiotów osobnych i szczegółowych regulacji.

Obecnie w zakresie regulacji aktów prawa wtórnego na temat równego traktowania na szczególną uwagę zasługuje *dyrektywa Rady 2000/43/WE*¹⁶⁴ dotycząca zasady równego traktowania bez względu na pochodzenie rasowe lub etniczne jako akt prawny mający najszerszy zakres wśród przyjętych dyrektyw antydyskryminacyjnych. Zgodnie z art. 3 ust. 1 jej zakres obejmuje osiem kategorii¹⁶⁵, m.in.: warunki dostępu do zatrudnienia lub pracy na własny

¹⁶² Zbiornicze omówienie dyrektyw, np.: D. Schiek, *A New Framework on Equal Treatment of Persons in EC Law? Directives 2000/43/EC, 2000/78/EC and 2002/??/EC changing Directive 76/207/EEC in context*, „European Law Journal” 2002, t. 8, nr 2, s. 290–314 oraz literatura przywoływana w *Prawo antydyskryminacyjne Unii Europejskiej, op. cit.* oraz *Prawo antydyskryminacyjne. System prawa Unii Europejskiej, op. cit.*

¹⁶³ „[...] materialny zakres stosowania danych przepisów antydyskryminacyjnych w prawie UE jest często ograniczony i nierówny. Na przykład dyrektywa 2000/78/WE odnosi się jedynie do kwestii zatrudnienia i wykonywania pracy, podczas gdy materialny zakres zastosowania dyrektywy 2000/43/WE jest znacznie szerszy i zawiera m.in. kwestie zabezpieczenia społecznego związanego z zatrudnieniem, dostępu do dóbr i usług, oraz inne kwestie takie jak edukacja czy ochrona społeczna. Wyjątkiem na tym tle jest zakaz dyskryminacji ze względu na narodowość, mający zastosowanie do całości unijnego prawa”. Ch. Tobler, *Equality and Non-Discrimination under the ECHR and EU Law A Comparison Focusing on Discrimination against LGBTI Persons*, „Zeitschrift für ausländisches öffentliches Recht und Völkerrecht” 2014, t. 74, s. 532.

¹⁶⁴ *Dyrektywa Rady 2000/43/WE z dnia 29 czerwca 2000 r. wprowadzająca w życie zasadę równego traktowania osób bez względu na pochodzenie rasowe lub etniczne* (dyrektywa Rady 2000/43/WE), Dz.Urz. WE 2000 L 180, s. 22–26 (polskie wydanie specjalne: rozdz. 20, t. 1, s. 23–27).

¹⁶⁵ „a) warunków dostępu do zatrudnienia, do prowadzenia działalności na własny rachunek oraz uprawiania zawodu, włączając również kryteria selekcji i warunków rekrutacji, niezależnie od rodzaju działalności i na wszystkich szczeblach hierarchii zawodowej, również w odniesieniu do awansu zawodowego; b) dostępu do wszystkich rodzajów i szczebli poradnictwa zawodowego, szkolenia zawodowego, doskonalenia i przekwalifikowania pracowników, łącznie ze zdobywaniem praktycznych doświadczeń; c) warunków zatrudnienia i pracy, łącznie z warunkami zwalniania i wynagradzania; d) wstępowania i działania w organizacjach pracowników lub pracodawców lub jakiegokolwiek organizacji, której członkowie wykonują określony zawód, łącznie z korzyściami jakie dają takie organizacje; e) ochrony społecznej, łącznie z zabezpieczeniem społecznym i opieką zdrowotną; f) świadczeń społecznych; g) edukacji; h) dostępu do dóbr i usług oraz dostarczania dóbr

rachunek oraz warunki zatrudnienia i pracy, ochronę społeczną, świadczenia społeczne czy edukację. Z kolei celem *dyrektywy Rady 2000/78/WE*¹⁶⁶ jest wyznaczenie ogólnych ram dla walki z dyskryminacją ze względu na religię lub przekonania, niepełnosprawność, wiek lub orientację seksualną w odniesieniu do zatrudnienia i pracy (art. 1). Zgodnie z art. 3 ust. 1 *dyrektywy 2000/78/WE* jej zakres zastosowania obejmuje kategorie dotyczące zatrudnienia i kształcenia zawodowego tożsame z tymi uwzględnionymi w *dyrektywie 2000/43*. W odróżnieniu od *dyrektywy Rady 2000/43/WE* nie odnosi się ona jednak do pozostałych obszarów dyskryminacji, np. edukacji czy świadczeń społecznych. *Dyrektywa 2006/54/WE*¹⁶⁷ dotyczy natomiast dyskryminacji ze względu na płeć w kwestiach dotyczących zatrudnienia i życia zawodowego (art. 14 ust. 1). Ponadto w *dyrektywie 2006/54/WE* został ujęty zakaz dyskryminacji ze względu na płeć w odniesieniu do wszelkich aspektów i warunków wynagrodzenia za taką samą pracę lub pracę o jednakowej wartości (art. 4), który w porządku prawnym UE został również ujęty w art. 157 TFUE. Zgodnie z art. 5 *dyrektywy 2006/54/WE* zakaz obejmuje ponadto dyskryminację ze względu na płeć w systemach zabezpieczenia społecznego pracowników¹⁶⁸. Również w wypadku *dyrektywy 2006/54/WE* jej zakres zastosowania jest węższy niż w wypadku aktu regulującego zakaz dyskryminacji ze względu na pochodzenie rasowe lub etniczne¹⁶⁹. Z kolei *dyrektywa Rady 2004/113/WE*¹⁷⁰, zgodnie z jej art. 3 ust. 1, dotyczy równego dostępu do towarów i usług oraz dostarczania towarów i usług bez względu na płeć. Należy podkreślić, że wszystkie wymienione dyrektywy odnoszą się do dyskryminacji bezpośredniej

i usług publicznie dostępnych, włącznie z zakwaterowaniem” – art. 3 ust. 1, *dyrektywa Rady 2000/43/WE*.

¹⁶⁶ *Dyrektywa Rady 2000/78/WE z dnia 27 listopada 2000 r. ustanawiająca ogólne warunki ramowe równego traktowania w zakresie zatrudnienia i pracy* (dyrektywa Rady 2000/78/WE), Dz.Urz. WE 2000 L 303, s. 16–22 (polskie wydanie specjalne: rozdz. 5, t. 4, s. 79–85).

¹⁶⁷ *Dyrektywa 2006/54/WE Parlamentu Europejskiego i Rady z dnia 5 lipca 2006 r. w sprawie wprowadzenia w życie zasady równości szans oraz równego traktowania kobiet i mężczyzn w dziedzinie zatrudnienia i pracy (wersja przedrządowana)* (dyrektywa 2006/54/WE), Dz.Urz. UE 2006 L 204, s. 23–36.

¹⁶⁸ Obejmujący: zakres zastosowania takich systemów i warunków przystępowania do nich, obowiązek opłacania i obliczania wysokości składek i obliczanie wysokości świadczeń, w tym świadczeń dodatkowych należnych małżonkowi lub osobie będącej na utrzymaniu, oraz warunków dotyczących okresu wypłaty świadczeń i zachowania prawa do nich.

¹⁶⁹ Zob. J. Maliszewska-Nienartowicz, *Rozdział I. Pojęcie i źródła europejskiego prawa antydyskryminacyjnego*, [w:] *Prawo antydyskryminacyjne. System...*, op. cit., s. 21.

¹⁷⁰ *Dyrektywa Rady 2004/113/WE z dnia 13 grudnia 2004 r. wprowadzająca w życie zasadę równego traktowania mężczyzn i kobiet w zakresie dostępu do towarów i usług oraz dostarczania towarów i usług* (dyrektywa Rady 2004/113/WE), Dz.Urz. UE 2004 L 373, s. 37–43.

i pośredniej¹⁷¹ oraz mają zastosowanie do wszystkich osób, zarówno sektora publicznego, jak i prywatnego, włącznie z instytucjami publicznymi¹⁷².

Głównym obszarem relacji między ramami prawnymi zakazu dyskryminacji a zautomatyzowanym podejmowaniem decyzji na gruncie prawa unijnego są kwestie związane z zatrudnieniem. Ze względu na fakt, że ochrona w odniesieniu do nich jest uwzględniona w trzech z przyjętych dyrektyw, przesłanki, w związku z którymi dyskryminacja jest zakazana, obejmują: płeć, pochodzenie rasowe lub etniczne, religię lub przekonania, niepełnosprawność, wiek i orientację seksualną. Tym samym systemy zautomatyzowanego podejmowania decyzji implementowane np. w zakresie dostępu do zatrudnienia powinny być zgodne z wymogami sformułowanymi w dyrektywach. Ponadto w odniesieniu do dyskryminacji opartej na pochodzeniu rasowym lub etnicznym w grę wchodzi konieczność zgodności z *dyrektywą Rady 2000/43/WE* rozwiązań wprowadzanych w pozostałych obszarach działań wymienionych w dyrektywie. Należałoby więc uwzględniać wymóg niedyskryminacji w zakresie zautomatyzowanego podejmowania decyzji odnoszącego się np. do edukacji czy opieki zdrowotnej w związku z przesłanką dotyczącą pochodzenia rasowego lub etnicznego. Kwestia dyskryminacji opartej na płci powinna natomiast być uwzględniana w związku z rozwiązaniami wdrażanymi w zakresie systemów zabezpieczenia społecznego pracowników. Ponadto powinna zostać zagwarantowana zgodność z zakazem dyskryminacji ze względu na płeć oraz pochodzenie etniczne i rasowe zautomatyzowanych rozwiązań wdrażanych w obszarze objętym regulacją dotyczącą dostępu do towarów i usług.

Podstawowym problemem związanym ze sformułowanymi powyżej postulatami dotyczącymi tego, jakie warunki powinno spełniać zautomatyzowane podejmowanie decyzji, jest brak dostępu do informacji umożliwiających weryfikację, czy dane rozwiązanie technologiczne jest z nimi zgodne¹⁷³. Z jednej strony, brak dostępu do kodu komputerowego stanowi barierę dla jednostek, które chciałyby zakwestionować ustaloną w ich sprawie decyzję i starać się wykazać, że została ona podjęta na podstawie dyskryminacyjnego traktowania. Z drugiej strony, działania państw członkowskich zostają w pewien sposób ukryte przed instytucjami UE. Potencjalnie w przypadku przyjęcia ustawy, która np. zawierałaby przepisy mówiące o tym, że

¹⁷¹ Art. 2 ust. 1, *dyrektywa Rady 2000/43/WE*; art. 2 ust. 1, *dyrektywa Rady 2000/78/WE*; art. 4, *dyrektywa Rady 2004/113/WE* oraz art. 4, *dyrektywa 2006/54/WE*.

¹⁷² Art. 3 ust. 1, *dyrektywa Rady 2000/43/WE*; art. 3 ust. 1, *dyrektywa Rady 2000/78/WE*; art. 3 ust. 1, *dyrektywa Rady 2004/113/WE* oraz art. 14 ust. 1, *dyrektywa 2006/54/WE* – w odniesieniu do art. 14 dyrektywy.

¹⁷³ Ciekawa propozycja systematyzacji zagadnień związanych z niekompatybilnością między prawem UE a dyskryminacyjnym potencjałem zautomatyzowanych rozwiązań, zob. R. Xenidis, *op. cit.*

dostęp do aktywizujących form wsparcia kierowanych do osób bezrobotnych faworyzuje mężczyzn, osoby w konkretnej grupie wiekowej i pochodzące z Polski, rozwiązanie takie mogłoby być kwestionowane jako dyskryminacyjne. Gdy jest ono wprowadzane na poziomie kodu komputerowego, do którego brak dostępu, wykazanie dyskryminacyjności takich rozwiązań staje się trudne¹⁷⁴.

Ponadto zautomatyzowane podejmowanie decyzji tworzy wyzwania w zakresie dyskryminacji ze względu na więcej niż jedno zabronione kryterium, czyli – zgodnie z terminologią proponowaną przez Monikę Domańską – dyskryminacji wielokrotnej *sensu stricto* (ze względu na więcej niż jedno kryterium, przy czym kryteria te oddziałują w różnym czasie i odgrywają inną rolę), dyskryminacji łączonej (ze względu na więcej niż jedno kryterium, których łączne oddziaływanie wpływa na sytuacje jednostki) i dyskryminacji zbieżnej, czyli „wspólnego/synergicznego działania wielu kryteriów na jeden podmiot, w jednym punkcie, w jednym czasie”¹⁷⁵. Szczególnie problematyczne jest zagadnienie dyskryminacji zbieżnej. Jest to problem, który nie znajduje dotychczas rozwiązania w prawie UE, a który może stawać się bardzo odczuwalny i jednocześnie zupełnie nieprzejrzysty w związku ze stosowaniem zautomatyzowanych rozwiązań¹⁷⁶. W wyniku podejmowania decyzji na podstawie segmentacji podmiotów poddanych danym decyzjom mogą zostać wyodrębnione grupy, które znajdują się w szczególnie nieuprzywilejowanej sytuacji, np. algorytm będzie najczęściej wybierał CV białych mężczyzn, następnie mężczyzn o innym niż biały kolorze skóry, następnie CV białych kobiet, po czym – najrzadziej – kobiet o niebiałym kolorze skóry. Taki sposób traktowania kobiet o niebiałym kolorze skóry spełnia kryteria definicyjne dyskryminacji zbieżnej. W efekcie ich stosowania pozycja tej grupy staje się radykalnie trudniejsza niż np. pozycja białych kobiet czy mężczyzn o niebiałym kolorze skóry. Jednocześnie w związku z nieprzejrzystym charakterem wdrażanych zautomatyzowanych rozwiązań trudno prowadzić działania mające na celu unikanie takiego sposobu projektowania

¹⁷⁴ Luźno nawiązuję tutaj do przypadku stosowania algorytmu profilującego osoby bezrobotne w Polsce, którego wnikliwą analizę przeprowadzili: K. Sztandar-Sztanderska, M. Kotnarowski, M. Zieleńska, *Czy algorytmy wprowadzają w błąd? Metaanaliza algorytmu profilowania bezrobotnych stosowanego w Polsce*, „Studia Socjologiczne” 2021, nr 1, s. 89–115. Profilowanie bezrobotnych w Polsce ostatecznie stało się przedmiotem postępowania przed Trybunałem Konstytucyjnym, zob. Wyrok Trybunału Konstytucyjnego, 11 K 53/16, 6 czerwca 2018 r., w którym za niezgodny z konstytucją został uznany brak ustawowej regulacji zbierania danych używanych do profilowania.

¹⁷⁵ Na ten temat zob. M. Domańska, *Zakaz dyskryminacji ze względu na więcej niż jedno zabronione kryterium*, Warszawa 2019 [Lex]. Za zwrócenie mi uwagi w recenzji na konieczność wspomnienia o tej kwestii dziękuję dr hab. prof. ALK Agnieszce Grzelak.

¹⁷⁶ Zob. R. Xenidis, *op. cit.*

systemów zautomatyzowanego podejmowania decyzji lub zarządzania ryzykiem pojawienia się tego typu dyskryminacyjnych mechanizmów. Dlatego szczególną rolę mogą odegrać rozwiązania oparte na zwiększaniu przejrzystości procedur zautomatyzowanego podejmowania decyzji, w tym badana w książce możliwość postrzegania algorytmów stosowanych w zautomatyzowanym podejmowaniu decyzji jako informacji publicznej lub dokumentów urzędowych.

Sytuacji, w których zautomatyzowane podejmowanie decyzji będzie wykorzystywane w obszarach objętych unijnym prawem, prawdopodobnie będzie coraz więcej, co zwiększa wagę opisanego problemu braku przejrzystości algorytmów¹⁷⁷. Jednocześnie zautomatyzowane podejmowanie decyzji nie stanowi odizolowanego problemu w odniesieniu do rozwoju nowych technologii i ich interakcji z prawem. Rozwój platform pośredniczących w możliwości wykonywania danej pracy ma kluczowy wpływ na kształtowanie współczesnych rynków pracy i utajnianie metod wyliczania wynagrodzenia¹⁷⁸. Niepewność w zakresie tego, kim jest osoba podejmująca pracę za pośrednictwem platformy, czy stopnia odpowiedzialności platform za umożliwianie przez nie pośrednictwo, powoduje kolejne utrudnienia w ocenie, czy stosowane rozwiązania są dyskryminujące. Przykładem wątpliwości, które mogą się pojawić, jest pytanie czy zalgorytmizowanie systemu wynagradzania pracowników oparte na nieznanymi kryteriach jest zgodne z art. 4 *dyrektywy 2006/54/WE* nakazującym wykluczenie wszelkiej dyskryminacji w wypadku ustalania wynagrodzenia opartego na systemie szeregowania pracowników¹⁷⁹. W obecnym stanie prawnym nie istnieją mechanizmy, które pozwalałyby kompleksowo ocenić, czy i do jakiego stopnia stosowane przez platformy rozwiązania technologiczne są dyskryminujące. Dlatego też refleksja nad rozwiązaniami prawnymi – nawet tymi obejmującymi jedynie część potencjalnie problematycznych sytuacji – umożliwiającymi weryfikację, czy w obszarach, w których ma zastosowanie unijne prawo, wprowadzane systemy wykorzystujące zautomatyzowane podejmowanie decyzji są niedyskryminujące, jest tak kluczowa.

¹⁷⁷ W literaturze jest poruszany również problem zmiany charakteru dyskryminacji ze względu na stosowanie SI. W kontekście prawa UE, zob. S. Wachter, B. Mittelstadt, Ch. Russell, *Why Fairness Cannot Be Automated: Bridging the Gap between EU Non-Discrimination law and AI*, „Computer Law & Security Review” 2021, t. 41, nr artykułu 105567.

¹⁷⁸ Zob. M. Kullmann, *op. cit.*

¹⁷⁹ „W szczególności, w przypadku gdy ustalanie wynagrodzenia odbywa się w oparciu o system szeregowania pracowników, za jego podstawę przyjmuje się te same kryteria w odniesieniu do kobiet i mężczyzn oraz sporządza się go w taki sposób, aby wykluczyć jakąkolwiek dyskryminację ze względu na płeć” – art. 4, *dyrektywa 2006/54/WE*.

1.2.4. Nieprzejrzyste zautomatyzowane podejmowanie decyzji w świetle zakazu dyskryminacji na gruncie prawa Rady Europy

Odminną perspektywę na zagadnienie zakazu dyskryminacji w prawie europejskim wnosi regulacja tego zagadnienia z EKPCz¹⁸⁰. W zakresie działalności Rady Europy podstawowym przepisem odwołującym się do zakazu dyskryminacji jest art. 14 EKPCz¹⁸¹. W jego ramach zostało przyjęte rozwiązanie, w którym zakaz dyskryminacji wiąże się z innymi prawami gwarantowanymi przez EKPCz. Dlatego, aby można było powołać się na art. 14, konieczny jest związek naruszenia z innym prawem zawartym w EKPCz¹⁸². W związku z takim ujęciem zakazu dyskryminacji wykładnia jego zakresu zależy od tego, w jaki sposób rozumiane są prawa gwarantowane przez EKPCz: „Z treści tego artykułu wyraźnie wynika, że w grę nie wchodzi ogólny zakaz dyskryminacji, ale tylko dyskryminacji w korzystaniu z praw i wolności wymienionych w materialnych postanowieniach Konwencji oraz w protokołach do niej”¹⁸³. Dlatego też uznawanie lub nieuznawanie danych praw, np. społecznych, jako gwarantowanych przez EKPCz, może rozszerzać lub ograniczać zakres obowiązywania zakazu dyskryminacji w świetle jego konstrukcji na tle EKPCz. Zgodnie z art. 14 EKPCz zakazana jest dyskryminacja ze względu na płeć, rasę, kolor skóry, język, religię, przekonania polityczne i inne, pochodzenie narodowe lub społeczne, przynależność do mniejszości narodowej, majątek, urodzenie, bądź z jakichkolwiek innych przyczyn. Katalog zawarty w art. 14 jest otwarty¹⁸⁴.

¹⁸⁰ Analiza zakazu dyskryminacji w EKPCz w świetle zautomatyzowanego podejmowania decyzji, zob. F.J. Zuiderveen Borgesius, *Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence*, „The International Journal of Human Rights” 2020, t. 24, nr 10, s. 1572–1593.

¹⁸¹ Kompleksowe omówienie ram prawnych zakazu dyskryminacji w porządkach prawnych UE i Rady Europy: Agencja Praw Podstawowych Unii Europejskiej, Rada Europy, *Handbook on European non-discrimination law. 2018 edition*, Luksemburg 2018.

¹⁸² „Korzystanie z praw i wolności wymienionych w niniejszej Konwencji powinno być zapewnione bez dyskryminacji [...]”. Jak formułuje to A. Schabas: „Artykuł 14 EKPCz gra przymiotnikową rolę, ponieważ jego odpowiedniość jest warunkowana stosowaniem jednego z innych samodzielnych praw wymienionych w Konwencji. Dlatego też, podczas gdy dyskryminacja ze względu na jedną z wymienionych przesłanek w odniesieniu do prawa do życia prywatnego i rodzinnego może stanowić naruszenie Konwencji, nie będzie to miało miejsca w odniesieniu do narodowości, ponieważ Konwencja nie gwarantuje prawa do narodowości”. W.A. Schabas, *The European Convention on Human Rights: a commentary*, Oxford University Press, Oxford 2015, s. 554.

¹⁸³ M.A. Nowicki, *Komentarz do Konwencji o ochronie praw człowieka i podstawowych wolności*, [w:] *Wokół Konwencji Europejskiej. Komentarz do Europejskiej Konwencji Praw Człowieka*, wyd. 7, Wolters Kluwer Polska, Warszawa 2017 (do art. 14).

¹⁸⁴ Agencja Praw Podstawowych Unii Europejskiej, Rada Europy, *op. cit.*, s. 60.

Rozszerzenie zakresu zakazu dyskryminacji nastąpiło w wyniku przyjęcia protokołu 12 do EKPCz¹⁸⁵. Zgodnie z protokołem 12 korzystanie z każdego prawa przewidzianego w prawie powinno być zapewnione bez dyskryminacji wynikającej z takich powodów, jak płeć, rasa, kolor skóry, język, religia, przekonania polityczne lub inne, pochodzenie narodowe lub społeczne, przynależność do mniejszości narodowej, majątek, urodzenie lub z jakichkolwiek innych przyczyn (protokół 12 do EKPCz, art. 1). Zmiana dotyczy zatem praw, do których odnosi się przepis: nie są to już prawa i wolności wymienione w EKPCz, ale wszystkie prawa gwarantowane w danym państwie. Dla państw, które ratyfikowały protokół 12, obowiązek zagwarantowania niedyskryminacyjnego traktowania w odniesieniu do zautomatyzowanych rozwiązań powinien dotyczyć wszelkich kwestii odnoszących się do praw jednostki, niezależnie od uwzględnienia tego prawa w katalogu praw sformułowanym w EKPCz.

Ze względu na niesamodzielny charakter art. 14 EKPCz zakaz dyskryminacji można postrzegać jako związany z zautomatyzowanym podejmowaniem decyzji w zakresie, w jakim może prowadzić ono do naruszenia innych praw gwarantowanych przez EKPCz. Typowym przykładem może być prawo do rzetelnego procesu sądowego (art. 6 EKPCz) w świetle implementowanych rozwiązań mających na celu np. zautomatyzowanie przydziału spraw¹⁸⁶. Brak jasności w zakresie kryteriów i zasad, które stoją za algorytmem używanym do przydzielania spraw danym sędziom, niweluje możliwość kontroli, czy przydzielanie jest rzeczywiście zbiektywizowane. Ponadto istnieje możliwość spojrzenia na zakaz dyskryminacji w związku z prawami, które są gwarantowane w EKPCz, a które stanowią przedmiot zainteresowania analizy, czyli np. poszanowania życia prywatnego i rodzinnego¹⁸⁷. W odniesieniu do państw stron protokołu 12 do EKPCz zakaz dyskryminacji powinien się odnosić do

¹⁸⁵ *Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms*, ETS No. 177. Nieoficjalne polskie tłumaczenie: Polskie Towarzystwo Prawa Antydyskryminacyjnego, tłumaczenie: *Protokół Nr 12 do Konwencji o ochronie praw człowieka i podstawowych wolności*. http://www.ptpa.org.pl/site/assets/files/1153/protokol_nr_12_do_kwslwfdk.pdf, dostęp: 1.04.2021. W czasie przygotowywania książki 20 państw ratyfikowało protokół 12 (lista ratyfikacji: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/177/signatures?p_auth=cWKVkrEV, dostęp: 1.04.2021), co prowadzi również w zakresie porządku prawnego tworzonego w ramach Rady Europy do różnicowania poziomu ochrony jednostki przed dyskryminacją. Polska nie przystąpiła do protokołu 12, stąd też posługuję się tłumaczeniem przygotowanym przez Polskie Towarzystwo Prawa Antydyskryminacyjnego.

¹⁸⁶ Zob. M. Matczak, *List do Trybunału Sprawiedliwości Unii Europejskiej ws. praworządności w Polsce*, „Archiwum Osiatyńskiego”, 1 czerwca 2018 r. <https://archiwum-osiatynskiego.pl/wpis-w-debacie/list-do-trybunalu-sprawiedliwosci-unii-europejskiej-ws-praworzadnosci-w-polsce>, dostęp: 1.04.2021.

¹⁸⁷ Przedstawione w rozdziale trzecim.

rozwiązań implementowanych w zakresie wszelkich praw gwarantowanych przez krajowy porządek prawny.

W świetle głównego przedmiotu zainteresowania tej książki kluczowym problemem jest jednak nie tyle sam charakter zakazu dyskryminacji w prawie europejskim, co możliwość zweryfikowania, czy i, jeśli tak, to do jakiego stopnia dany system zautomatyzowanego podejmowania decyzji rzeczywiście działa wbrew zakazowi dyskryminacji. Jej głównym celem jest zbadanie, czy możliwe jest na podstawie prawa dostępu do informacji lub dokumentów urzędowych w prawie europejskim dążenie do tego, aby zautomatyzowane podejmowanie decyzji było bardziej przejrzyste. Stąd też uzasadniona jest refleksja nad tym, jak prawo może odpowiedzieć na wyzwanie dotyczące samej możliwości dowiedzenia się, czy dane rozwiązanie ma (czy nie ma) charakter dyskryminacyjny, jeśli czyniłoby to je niezgodnym z prawem europejskim. Kluczowe staje się w tym wypadku przesunięcie akcentu na pytanie o samo stosowane rozwiązanie, nie zaś o indywidualną decyzję podjętą wobec jednostki. To przejrzystość algorytmów determinuje możliwość całościowej oceny zautomatyzowanego podejmowania decyzji, nie zaś wyjaśnienie konkretnej sytuacji jednostki poddanej traktowaniu opartemu na takim systemie.

1.3. Kolektywny wymiar dyskryminacji w ramach zautomatyzowanego podejmowania decyzji

Chociaż zautomatyzowane podejmowanie decyzji, do których odnosi się RODO, określone jest jako podejmowane w indywidualnych przypadkach, to nie ulega wątpliwości, że ma ono bardziej zbiorowy wymiar. Może on wynikać ze specyfiki przetwarzania danych w sposób zautomatyzowany i podejmowania na podstawie przetwarzania decyzji: zasadniczo opiera się ono na przypisywaniu jednostki do danej grupy, i w związku z owym przypisaniem, podejmowaniu wobec niej konkretnej decyzji. Potencjalny wpływ zautomatyzowanego podejmowania decyzji na dane grupy społeczne czy mniejszości został odnotowany we wspomnianych wytycznych Grupy Roboczej Art. 29: „Przetwarzanie danych, które może wywierać niewielki wpływ na ogół osób, może w istotny sposób wpływać na niektóre grupy społeczne takie jak mniejszości lub grupy osób dorosłych szczególnej troski”¹⁸⁸.

Spostrzeżenie to wiąże się z rozwijaniem w literaturze nurtem myślenia o prywatności jako o kwestii, która ze względu na rozwój technologii opartych na danych ma nie tylko wymiar indywidualny, lecz również kolektywny¹⁸⁹.

¹⁸⁸ Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji...*, *op. cit.*, s. 25.

¹⁸⁹ *Group Privacy. New Challenges of Data Technologies*, red. L. Taylor, L. Floridi, B. van der Sloot, Springer, Cham 2017; P. Helm, *Group Privacy in Times of Big Data. A Literature Review*, „Digital Culture and Society”, t. 2, nr 2, s. 137–151; S. Dreyer, W. Schulz, *The Gene-*

Można wskazać następujące przyczyny wzrostu znaczenia prywatności grupowej w związku z rozwojem nowych technologii:

[...] po pierwsze w związku z tym, że odkryć można więcej informacji na temat istniejących grup; po drugie, przez wzrastające możliwości *ekstrakcji* grup z danych, nawet jeśli ich członkowie nie są świadomi zachodzącego procesu przypisywania ich do danych grup; oraz po trzecie, potencjalnie, przez dozwolenie na nieuchwytny proces *grupowania* pojawiający się na etapie analizy danych, niezrozumiały nawet dla samego analityka¹⁹⁰.

W związku z tymi procesami „grupy” tworzone w powiązaniu z analizą danych mogą być podzielone na trzy typy¹⁹¹. Po pierwsze, można zastanawiać się nad prawami przysługującymi grupom, które powstają *ad hoc*, w wyniku analizy danych i definiowane są jako „grupy, w których członkostwo jest określone ze względu na interesy stron trzecich w oparciu o spostrzeżone (*perceived*) połączenia między członkami, często tworzone na dany okres lub dla określonego celu z niestabilizowanymi warunkami członkostwa”¹⁹². Grupy takie powstają w wyniku np. segmentacji rynku czy profilowania. Po drugie, można wyróżnić grupy askryptywne (*ascriptive*), których bycie członkiem jest determinowane przez dziedziczenie lub przypadkowo rozwiniętą cechę. Do grupy takiej nie można celowo dołączyć czy jej opuścić. Przykładem są grupy etniczne. Trzeci typ grup to kolektywy, do których można celowo dołączyć i które powstają dla ochrony wspólnych interesów czy na podstawie wspólnego pochodzenia, np. związki zawodowe.

Należy postawić pytanie o związek między prywatnością grupową a problemem dyskryminacji. W wypadku zautomatyzowanego podejmowania decyzji mającego zastosowanie wobec członków grup askryptywnych oraz kolektywów, wyróżnionych ze względu na przesłanki chronione przed dyskryminacją i prowadzących do podejmowania wobec nich mniej korzystnych rozstrzygnięć, możliwe będzie rozważenie, czy nie zachodzi dyskryminacja bezpośrednia. Bardziej prawdopodobne jest jednak, że większość sytuacji wykorzystywania zautomatyzowanego podejmowania decyzji opierać się

ral Data Protection Regulation and Automated Decision-making: Will it deliver? Potentials and limitations in ensuring the rights and freedoms of individuals, groups and society as a whole, Gütersloh 2019, s. 15–16. <https://www.hiig.de/publication/the-general-data-protection-regulation-and-automated-decision-making-will-it-deliver-potentials-and-limitations-in-ensuring-the-rights-and-freedoms-of-individuals-groups-and-society-as-a-whole>, dostęp: 1.04.2021.

¹⁹⁰ L. Kammourieh, T. Baar, J. Berens, E. Letouzé, J. Manske, J. Palmer, D. Sangokoya, P. Vinck, *Group Privacy in the Age of Big Data*, [w:] *Group Privacy...*, *op. cit.*, s. 52.

¹⁹¹ Klasyfikacja przedstawiona za: B. Mittelstadt, *From Individual to Group Privacy in Big Data Analytics*, „*Philosophy and Technology*” 2017, t. 30, s. 484–485.

¹⁹² B. Mittelstadt, *From Individual to Group Privacy...*, *op. cit.*, s. 485.

będzie na tworzeniu grup *ad hoc*, w odniesieniu do których trudniejsze okaże się zidentyfikowanie, czy kryteria uwzględniane podczas podejmowania decyzji mają charakter dyskryminacyjny. Kryteria używane podczas kreowania grup *ad hoc* mogą mieć charakter teoretycznie neutralny, prowadzący jednak do rezultatów dyskryminacyjnych w związku z zachodzeniem zjawiska dyskryminacji pośredniej. Przykładem będzie tworzenie grup oparte na takich informacjach jak adres zamieszkania w odniesieniu do miejsc, gdzie konkretne dzielnice zamieszkiwane są przez osoby o innym pochodzeniu etnicznym niż grupa dominująca. W takich wypadkach możliwe jest analizowanie danego systemu zautomatyzowanego podejmowania decyzji w odniesieniu do naruszenia przez niego zakazu dyskryminacji pośredniej ze względu na pochodzenie rasowe lub etniczne.

Oparcie zautomatyzowanego podejmowania decyzji na przypisywaniu jednostek do grup sprawia, że konieczne jest uwzględnienie kolektywnego wymiaru potencjalnej dyskryminacji w instrumentach prawnych używanych w celu sprostania wyzwaniom stworzonym przez nowe technologie. Aby skutecznie badać, czy w związku z używaniem danego systemu zautomatyzowanego podejmowania decyzji występuje dyskryminacja ze względu na zakazane prawem przesłanki, należy przeanalizować, w jaki sposób ów system grupuje jednostki poddawane procesom decyzyjnym. Taka perspektywa wymusza konieczność skupienia się na analizie samego systemu zautomatyzowanego podejmowania decyzji, tego jak tworzone są grupy poddawane danemu typowi decyzji, nie zaś jedynie na konkretnych decyzjach podejmowanych wobec jednostek. Uzasadnia ona również konieczność zastanowienia się nad rolą prawa dostępu do informacji dotyczących zautomatyzowanego podejmowania decyzji: wiedza o tym, w jaki sposób kod komputerowy ma grupować jednostki, jest niezbędna do sprawdzenia, czy zachodzi zakazana dyskryminacja, czy nie.

Jako jedną z konceptualizacji odnoszących się do różnicy między ochroną prywatności jednostki a ochroną prywatności kolektywnej można postrzegać rozróżnienie między wyjaśnieniem stawiającym w centrum podmiot danych a wyjaśnieniem stawiającym w centrum sam model¹⁹³. Lilian Edwards i Michaela Veale, którzy opisują te typy wyjaśnień, odnoszą się w swoich pracach do rozwiązań wykorzystujących uczenie maszynowe. Ukute przez nich kategorie prawa do wyjaśnienia można jednak rozszerzyć na rozwiązania polegające na zautomatyzowanym podejmowaniu decyzji, które nie wykorzystują tej

¹⁹³ Zaproponowane i rozwijane w odniesieniu do prawa ochrony danych osobowych przez Lilian Edwards i Michaela Vealego: L. Edwards, M. Veale, *Enslaving the Algorithm: From a "Right to an Explanation" to a "Right to Better Decisions"?*, „IEEE Security and Privacy” 2018, t. 16, nr 3, s. 46–54 oraz przede wszystkim L. Edwards, M. Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, „Duke Law and Technology Review” 2017, t. 16, nr 1, s. 18–84.

technologii. Podstawowym kryterium rozróżniającym wyjaśnienie stawiające w centrum podmiot od tego, którego głównym przedmiotem zainteresowania jest sam model, stanowi pytanie o to, co właściwie podlega wyjaśnieniu. W wypadku wyjaśnienia stawiającego w centrum podmiot jest to konkretna decyzja podjęta w odniesieniu do danej osoby¹⁹⁴.

Edwards i Veale ukazują trudności wiążące się ze stosowaniem przepisów RODO dotyczących udzielania podmiotom danych informacji na temat logiki stojącej za podjętą wobec nich w zautomatyzowany sposób decyzją¹⁹⁵. Przepisy rozporządzenia nie precyzują, czego dokładnie mają dotyczyć te informacje. W wypadku wyjaśnienia stawiającego w centrum model punkt ciężkości przesunęła się w stronę samej architektury rozwiązania wykorzystywanego w celu podejmowania wszystkich decyzji z użyciem tego systemu zautomatyzowanego podejmowania decyzji. Wyjaśnienie może zatem obejmować elementy dotyczące samego systemu zautomatyzowanego podejmowania decyzji, takie jak np. informacje dotyczące samego procesu przygotowania modelu i wyborów dokonanych na tym etapie, dane użyte do jego kształtowania i rozwijania, dane dotyczące skuteczności modelu wynikającej z jego testowania, uproszczone zasady, na których model jest oparty, oraz informacje dotyczące sposobu jego rozwijania¹⁹⁶.

Analiza Edwards i Vealego identyfikuje różnorodne możliwości rozumienia terminu „wyjaśnienie” i to, jakiego typu informacje dotyczące zautomatyzowanego podejmowania decyzji mogłyby mieścić się w tej kategorii. Poddana analizie propozycja postrzegania systemu zautomatyzowanego podejmowania decyzji jako informacji samej w sobie jest zrobieniem kroku wstecz w stosunku do ich koncepcji. Sięga ona do idei dotyczącej dostępu do informacji, która już jest „gotowa”, nie zaś wyjaśnień, które – z dużym prawdopodobieństwem – musiałyby zostać przygotowane. Istotnymi cechami wspólnymi koncepcji wyjaśnienia skupionego na modelu i kwestii prawa dostępu do informacji jest zaś, po pierwsze, odejście od postrzegania

¹⁹⁴ W zakresie rozwiązań skupionych na wyjaśnieniu konkretnej decyzji autorzy wymieniają cztery typy wyjaśnień: (1) odpowiadające na pytanie, co należałoby zmienić w danych wprowadzonych do modelu, aby decyzja wobec jednostki była inna (określone jako *sensitivity-based subject-centric explanations*); (2) skupione na kwestii, jakie z danych użytych do kształtowania tego modelu były najbardziej zbliżone do danych wprowadzonych przez jednostkę (*case-based subject-centric explanations*); (3) opis charakterystyki podmiotów, wobec których została podjęta podobna decyzja (*demographic based subject-centric explanations*); (4) odpowiedź na pytanie o to, jaka jest pewność w zakresie trafnego podjęcia decyzji, czyli np. kwestia tego, jak wiele z ocenianych podmiotów zostało źle zakwalifikowanych przez ten model (*performance-based subject-centric explanations*). Cechą wspólną tych możliwości jest koncentracja na okolicznościach ściśle odnoszących się do danej sprawy. Zob. L. Edwards, M. Veale, *Slave to the Algorithm...*, *op. cit.*, s. 58.

¹⁹⁵ Analizowanych w rozdziale drugim.

¹⁹⁶ L. Edwards, M. Veale, *Slave to the Algorithm...*, *op. cit.*, s. 55–56.

problemu zautomatyzowanego podejmowania decyzji ściśle związanego z myśleniem o jednostce i jej danych osobowych, na rzecz myślenia o całości kształcie implementowanego rozwiązania. Po drugie, zarówno analiza prawa dostępu do wyjaśnień zasad działania systemów zautomatyzowanego podejmowania decyzji, jak i poczyniona próba postrzegania tych systemów jako informacji podlegających prawu dostępu do informacji są krokami w stronę zagwarantowania wyższego stopnia przejrzystości systemów zautomatyzowanego podejmowania decyzji.

Wzrost poziomu przejrzystości w odniesieniu do zautomatyzowanego podejmowania decyzji nie jest celem samym w sobie. W świetle powyższych uwag dotyczących dyskryminacyjnego potencjału zautomatyzowanego podejmowania decyzji oraz kolektywnego charakteru wyzwań tworzonych przez tego typu narzędzia wyraźna staje się waga przejrzystości algorytmów dla możliwości oceny ich zgodności z zakazem dyskryminacji. Przejrzystość algorytmiczna, rozumiana jako szeroki dostęp jednostek do informacji na temat działania, np. zautomatyzowanego podejmowania decyzji, nie oznacza jednak, że rozwiązania te będą w większym stopniu rozliczalne (*accountable*)¹⁹⁷. Jednocześnie zwiększenie poziomu przejrzystości jest warunkiem niezbędnym do dokonywania prób rozliczania podmiotów używających tych narzędzi¹⁹⁸. Przykładem służą przepisy RODO dotyczące DPIA. Jego obecność w przepisach RODO mogłaby ewentualnie prowadzić do zwiększenia stopnia przejrzystości rozwiązań implementowanych w zakresie przetwarzania danych¹⁹⁹. Dopiero instrumenty umożliwiające pociągnięcie do odpowiedzialności podmiotów wykorzystujących zautomatyzowane podejmowanie decyzji w sposób niezgodny z przepisami RODO – w tym z obowiązkiem samego wykonania w określonych sytuacjach DPIA – wprowadzają element rozliczalności. Analogicznie, możliwość pozyskania informacji o systemie zautomatyzowanego podejmowania decyzji jest niezbędnym krokiem, który pozwala zweryfikować, czy jest on potencjalnie

¹⁹⁷ Decyduję się na używanie pojęcia rozliczalności, a nie odpowiedzialności jako tłumaczenia *accountable*, ze względu na używanie pojęcia odpowiedzialności głównie w odniesieniu do odpowiedzialności cywilnej czy karnej, co zaciemniałoby znaczenie rozliczalności jako możliwości weryfikacji i – niejako wtórnie – pociągania do odpowiedzialności instytucji czy organizacji za ich działania. Kluczowy w rozliczalności jest etap możliwości pozyskania informacji na temat danego działania czy problemu – stąd też jej powiązanie z przejrzystością. Więcej o rozliczalności, zob. np. R. Grzeszczak, *Władza wykonawcza w systemie Unii Europejskiej*, Stowarzyszenie Absolwentów WPiA UW, Warszawa 2011, s. 288–290.

¹⁹⁸ „Przejrzystość i rozliczalność są związane, ponieważ przejrzystość procesów podejmowania decyzji czy systemów zautomatyzowanego podejmowania decyzji jest niezbędna (choć niewystarczająca) dla uczynienia tego procesu lub systemu rozliczalnymi”. M. Zalnieriute, L.B. Moses, G. Williams, *The Rule of Law and Automation of Government Decision Making*, „The Modern Law Review” 2019, t. 82, nr 3, s. 431.

¹⁹⁹ Na przykład przez wprowadzenie obowiązku konsultacji w określonych sytuacjach z organem nadzorczym, zob. art. 36, RODO.

dyskryminujący przy jednoczesnym uwzględnianiu możliwości rozpowszechniania wiedzy na temat mechanizmów wykorzystywanych w ramach takiego systemu.

1.4. Podsumowanie

Opisane powyżej inspiracje teoretyczne prowadzą do przyjęcia następujących założeń teoretycznych przyświecających badaniom przedstawionym w dalszych rozdziałach. Po pierwsze, interakcje zachodzące między prawem a algorytmami w zakresie zautomatyzowanego podejmowania decyzji mają wpływ na to, czym staje się prawo – tak jak kod może być prawem w cyberprzestrzeni, tak może on również stawać się *de facto* prawem rządzącym danymi elementami świata fizycznego. Wykazuję, że niezbędny jest namysł nad granicami algorytmizacji prawa i obserwacja wykorzystywania nowych technologii w obszarach, które dotyczą praw i wolności jednostek, niezależnie od tego, czy wdrażane technologie oparte są na prostych czy na wysublimowanych algorytmach.

Sceptycyzm wobec możliwości wykorzystywania kodu komputerowego jako *de facto* prawa, regulującego dostęp jednostek do usług publicznych czy reguły stojące za wykonywaniem wobec nich przez państwa określonych działań opartych na zautomatyzowanym podejmowaniu decyzji, prowadzi do wniosku, że konieczne jest zagwarantowanie możliwości poddania stosowanych rozwiązań analizie. Wymóg taki powinien być postrzegany jako podstawowy w demokratycznym państwie prawa, w którym dostęp do norm prawnych, którym się podlega, jest prawem jednostki²⁰⁰. Badanie zautomatyzowanego podejmowania decyzji jest zatem po części badaniem zmian, jakie dotyczą problemu dostępu do prawa w demokratycznym państwie prawa. W analizie uwzględniam jednak również sytuacje, w których zautomatyzowane podejmowanie decyzji nie zastępuje bezpośrednio przepisów. Dlatego też koncentruję się na badaniu możliwości traktowania algorytmów jako informacji publicznej lub dokumentów urzędowych.

Po drugie, świadomość interakcji zachodzących między prawem a algorytmami wymusza rozważenie rozwiązań skupionych na samym modelu podejmowania zautomatyzowanych decyzji. Kolektywny wymiar zachodzących procesów, opierających się zwłaszcza na przypisywaniu jednostki do danych grup, pozwala rozważyć, jakiego rodzaju rozwiązania prawne stanowią możliwe odpowiedzi na tak kompleksowe wyzwania. Jest to problem szczególnie

²⁰⁰ Jak zauważają Bayamlioglu i Leenes: „Magiczny algorytm może uczynić prawo w pełni przewidywalnym, ale nadal będzie pozbawiony niezbędnej przejrzystości i moralnej rozliczalności w sensie bycia otwartym na kontrolę, a co za tym idzie: bycia zgodnym z zasadami stojącymi u podstaw państwa prawa”. E. Bayamlioglu, R. Leenes, *op. cit.*, s. 311.

istotny, zważywszy na zakres obowiązywania zakazu dyskryminacji w prawie europejskim. Opisane powyżej źródła różnego rodzaju stroniczości, która może pojawić się w procesie zautomatyzowanego podejmowania decyzji, powinny stanowić przedmiot zainteresowania prawników, jako potencjalnie ingerujące w prawa i wolności jednostki na skalę, jakiej w demokratycznych społeczeństwach nie należy ignorować. Obszary, w których wdrażane jest zautomatyzowane podejmowanie decyzji, to kwestie często będące przedmiotem antydyskryminacyjnych regulacji prawa UE (np. zatrudnienie, pomoc społeczna) czy praw gwarantowanych w EKPCz (np. dostęp do sądu). Potencjalny brak zgodności zautomatyzowanego podejmowania decyzji z zakazem dyskryminacji wymusza rozważenie, na ile istniejące instrumenty prawne, które odnoszą się do możliwości pozyskania informacji na temat systemów zautomatyzowanego podejmowania decyzji, pozwalają ocenić jego potencjalnie dyskryminacyjny charakter. Stanowi to uzasadnienie koncentracji na badaniu możliwości dostępu do algorytmów stosowanych w zautomatyzowanym podejmowaniu decyzji jako informacji publicznej lub dokumentów urzędowych.

Po trzecie, książka jest osadzona w refleksji nad formami przybieranymi przez relacje władzy w cyfrowym świecie²⁰¹. Jak zauważył już Mitchell: „kontrola nad kodem to władza”²⁰². Dlatego uzasadnione jest badanie możliwości żądania dostępu do algorytmów stosowanych w ramach systemów zautomatyzowanego podejmowania decyzji przez traktowanie ich jako informacji publicznej lub dokumentów urzędowych. Stosowanie takich rozwiązań jest sposobem sprawowania władzy nad jednostkami, decydowaniem o tym, w jaki sposób mogą korzystać ze swoich praw. Dlatego też dostęp do informacji na temat zautomatyzowanego podejmowania decyzji jest ważny do realizacji innych praw przysługujących jednostkom w demokratycznym państwie prawa. Praca stanowi analizę szczegółowego zagadnienia dotyczącego zautomatyzowanego podejmowania decyzji na szerszym tle relacji między tymi rozwiązaniami a realizacją zasad tak fundamentalnych dla demokratycznego państwa prawa jak zakaz dyskryminacji czy przejrzystość.

²⁰¹ Na przykład słynna pozycja S. Zuboff, *Wiek kapitalizmu inwigilacji. Walka o przyszłość ludzkości na nowej granicy władzy*, tłum. A. Unterschuetz, Wydawnictwo Zysk i S-ka, Poznań 2020.

²⁰² W.J. Mitchell, *op. cit.*, s. 112.

Zautomatyzowane podejmowanie decyzji z perspektywy ochrony danych osobowych w prawie europejskim

2.1. Zautomatyzowane podejmowanie decyzji w prawie Unii Europejskiej: od dyrektywy 95/46/WE do RODO

Regulacja zautomatyzowanego podejmowania decyzji na poziomie unijnym nie stanowi nowości. Już *dyrektywa 95/46/WE*²⁰³ w art. 15 wprowadzała prawo każdej osoby do nieobjęcia jej zautomatyzowaną decyzją indywidualną. Zgodnie z wymogami *dyrektywy 95/46/WE* decyzja taka musiała po pierwsze wywoływać skutki prawne dotyczące jednostki lub mające na nią istotny wpływ²⁰⁴, po drugie zaś być oparta wyłącznie na zautomatyzowanym

²⁰³ Artykuł 15 *dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych* (dyrektywa 95/46) Dz.Urz. WE 1995 L 281, s. 31–50. Na temat systematycznej analizy różnic między *dyrektywą 95/46/WE* a RODO, zob. Ch. Tikkinen-Piri, A. Rohunen, J. Markkula, *EU General Data Protection Regulation: Changes and Omplications for Personal Data Collecting Companies*, „Computer Law & Security Review” 2017, t. 34, nr 1, s. 134–153.

²⁰⁴ Polskie tłumaczenie dyrektywy może budzić wątpliwości w odniesieniu do tego fragmentu. Wersja polska brzmi: „Państwa Członkowskie przyznają każdej osobie prawo do nieobjęcia jej decyzją, która wywołuje skutki prawne, które jej dotyczą lub mają na nią istotny wpływ [...]” – fragment „lub mają na nią istotny wpływ” odnosi się do skutków prawnych. Tymczasem wersja angielska brzmi: *Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him [...]* – który to sposób sformułowania tworzy dwie osobne kategorie (decyzja wywołująca skutki prawne lub decyzja w znaczny sposób wpływająca na osobę). Podobnie, zob. „Artykuł 15 ust. 1 znajduje zastosowanie tylko do sytuacji, z których wynika znaczący lub prawny skutek (z założeniem, że skutek prawny ze swej natury jest znaczący”. A. Savin, *Profiling in the Present and New EU Data Protection Frameworks*, [w:] *Erhvervsretlige emner*, red. P.A. Nielsen, P.K. Schmidt, K. Dyppeel Weber, *Erhvervsretlige emne*, Juridisk Institut CBS, Djøf 2015, s. 4 wersji dostępnej pod: <https://ssrn.com/abstract=2697531>, dostęp: 1.04.2021. Z kolei wersja niemiecka: *Die Mitgliedstaaten räumen jeder Person das Recht ein, keiner*

przetwarzaniu danych, którego celem było dokonanie oceny niektórych dotyczących danej osoby aspektów o charakterze osobistym. Na podkreślenie zasługuje innowacyjność rozwiązania przyjętego w *dyrektywie 95/46/WE*. Zautomatyzowane podejmowanie decyzji było na początku lat 90. XX w. uregulowane jedynie w kilku państwach, wśród których pionierem była Francja²⁰⁵. Tymczasem w komunikacie Komisji dotyczącym propozycji przyjęcia dyrektywy można znaleźć następujące uzasadnienie dla artykułu, który ostatecznie przyjął formę art. 15 *dyrektywy 95/46/WE*:

Ten przepis ma na celu ochronę interesów podmiotu danych w zakresie uczestniczenia w podejmowaniu istotnych dla niego decyzji. Używanie rozbudowanych profilów danych jednostek przez mające władzę publiczne i prywatne instytucje pozbawia jednostki możliwości wpływania na procesy podejmowania decyzji w ramach tych instytucji, w razie gdyby decyzje te podejmowane miały być jedynie w oparciu o „cień danych” (*data shadow*)²⁰⁶.

Można zaryzykować stwierdzenie, że w tym zakresie *dyrektywa 95/46/WE* wyprzedziła swoje czasy. Możliwe, że w związku z tym m.in. rola art. 15 była „ekstremalnie skromna, jeśli nie marginalna”²⁰⁷, jak stwierdza Lee Andrew

für sie rechtliche Folgen nach sich ziehenden und keiner sie erheblich beeinträchtigenden Entscheidung unterworfen zu werden... również odnosi się do dwóch różnych typów decyzji, nie zaś typów skutków prawnych. Rozbieżność ta nie miała wpływu na formę transpozycji art. 15 do polskiej ustawy o ochronie danych osobowych, której art. 26a ust. 1 przybrał formę pomijającą ten warunek: „Niedopuszczalne jest ostateczne rozstrzygnięcie indywidualnej sprawy osoby, której dane dotyczą, jeżeli jego treść jest wyłącznie wynikiem operacji na danych osobowych, prowadzonych w systemie informatycznym” – Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.U. 1997 nr 133, poz. 883. Polski komentarz do art. 26a, zestawiający jego treść z art. 15 *dyrektywy 95/46/WE*: J. Barta, P. Fajgielski, R. Markiewicz, [w:] *Ochrona danych osobowych. Komentarz*, J. Barta, P. Fajgielski, R. Markiewicz, wyd. 6, Wolters Kluwer Polska, Warszawa 2015 (do art. 26(a)).

²⁰⁵ Francuski akt prawny dotyczący ochrony danych osobowych: *Loi no. 78-17 du 6. janvier 1978 relative à l'informatique, aux fichiers et aux libertés*. <https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006068624/2020-10-09/>, dostęp: 1.04.2021. Treść artykułów cytowana jest przez L.A. Bygrave, *Automated Profiling Minding The Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, „Computer Law & Security Review” 2001, t. 17, nr 1, s. 22, przypis 2.

²⁰⁶ Komisja, *Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security*, COM (90) 314 final – SYN 287, s. 29.

²⁰⁷ I. Mendoza, L.A. Bygrave, *The Right Not to be Subject to Automated Decisions Based on Profiling*, [w:] *EU Internet Law. Regulation and Enforcement*, red. T.-E. Synodinou, P. Jougoux, Ch. Markou, T. Prastitou, Springer, Cham 2017, s. 81. Podobnie: B.W. Schermer, *The Limits of Privacy in Automated Profiling and Data Mining*, „Computer Law & Security Review” 2011, t. 27, nr 1, s. 51.

Bygrave, jeden z nielicznych autorów podejmujących ten temat przed unijną reformą ochrony danych. Zgodnie z jego ustaleniami²⁰⁸ art. 15 nie był przedmiotem ani wykładni TSUE, ani – z jednym nadzwyczaj skromnym wyjątkiem – sądów krajowych²⁰⁹.

W związku z brakiem, jak dotąd, wypowiedzi TSUE dotyczących art. 15 *dyrektywy 95/46/WE* wątpliwości dotyczące treści prawa każdej osoby do nieobjęcia jej zautomatyzowaną decyzją indywidualną nie zostały rozwiązane. Tymczasem wiele pojęć i rozwiązań pojawiających się w art. 15 jest niejasnych. Po pierwsze, sposób sformułowania art. 15 nie pozwalał jednoznacznie stwierdzić, czy ustanawiał on zakaz podejmowania zautomatyzowanych decyzji, czy prawo jednostki aktualizujące się w momencie podjęcia zautomatyzowanej decyzji i próby jednostki wyrażenia wobec tej decyzji sprzeciwu²¹⁰. Po drugie, niejasne były warunki możliwości powołania się na prawo z art. 15. Zgodnie z analizą Bygrave'a, aby można było powołać się na prawo z art. 15 niezbędne było spełnienie kumulatywnie czterech przesłanek: istnienie podjętej decyzji; decyzja musiała mieć skutki prawne lub inne ważne skutki dla danej jednostki; decyzja musiała być w całości wynikiem zautomatyzowanego przetwarzania danych; przetwarzanie danych musiało mieć na celu ocenę pewnych aspektów osoby, wobec której podejmowana była decyzja²¹¹. Wątpliwości budzi znaczenie użytych pojęć, takich jak: „decyzja”, „ważne skutki” czy „całkowicie zautomatyzowana”. Ze względu na fakt, że nie zostały one na tle stanu prawnego wynikającego z obowiązywania *dyrektywy 95/46/WE* wyjaśnione przez TSUE, a terminy te zostały powtórzone w RODO, próbami ich zdefiniowania zajmują się w dalszej części rozdziału.

Ponadto należy podkreślić, że art. 15 formułował dwa wyjątki od prawa ujętego w ust. 1, czyli po pierwsze, podjęcie decyzji w celu wykonania umowy, pod warunkiem, że wniosek w sprawie zawarcia lub realizacji umowy, wniesiony przez osobę, której dane dotyczą, zostanie przyjęty lub że istnieją odpowiednie sposoby zabezpieczenia jego uzasadnionych interesów. Po drugie zaś, w sytuacji, w której decyzja zostanie dozwolona przez prawo,

²⁰⁸ Zgodnie z I. Mendoza, L.A. Bygrave, *op. cit.*, s. 81, a także moją najlepszą wiedzą.

²⁰⁹ Z wyjątkiem wyroku niemieckiego z 2014 r.: *Urteil des VI. Zivilsenats vom 28.1.2014 – VI ZR 156/13*. Jego omówienie: I. Mendoza, L.A. Bygrave, *op. cit.*, s. 88. Sąd odrzucił w nim interpretację zautomatyzowanego systemu służącego do określania zdolności kredytowej jako podlegającego pod definicję zautomatyzowanego podejmowania decyzji zgodnie z transpozycją dyrektywy dokonaną przez Niemcy, ponieważ ostatecznie decyzję podejmował człowiek.

²¹⁰ Zob. I. Mendoza, L.A. Bygrave, *op. cit.*, s. 86.

²¹¹ L.A. Bygrave, *Automated Profiling Minding The Machine...*, *op. cit.*, s. 18 i omówienie tych warunków, s. 18–20.

które określa również sposoby zabezpieczenia uzasadnionych interesów osoby, której dane dotyczą²¹².

Brak precyzji art. 15 i uwzględnienie w nim wyjątków doprowadziło do znacznych różnic w sposobie transpozycji tego artykułu do porządków krajowych państw członkowskich²¹³. Część państw zdecydowała się wprowadzić ogólny zakaz podejmowania zautomatyzowanych decyzji (np. Austria, Belgia, Niemcy, Finlandia, Niderlandy, Portugalia, Szwecja czy Irlandia), jednocześnie decydując się na wprowadzenie wyjątków nieobjętych zakresem art. 15 (np. decyzje oparte na zgodzie podmiotu danych w Irlandii). Różnice uwidaczniały się również na poziomie środków uznawanych przez państwa za wystarczające zabezpieczenie interesów jednostek (np. w Grecji możliwość sądowego zawieszenia stosowania lub zaprzestania stosowania decyzji podjętej w wyniku zautomatyzowanego podejmowania decyzji). Dokonana przez Douwe Korffa analiza wykazuje zasadnicze różnice między państwami członkowskimi nie tylko na poziomie pojęć, lecz również materialnych skutków w odniesieniu do rzeczywistej treści prawa zawartego w art. 15 *dyrektywy* 95/46/WE. Jest to problem, który nie do końca udało się zwalczyć przez przyjęcie w RODO ujednoczonej formy rozwiązania w zakresie zautomatyzowanego podejmowania decyzji.

Na podkreślenie zasługuje również obecność w *dyrektywie* 95/46/WE drugiego elementu regulacji zautomatyzowanego podejmowania decyzji, czyli zawartego w art. 12 prawa dostępu do danych. Zgodnie z treścią tego przepisu państwa członkowskie miały zapewnić każdej osobie, której dane dotyczą, prawo do uzyskania od administratora danych, w tym wiadomości na temat zasad automatycznego przetwarzania dotyczących jej danych przynajmniej w przypadku zautomatyzowanego procesu decyzyjnego określonego w art. 15 ust. 1. Na tle treści art. 12 toczyła się debata, jak należy rozumieć sformułowanie „zasady automatycznego przetwarzania” (*knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions referred to in Article 15 (1)*)²¹⁴. Podobnie, jak w art. 15, brakowało w niej jednak ujednoczenia rozumienia użytych

²¹² Katalog ten stanowi istotną różnicę w stosunku do formy, którą prawo osoby do nieobjęcia jej zautomatyzowaną decyzją przyjęło w RODO, o czym dalej w rozdziale.

²¹³ Dokładne omówienie porządków prawnych państw członkowskich w tym aspekcie, zob. D. Korff, *New Challenges to Data Protection Study – Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments*, European Commission DG Justice, Freedom and Security Report, 2010, s. 82–86. <https://ssrn.com/abstract=1638949>, dostęp: 1.04.2021. W akapicie powołuję się na ustalenia dokonane przez Douwe Korffa.

²¹⁴ Zob. S. Wachter, B. Mittelstadt, L. Floridi, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, „International Data Privacy Law” 2017, t. 7, nr 2, s. 85 i literatura tam cytowana.

w art. 12 pojęć za sprawą orzecznictwa TSUE. Transpozycja normy do porządków prawnych państw członkowskich również zaowocowała rozbieżnościami w zakresie rozumienia treści art. 12²¹⁵ obejmującymi takie kwestie jak możliwość lub brak możliwości kontestowania decyzji pozytywnych²¹⁶ czy pojęć opisujących informacje, które miały być przekazane jednostce (*rules, operating principles, reasoning*²¹⁷).

Podsumowując wkład *dyrektywy 95/46/WE* w regulację zautomatyzowanego podejmowania decyzji, należy podkreślić, że stanowiła ona nowatorską, choć niedoskonałą, próbę zmierzenia się z wyzwaniem, którego rzeczywista waga na początku lat 90. nie mogła być jeszcze oczywista. Artykuły 15 i 12 *dyrektywy 95/46/WE* położyły podwaliny pod kluczowe elementy rozwiązań prawnych, podtrzymanych w dużym stopniu w RODO. Jednocześnie dopiero prace nad unijną reformą dotyczącą ochrony danych osobowych zaowocowały akademicką debatą dotyczącą regulacji zautomatyzowanego podejmowania decyzji, której jest poświęcona dalsza część rozdziału.

Ogólna architektura rozwiązań dotyczących zautomatyzowanego podejmowania decyzji nie została poddana znacznym zmianom. Odpowiednikiem art. 15 z *dyrektywy 95/46/WE* jest w RODO art. 22, natomiast obowiązki informacyjne, określone w art. 12 *dyrektywy 95/46/WE*, obecnie znajdują się w art. 13–15²¹⁸. Ponadto zgodnie z koncepcjami przedstawianymi w literaturze inne prawa podmiotów danych mogą mieć wpływ na zautomatyzowane podejmowanie decyzji. Kolejne podrozdziały są poświęcone tym trzem aspektom regulacji zautomatyzowanego podejmowania decyzji w RODO. Jako kwestię odrębną potraktowałam ocenę skutków dla ochrony danych oraz wiążące reguły korporacyjne. Podział ten wynika z faktu, że o ile art. 22, 13–15 oraz inne prawa podmiotów danych skupione są na jednostce, to ocena skutków dla ochrony danych i wiążące reguły korporacyjne mają

²¹⁵ Zob. D. Korff, *op. cit.*, s. 86; S. Wachter, B. Mittelstadt, L. Floridi, *op. cit.*, s. 86–89.

²¹⁶ Przykład Niemiec, gdzie umożliwiono żądanie wyjaśnienia decyzji podjętej nie po myśli jednostki, zob. S. Wachter, B. Mittelstadt, L. Floridi, *op. cit.*, s. 86.

²¹⁷ Zob. D. Korff, *op. cit.*, s. 86.

²¹⁸ Wśród polskich komentarzy do RODO należy wymienić: *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Wolters Kluwer Polska, Warszawa 2017; P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Wolters Kluwer Polska, Warszawa 2018; *Ogólne rozporządzenie o ochronie danych osobowych: komentarz*, red. M. Sakowska-Baryła, C.H. Beck, Warszawa 2018; 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*, C.H. Beck, Warszawa 2017. Ze względu na charakter dalszej analizy, która ma na celu przedstawienie zróżnicowanych stanowisk doktryny w zakresie poszczególnych elementów regulacji zautomatyzowanego podejmowania decyzji w prawie europejskim, odwołuję się głównie do publikacji odnoszących się szczegółowo do tego zagadnienia.

znaczenie dla całościowej oceny systemów zautomatyzowanego podejmowania decyzji. Odwołując się do kategorii przedstawionych w rozdziale pierwszym, mogą być one postrzegane jako rozwiązania dotyczące wyjaśnień skupionych na modelu, nie na jednostkowej decyzji.

2.1.1. Zakaz zautomatyzowanego podejmowania decyzji w art. 22 RODO

Zgodnie z treścią art. 22 ust. 1 RODO²¹⁹ osoba, której dane dotyczą, ma prawo do tego, aby nie podlegać decyzji opierającej się wyłącznie na zautomatyzowanym przetwarzaniu danych, czyli zautomatyzowanemu podejmowaniu decyzji w indywidualnych przypadkach²²⁰. Decyzje, które objęte są treścią art. 22, muszą wywoływać wobec jednostki skutki prawne lub w podobny sposób istotnie na nią wpływać, co stanowi powtórzenie rozwiązania przyjętego w *dyrektywie 95/46/WE*. Treść art. 22 ust. 1 wprost odnosi się również do profilowania²²¹, potraktowanego jako rodzaj zautomatyzowanego przetwarzania danych, które może prowadzić do wydania decyzji. Na tle art. 22 należy stwierdzić, że ust. 1 odnosi się do decyzji spełniających wymienione powyżej warunki, niezależnie od tego, czy zachodzące w ich celu przetwarzanie danych jest kwalifikowane jako profilowanie, czy nie. Językowa

²¹⁹ Treść art. 22: „1. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa. 2. Ust. 1 nie ma zastosowania, jeżeli ta decyzja: a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem; b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą. 3. W przypadkach, o których mowa w ust. 2 lit. a) i c), administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji. 4. Decyzje, o których mowa w ust. 2, nie mogą opierać się na szczególnych kategoriach danych osobowych, o których mowa w art. 9 ust. 1, chyba że zastosowanie ma art. 9 ust. 2 lit. a) lub g) i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą”. RODO.

²²⁰ W 2020 r. ukazała się monografia poświęcona tematowi regulacji zautomatyzowanego podejmowania decyzji w RODO, zob. A. Drożdż, *Protection of Natural Persons with Regard to Automated Individual Decision-Making in the GDPR*, Kluwer Law International, Alphen aan den Rijn 2020. Główne konkluzje analizy przeprowadzonej przez autorkę są podobne do konkluzji tego rozdziału: RODO nie stworzyło ram prawnych umożliwiających skuteczne zaradzenie problemom wynikającym z rozwoju zautomatyzowanego podejmowania decyzji.

²²¹ Jak wspomniałam we Wstępie, zgodnie z definicją zawartą w art. 4 ust. 4 RODO profilowanie jest formą zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej – niekoniecznie zaś podejmowania decyzji.

wykładnia art. 22 pozwala zauważyć, że profilowanie zostało potraktowane jako jeden z możliwych (lecz nie jedyny) sposobów postępowania mogący prowadzić do zautomatyzowanego podejmowania decyzji. Tym samym na gruncie RODO postulowane jest dokonanie rozróżnienia między „profilowaniem prowadzonym w celu automatycznego podjęcia decyzji, która wywołuje wobec podmiotu danych skutki prawne lub w podobny sposób istotnie na niego wpływa” i „pozostałym profilowaniem”²²². Tylko to pierwsze objęte jest zakresem stosowania art. 22 ust. 1.

Kolejne dwa ustępy art. 22 odnoszą się do wyjątków od sytuacji opisanych w ust. 1. Zgodnie z treścią art. 22 ust. 2 decyzje mogą być podejmowane w trzech sytuacjach: niezbędności do zawarcia lub wykonania umowy, dozwolenia prawem UE lub państwa członkowskiego oraz w przypadku wyraźnej zgody podmiotu danych. Nawet w tych sytuacjach administrator jest jednak zobowiązany wdrożyć właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów podmiotu danych (art. 22 ust. 2 lit. b oraz art. 22 ust. 3). Ostatni ustęp art. 22 odnosi się do relacji między zautomatyzowanym podejmowaniem decyzji a szczególnymi kategoriami danych osobowych, formułując warunki, pod którymi możliwe jest używanie tej kategorii danych do zautomatyzowanego podejmowania decyzji.

Wątpliwość, która istniała na gruncie *dyrektywy 95/46/WE*, a która nie została ostatecznie rozstrzygnięta przez samą treść art. 22, to kwestia możliwości interpretacji normy z art. 22 ust. 1 bądź jako prawa jednostki, bądź jako zakazu zautomatyzowanego podejmowania decyzji. Jak zauważa Maja Brkan: „Prawo to może być rozumiane bądź jako prawo, które podmiot danych musi aktywnie wykonać, bądź jako «pasywne» prawo, którego administratorzy danych muszą sami przestrzegać, bez aktywnego powołania się na nie przez podmiot danych”²²³. Brkan zauważa również, że o postrzeganiu art. 22 jako prawa, które musi być aktywnie wykonane przez jednostkę, może świadczyć jego usytuowanie w ramach rozdziału III „Prawa osoby, której dane dotyczą”. Dla porównania art. 11 *dyrektywy 2016/680*, regulujący zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach,

²²² Ł. Zięba, *Rozdział IX. Budowanie profili osobowych a wymogi wynikające z nowych przepisów o ochronie danych osobowych*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osiej, C.H. Beck, Warszawa 2017, s. 132.

²²³ M. Brkan, *Do algorithms rule the world? Algorithmic decision-making and data protection in the framework of the GDPR and beyond*, „International Journal of Law and Information Technology” 2019, t. 27, nr 2, s. 99 (wersja dostępna online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3124901, dostęp: 1.04.2021, s. 7. Dalej numery stron podaję za wersją z „International Journal of Law and Information Technology” dostępną w trybie *early view*).

został umieszczony w rozdziale II zatytułowanym „Zasady”²²⁴. Należy również podkreślić, że art. 11 *dyrektywy 2016/680* jest sformułowany wprost jako zakaz („Państwa członkowskie zapewniają, by decyzje, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i mają niekorzystne skutki prawne dla osoby, której dane dotyczą, lub poważnie na nią wpływają, były zakazane [...]”), co może pogłębiać wątpliwości co do intencji przyświecających sposobowi sformułowania treści art. 22 RODO.

Literalna wykładnia art. 22 wskazuje jednak, że mimo braku użycia wyrażenia „zakaz” RODO ma na celu uniemożliwienie podejmowania zautomatyzowanych decyzji wobec jednostki („prawo do bycia nieobjętym”²²⁵). Po pierwsze, jednostka ma prawo takiej decyzji nie podlegać, nie zaś ją kwestionować. Tym samym art. 22 dotyczy samego etapu podejmowania decyzji wobec jednostki: uniemożliwienie jej podjęcia jest jedynym sposobem wykonania prawa jednostki do niepodlegania decyzji. Po drugie, o interpretacji art. 22 ust. 1 jako zakazu świadczy obecność ust. 2, który wprowadza wyjątki umożliwiające podejmowanie zautomatyzowanych decyzji²²⁶. Dopuszczenie możliwości podejmowania zautomatyzowanych decyzji w określonych sytuacjach ma sens jedynie wówczas, gdy z zasady jest ono zakazane. Taki sposób interpretacji art. 22 został potwierdzony przez Grupę Roboczą Art. 29, której wytyczne wprost określają treść tego przepisu jako „ogólny zakaz podejmowania decyzji wyłącznie na podstawie zautomatyzowanego przetwarzania”²²⁷. Grupa Robocza Art. 29 podkreśla, że określenie normy dotyczącej zautomatyzowanego podejmowania decyzji jako prawa nie powinno być odczytywane

²²⁴ Zob. M. Brkan, *op. cit.*, s. 7–9. Problematyczne jest nieuwzględnienie w traktowaniu zakazu zautomatyzowanego podejmowania decyzji jako zasady specyfiki znaczenia tego terminu w prawie ochrony danych osobowych. Odnosi się ono do katalogu zasad dotyczących przetwarzania danych sformułowanego w art. 5 RODO (a szerzej: rozdziale II RODO). Katalog ten jest w pewnym stopniu pokłosiem wypracowywanych od lat 80. przez OECD zasad prawa ochrony danych osobowych: OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980. <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm#part2>, dostęp: 1.04.2021, zaktualizowane w 2013: OECD, *The OECD Privacy Framework*, 2013. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, dostęp: 1.04.2021. Celem wypracowywania zasad dotyczących prawa ochrony danych osobowych jest zagwarantowanie ogólnych wytycznych dla interpretacji norm i określenie rodzaju wartości, które mają być przez te normy chronione, nie zaś tworzenie konkretnych środków prawnych, jakim jest zakaz zautomatyzowanego podejmowania decyzji, zob. L.A. Bygrave, *Data Privacy Law. An International Perspective*, Oxford University Press, Oxford 2014, s. 145.

²²⁵ Taka interpretacja art. 22 – I. Mendoza, L.A. Bygrave, *op. cit.*, s. 85.

²²⁶ Argumentacja ta pojawia się np. u I. Mendoza, L.A. Bygrave, *op. cit.*, s. 85–87; M. Brkan, *op. cit.*, s. 9.

²²⁷ Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji...*, *op. cit.*, s. 22.

jako konieczność czynnego powołania się na to prawo przez jednostkę czy podjęcia przez nią działań²²⁸.

Kolejne pytanie, jakie należy postawić, dotyczy zakresu obowiązywania zakazu z art. 22, czyli znaczenia pojęć takich jak „decyzja”²²⁹ czy bardziej precyzyjnie: „decyzja, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu” i „wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa”. Na tle pojęcia decyzji istotne jest podkreślenie, że art. 22 odnosi się do decyzji opartych na zautomatyzowanym przetwarzaniu danych osobowych. Tym samym można zakładać, że np. wysłanie automatycznego powiadomienia o istnieniu braków formalnych w składanej dokumentacji nie będzie należeć do kategorii decyzji regulowanych przez art. 22 ze względu na brak elementu wykorzystywania danych osobowych jako kryterium determinującego jej wynik. Tymczasem jeśli w ramach procesu decyzyjnego, rozumianego jako dokonywanie wyboru między możliwymi rozwiązaniami danej kwestii, zostaje wykorzystana technologia oparta na przetwarzaniu danych osobowych, sytuacja taka może być rozważana jako zautomatyzowane podejmowanie decyzji.

Niemniej musi ona spełnić pozostałe kryteria sformułowane w art. 22²³⁰, czyli po pierwsze, być oparta wyłącznie na zautomatyzowanym przetwarzaniu. Sformułowanie to budzi kontrowersje w literaturze. W ocenie Sandry Wachter, Brenta Mittelstadta i Luciano Floridego: „podczas gdy wymagany poziom ludzkiego zaangażowania nie jest w praktyce jasny, sformułowanie «wyłącznie» sugeruje, że nawet nominalne ludzkie zaangażowanie może

²²⁸ Z kolei autorzy komentarza do RODO *The EU General Data Protection Regulation (GDPR). A Commentary*, red. Ch. Kuner, L.A. Bygrave, Ch. Docksey, Oxford University Press, Oxford 2020, s. 530–531, chociaż dostrzegają wagę argumentów przemawiających za uznaniem art. 22 za zakaz, stają po stronie postrzegania tego przepisu jako prawa jednostki. Argumentacja w komentarzu opiera się na wykładni odwołującej się do intencji ustawodawcy, faktu uwzględnienia np. w art. 13 ust. 2 lit f RODO zautomatyzowanego podejmowania decyzji w sposób zakładający, że może on mieć miejsce czy wprowadzenia w RODO DPIA. Argumenty te wydają się o tyle nieprzekonujące, że art. 22 odczytywany jako zakaz jest obwarowany szeregiem dopuszczalnych wyjątków, które mogą prowadzić do stosowania zautomatyzowanego podejmowania decyzji w oparciu o nie. Argumenty mówiące o obecności innych przepisów dotyczących tego mechanizmu jako przyczynie stojącej za koniecznością postrzegania art. 22 jako prawa mogą być odparte właśnie poprzez odnotowanie tej cechy rozwiązań przyjętych w RODO. Podobnie, zob. L. Tosoni, *The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation*, „International Data Privacy Law” 2021, ipaa024 (online first).

²²⁹ Rozważania o pojęciu decyzji, jeszcze na gruncie *dyrektywy 95/46/WE*, zob. L.A. Bygrave, *Automated Profiling Minding The Machine...*, *op. cit.*, s. 18–19.

²³⁰ Warunki te można sformułować również w sposób wyodrębniający samo podjęcie decyzji jako jeden z nich, zob. *The EU General Data Protection Regulation (GDPR). A Commentary*, *op. cit.*, s. 532.

być wystarczające”²³¹. Skutkiem przyjęcia takiej interpretacji byłoby jednak pozbawienie sensu całego art. 22. Po pierwsze, stanowiłoby ono pokusę do tworzenia rozwiązań polegających na wprowadzaniu pozornego udziału człowieka w podejmowaniu decyzji, polegającego np. na przystawieniu pieczętki czy podpisu na dokumencie zawierającym decyzję podjętą w sposób zautomatyzowany. Po drugie, samo wprowadzanie zautomatyzowanych sposobów wspomagania podejmowania decyzji może mieć wpływ na osoby korzystające z zautomatyzowanych systemów i ich gotowość do kwestionowania decyzji sugerowanej przez algorytm. Niechęć do zmiany sugerowanej decyzji, chociaż wynikająca z przyczyn natury psychologicznej lub instytucjonalnej, może być wzmacniana przez rozwiązania prawne. Przyjęcie wąskiej interpretacji sformułowania „wyłącznie” mogłoby prowadzić do wzmacniania niepokojących tendencji w zachowaniu urzędników mających kontakt z narzędziami zautomatyzowanego podejmowania decyzji i tym samym legitymizowania zachowań przyczyniających się do realizacji opisanych w rozdziale pierwszym zagrożeń związanych z potencjalną dyskryminacją zachodzącą w wyniku ich stosowania.

Wąska interpretacja określenia „wyłącznie” nie przeważa wśród stanowisk prezentowanych przez badaczy. Dominująca i potwierdzona przez wytyczne Grupy Roboczej Art. 29 interpretacja podkreśla konieczność znaczącego wkładu człowieka w podejmowanie decyzji, aby mogła ona być uznana za niepodjętą w sposób zautomatyzowany. Argumentację za taką interpretacją można oprzeć, jak robią to Gianclaudio Malgieri i Giovanni Comandé, na wykładni językowej treści art. 22²³². Zauważają oni, że treść art. 22 ust. 1 nie dotyczy „wyłącznie zautomatyzowanego podejmowania decyzji”, lecz decyzji, które „są oparte” wyłącznie na zautomatyzowanym podejmowaniu decyzji. Tym samym decyzja podejmowana teoretycznie przez człowieka, w której ludzki wkład ogranicza się do potwierdzenia decyzji opartej wyłącznie na zautomatyzowanym przetwarzaniu, powinna być objęta zakresem zakazu z art. 22 RODO. Potwierdzenie takiej interpretacji można znaleźć w wytycznych Grupy Roboczej Art. 29, które dodatkowo formułują wymóg dotyczący uprawnień i kompetencji osoby odpowiedzialnej za

²³¹ S. Wachter, B. Mittelstadt, L. Floridi, *op. cit.*, s. 92.

²³² „[...] nawet z językowej wykładni art. 22 ust. 1, można zauważyć, że zakres stosowania artykułu nie jest ograniczony do «wyłącznie zautomatyzowanego podejmowania decyzji», lecz że uwzględnia (ludzkie lub maszynowe) decyzje, które «są oparte» wyłącznie na zautomatyzowanym podejmowaniu decyzji. Uważamy, że sformułowanie «oparte wyłącznie na zautomatyzowanym podejmowaniu decyzji» odnosi się do każdego podejmowania decyzji, w którym przygotowywanie dowodów i sądy dyskrecjonalne (np. *scoring*) są w pełni oparte na zautomatyzowanych środkach. Zgodnie z taką wykładnią, nawet jeśli w procesie podejmowania decyzji ma miejsce nominalna interwencja ludzka, art. 22 nadal znajduje zastosowanie”. G. Malgieri, G. Comandé, *op. cit.*, s. 251.

interwencję ludzką w zautomatyzowane podejmowanie decyzji. *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji...* kładą nacisk na to, aby nadzór nad podejmowaniem decyzji był znaczący i obejmował kompetencje i uprawnienia do zmiany decyzji opartej wyłącznie na zautomatyzowanym podejmowaniu decyzji²³³. Treść dokumentu sugeruje, że osoba mająca uprawnienia do zmiany decyzji powinna być w stanie dokonać merytorycznej analizy sugestii decyzji wydanej przez system zautomatyzowanego podejmowania decyzji. Tym samym należy stwierdzić, że wymóg pierwszy dotyczący decyzji zakazanych w art. 22 RODO odnosi się do podejmowania decyzji opartych na zautomatyzowanym przetwarzaniu, w którym rola człowieka nie jest istotna i nie może prowadzić do zmiany decyzji opartej na wszystkich istotnych danych.

Wymóg drugi dotyczący decyzji objętych treścią art. 22 ust. 1 RODO odnosi się do ich skutków. Zgodnie z rozporządzeniem zakazane są decyzje, które wywierają skutki prawne lub w podobny sposób istotnie wpływają na jednostkę. Interpretacja sformułowania „skutki prawne” może przyjąć węższą i szerszą formułę. Węższa odnosi się do decyzji mających wpływ na status prawny jednostki, czyli „skutki, które mogą zmienić lub determinować (częściowo lub w pełni) prawa lub obowiązki jednostki wynikające z prawa”²³⁴. Interpretacja szersza oparta jest na perspektywie prawnoczułowieczej, zgodnie z którą: „możemy wnioskować, że każdy wpływ na prawa człowieka lub konstytucyjne prawa jednostki jest skutkiem prawnym”²³⁵. Tym samym każda decyzja odnosząca się do praw jednostki gwarantowanych prawem, takich jak np. prawo do bycia niedyskryminacyjnie traktowanym czy prawo do sprawiedliwego sądu, powinna być traktowana jako decyzja wywołująca skutki prawne. Wytyczne Grupy Roboczej Art. 29 w tym aspekcie nie precyzują, która interpretacja jest trafniejsza, stwierdzając jedynie, że pojęcie „skutek prawny” odnosi się do decyzji, która „ma [...] wpływ na prawa danej osoby przewidziane w przepisach, takie jak wolność do zrzeczania się, głosowania w wyborach lub wystąpienia na drogę sądową”²³⁶. Ponadto skutek prawny rozumiany jest również jako konsekwencje zmian statusu prawnego danej osoby lub jej praw, które wynikają z mocy umowy²³⁷. Tym

²³³ Zob. Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji...*, *op. cit.*, s. 23.

²³⁴ L.A. Bygrave, *Automated Profiling Minding The Machine...*, *op. cit.*, s. 19 (na tle dyrektywy 95/46/WE).

²³⁵ G. Malgieri, G. Comandé, *op. cit.*, s. 252.

²³⁶ Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji...*, *op. cit.*, s. 24.

²³⁷ Zob. Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji...*, *op. cit.*, s. 24.

samym, uogólniając, skutek prawny jest pojęciem, które odsyła nie jedynie do relacji publicznoprawnych, lecz również w obrębie prawa prywatnego.

Szeroką interpretację warunku dotyczącego skutków prawnych potwierdza uwzględnienie w art. 22 kategorii decyzji w podobny sposób istotnie wpływających na jednostkę. Zgodnie z przykładami podanymi w motywie 71 RODO decyzje w podobny sposób istotnie wpływające na jednostkę to „automatyczne odrzucenie elektronicznego wniosku kredytowego czy elektroniczne metody rekrutacji bez interwencji ludzkiej”²³⁸. Zbiór sytuacji, w których decyzja nie może być interpretowana jako mająca skutki prawne dla jednostki, jednak z pewnością mająca na nią istotny wpływ, odnosi się do rosnącej roli podmiotów prywatnych w determinowaniu kluczowych elementów życia jednostek. Stąd też pozytywnie należy ocenić uwzględnienie przez Grupę Roboczą Art. 29 możliwości istotnego wpływu na jednostkę wynikającego z decyzji podejmowanych w zakresie marketingu, np. w związku z wysokim stopniem inwazyjności profilowania czy wykorzystywania wiedzy o czynnikach zwiększających podatność osób, których dane dotyczą, na przekaz marketingowy²³⁹. Propozycja szerokiej interpretacji kategorii decyzji mających istotny wpływ na jednostkę potwierdza obecne już w odniesieniu do art. 15 *dyrektywy 95/46/WE* przekonanie o większym znaczeniu regulacji zautomatyzowanego podejmowania decyzji dla sektora prywatnego²⁴⁰. Jednocześnie jednak rosnący udział podmiotów publicznych wśród podmiotów wykorzystujących zautomatyzowane podejmowanie decyzji²⁴¹ może prowadzić do zmiany w tym aspekcie.

2.1.2. Wyjątki od zakazu zautomatyzowanego podejmowania decyzji w art. 22 RODO

Elementem przepisów RODO dotyczących zautomatyzowanego podejmowania decyzji, który wprowadza zasadnicze różnice w stosunku do *dyrektywy 95/46/WE*, jest katalog ujętych w art. 22 ust. 2 trzech wyjątków od zakazu sformułowanego w art. 22 ust. 1²⁴². Są to: niezbędność do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem; dozwoleńie prawem Unii lub prawem państwa członkowskiego, któremu podlega

²³⁸ Motyw 71, RODO.

²³⁹ Zob. Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji...*, *op. cit.*, s. 25.

²⁴⁰ Zob. L.A. Bygrave, *Automated Profiling Minding The Machine...*, *op. cit.*, s. 17.

²⁴¹ Zob. AlgorithmWatch, Bertelsmann Stiftung i Open Society Foundations, *op. cit.*; Fundacja ePaństwo, *op. cit.*

²⁴² Dwie z trzech najważniejszych różnic między przepisami *dyrektywy 95/46/WE* a RODO w odniesieniu do zautomatyzowanego podejmowania decyzji wskazywane przez Wachter i innych dotyczą katalogu sformułowanych w art. 22 wyjątków, zob. S. Wachter, B. Mittelstadt, L. Floridi, *op. cit.*, s. 81–82.

administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub oparcie na wyraźnej zgodzie osoby, której dane dotyczą. Wyjątki należy traktować rozłącznie, czyli jeśli dana sytuacja może zostać podporządkowana pod jedną z uwzględnionych w RODO kategorii, jest to wystarczające dla uzasadnienia zautomatyzowanego podejmowania decyzji.

Nowością, w stosunku do *dyrektywy 95/46/WE*, jest uwzględnienie w katalogu sytuacji z art. 22 ust. 2 wyraźnej zgody osoby, której dane dotyczą, jako przyczyny, w związku z którą ust. 1 może nie mieć zastosowania. „Zgoda” osoby, której dane dotyczą, została zdefiniowana w art. 4 RODO jako „dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych”. Przymiotniki użyte w tej definicji podkreślają konieczność pozyskania zgody, będącej wynikiem podjęcia przez jednostkę świadomej decyzji. Ich wagę podkreśla art. 7 RODO, w którego ust. 4 zostało zakazane uzależnianie wykonania umowy od wyrażenia zgody, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania umowy. Zważywszy na fakt, że w RODO brak definicji „wyraźnej zgody”, można domniemywać, że kryteria ocenienia zgody jako wyraźnej powinny być jeszcze surowsze, niż te odnoszące się do „zgody” samej w sobie.

Można wyobrazić sobie jednak sytuację, w której zgoda na przetwarzanie danych zostaje uzasadniona, jako niezbędna np. do udoskonalania świadczonej usługi. W świetle zachodzących w gospodarce cyfrowej procesów rosnącej koncentracji siły rynkowej potentatów przetwarzania danych osobowych możliwy do rozważenia jest również scenariusz, w którym udzielenie zgody przez jednostkę będzie uwarunkowane brakiem alternatywy w stosunku do danego usługodawcy²⁴³. Tym samym obecność wyjątku w postaci zgody będzie stanowić, prawdopodobnie, poważne utrudnienie w skutecznym korzystaniu przez podmioty danych z rozwiązań przyjętych w art. 22. Dlatego też uwzględnienie tego wyjątku w RODO, mimo wzmocnienia roli zgody i sprecyzowania przepisów dotyczących warunków, jakie musi ona spełniać²⁴⁴, pozostawia aktualny problem, który najkrócej można ująć pytaniem: „dlaczego w prywatności chodzi o władzę, a nie o zgodę (lub szkodę)?”²⁴⁵.

²⁴³ Czego najoczywistszymi przykładami są próby wspólnej pracy nad dokumentami *online* bez konta na Gmailu czy przejścia przez studia bez dostępu do Facebooka.

²⁴⁴ Zob. E. Politou, E. Alepis, C. Patsakis, *Forgetting personal data and revoking consent under the GDPR: Challenges and proposed solutions*, „Journal of Cybersecurity” 2018, s. 5–9 i dokonany w tym artykule przegląd literatury.

²⁴⁵ L.M. Austin, *Enough About Me: Why Privacy is About Power, not Consent (or Harm)*, [w:] *A World Without Privacy: What Law Can and Should Do?*, red. A. Sarat, Cambridge University Press, Cambridge 2015, s. 131–189.

W odniesieniu do wyjątku dotyczącego zawierania lub wykonania umowy, obecnego już w *dyrektywie 95/46/WE*, w RODO został usunięty wymóg, który dotyczył wniesienia wniosku w sprawie zawarcia lub realizacji umowy przez osobę, której dane dotyczą, i jego przyjęcia²⁴⁶. Treść RODO definiuje wyjątek w postaci sytuacji, w której decyzja jest niezbędna do zawarcia lub wykonania umowy – nie musi ona zatem wynikać z inicjatywy podmiotu danych. Jak zauważają Bygrave i Isak Mendoza „ciężko jest podać przykład, w którym zautomatyzowana decyzja musi zostać podjęta bez udziału człowieka”²⁴⁷. Racjonalizują oni przyjęcie takiego kryterium przeciwdziałaniem próbom obejścia art. 22 ust. 1 przez odwołanie do wystandaryzowanej umowy z podmiotem danych. Istotniejszym elementem tego wyjątku jest sytuacja, w której zautomatyzowana decyzja będzie niezbędna do wykonania umowy, np. świadczenia danej usługi.

Oba te wyjątki znajdują uzupełnienie w art. 22 ust. 3, który nakazuje administratorowi – w przypadku podejmowania zautomatyzowanych decyzji na ich podstawie – wdrażać właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą. Jako środki takie, które muszą zostać wdrożone, wymienione są: prawo do uzyskania interwencji ludzkiej ze strony administratora, prawo do wyrażenia własnego stanowiska oraz prawo do zakwestionowania decyzji²⁴⁸. Zestaw ten stanowi rozszerzoną wersję środków wymienianych w *dyrektywie 95/46/WE*, co może zostać ocenione jako wzmocnienie ochrony praw podmiotów danych²⁴⁹.

W odniesieniu do trzeciego z pojawiających się w art. 22 ust. 2 wyjątków, dotyczącego decyzji dozwolonych prawem Unii lub prawem państwa członkowskiego (art. 22 ust. 2 lit. b), wymóg przewidzenia właściwych środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, został wprowadzony bezpośrednio do treści wyjątku. Nie został w nim jednak uwzględniony konkretny wykaz środków, które powinny być wdrożone, aby zadośćuczynić temu obowiązkowi. Tym samym zautomatyzowane podejmowanie decyzji przewidziane w prawie państw członkowskich może podlegać różnego typu mechanizmom mających stanowić ochronę dla jednostek mu poddanych.

Podobny brak występuje w treści art. 22 ust. 4, zabraniającej podejmowania zautomatyzowanych decyzji, o których mowa w ust. 2, na podstawie szczególnych kategorii danych osobowych²⁵⁰ (wyjątek od wyjątków).

²⁴⁶ Zob. S. Wachter, B. Mittelstadt, L. Floridi, *op. cit.*, s. 82; I. Mendoza, L.A. Bygrave, *op. cit.*, s. 92.

²⁴⁷ I. Mendoza, L.A. Bygrave, *op. cit.*, s. 92.

²⁴⁸ Ich krytyczne omówienie, zob. M. Brkan, *op. cit.*, s. 17–19.

²⁴⁹ Zob. I. Mendoza, L.A. Bygrave, *op. cit.*, s. 92.

²⁵⁰ Art. 9 ust. 1 RODO „Przetwarzanie szczególnych kategorii danych osobowych” wymienia następujące kategorie danych: „dane osobowe ujawniające pochodzenie rasowe

Możliwość ewentualnego zautomatyzowanego podejmowania decyzji opartego na szczególnych kategoriach danych osobowych (uzasadnienie wyjątku od wyjątków) musi spełniać dwa warunki. Pierwszym warunkiem jest oparcie jej na jednej z dwóch przesłanek wymienionych w art. 9 RODO. Przesłanka sformułowana w art. 9 ust. 2 lit. a to wyraźna zgoda na przetwarzanie tych danych osobowych²⁵¹. Przesłanka sformułowana w art. 9 ust. 2 lit. g to sytuacja, w której przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym na podstawie prawa Unii lub prawa państwa członkowskiego. Działanie takie musi być proporcjonalne i nie może naruszać istoty prawa do ochrony danych. Ponadto przewidziane muszą być odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą. Drugim warunkiem jest istnienie właściwych środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą. Wymóg ten, w odniesieniu do wyjątku opartego na art. 9 ust. 2 lit. g RODO, jest redundantny, ponieważ jest on wspomniany zarówno w tym przepisie, jak i w art. 22 ust. 4 RODO.

W celu oceny, czy zautomatyzowane podejmowanie decyzji jest objęte zakazem z art. 22 RODO, jest zatem konieczne przeprowadzenie trzystopniowego testu. Po pierwsze, stwierdzenie, czy dana decyzja spełnia wymogi definicyjne RODO. Po drugie, sprawdzenie, czy należy ona do jednej z kategorii wyjątków z art. 22 ust. 2 i czy są wprowadzone przewidziane w rozporządzeniu środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą (w wypadku lit. a i c – co najmniej wymienione w RODO, w wypadku lit. b – istnieje w tym zakresie niejasność interpretacyjna). Po trzecie, należy sprawdzić, czy decyzja, która przeszła pozytywnie dwa pierwsze etapy testu, nie jest oparta na szczególnych kategoriach danych osobowych. Z zasady nie będzie ona wówczas dozwolona. Wyjątki wynikające z art. 9 ust. 2 lit. a i g będą musiały być obwarowane również istnieniem właściwych środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą. Już to krótkie podsumowanie ukazuje rolę rozumienia pojęcia „środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą” jako istotnego elementu budującego ramy prawne ochrony podmiotów danych, a niebędącego całkowicie zuniifikowanym na poziomie RODO.

lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby”. Dane genetyczne, biometryczne i dotyczące zdrowia są ponadto zdefiniowane w art. 4 RODO (pkt 13–15).

²⁵¹ „[...] chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu przetwarzania szczególnych kategorii danych osobowych” – art. 9 ust. 2 lit. a, RODO.

Problem wdrażania środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, stanowi bardzo wyraźny przejaw przemawiający za możliwością pozytywnej weryfikacji drugiej z hipotez badanych w tym rozdziale. Poziom zróżnicowania realizacji obowiązków wynikających z art. 22 ust. 2 lit. b oraz ust. 3 ciążących na państwach jest wysoki. W odniesieniu do art. 22 ust. 2 lit. b poziom zróżnicowania wprowadzanych rozwiązań wykazało przeprowadzone przez Malgierego badanie porównawcze²⁵². Badacz ten wyodrębnił cztery podejścia do problemu: (1) negatywne, czyli państwa członkowskie, które nie wprowadziły żadnych wyjątków na podstawie art. 22 ust. 2 lit. b, np. Włochy, Rumunia, Szwecja, Dania, Finlandia oraz – ogólnie – większość państw UE²⁵³; (2) neutralne, czyli wprowadzenie art. 22 ust. 2 lit. b do porządku krajowego, ale bez definiowania dodatkowych uprawnień dla podmiotów danych, np. w Niemczech, Austrii i Belgii, a jedynie posłużenie się rozwiązaniami proponowanymi w RODO; (3) proceduralne, czyli gwarantujące konkretniejsze uprawnienia podmiotom danych, przez opis procedur koniecznych podczas zautomatyzowanego podejmowania decyzji lub formę oceny skutków używania algorytmu, np. w Zjednoczonym Królestwie i Irlandii; (4) proaktywne, zaobserwowane we Francji i Węgrzech, czyli propozycje nowych i konkretnych zabezpieczeń dla jednostki, np. prawo do informacji na temat wag przybieranych przez różne parametry w ramach posługiwania się algorytmem.

Analiza Malgierego dostarcza przykładu zróżnicowania pojawiającego się w wyniku pozostawienia państwu członkowskim UE swobody decyzyjnej w zakresie wdrażania do porządków krajowych niektórych z przepisów RODO. Zważywszy na szybki rozwój rozwiązań, które mają służyć „automatyzacji prawa”, brak precyzji w zakresie rozwiązań mających zabezpieczać jednostki jest niepokojący. Prowadzi on do dywersyfikacji standardów ochrony jednostki, wbrew intencji unifikacji prawa ochrony danych osobowych w UE stojącej za przyjęciem RODO. Na uwagę zasługuje fakt, że ten brak precyzji

²⁵² Zob. G. Malgieri, *Automated Decision-Making in the EU Member States: The Right to Explanation and Other “Suitable Safeguards” for Algorithmic Decisions in the EU National Legislations*, „Computer Law & Security Review” 2019, t. 35, nr 5.

²⁵³ G. Malgieri wymienia wśród tych państw Polskę, ale w związku z przyjęciem art. 70a prawa bankowego, którego ust. 1 brzmi: „Banki i inne instytucje ustawowo upoważnione do udzielania kredytów na wniosek osoby fizycznej, prawnej lub jednostki organizacyjnej niemającej osobowości prawnej, o ile posiada zdolność prawną, ubiegającej się o kredyt przekazują, w formie pisemnej, wyjaśnienie dotyczące dokonanej przez siebie oceny zdolności kredytowej wnioskującego”, oraz ust. 2: „Wyjaśnienie, o którym mowa w ust. 1, obejmuje informacje na temat czynników, w tym danych osobowych wnioskującego, które miały wpływ na dokonaną ocenę zdolności kredytowej”, taki sposób zakwalifikowania Polski jest nieaktualny – zob. *Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe*, Dz.U. 1997 nr 140 poz. 939.

odnosi się szczególnie do wyjątków dozwolonych prawem Unii lub prawem państwa członkowskiego.

Tym samym waga zautomatyzowanego podejmowania decyzji w obszarze działań sektora prywatnego może ulec odwróceniu na dwa sposoby. Po pierwsze, państwa mogą wprowadzać przepisy umożliwiające zautomatyzowane podejmowanie decyzji w stosunku do spraw objętych prawem publicznym, np. w odniesieniu do usług publicznych. Można wyobrazić sobie sytuację, w których rozwiązania takie byłyby wprowadzane na podstawie wyjątków z art. 22 ust. 4 w zw. z art. 9 ust. 2 lit g (ważny interes publiczny), a tym samym możliwe byłoby korzystanie z przetwarzania szczególnych kategorii danych. Niejasność w zakresie koniecznych do zastosowania zabezpieczeń interesów jednostki w takim scenariuszu jest istotnym argumentem za poszukiwaniem rozwiązań opartych niekoniecznie na reżimie ochrony danych osobowych. Po drugie zaś, państwa mogą wprowadzać aktem prawnym wyjątki dotyczące zautomatyzowanego podejmowania decyzji w danych sektorach, jak np. w zakresie bankowości czy ubezpieczeń. Ponownie to od państwa zależy w takim układzie, co zostanie potraktowane jako środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

2.1.3. Obowiązki informacyjne i prawo dostępu: kontrowersje wokół „prawa do wyjaśnienia”

Rozwiązania dotychczas wdrażane przez państwa i opisane przez Malgierego – szczególnie te proaktywne, czyli prawo do informacji na temat wag przybieranych przez różne parametry w ramach posługiwania się algorytmem – odsyłają do drugiego filaru regulacji zautomatyzowanego podejmowania decyzji w rozporządzeniu. Są to przepisy dotyczące informacji o logice stojącej za zautomatyzowanym podejmowaniem decyzji, które ma prawo otrzymać podmiot danych, nazywanych w debacie akademickiej „prawem do wyjaśnienia”²⁵⁴. Prawo to jest wymienione w RODO tylko raz, w motywie 71, gdzie

²⁵⁴ Kluczowe artykuły na ten temat to tekst Bryce’a Goodmana i Seta Flaxmana, który zapoczątkował debatę o prawie do wyjaśnienia, w ramach której istotną rolę odegrały przywoływane już analizy Wachter, Mittelstadta i Floridego (*Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*), Malgierego i Comandé (*Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*), Selbsta i Julii Powles (A.D. Selbst, J. Powles, *Meaningful information and the right to explanation*, „International Data Privacy Law” 2017, t. 7, nr 4, s. 233–242), prace Edwardsa i Vealego oraz Brkan. Na tle tej debaty pojawiły się również inne propozycje oraz bardziej szczegółowe analizy dotyczące samego pojęcia wyjaśnienia i do czego może lub powinno się odnosić, jak wspominał wyżej prace autorstwa Edwardsa i Vealego, rozważania Wachter, Mittelstadta i Chrisa Russela dotyczące wyjaśnień kontrfaktycznych (S. Wachter, B. Mittelstadt, Ch. Russel, *Counterfactual Explanations without Opening the Black Box: Automated Decisions and the GDPR Article*, „Harvard Journal of Law and Technology” 2018, t. 31, nr 2, s. 841–887) oraz próby integrowania przepisów

pojawiają się przykłady odpowiednich zabezpieczeń, jakie powinny być wdrażane w razie korzystania z wyjątków do zakazu podejmowania zautomatyzowanych decyzji. Wymienione wśród nich zostały: „informowanie osoby, której dane dotyczą, prawo do uzyskania interwencji człowieka, prawo do wyrażenia własnego stanowiska, prawo do uzyskania wyjaśnienia co do decyzji wynikłej z takiej oceny oraz prawo do zakwestionowania takiej decyzji”²⁵⁵. Pojawiające się w motywie 71 prawo do uzyskania wyjaśnienia, jako jedyny ze środków wymienionych w motywie, nie jest jednak przywołane w treści samych przepisów. Należy postawić pytanie, czy mimo to można stwierdzić, że jest on obecny wśród praw przysługujących podmiotom danych?

W porównaniu z rozwiązaniami istniejącymi na gruncie *dyrektywy 95/46/WE*, RODO znacznie rozbudowuje obowiązki informacyjne administratora danych. W odniesieniu do zautomatyzowanego podejmowania decyzji prawa osoby, której dane dotyczą, obejmują trzy elementy. Po pierwsze, zgodnie z art. 13 ust. 2 lit. f, podczas pozyskiwania danych osobowych od osoby, której dane dotyczą, administrator podaje tej osobie informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą. Po drugie, zgodnie z art. 14 ust. 2 lit. g, w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą, administrator ma identyczny obowiązek przekazania informacji na temat zautomatyzowanego podejmowania decyzji osobie, której dane dotyczą. Po trzecie, na podstawie art. 15 ust. 1 lit. h, osobie, której dane dotyczą, przysługuje prawo dostępu. W związku z tym ma ona prawo do uzyskania od administratora potwierdzenia, czy są przetwarzane jej dane osobowe, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz informacji o zautomatyzowanym podejmowaniu decyzji obejmujących dokładnie te same elementy co w przypadku art. 13 ust. 2 lit. f i art. 14 ust. 2 lit. g²⁵⁶.

W związku z tymi przepisami Bryce Goodman i Seth Flaxman postawili hipotezę, zgodnie z którą RODO stworzyć miało „prawo do wyjaśnienia” umożliwiające jednostce zapytanie o wyjaśnienie podjętej w stosunku do niego zalgorytmizowanej decyzji²⁵⁷. Odnotowując obecność podobnego

RODO z perspektywą technologiczną: T.W. Kim, B.R. Routledge, *Informational Privacy, A Right to Explanation, and Interpretable AI*, „Conference: IEEE PAC (Privacy-Aware Computing) 2018”. <https://ieeexplore.ieee.org/document/8511831>, dostęp: 1.04.2021.

²⁵⁵ Co może również rodzić pytanie, czy sformułowanie „prawo do zakwestionowania takiej decyzji” odnosi się do tych sytuacji, które podlegają wyjątkom przewidzianym w art. 22, w których decyzja może być podjęta.

²⁵⁶ Art. 13–15 skomentowane są ponadto w motywach 60–63, RODO.

²⁵⁷ Zob. B. Goodman, S. Flaxman, *op. cit.*, s. 1.

rozwiązania w *dyrektywie 95/46/WE*, swoje optymistyczne założenie co do „efektywności” nowych rozwiązań oparli oni na trzech przesłankach²⁵⁸: przyjęciu rozporządzenia w miejsce dyrektywy²⁵⁹; wysokich karach grożących zgodnie z RODO za naruszenia w zakresie ochrony danych osobowych; oraz na globalnym charakterze RODO jako rozporządzenia mającego skutki eksterytorialne. Nie podali oni w wątpliwość samej treści przepisów dotyczących informacji na temat zautomatyzowanego podejmowania decyzji i tego, do jakiego stopnia w rzeczywistości wprowadzają one prawo do wyjaśnienia.

Tekst Goodmana i Flaxmana zapoczątkował dyskusję w środowiskach naukowych, zajmujących się prawem ochrony danych osobowych, a dotyczącą tego, czy i jeśli tak, to w jakiej formie, RODO wprowadza prawo do wyjaśnienia. Pierwszym głosem krytycznym wobec ich hipotezy była publikacja Wachter, Mittelstadta i Floridego. Ich ocena istnienia w RODO prawa do wyjaśnienia jest bardzo sceptyczna i sprowadza się do postrzegania go jako prawa do bycia poinformowanym. Autorzy wskazują trzy możliwe do rozważenia źródła prawa do wyjaśnienia w RODO, czyli art. 22 ust. 3 i związany z nim motyw 71, obowiązki informacyjne sformułowane w art. 13–14 i związane z nimi motywy 60–62 oraz prawo dostępu w art. 15 i związany z nim motyw 63²⁶⁰. Pierwsza możliwość zostaje wykluczona przez wykładnię art. 22. Nie jest w nim wymienione wprost prawo do wyjaśnienia jako jeden ze środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą. Autorzy wskazują, że w ramach prac nad rozporządzeniem, w propozycji poprawek wystosowanych przez Parlament Europejski, prawo do wyjaśnienia miało znaleźć się w treści obecnego art. 22, lecz w toku dalszych negocjacji zrezygnowano z takiego rozwiązania²⁶¹. Dlatego też należy stwierdzić, że nie było intencją unijnych prawodawców, aby obowiązek wyjaśnienia zautomatyzowanej decyzji na gruncie art. 22 RODO był prawnie wiążący.

Pozostałe dwie możliwości rozważane przez Wachter, Mittelstadta i Floridego odnoszą się do zaproponowanego przez nich podziału wyjaśnień zgodnie z dwoma kryteriami. Po pierwsze, wyjaśnienia mogą dotyczyć funkcjonalności danego systemu albo konkretnej decyzji²⁶². Po drugie, wyjaśnienia mogą być tworzone przed wydaniem zautomatyzowanej decyzji lub po jej

²⁵⁸ *Ibidem*, s. 2.

²⁵⁹ Co w świetle opisanych powyżej rozbieżności interpretacyjnych na tle art. 22 może wzbudzać pewną podejrzliwość.

²⁶⁰ Zob. S. Wachter, B. Mittelstadt, L. Floridi, *op. cit.*, s. 79.

²⁶¹ *Ibidem*, s. 81.

²⁶² Podział ten jest bardzo podobny do opisanego w rozdziale pierwszym podziału na wyjaśnienie stawiające w centrum model i wyjaśnienie stawiające w centrum podmiot danych proponowanego przez L. Edwards, M. Veale, *Slave to the Algorithm...*, *op. cit.*

wydaniu (*ex ante* lub *ex post*)²⁶³. Zgodnie z interpretacją art. 13–14 RODO informacje dotyczące istnienia zautomatyzowanego podejmowania decyzji, istotne informacje o zasadach ich podejmowania, o znaczeniu zautomatyzowanego podejmowania decyzji i jego przewidywanych konsekwencjach dla osoby, której dane dotyczą, mogą być przekazane podmiotowi danych przed wydaniem decyzji (podczas pozyskiwania danych osobowych). W związku z tym w przekonaniu autorów mogą one dotyczyć jedynie funkcjonalności systemu podejmowania decyzji, nie zaś konkretnej decyzji (ponieważ nie została ona jeszcze wydana). Według Wachter, Mittelstadta i Floridego ten sam problem dotyczy prawa dostępu z art. 15. Swoją interpretację uzasadniają oni faktem, że w art. 15 zostaje powtórzone sformułowanie „przewidywane” konsekwencje, co wskazywałoby na dostarczanie informacji dotyczących jeszcze niewydanej decyzji²⁶⁴. Autorzy odwołują się również do analizy różnych sposobów implementacji przepisów *dyrektywy 95/46/WE*, dochodząc ostatecznie do konkluzji, że przyjęte w RODO rozwiązanie dotyczące prawa dostępu do informacji na temat zautomatyzowanego podejmowania decyzji prowadzi do przyjęcia standardu ochrony niższego niż obowiązujący dotychczas w części państw członkowskich UE²⁶⁵. Konkluzją analizy Wachter, Mittelstadta i Floridego jest stwierdzenie, że w RODO nie uwzględniono prawa do wyjaśnienia, chociaż zawarto w jego przepisach prawo do bycia poinformowanym (*right to be informed*) o zautomatyzowanym podejmowaniu decyzji, włączając w to elementy informacji wymienione w art. 13–15.

Takiej optyce przeciwstawiają się Malgieri i Comandé, którzy określają prawo do wyjaśnienia jako prawo do czytelności (*legibility*)²⁶⁶ zautomatyzowanych decyzji. Ich argumentacja w dużym stopniu opiera się na systemowej wykładni art. 15. Podkreślają oni, że mimo literalnie takiego samego brzmienia art. 13 ust. 2 lit. f, art. 14 ust. 2 lit. g i art. 15 ust. 1 lit. h, ich systemowe znaczenie jest zupełnie inne. Prawo dostępu może być wykonane w każdym momencie przez jednostkę, podczas gdy obowiązki informacyjne ciążyą na administratorze danych w momencie rozpoczęcia przetwarzania danych²⁶⁷.

²⁶³ Zob. S. Wachter, B. Mittelstadt, L. Floridi, *op. cit.*, s. 78.

²⁶⁴ Oraz z zestawienia różnych wersji językowych RODO, zob. S. Wachter, B. Mittelstadt, L. Floridi, *op. cit.*, s. 83.

²⁶⁵ S. Wachter, B. Mittelstadt, L. Floridi, *op. cit.*, s. 89.

²⁶⁶ Pojęcie *legibility* nastrocza trudności w tłumaczeniu, przede wszystkim ze względu na fakt, że Malgieri i Comandé czynią rozróżnienie między *readability* i *legibility*. Proponują odnosić się do tych pojęć jako odpowiednio do „odczytywalności” i „czytelności”. Zob. G. Malgieri, G. Comandé, *op. cit.*, s. 245.

²⁶⁷ „Chociaż sformułowanie jest dokładnie takie samo w art. 13 ust. 2 lit. f, 14 ust. 2 lit. g i 15 ust. 1 lit. h, rola tych przepisów znacznie się różni. Podczas gdy art. 13 i 14 wprowadzają «obowiązki informacyjne», tj. informacja musi być dostarczona, kiedy przetwarzanie danych się rozpoczyna (tj. kiedy dane osobowe zostają otrzymane przez administratora),

Odwolując się do kategorii stworzonych przez Wachter, Mittelstadta i Floridego, można powiedzieć, że Malgieri i Comandé stwierdzają, że art. 15 może dotyczyć zarówno wyjaśnienia *ex ante*, jak i wyjaśnienia *ex post* – a tym samym może odnosić się do konkretnej decyzji podjętej wobec danej jednostki. Ich interpretacja jest rozbieżna z interpretacją Wachter, Mittelstadta i Floridego: na podstawie art. 15 pojawia się możliwość otrzymania wyjaśnienia danej decyzji *ex post*.

Po pierwsze, odwołują się oni do brzmienia art. 15, który np. w ust. 1 lit. a pomija pojawiające się w art. 13–14 sformułowanie „do których mają posłużyć” (*intended*) cele przetwarzania²⁶⁸, co może wskazywać na – w przeciwieństwie do art. 13–14 – brak jednoznacznego ukierunkowania art. 15 na przyszłość. O podobnie dwoistej orientacji art. 15 może świadczyć sformułowanie „zostały lub zostaną ujawnione” (art. 15 ust. 1 lit. c). Po drugie, w art. 15 sformułowanie „przewidywane konsekwencje” może odnosić się do konsekwencji występujących w przyszłości w stosunku do wykonywania prawa dostępu (względna przyszłość liczona w stosunku do wykonania prawa dostępu). Tym samym niekoniecznie konsekwencje te muszą być przewidywane w czasie podejmowania decyzji (względna przyszłość liczona w stosunku do podejmowania decyzji). Dzięki takiej perspektywie autorzy wykazują możliwość interpretacji art. 15 jako źródła szerszych uprawnień dotyczących szans pozyskania dostępu do informacji o zautomatyzowanym przetwarzaniu, niż w wypadku perspektywy prezentowanej przez Wachter, Mittelstadta i Floridego.

Ponadto Malgieri i Comandé zwracają uwagę na dualną budowę prawa dotyczącego otrzymania informacji o zautomatyzowanym podejmowaniu decyzji. Składa się ono z członu pierwszego, czyli informacji o istnieniu (*existence*)²⁶⁹ zautomatyzowanego podejmowania decyzji, oraz członu drugiego, czyli istotnych (*meaningful*) informacji o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania. Kluczem do interpretacji treści art. 15 jest zdaniem autorów słowo „istotne”, które – zwłaszcza w angielskiej wersji językowej – ma co najmniej dwa znaczenia: „mające na celu ukazać znaczenie” (tj. wyjaśniające)

art. 15 wprowadza prawo dostępu, które może być wykonane w dowolnym momencie”. G. Malgieri, G. Comandé, *op. cit.*, s. 255.

²⁶⁸ W polskim tłumaczeniu RODO sformułowanie „do których mają posłużyć” pojawia się jedynie w art. 14 ust. 1 lit. c: „cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania”. Brakuje go w art. 13 ust. 1 lit. c: „cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania”. Tymczasem wersja angielska w obydwu wypadkach zawiera sformułowanie: *the purposes of the processing for which the personal data are intended as well as the legal basis for the processing*, podczas gdy w art. 15 ust. 1 lit. a pojawia się jedynie sformułowanie: *the purposes of the processing*.

²⁶⁹ Słowo to również zostało pominięte w polskim tłumaczeniu.

i „poważne, ważne, użyteczne” (tj. znaczące)²⁷⁰. Fraza ta prowadzi autorów do konkluzji, zgodnie z którą art. 15 zawiera prawo do czytelności zautomatyzowanych decyzji. Informacja, którą powinien otrzymać podmiot danych, ma nie tylko zwiększać przejrzystość procesu zautomatyzowanego podejmowania decyzji, lecz również zwiększać jego zrozumiałość dla podmiotu danych. Przekazane informacje mają być, z perspektywy podmiotu danych, znaczące do zrozumienia przez niego, jakiego rodzaju procesowi, o jakim znaczeniu i o jakich skutkach, jest on poddany²⁷¹.

Trzecią ważną ścieżkę interpretacyjną zaproponowali Selbst i Powles, definiujący prawo do wyjaśnienia jako prawo do informacji istotnej dla podmiotu danych. Swoją wykładnię prawa do wyjaśnienia oparli oni na systemowej i teleologicznej interpretacji przepisów zawartych w art. 13–15, czyli powiązaniu obowiązków informacyjnych administratora i prawa dostępu podmiotu danych z innymi prawami w RODO, których realizacji mają one służyć. Skoro celem zawarcia tych przepisów w RODO jest umożliwienie podmiotowi danych zrozumienia, na czym polega i jakie może mieć konsekwencje przetwarzanie jego danych, niezbędne jest dokonywanie wykładni tego, czym jest informacja na temat tego przetwarzania, z uwzględnieniem jej użyteczności dla podmiotu danych. W związku z tym Selbst i Powles kładą nacisk na konieczność uwzględnienia niewysokich kompetencji technicznych jednostek, które powinny być brane pod uwagę podczas formułowania informacji istotnych z perspektywy podmiotu danych²⁷².

Dzięki skupieniu się na interpretacji sformułowania „istotne informacje” Selbst i Powles kwestionują dokonany przez Wachter, Mittelstadta i Floridego podział na wyjaśnienie ogólnej funkcjonalności systemu zautomatyzowanego podejmowania decyzji i wyjaśnienie konkretnej decyzji. Na podstawie argumentów odnoszących się do technologii używanych w celu tworzenia systemów zautomatyzowanego podejmowania decyzji Selbst i Powles twierdzą, że nie jest możliwe oddzielenie wyjaśnienia logiki, zgodnie z którą operuje system zautomatyzowanego podejmowania decyzji, i zasad stojących

²⁷⁰ Zob. G. Malgieri, G. Comandé, *op. cit.*, s. 257. Polska wersja językowa sprawia wrażenie podkreślającej konieczność wypełnienia przez informację raczej drugiego z wymienionych znaczeń.

²⁷¹ W celu ułatwienia implementacji koncepcji czytelności zautomatyzowanego podejmowania decyzji Malgieri i Comandé opracowali zestaw kilkudziesięciu pytań, które mogą pomóc w przygotowaniu istotnych informacji na temat systemu zautomatyzowanego podejmowania decyzji. G. Malgieri, G. Comandé, *op. cit.*, s. 258–261.

²⁷² „ponieważ artykuły 13–15 wszystkie odnoszą się do praw podmiotu danych, istotna informacja powinna być interpretowana w odniesieniu do podmiotu danych. W związku z tym informacja na temat zasad podejmowania zautomatyzowanej decyzji musi być istotna dla podmiotu danych, przede wszystkim człowieka i z założenia niemającego szczególnie zaawansowanych umiejętności technicznych”. A.D. Selbst, J. Powles, *op. cit.*, s. 236.

za podjęciem konkretnej decyzji²⁷³. Zważywszy na to, że dany model jest używany do zdeterminowania sytuacji jednostki, informacje na temat modelu powinny także dostarczać danych na temat konkretnej decyzji. W związku z tym autorzy kwestionują również dokonany przez Wachter, Mittelstadta i Floridego podział na wyjaśnienia *ex ante* i *ex post*: jak długo możliwe jest wyjaśnienie funkcjonalności modelu, tak długo można przewidzieć wynik decyzji dla konkretnej jednostki, w związku z tym możliwe jest udzielenie jej informacji na temat danej decyzji w dowolnym momencie procesu jej podejmowania, nie zaś jedynie po jej wydaniu²⁷⁴.

Wytyczne Grupy Roboczej Art. 29 wydają się potwierdzać interpretację przedstawioną przez Selbsta i Powles. Po pierwsze, wytyczne wskazują na skupienie dostarczanych jednostce informacji na przyczynach podjęcia wobec niej konkretnej decyzji. Nie jest konieczne, żeby wyjaśnienie uwzględniało w bardzo szczegółowym stopniu informacje dotyczące stojących za decyzją rozwiązań technicznych²⁷⁵. Zgodnie z wytycznymi wskazane jest raczej skupienie na tym, aby informacje były zrozumiałe, w tym np. podawały konkretne przykłady potencjalnego wpływu przetwarzania²⁷⁶. Po drugie, wytyczne potwierdzają związek między celem dostarczania jednostce wymienionych informacji a umożliwieniem jej wykonywania innych praw zdefiniowanych w RODO, przede wszystkim zakwestionowania podjętej wobec niej decyzji²⁷⁷. Sugerowany jest również związek między wypełnianiem obowiązków

²⁷³ Zob. A.D. Selbst, J. Powles, *op. cit.*, s. 239–240.

²⁷⁴ „Od momentu, w którym można wyjaśnić *funkcjonalność systemu*, można również wyjaśnić *konkretną decyzję*. Wynika to z faktu, że większość modeli jest deterministycznych od momentu ich stworzenia. Żeby określić wynik, prawdą jest, że niezbędne jest wprowadzenie do modelu danych, co oznacza, że dane są przetwarzane. Ale podział *ex ante* – *ex post* zarysowany przez autorów nie dotyczy kategorii przed i po przetwarzaniu, a raczej przed i podjęciu decyzji. Ze względu na fakt, że *konkretna decyzja* może być ujawniona po przetwarzaniu danych, bez konieczności jej podjęcia, podział zgodnie z kryterium czasu nie ma sensu; wyjaśnienie zarówno *konkretnej decyzji* jak i *funkcjonalności systemu* jest dostępne przed podjęciem ostatecznej decyzji”. A.D. Selbst, J. Powles, *op. cit.*, s. 240.

²⁷⁵ „Zgodnie z przepisami RODO administrator jest zobowiązany do przekazania osobie, której dane dotyczą, istotnych informacji o zasadach podejmowania decyzji – informacje te niekoniecznie muszą mieć postać szczegółowego objaśnienia stosowanych algorytmów lub ujawnienia ich w całości. Przekazywane informacje powinny jednak być na tyle wyczerpujące, by osoba, której dane dotyczą, zrozumiała powody podjętej decyzji”. Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji...*, *op. cit.*, s. 29.

²⁷⁶ „Aby przekazywane informacje były istotne i zrozumiałe, administrator powinien przedstawić autentyczne, konkretne przykłady takiego potencjalnego wpływu przetwarzania na osobę, której dane dotyczą”. Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji...*, *op. cit.*, s. 30.

²⁷⁷ Zob. Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji...*, *op. cit.*, s. 31.

informacyjnych a zabezpieczeniami przywoływanymi w art. 22 ust. 3²⁷⁸. Po trzeciej zaś, kwestionują one – chociaż nie w duchu argumentacji przedstawionej przez Selbsta i Powles – podział możliwych do otrzymania przez podmiot danych informacji zgodnie z kryterium czasowym, przez odwołanie do możliwości otrzymania informacji na temat „podjętej decyzji”²⁷⁹.

2.1.4. Zakaz podejmowania zautomatyzowanych decyzji i prawo do wyjaśnienia: podsumowanie ustaleń

W świetle braku orzecznictwa TSUE dotyczącego zautomatyzowanego podejmowania decyzji niezbędne jest dokonanie pewnych wyborów w odniesieniu do problemów wynikających ze sposobu sformułowania artykułów 13–15 oraz 22 RODO. Dokładna lektura przepisów RODO oraz literatury powstałej w związku z próbą dokonania ich interpretacji pozwala stwierdzić, że art. 13–15 potwierdzają istnienie w rozporządzeniu prawa, które niekoniecznie może być nazwane prawem do wyjaśnienia, lecz raczej bardziej precyzyjnie: „prawem podmiotu danych do bycia poinformowanym o powodach stojących za podjętą wobec niego zautomatyzowaną decyzją” (*right of the data subject to be informed about the reasons for the automated decision*)²⁸⁰.

Prawo to obejmuje dwa elementy: po pierwsze prawo do otrzymania informacji o samym istnieniu systemu zautomatyzowanego podejmowania decyzji, który ma być użyty w danym przypadku wobec jednostki, po drugie katalogu bardziej szczegółowych informacji dotyczących tego systemu. W związku z uwzględnieniem tych kategorii informacji w art. 13–15 RODO można stwierdzić, że informacje takie powinny być udzielone jednostce w związku ze zbieraniem od niej danych, które mają być wykorzystane do przetwarzania w systemie zautomatyzowanego podejmowania decyzji (art. 13: podczas pozyskiwania danych osobowych od podmiotu danych i art. 14: w wypadku, w którym dane zostały pozyskane w inny sposób w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca²⁸¹) oraz w każdym innym dowolnym momencie, na żądanie podmiotu danych na podstawie treści art. 15²⁸².

Charakter tych przepisów powinien być postrzegany z perspektywy dwójnej funkcji, którą pełnią. Z jednej strony są one same w sobie prawami

²⁷⁸ „Udzielanie takich informacji ułatwi również administratorom wypełnienie wymogów w zakresie zabezpieczeń, o których mowa w art. 22 ust. 3 i motywie 71”. Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji...*, *op. cit.*, s. 28.

²⁷⁹ Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji...*, *op. cit.*, s. 31.

²⁸⁰ M. Brkan, *op. cit.*, s. 23.

²⁸¹ Art. 14 ust. 3 lit. a, RODO.

²⁸² Zob. M. Brkan, *op. cit.*, s. 24.

podmiotu danych (tudzież w wypadku art. 13–14: obowiązkami administratora danych). Z drugiej jednak pozostają w funkcjonalnym związku z treścią art. 22, a także z prawami podmiotu danych wynikającymi z RODO i wprowadzonych w nim zakazów. Uzasadnienie dla takiej perspektywy można oprzeć na orzecznictwie TSUE powstałym na kanwie *dyrektywy 95/46/WE*, w którym obecne jest postrzeganie prawa dostępu jako instrumentu służącego realizacji innych praw podmiotów danych. To właśnie art. 12 dyrektywy, w związku z art. 14, stanowił podstawę wykładni jej przepisów prowadzącej do sformułowania tzw. prawa do bycia zapomnianym²⁸³. Tym samym nie należy wątpić w istotną rolę, którą prawo podmiotu danych do bycia poinformowanym o powodach stojących za podjętej wobec niego zautomatyzowanej decyzji może odegrać w przyszłym orzecznictwie i ochronie praw podmiotów danych w UE.

Należy jednak rozważyć możliwe scenariusze wpływu przyjętych w RODO rozwiązań na zautomatyzowane podejmowanie decyzji w Europie, w świetle opisanych w rozdziale pierwszym wyzwań tworzonych przez nie dla zakazu dyskryminacji. Można postawić pytanie, czy na podstawie przepisów RODO możliwe jest zweryfikowanie, czy dana decyzja została przyjęta zgodnie z przesłankami o charakterze dyskryminacyjnym? Pytanie to odsyła zaś do bardziej szczegółowego zagadnienia, czyli: czym mają być dokładniej „istotne informacje o zasadach” podejmowania zautomatyzowanych decyzji, o ich „znaczeniu” i o „przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą”? Wymagane informacje wydają się odnosić do dwóch różnych kategorii. „Istotne informacje o zasadach ich podejmowania” odsyłają do samej logiki systemu stojącego za decyzją podjętą w zautomatyzowany sposób. Informacje o znaczeniu i przewidywanych konsekwencjach zautomatyzowanego podejmowania decyzji natomiast bezpośrednio odsyłają do „osoby, której dane dotyczą”. Tym samym problematyczne jest pytanie, czy mogą one stanowić istotne źródło wiedzy na temat całokształtu rozwiązań implementowanych w ramach systemu zautomatyzowanego podejmowania decyzji. Istnieje możliwość, że będą one albo sformułowane dość ogólnie (np. „znaczenie danej decyzji przejawia się we wpływie na to, jaki rodzaj pomocy może być udzielony osobie bezrobotnej” i „konsekwencją podjęcia danej decyzji jest zakwalifikowanie do danej kategorii bezrobotnych otrzymujących dany rodzaj pomocy”), albo będą szczegółowo odnosić się do danej sytuacji (np. „konsekwencją podjęcia danej decyzji będzie zmiana kwalifikacji podmiotu danych

²⁸³ Zob. M. Brkan, *op. cit.*, s. 22, a przede wszystkim Wyrok Trybunału z dnia 13 maja 2014 r. w sprawie połączonych C-131/12, *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi*, ECLI:EU:C:2014:317.

z grupy X do grupy Y”). Nie wydaje się jednak prawdopodobne, aby ten typ informacji mógł pozwolić ocenić, czy dany system zautomatyzowanego podejmowania decyzji jest dyskryminujący.

Tym samym należy zwrócić uwagę na znaczenie pojęcia istotnych informacji o zasadach ich podejmowania²⁸⁴. Po pierwsze, w świetle rozwoju technologii np. uczenia maszynowego, warto postawić pytanie: czy wymóg udzielenia podmiotowi danych tych informacji nie jest *de facto* zakazem posługiwania się algorytmami, których sposób działania jest niejasny dla ich twórców²⁸⁵? Skoro administrator danych nie byłby w stanie wyjaśnić zasad stojących za daną decyzją, w razie posługiwania się samouczącą technologią, to czy może na jej podstawie wydawać decyzję, skoro powinien poinformować podmiot danych właśnie o zasadach, na których się ona opiera? Można stwierdzić, że w takim wypadku wystarczające byłyby ogólne informacje przyświecające założeniom w procesie tworzenia danego kodu komputerowego²⁸⁶. Można jednak zastanawiać się, czy wymóg z art. 13–15 nie prowadzi do niemożności stosowania takich rozwiązań, dopóki nie zostanie stworzone istotne (*meaningful*) wyjaśnienie logiki decyzji podejmowanych przez zautomatyzowany system. Zgodnie jednak z uwagami poczynionymi w rozdziale pierwszym interpretacja treści art. 13–15 jako zakazu używania samouczących się technologii nie rozwiązuje problemów związanych z możliwą dyskryminacją za sprawą systemów zautomatyzowanego podejmowania decyzji.

Po drugie, prawo dostępu nie jest ograniczone do decyzji negatywnych. Można rozważać jego potencjalne „kolektywne” wykorzystanie w celu osiągnięcia jak najpełniejszych informacji na temat zasad podejmowania zautomatyzowanych decyzji. Jeśli informacje mają być istotne dla jednostki (a nie dla ich abstrakcyjnego odbiorcy), powinny różnić się w zależności od tego, kto prosi o dostęp do nich. Teoretycznie można by więc wyobrazić sobie scenariusz, zgodnie z którym skoordynowane wykonywanie prawa dostępu prowadzi do uzyskania szerszego obrazu logiki wykorzystywanej w ramach danego systemu podejmowania zautomatyzowanych decyzji. W praktyce możliwość skorzystania z takiego scenariusza odsyła do rozumienia sformułowania „istotne informacje” zarówno pod względem treści, którą takie

²⁸⁴ Na znaczenie tego wymogu w RODO w świetle antydyskryminacji zwraca uwagę M. Brkan, *op. cit.*, s. 28.

²⁸⁵ Podobnie twierdzi M. Brkan: „[...] że przejrzystość algorytmów, mówiąc z perspektywy prawnej, powinna obejmować przejrzystość procesu podejmowania decyzji algorytmicznych w zakresie, w jakim jest to konieczne do zapewnienia poszanowania innych praw wynikających z RODO, w szczególności w odniesieniu do poinformowania osoby, której dane dotyczą, na temat istotnych informacji o zasadach, o których mowa w art. 13–15”. M. Brkan, *op. cit.*, s. 28.

²⁸⁶ Szczególnie w świetle cytowanych wytycznych Grupy Roboczej Art. 29, które wprost mówią o braku konieczności ujawniania całości algorytmu.

„istotne informacje” miałyby zawierać, jak i pod względem tego, dla kogo miałyby one być istotne.

Po trzecie, warto zauważyć, że w treści art. 15 brak jest odesłania do ochrony praw lub wolności innych osób w odniesieniu do reżimu ochrony własności intelektualnej czy tajemnicy handlowej. Pojawia się ono jednak w motywie 63 RODO, komentującym treść prawa dostępu: „Prawo to nie powinno negatywnie wpływać na prawa lub wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie chroniące oprogramowanie”²⁸⁷. Wzmocniona zostaje więc interpretacja, w której „istotne informacje” nie powinny być odczytywane jako dostęp do kodu źródłowego czy nawet jego fragmentów lub ogólnej architektury systemów zautomatyzowanego podejmowania decyzji.

W odniesieniu do praw i zakazu dotyczących zautomatyzowanego podejmowania decyzji uwzględnionych w RODO należy wskazać również na ograniczenia związane z samym zakresem stosowania tego rozporządzenia. Zgodnie z art. 2 ust. 2 RODO nie ma zastosowania m.in. w odniesieniu do przetwarzania danych osobowych w sytuacjach nieobjętych zakresem prawa UE. Rozwiązanie to może generować wątpliwości dotyczące sytuacji, w których zautomatyzowane podejmowanie decyzji jest wdrażane w obszarach niepodlegających unijnym regulacjom. Przynajmniej w odniesieniu do części decyzji podejmowanych na podstawie implementowanych systemów zautomatyzowanego podejmowania decyzji na poziomie krajowym, jednostka prawdopodobnie nie będzie miała możliwości powoływania się na przepisy RODO w celu egzekwowania dostępu do wyjaśnienia danej decyzji czy wyrażenia sprzeciwu wobec samego stosowania takiego systemu²⁸⁸.

²⁸⁷ Motyw 63, RODO.

²⁸⁸ Specyficzna na tym tle jest sytuacja prawna dotycząca stosowania zautomatyzowanego podejmowania decyzji w obszarze przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, które regulowane jest przez *dyrektywę 2016/680*. W świetle jej art. 11 decyzje, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i mają niekorzystne skutki prawne dla osoby, której dane dotyczą, lub poważnie na nią wpływają, są zakazane. Systemy takie mogą mieć zastosowanie jednak, jeśli dopuszcza je prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator oraz przewidziane są odpowiednie zabezpieczenia praw i wolności osoby, której dane dotyczą, a przynajmniej prawo do uzyskania interwencji ludzkiej ze strony administratora. Ponadto, zgodnie z art. 11 *dyrektywy 2016/680* zautomatyzowane decyzje nie mogą opierać się na danych osobowych szczególnych kategorii (ponownie, chyba że istnieją właściwe środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą), a zabronione jest profilowanie skutkujące dyskryminacją osób fizycznych na podstawie danych osobowych szczególnych kategorii. Z takim sposobem regulacji tego zagadnienia wiąże się wiele problemów. Po pierwsze, trudności związane z wykazaniem zautomatyzowanej dyskryminacji (których źródła opisane są w rozdziale pierwszym). Po drugie, możliwe zróżnicowanie podejścia do tego

Ograniczenia mogą być wprowadzane również na podstawie art. 23 RODO. Przewiduje on, że UE i państwa członkowskie mogą „aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5”. Zgodnie z treścią art. 23 RODO ograniczenie takie musi służyć realizacji jednego z interesów wymienionych w ust. 1, nie naruszać istoty podstawowych praw i wolności oraz być środkiem niezbędnym i proporcjonalnym w demokratycznym społeczeństwie. Wśród przyczyn, w związku z którymi można wprowadzać odpowiednie ograniczenia, znajdują się te służące m.in. „innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu”. Można zakładać, że możliwość wprowadzania ograniczeń w zakresie praw i zakazu dotyczącego zautomatyzowanego podejmowania decyzji będzie stanowić barierę dla szerokiej wykładni prawa dostępu czy praw dotyczących informacji o zautomatyzowanym podejmowaniu decyzji.

Przede wszystkim jednak należy jednoznacznie stwierdzić, że system ochrony danych osobowych jest skoncentrowany na ochronie jednostki i jej praw. To ona jest podmiotem umiejscowionym w centrum tworzonych w ramach tego dynamicznie rozwijanego obszaru regulacji. Mimo teoretycznych inspiracji, opisywanych w rozdziale pierwszym, a przede wszystkim mimo zmiany roli odgrywanej przez dane osobowe we współczesnym świecie, niemal brak jest przesłanek²⁸⁹ pozwalających patrzeć na ochronę danych osobowych jako ochronę pewnych grup, nie zaś pojedynczych osób. Aby z pełnym przekonaniem zweryfikować hipotezę dotyczącą niewystarczalności

zagadnienia w ramach transpozycji dyrektywy przez państwa członkowskie. Po trzecie, do regulacji zautomatyzowanego podejmowania decyzji wdrażanego np. przez policję odnoszą się przedstawione powyżej rozważania dotyczące braku jasności co do rozumienia terminu «odpowiednie zabezpieczenia praw i wolności osoby, której dane dotyczą». Szczegółowa analiza zagadnienia, zob. M. Brkan, *op. cit.*

²⁸⁹ Do pewnego stopnia wyjątkiem w tym aspekcie są dzieci, w odniesieniu do których sytuacji RODO tworzy grupę szczególnie chronioną, zob. literatura na ten temat: K. McCullagh, *The General Data Protection Regulation: A Partial Success for Children on Social Network Sites?*, [w:] *Data Protection, Privacy and European Regulation in the Digital Age*, red. T. Bräutigama, S. Miettinen, Helsingin yliopiston oikeustieteellinen tiedekunta, Helsinki 2016, s. 110–139; S. van der Hof, E. Lievens, *The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children's Personal Data Under the GDPR*, „Communications Law” 2018, t. 23, nr. 1, s. 33–43; E. Lievens, V. Verdoodt, *Looking for needles in a haystack: Key issues affecting children's rights in the General Data Protection Regulation*, „Computer Law & Security Review” 2018, t. 34, nr 2, s. 269–278; Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji...*, *op. cit.*, s. 32–33.

RODO w świetle prób pozyskiwania informacji na temat zautomatyzowanego podejmowania decyzji niezbędne jest jednak dokonanie przeglądu dwóch innych elementów unijnego systemu ochrony danych osobowych. Po pierwsze, konieczna jest analiza innych praw podmiotu danych jako potencjalnego źródła uprawnień pozwalających na przeciwstawienie się zautomatyzowanemu podejmowaniu decyzji. Po drugie, należy przedstawić rozwiązania dotyczące nie jednostek, lecz systemów zautomatyzowanego podejmowania decyzji samych w sobie, czyli DPIA i BCR. Poświęcone są im kolejne podrozdziały.

2.1.5. Prawo do usunięcia danych i prawo do przenoszenia danych a problem zautomatyzowanego podejmowania decyzji

Oprócz przepisów odnoszących się bezpośrednio do zautomatyzowanego podejmowania decyzji prawa podmiotu danych zbliżone do „bycia poinformowanym o powodach stojących za podjętą wobec podmiotu danych zautomatyzowaną decyzją” można próbować wywodzić z dwóch innych rozwiązań przewidzianych w RODO: prawa do usunięcia danych z art. 17 oraz prawa do przenoszenia danych z art. 20²⁹⁰.

Możliwość potraktowania prawa do usunięcia danych²⁹¹ z art. 17 RODO jako alternatywy dla rozwiązań związanych z zautomatyzowanym podejmowaniem decyzji oparta jest na koncentracji na danych używanych do podejmowania danej decyzji. Podmiot danych, zamiast wyrazić sprzeciw wobec podejmowania zautomatyzowanej decyzji czy kwestionowania samej decyzji, może zażądać usunięcia podstaw jej podjęcia, czyli przetwarzanych w tym celu danych. Zgodnie z treścią art. 17 RODO podmiot danych ma prawo do „niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe”. Prawo to może jednak zostać wykorzystane jedynie w ograniczonej liczbie sytuacji. Wśród nich potencjalnie najistotniejsze jest wycofanie zgody, na której opiera się przetwarzanie, przez podmiot danych (art. 17 ust. 1 lit. b), czy wniesienie sprzeciwu wobec przetwarzania (art. 17 ust. 1 lit. c). W świetle opisanych powyżej wyjątków od zakazu podejmowania zautomatyzowanych decyzji, a zwłaszcza wyjątku opartego na wyraźnej zgodzie podmiotu danych, skorzystanie z prawa do usunięcia danych jest formą umożliwiającą jednostce pośrednio sprzeciw wobec podjęcia w stosunku do niej zautomatyzowanej decyzji.

²⁹⁰ Możliwości te analizują L. Edwards, M. Veale, *Slave to the Algorithm...*, *op. cit.*, w związku z czym uznałam za konieczne uwzględnienie ich w analizie. Jak wykazuję dalej, nie uważam, żeby były one odpowiedzią na wyzwania wynikające z rozwoju zautomatyzowanego podejmowania decyzji, ale uczciwość badawcza nakazuje wprowadzenie ich jako praw analizowanych w tym kontekście.

²⁹¹ Inaczej: prawo do bycia zapomnianym.

Pierwszym problemem, który można zaobserwować na tle takiego rozwiązania, jest zakres danych, które miałyby zostać usunięte. Jak słusznie zauważają Edwards i Veale, nie jest jasne, czy usunięcie danych obejmuje tylko dane podane przez użytkownika czy również dane wywnioskowane na podstawie analizy na jego temat²⁹². Autorzy odnotowują rozbieżność w odniesieniu do kwestii uwzględniania danych wywnioskowanych z danych, co do których jednostka może domagać się wykonywania jej praw, między perspektywą prezentowaną przez TSUE w sprawie *Google Spain* i perspektywą prezentowaną przez Grupę Roboczą Art. 29²⁹³. W jednej z tez orzeczenia *Google Spain* TSUE stwierdził, że:

[...] operator wyszukiwarki internetowej jest zobowiązany do usunięcia z wyświetlanej listy wyników wyszukiwania mającego za punkt wyjścia imię i nazwisko danej osoby linków do publikowanych przez osoby trzecie stron internetowych zawierających dotyczące tej osoby informacje, również w przypadku gdy to imię czy nazwisko czy też te informacje nie zostały uprzednio czy też jednocześnie usunięte z tych stron internetowych, i, w odpowiednim przypadku, nawet jeśli ich publikacja na tych stronach jest zgodna z prawem²⁹⁴.

W świetle tego wyroku TSUE prawo do żądania usunięcia danych powinno zatem obejmować usuwanie informacji wytworzonych na podstawie przetwarzania danych osobowych (czyli linki znajdujące się na liście wyników wyszukiwania). Obowiązek usunięcia nie dotyczy – w ujęciu zaproponowanym przez TSUE – imienia i nazwiska danej osoby, lecz linku do strony, która została przez wyszukiwarkę zindeksowana na liście wyników związanych

²⁹² „Wydaje się oczywiste, że jednostka ma prawo do usunięcia *wprost podanych danych* użytych jako wkład do ML [*machine learning* – J.M.] systemu (np. imię, wiek, historia chorób), ale czy ma ona również prawo do usunięcia *zaobserwowanych* danych na temat jej zachowania i poruszania się zarówno po fizycznym jak i wirtualnym świecie?”. L. Edwards, M. Veale, *Slave to the Algorithm...*, *op. cit.*, s. 68.

²⁹³ Autorzy odwołują się do fragmentu wytycznych Grupy Roboczej Art. 29 dotyczących przenoszenia danych, jednak uwagi powinny być odczytywane na szerszym tle pytania o zakres danych, które objęte są prawami podmiotu danych z RODO, zob. „Generalnie, zważywszy na cele polityki prawa do przenoszenia danych, termin «przekazane przez osobę, której dane dotyczą» musi być interpretowany szeroko, z wyłączeniem tylko «danych wywnioskowanych» i «danych wywiedzionych», które obejmują dane osobowe, które są generowane przez dostawcę usług (na przykład wyniki algorytmiczne). Administrator może wyłączyć takie wywnioskowane dane, ale powinien uwzględnić wszystkie inne dane osobowe przekazane przez osobę, której dane dotyczą, za pomocą środków technicznych przekazanych przez administratora”. Grupa Robocza Art. 29, *Wytyczne dotyczące prawa do przenoszenia danych. Przyjęte w dniu 13 grudnia 2016 r.*, 16/EN WP 242, s. 9.

²⁹⁴ Wyrok Trybunału z dnia 13 maja 2014 r. w sprawie połączonych C-131/12, *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi*, ECLI:EU:C:2014:317, pkt 62.

z tym imieniem i nazwiskiem. Przekładając taką perspektywę na możliwość posłużenia się prawem do usunięcia danych w odniesieniu do zautomatyzowanego podejmowania decyzji, obowiązek usunięcia danych powinien dotyczyć zarówno samych danych, jak i wysnutych na ich podstawie przez administratora danych konkluzji. Obecnie brakuje jednak jasności co do tego, czy taka wykładnia zostanie podtrzymana na gruncie RODO.

Drugim problemem mogącym uniemożliwić korzystanie z prawa do usunięcia danych, jako swoistej alternatywy dla art. 22, jest katalog wprowadzonych w art. 17 wyjątków, w tym zwłaszcza jego ust. 3 lit. b, który stwierdza, że ust. 1 i 2 nie mają zastosowania w zakresie, w jakim przetwarzanie jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym bądź w ramach sprawowania władzy publicznej powierzonej administratorowi. Źródłem ograniczeń w korzystaniu z art. 17 może być również, wprowadzony w lit. c, brak zastosowania art. 17 z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego. Należy odnotować, że wyjątki te – w perspektywie wiążącej art. 17 z zautomatyzowanym podejmowaniem decyzji – odsyłają do potencjalnych sytuacji wykorzystywania zautomatyzowanego podejmowania decyzji w sektorze publicznym. Używane są pojęcia „interesu publicznego”, „wykonywania władzy publicznej” i „interesu publicznego w dziedzinie zdrowia”²⁹⁵. Tym samym możliwości ograniczania praw jednostki w zakresie prawa do usunięcia danych wydają się dość szerokie, a w związku z tym znacznie zawężają możliwości posłużenia się prawem do usunięcia danych jako alternatywą dla art. 22 RODO.

Z kolei prawo do przenoszenia danych²⁹⁶, stanowiące nowość w RODO w stosunku do *dyrektywy 95/46/WE*, ma na celu umożliwienie podmiotowi danych otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych jego dotyczących²⁹⁷. Dane te, zgodnie z treścią art. 20 RODO, obejmują dane dostarczone przez jednostkę administratorowi. Esencją prawa do przenoszenia danych jest możliwość ich przesłania innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Prawo to,

²⁹⁵ RODO odsyła w tym miejscu do art. 9 ust. 2 lit. h oraz art. 9 ust. 3, RODO. Przepisy te zawierają, w moim przekonaniu, szeroką charakterystykę tego, co należy rozumieć jako przetwarzanie danych związane z interesem publicznym w dziedzinie zdrowia (jednocześnie nie posługują się one wprost tym pojęciem).

²⁹⁶ Zob. W.R. Wiewiórowski, *Prawo do przenoszenia danych w ogólnym rozporządzeniu o ochronie danych osobowych*, „Europejski Przegląd Sądowy” 2017, nr 5, s. 23–30.

²⁹⁷ Art. 20, RODO.

oprócz wzmocnienia pozycji podmiotu danych, ma przede wszystkim na celu pobudzenie konkurencji między dostawcami usług cyfrowych²⁹⁸.

Tym samym jego związek z możliwością przeciwdziałania skutkom zautomatyzowanego podejmowania decyzji opiera się jedynie na zwiększeniu możliwości zasięgnięcia przez podmiot danych wiedzy na temat tego, jakimi danymi osobowymi administrator dysponuje. Zakres możliwej do zdobycia wiedzy, czyli tego, jakie dane podmiot powinien właściwie otrzymać, pozostaje dyskusyjny. Treść art. 20 wskazuje na dane, które jednostka „dostarczyła administratorowi”. Pojęcie to można rozumieć jako bądź dane, które jednostka aktywnie dostarczyła (np. wypełniając formularz), bądź szerzej jako dane, które administrator zaobserwował na podstawie danych aktywnie dostarczonych²⁹⁹. Jak wspomniano powyżej, wytyczne Grupy Roboczej Art. 29 wydają się sugerować węższą wykładnię tego pojęcia.

Prawo do przenoszenia danych budzi wątpliwości co do swojej treści ze względu na to, że jest nowe oraz sformułowane w mało precyzyjny sposób. Relatywnie ograniczony jest zakres sytuacji, w jakich możliwe jest powołanie się na prawo do przenoszenia danych. Zgodnie z art. 20 ust. 1 jest to możliwe w razie spełnienia jednego z warunków odnoszących się do podstaw przetwarzania (oparte na zgodzie lub na podstawie umowy) oraz w sytuacji, w której przetwarzanie odbywa się w sposób zautomatyzowany. Konieczność kumulatywnego spełnienia tych dwóch warunków sprawia, że prawo do przenoszenia danych nie dotyczy sytuacji, w których ich przetwarzanie oparte jest np. na przepisach.

Podobnie jak w przypadku prawa do usunięcia danych, prawo do ich przenoszenia stanowi rozwiązanie, które prawdopodobnie będzie miało większe znaczenie dla przetwarzania danych w sektorze prywatnym³⁰⁰. Przymuszenie takie potwierdza uwzględnienie w art. 20 ust. 3 wyłączenia, zgodnie z którym: „prawo to nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi”. Podobnie

²⁹⁸ Czego świadectwem jest również zainteresowanie badaczy prawem do przenoszenia danych głównie z perspektywy prawa konkurencji, zob. J. Kaźmierczak, *Prawo do przenoszenia danych osobowych – wybrane zagadnienia na tle realizacji nowego uprawnienia przyznanego przez RODO*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny” 2018, nr 4(7), s. 86–97 i literatura tam cytowana.

²⁹⁹ Rozważania na temat dwóch interpretacji tego pojęcia, zob. P. De Hert, V. Papakonstantinou, G. Malgieri, L. Beslay, I. Sanchez, *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, „Computer Law & Security Review” 2018, t. 34, nr 2, s. 199–200.

³⁰⁰ „[...] prawa do przeniesienia danych, które jak wskazano na wstępie, odnosi się przede wszystkim do relacji konsument (podmiot danych) – usługodawca (administrator danych)”. J. Kaźmierczak, *op. cit.*, s. 89.

jak w przypadku prawa do usunięcia danych, możliwości posłużenia się tym prawem w odniesieniu do relacji państwo–obywatel wydają się bardzo ograniczone. Stanowi to drugi – po problemie niejasności prawa do przenoszenia danych i obwarowania go wieloma wyjątkami i ograniczeniami – argument za niewielką rolą, jaką może ono odegrać w odniesieniu do zautomatyzowanego podejmowania decyzji wykorzystywanego przez instytucje państwowe.

Możliwości związane z korzystaniem z prawa do usunięcia danych i prawem do ich przenoszenia nie będą miały dużego praktycznego znaczenia dla problemu braku dostępu do informacji na temat potencjalnie dyskryminujących zautomatyzowanych decyzji. Są one obciążone podobnymi mankamentami, jak opisane w rozdziale rozwiązania z art. 13–15 i 22, czyli brakiem precyzji użytych pojęć i strukturą uwzględniającą wiele wyjątków bądź ograniczone sytuacje, w których prawo w ogóle może zostać przez jednostkę użyte. Ponadto celem ich wprowadzenia do RODO nie było zmierzenie się z problemem zautomatyzowanego podejmowania decyzji. Wykładnia sprzyjająca użyciu tych praw podmiotu danych w celu osiągnięcia wyższego poziomu przejrzystości zautomatyzowanego podejmowania decyzji odbiegałaby znacznie od intencji przyświecających zawarciu ich w RODO. Uzasadnione jest zwrócenie się raczej ku rozwiązaniom, które nie dotyczą jednostki i jej praw w odniesieniu do zautomatyzowanego podejmowania decyzji, lecz raczej całościowego spojrzenia na wprowadzanie tego typu systemów.

2.1.6. Systemowe ujęcie problematyki zautomatyzowanego podejmowania decyzji w RODO: ocena skutków dla ochrony danych i wiążące reguły korporacyjne

Podążając za stwierdzeniem, że „RODO ustanawia system „kwalifikowanej przejrzystości w odniesieniu do zautomatyzowanego podejmowania decyzji, które prowadzi do udostępnienia jednostkom jednego typu informacji, a ekspertom i prawodawcy innego”³⁰¹, należy poddać analizie rozwiązania umożliwiające dostęp do informacji na temat systemów zautomatyzowanego podejmowania decyzji ciałom eksperckim. Rozwiązania te powinny być postrzegane z dualnej perspektywy. Wprowadzają one przepisy regulujące instrumenty prawne, czyli DPIA³⁰² i BCR³⁰³, a normy ich dotyczące bezpośrednio odnoszą się do zautomatyzowanego podejmowania decyzji³⁰⁴. Jednocześnie stanowią one elementy całego unijnego systemu ochrony danych osobowych i jako takie są częścią instrumentarium prawnego umożliwiającego

³⁰¹ M.E. Kaminski, *The Right to Explanation, Explained*, „Berkeley Technology Law Journal” 2019, t. 34, nr 1, s. 217.

³⁰² Dla przypomnienia: ocena skutków dla ochrony danych (*data protection impact assessment*).

³⁰³ Dla przypomnienia: wiążące reguły korporacyjne (*binding corporate rules*).

³⁰⁴ Odpowiednio art. 35 i art. 47 ust. 1 lit e, RODO.

realizację zasad ogólnych sformułowanych w RODO, np. zgodności z prawem, rzetelności i przejrzystości, minimalizacji danych czy rozliczalności³⁰⁵. Stąd też użycie słowa „systemowe” w tytule tego podrozdziału jest dwuznaczne: z jednej strony systemowa jest próba spojrzenia na zautomatyzowane podejmowanie decyzji w analizowanych poniżej instrumentach prawnych, z drugiej zaś strony systemowo należy patrzeć na wdrożenie tych rozwiązań – jako elementów realizacji zasad ochrony danych osobowych zdefiniowanych w art. 5 RODO.

Wśród zidentyfikowanych w literaturze środków prawnych służącej tzw. „przejrzystości algorytmów”³⁰⁶, czyli kodeksów postępowania, certyfikacji i DPIA, ta ostatnia odgrywa szczególną rolę ze względu na swój obligatoryjny charakter³⁰⁷. Istotą DPIA jest próba stworzenia ram dla przyjmowania środków pozwalających zapobiegać sytuacjom mogącym prowadzić do naruszenia praw związanych z ochroną danych osobowych. W treści art. 35 ust. 1 sformułowano następujące warunki, które prowadzą do obowiązku przeprowadzenia DPIA. Zgodnie z treścią przepisu administrator jest zobowiązany przed rozpoczęciem przetwarzania wykonać DPIA w sytuacji przetwarzania danych, które ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych³⁰⁸. W szczególności uwzględnione powinno zostać przetwarzanie dokonywane z użyciem nowych technologii.

W art. 35 ust. 3 został zawarty otwarty katalog typów przetwarzania danych, w których DPIA jest wymagane. W katalogu znalazła się systematyczna, kompleksowa ocena czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną (art. 35 ust. 3 lit. a). Sytuacje objęte art. 22 są więc jednocześnie określone jako typ przetwarzania, w związku z którym przeprowadzenie DPIA jest obowiązkowe. Ponadto organy nadzorcze w państwach członkowskich publikują listy typów przetwarzania, które również mają być objęte

³⁰⁵ Art. 5, RODO.

³⁰⁶ Zob. B. Goodman, *A Step Towards Accountable Algorithms?: Algorithmic Discrimination and the European Union General Data Protection*, „29th Conference on Neural Information Processing Systems (NIPS 2016), Barcelona, Spain” 2016, s. 4-5.

³⁰⁷ Więcej o DPIA pisałam m.in. w J. Mazur, *Automated Decision-Making and the Precautionary Principle in EU Law*, „Baltic Journal of European Studies” 2019, t. 9, nr 4, s. 3–18. W kontekście zautomatyzowanego podejmowania decyzji, zob. H.L. Janssen, *An Approach for a Fundamental Rights Impact Assessment to Automated Decision-Making*, „International Data Privacy Law” 2020, t. 10, nr 1, s. 76-106.

³⁰⁸ Art. 35 ust. 1, RODO.

DPIA³⁰⁹. Prewencyjny charakter DPIA sprawia, że instrument ten może być postrzegany jako środek służący dostosowaniu przetwarzania do wymogów zgodności z zasadami ochrony danych w fazie projektowania i domyślnej ochrony danych, które zostały sformułowane w art. 25 RODO³¹⁰.

W odniesieniu do zautomatyzowanego podejmowania decyzji istotne elementy przepisów dotyczących DPIA są następujące. Po pierwsze, sposób sformułowania art. 35 ust. 3 lit. a pozwala stwierdzić, że zakres sytuacji zautomatyzowanego podejmowania decyzji uwzględniony w tym wypadku jest szerszy niż w art. 22. Świadczy o tym posłużenie się terminem „opiera się na zautomatyzowanym przetwarzaniu”, nie zaś „opiera się wyłącznie na...”. Interpretację taką potwierdzają wytyczne Grupy Roboczej Art. 29³¹¹. Po drugie, nie ulega wątpliwości, że DPIA jest instrumentem prawnym służącym identyfikacji i zarządzaniu ryzykiem, zanim dane przetwarzanie miałyby zostać wykonane. Może ona być więc postrzegana jako narzędzie pozwalające zidentyfikować niepokojące, dyskryminujące mechanizmy jeszcze na etapie przygotowywania danego systemu zautomatyzowanego podejmowania decyzji. Po trzecie, w przeciwieństwie do rozwiązań prawnych przyjętych w art. 13–15 i 22 RODO, DPIA jest narzędziem służącym do oceny całego systemu zautomatyzowanego podejmowania decyzji. Artykuł 35 ust. 7, wśród minimalnych wymogów dotyczących treści przeprowadzanej oceny, uwzględnia „ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1”. Ustęp 1, do którego odsyła, zawiera z kolei sformułowanie: „wysokie ryzyko naruszenia praw lub wolności osób fizycznych”. Sformułowanie to, co potwierdzają wytyczne Grupy Roboczej Art. 29, odnosi się nie tylko do praw związanych z ochroną danych osobowych. Może ono obejmować: „inne prawa podstawowe, takie jak wolność słowa, wolność myśli, swoboda poruszania się, zakaz dyskryminacji, prawo do wolności, wolność sumienia i wolność religii”³¹². DPIA powinna uwzględniać konieczność sprawdzenia, czy dany system zautomatyzowanego podejmowania decyzji nie niesie za sobą ryzyka dyskryminacji.

³⁰⁹ W celu ułatwienia oceny, jakie typy przetwarzania powinny podlegać DPIA, Grupa Robocza Art. 29 wydała wytyczne zawierające m.in. kryteria oceny, które należy uwzględnić, oceniając daną sytuację, zob. Grupa Robocza Art. 29, *Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679*, 4 kwietnia 2017 r., ostatnio zmienione i przyjęte w dniu 4 października 2017 r., 17/PL WP 248 rev.01, s. 10–12.

³¹⁰ Zob. L. Edwards, M. Veale, *Enslaving the Algorithm...*, *op. cit.*, s. 50–51; B. Casey, A. Farhangi, R. Vogl, *Rethinking Explainable Machines: The GDPR’s ‘Right to Explanation’ Debate and the Rise of Algorithmic Audits in Enterprise*, „Berkeley Technology Law Journal” 2019, t. 34, s. 173–174.

³¹¹ Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji...*, *op. cit.*, s. 34.

³¹² *Ibidem*, s. 7.

Tak pozytywny obraz możliwości wpływu DPIA na weryfikację istnienia mechanizmów dyskryminacyjnych w ramach zautomatyzowanego podejmowania decyzji należy jednak uzupełnić o problematyczne elementy art. 35. Przede wszystkim konieczne jest odnotowanie ściśle wewnętrznego charakteru dokumentów powstających w wyniku przeprowadzenia DPIA. RODO w żaden sposób nie wprowadza obowiązku publikacji DPIA³¹³, które tym samym nie ma żadnego wpływu na dostęp do informacji dla jednostek na temat tego, jak działa zautomatyzowane podejmowanie decyzji. Decyzja o udostępnieniu jego wyników zależy od dobrej woli administratora danych. Ponadto nie została w jasny sposób określona rola podmiotów danych w ramach procesów związanych z DPIA. Zgodnie z art. 35 ust. 9: „W stosownych przypadkach administrator zasięga opinii osób, których dane dotyczą, lub ich przedstawicieli w sprawie zamierzonego przetwarzania, bez uszczerbku dla ochrony interesów handlowych lub publicznych lub bezpieczeństwa operacji przetwarzania”. Możliwość konsultacji z osobami, których dane dotyczą, jest zatem ograniczona po pierwsze do enigmatycznej kategorii „stosownych przypadków”, po drugie zaś wymogiem dokonywania ich bez uszczerbku dla ochrony interesów administratora danych. Ustęp ten w znaczący sposób osłabia możliwość rozwijania partycypacyjnego charakteru DPIA.

Kluczowym problemem jest ponadto kwestia uregulowania relacji między administratorem danych a organem nadzorczym. W świetle art. 36 ust. 1 dopiero po przeprowadzeniu DPIA, jeśli wskaże ona, że przetwarzanie powodowałoby wysokie ryzyko w razie niezastosowania środków w celu jego zminimalizowania, administrator jest zobowiązany skonsultować się z organem nadzorczym. DPIA, która nie wykaże takich prawdopodobieństw, pozostaje ściśle wewnętrznym dokumentem danego przedsiębiorstwa czy instytucji³¹⁴.

³¹³ Potwierdzają to wytyczne Grupy Roboczej Art. 29: „RODO nie zawiera prawnego wymogu publikacji oceny skutków dla ochrony danych; decyzja o publikacji należy do administratora. Administratorzy powinni jednakże rozważyć publikację choćby części przeprowadzonych przez nich ocen skutków dla ochrony danych, takich jak podsumowanie lub wnioski”. Grupa Robocza Art. 29, *Wytyczne dotyczące oceny skutków dla ochrony danych...*, op. cit., s. 22.

³¹⁴ Zgodnie z pozyskaną przeze mnie 10 czerwca 2019 r. w trybie dostępu do informacji publicznej notatką od UODO w 2018 r. do UODO spłynęły dwa wnioski o udzielenie takich konsultacji, które jednak ze względu na brak spełnienia wymogów z art. 36 ust. 3 RODO i art. 63 kodeksu postępowania administracyjnego nie zostały rozpatrzone. W maju 2019 r. wpłynął do UODO kolejny wniosek, który w momencie otrzymania przeze mnie dostępu do informacji publicznej, nie został jeszcze rozpatrzony. Łącznie w 2019 r. z prośbą o konsultację zgłosiło się do UODO 5 podmiotów, jednak wszystkie wnioski były obciążone brakami formalnymi i w związku z tym konsultacje nie zostały przeprowadzone (zob. Prezes Urzędu Ochrony Danych Osobowych, *Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2019*, s. 141–142. <https://uodo.gov.pl/437>, dostęp:

Kolejnym problemem wiążącym się z DPIA jest ograniczenie możliwości jego przeprowadzenia przez uwzględnienie w art. 35 ust. 10 wielu wyjątków. Odnoszą się one do zdefiniowanych w art. 6 ust. 1 lit. c i e sytuacji, czyli przetwarzania niezbędnego do wypełnienia obowiązku prawnego ciążącego na administratorze oraz przetwarzania niezbędnego do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. W tych sytuacjach, jeśli przetwarzanie „ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator, i prawo takie reguluje daną operację przetwarzania lub zestaw operacji, a oceny skutków dla ochrony danych dokonano już w ramach oceny skutków regulacji w związku z przyjęciem tej podstawy prawnej”³¹⁵, art. 35 ust. 1–7 nie mają zastosowania. Państwowym członkowskim UE pozostawiono więc możliwość wyłączenia spod DPIA części sytuacji. Nie jest jasne, czy w stosunku do DPIA, która ma być dokonana w ramach oceny skutków regulacji, odnoszą się obowiązki zawarcia w niej elementów wymienionych w art. 35 ust. 7. Zważywszy na fakt, że do tych sytuacji art. 35 ust. 1–7 nie mają zastosowania, można podejrzewać, że również te wymogi nie odnoszą się do sytuacji określonych w art. 35 ust. 10³¹⁶. Co prawda, zgodnie z art. 36 ust. 5, państwa członkowskie mają możliwość wprowadzenia obowiązkowych konsultacji i uzyskania uprzedniej zgody organu nadzorczego na przetwarzanie danych osobowych do celów wykonania zadania realizowanego przez administratora w interesie publicznym, w tym przetwarzania w związku z ochroną socjalną i zdrowiem publicznym. Jest to jednak przepis pozostawiający decyzję w odniesieniu do wprowadzenia takiego obowiązku w gestii państw.

DPIA ma potencjał do stania się ważnym instrumentem prawnym w zakresie realizacji „prawa do wyjaśnienia” w bardziej systemowym

19.07.2021). W związku z brakiem dostępu do danych dotyczących skali przeprowadzania DPIA w Polsce nie jest możliwe sprawdzenie, jakim odsetkiem przeprowadzonych ocen są te, które zostały zgłoszone do konsultacji. Niemniej w ujęciu bezwzględny liczbą ta wskazuje na skromne używanie uprzednich konsultacji DPIA przez przedsiębiorstwa. Odpowiedź ZO.0143.148.2019.EB na wniosek z dnia 27 maja 2019 r., informacja potwierdzona: Prezes Urzędu Ochrony Danych Osobowych, *Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2018*, s. 83. <https://uodo.gov.pl/pl/437/1173>, dostęp: 1.04.2021. Ze względu na pandemię nie zdecydowałam się składać nowego wniosku o dostęp do informacji publicznej dotyczącego danych za 2020 r., wychodząc z założenia, że okres ten nie jest miarodajnym czasem, który dałby wiarygodne świadectwo o skali przeprowadzania DPIA.

³¹⁵ Art. 35 ust. 10, RODO.

³¹⁶ Wątpliwości tych nie rozwiewają wytyczne Grupy Roboczej Art. 29, które raczej odnoszą się do momentu w ramach procesu legislacyjnego, kiedy DPIA należy przeprowadzić, zob. Grupa Robocza Art. 29, *Wytyczne dotyczące oceny skutków dla ochrony danych...*, op. cit., s. 15.

wymiarze³¹⁷. Mogłaby ona pomagać w dokonywaniu kompleksowej oceny systemów zautomatyzowanego podejmowania decyzji, uwzględniającej konieczność sprawdzenia, czy wdrażane mechanizmy nie mają charakteru dyskryminującego. Jednak ze względu na niewysoki poziom przejrzystości tego rozwiązania, będącego głównie narzędziem wewnętrznej organizacji przetwarzania danych w danym podmiocie³¹⁸ i dopiero wtórnie przedmiotem ewentualnych konsultacji z organem nadzorczym, potencjał ten nie będzie w pełni wykorzystany. Przede wszystkim jednak instrument ten *de facto* pozostaje narzędziem wewnętrznym w przedsiębiorstwach i instytucjach, jedynie w wyjątkowych sytuacjach będąc przedmiotem konsultacji³¹⁹ z organem nadzorczym. Mimo jego potencjału nie wpływa on w znaczący sposób na wspieranie ochrony kolektywnego wymiaru prywatności i ochrony danych osobowych, czego świadectwem są chociażby dane mówiące o niskim stopniu korzystania z konsultacji DPIA przez podmioty wprowadzające rozwiązania wykorzystujące zautomatyzowane podejmowanie decyzji.

Funkcją BCR jest z kolei „umożliwienie swobodnej wymiany danych osobowych między poszczególnymi podmiotami grupy korporacyjnej na całym świecie”³²⁰. BCR w swej istocie służyć mają ułatwieniu transferów danych między państwami należącymi do EOG a nienależącymi, w odniesieniu do transnarodowych korporacji w ramach jednej grupy kapitałowej. Przyjęcie ich służyć ma ujednoczeniu standardów ochrony przez takie przedsiębiorstwa w celu ułatwienia dokonywania transferów danych w ramach danej korporacji. W odniesieniu do BCR kwestia zautomatyzowanego podejmowania decyzji pojawia się jako jeden z elementów, który muszą one uwzględniać wśród wypracowanych w nich standardów.

W katalogu zawartym w art. 47 ust. 2, w lit. e został sformułowany wymóg określenia „praw osób, których dane dotyczą, w związku z przetwarzaniem oraz sposoby wykonywania tych praw, w tym z prawa do

³¹⁷ Zob. B. Casey, A. Farhangi, R. Vogl, *op. cit.*, s. 180–184 oraz relatywnie optymistyczna analiza DPIA w kontekście algorytmicznej dyskryminacji: P. Hacker, *Teaching Fairness To Artificial Intelligence: Existing And Novel Strategies Against Algorithmic Discrimination Under EU Law*, „Common Market Law Review” 2018, t. 55, s. 1143–1186.

³¹⁸ Analogiczne wątpliwości można żywić co do tego, jaką rolę będą odgrywać przepisy proponowane w *Akcie w sprawie SI* w odniesieniu do zastosowań SI wysokiego ryzyka (Rozdział II, *Akt w sprawie SI*). Teoretycznie wprowadzają one obowiązek przeprowadzania wielu analiz dotyczących np. jakości danych stosowanych w określonych systemach SI, ich przejrzystości. Propozycja rozporządzenia nie gwarantuje jednak, że zostanie wprowadzona prewencyjna, zewnętrzna kontrola nad wywiązywaniem się z tych obowiązków.

³¹⁹ A w przypadku Polski, według danych dostępnych w czasie przygotowywania książki, nieudanych prób odbycia konsultacji.

³²⁰ M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (EU) 2016/679*, C.H. Beck, Warszawa 2016, s. 267.

niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu – w tym profilowaniu – zgodnie z art. 22³²¹. RODO ma na celu przede wszystkim wprowadzenie unijnego standardu ochrony praw podmiotów danych w odniesieniu do zautomatyzowanego podejmowania decyzji do dokumentu opisującego BCR. Akty formułujące BCR są, po spełnieniu warunków wymienionych w art. 47 ust. 1, zatwierdzane przez organy nadzorcze.

Chociaż trudno odmówić BCR znaczenia w odniesieniu do określania poziomu ochrony podmiotów danych w razie międzynarodowych transferów danych osobowych, to ich znaczenie dla problemu potencjalnej dyskryminacji zachodzącej z wykorzystaniem zautomatyzowanego podejmowania decyzji jest marginalne. Przede wszystkim są one instrumentem, w którym prawa podmiotów danych – wywodzące się z RODO – są zagwarantowane w razie przetwarzania przez międzynarodową korporację poza granicami EOG. Nie tworzą one zatem nowych mechanizmów gwarantujących większą przejrzystość zautomatyzowanych rozwiązań. Są raczej instrumentem, którego celem jest ułatwienie funkcjonowania drugiego z filarów unijnego reżimu dotyczącego danych, czyli ich swobodnego przepływu. Dlatego nie prowadzą do udostępniania informacji na jego temat podmiotom danych.

2.1.7. Kolektywny wymiar zautomatyzowanego podejmowania decyzji a RODO

W świetle tematu tej książki należy odnotować, że kolejnym problemem podnoszonym w literaturze już w związku z rozwiązaniem zawartym w art. 15 *dyrektywy 95/46/WE* był również sam fakt oparcia ochrony przed zautomatyzowanym podejmowaniem decyzji na ochronie danych osobowych. Wzrost zainteresowania tematem profilowania wśród badaczy zaowocował refleksją dotyczącą wątpliwości co do możliwości stosowania *dyrektywy 95/46/WE* w sytuacji, w której decyzja jest oparta na analizie zanonimizowanych danych i na ich podstawie stworzonych grupowych profili³²². Mechanizm ten stał się przedmiotem jednej z decyzji wydanych przez austriacką Komisję ds. Ochrony Danych, która stwierdziła, że w związku z faktem, że zautomatyzowana decyzja została podjęta na podstawie analizy grupy, a nie danych o jednostce, prawo dostępu nie znajduje w takiej sytuacji zastosowania³²³. Stąd też, jak odnotowuje Guido Noto La Diega, bezpośrednie odwołanie do profilowania

³²¹ Art. 47 ust. 2 lit. e, RODO.

³²² Zob. E. Benoit, *Collecting Data for the Profiling of Web Users*, [w:] *Profiling the European Citizen. Cross-Disciplinary Perspectives*, red. M. Hildebrandt, S. Gutwirth, Springer, Nowy Jork 2008, s. 179; M. Hildebrandt, *Profiling...*, *op. cit.*, s. 551.

³²³ Decyzja austriackiej Komisji do spraw Ochrony Danych z 10 marca 2016 r., App no DSB-D122.322/0001-DSB/2016 omówiona przez S. Wachter, B. Mittelstadt, L. Floridi, *op. cit.*, s. 88–89.

w wersji art. 15 przyjętej w RODO stanowi jedną z najważniejszych zmian w stosunku do treści *dyrektywy 95/46/WE*³²⁴. Nie jest jednak jasne, w jakim stopniu uwzględnienie profilowania w treści art. 13–15 i 22 będzie prowadziło do przyjęcia jasnego stanowiska w odniesieniu do tworzenia profili na podstawie danych zanonimizowanych i wykorzystywania ich do zautomatyzowanego podejmowania decyzji. Ostatecznie prawa te są ściśle związane z przetwarzaniem danych osobowych.

Paradoksalnie, w świetle wyzwań dla zakazu dyskryminacji, które tworzy zautomatyzowane podejmowanie decyzji, to DPIA mogłoby okazać się najbardziej skuteczną odpowiedzią regulacyjną. W przeciwieństwie do skoncentrowanych na prawach jednostki art. 13–15 i 22 pozwala ona obrać szerszą perspektywę w odniesieniu do badanego systemu zautomatyzowanego podejmowania decyzji i uwzględnić kolektywny wymiar problemów związanych z przetwarzaniem danych. Poważnym mankamentem rozwiązań wprowadzonych w RODO jest jednak zamknięty krąg podmiotów mogących uczestniczyć w procesie przygotowywania DPIA, a także mających potencjalnie dostęp do jego rezultatów. Z jednej strony można uzasadniać takie ukształtowanie ram prawnych dla DPIA wyższą gwarancją eksperckości, z drugiej strony nie zwiększa ono przejrzystości wprowadzanych zautomatyzowanych rozwiązań. Chociaż rozwiązanie może dotyczyć interesów całych grup, w jego analizowaniu i weryfikowaniu wyników tej analizy będą uczestniczyć nieliczni.

Jedynym wprowadzonym w RODO rozwiązaniem, które łączy wymiar ochrony danych osobowych jako kwestii dotyczącej jednostki i ochrony danych osobowych jako źródła problemów dotyczących grup, jest art. 80³²⁵. Przewiduje on pewne uprawnienia dla podmiotu, organizacji lub zrzeszenia, które nie mają charakteru zarobkowego, zostały należycie ustanowione zgodnie z prawem państwa członkowskiego, mają cele statutowe leżące w interesie publicznym i działają w dziedzinie ochrony praw i wolności osób, których dane dotyczą, w związku z ochroną ich danych osobowych. Zgodnie z art. 80 ust. 1 podmioty takie mogą wnieść skargę do organu nadzorczego w imieniu osoby, której dane dotyczą skargi, oraz korzystać ze środków ochrony prawnej przed sądem, zarówno przeciwko organowi nadzorcemu, jak i administratorowi lub podmiotowi przetwarzającemu dane.

Z kolei art. 80 ust. 2 nie zobowiązuje państw, lecz jedynie umożliwia im wprowadzenie proponowanego w nim rozwiązania. W jego treści zostało sformułowane uprawnienie podmiotów scharakteryzowanych w ust. 1 do wykonywania tych praw niezależnie od upoważnienia otrzymanego od osoby,

³²⁴ Zob. G. Noto La Diega, *op. cit.*, s. 17.

³²⁵ Omówienie tego artykułu: J. Wagner, A. Benecke, *National Legislation within the Framework of the GDPR*, „European Data Protection Law Review” 2016, nr 2, s. 355–356.

której dane dotyczą, jeżeli uznają, że w wyniku przetwarzania zostały naruszone prawa osoby, której dane dotyczą. Tymczasem, jak zauważają Edwards i Veale:

Takie podmioty mogłyby stać się efektywnymi strażnikami w poszczególnych obszarach lub sektorach, ale będzie to dla nich trudne bez dostępu do danych wykorzystywanych do trenowania algorytmu, danych używanych do przetwarzania, ich wyników, modeli zalgorytmizowanych systemów, aby ustalić, gdzie pojawiają się naruszenia. Ogromnym problemem jest w tej kwestii fakt, że sądy zwykle odmawiają dostępu do kodu źródłowego systemów podejmowania decyzji, nawet w odniesieniu do tradycyjnych, niezalgorytmizowanych systemów³²⁶.

Gdyby państwa zdecydowały się wprowadzać rozwiązanie przewidziane w art. 80 ust. 2 RODO do krajowych porządków prawnych – co jest im umożliwione, ale do czego nie są zobowiązane – mogłoby ono być narzędziem nieco równoważącym dysproporcje w kwestii tego, kto dysponuje wiedzą o zautomatyzowanym podejmowaniu decyzji. Zwłaszcza w odniesieniu do grup nieuprzywilejowanych i narażonych na dyskryminację mógłby on przyczynić się do wzmocnienia szans na przeciwdziałanie stosowaniu wobec nich zautomatyzowanego podejmowania decyzji, które byłoby w pewien sposób stronnicze. Na razie jednak jest kolejnym chwiejnym elementem dość enigmatycznej układanki niejasnych przepisów dotyczących zautomatyzowanego podejmowania decyzji.

2.2. Zautomatyzowane podejmowanie decyzji w prawie Rady Europy

Ochrona prywatności oraz danych osobowych stała się przedmiotem zainteresowania Rady Europy, zanim w prawie UE pojawiły się akty prawne odnoszące się do tych kwestii. *Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych*, czyli *Konwencja 108*, została w swej pierwotnej formie sformułowana w 1981 r. i weszła w życie w 1985 r. W związku z tempem rozwoju technologicznego w zakresie wykorzystywania danych osobowych została dostrzeżona konieczność dostosowania *Konwencji 108* do nowych realiów ekonomiczno-społecznych. Zainicjowane w 2010 r.³²⁷ prace nad uaktualnieniem *Konwencji 108* zakończyły się przyjęciem w 2018 r. protokołu znacząco zmieniającego jej treść. W czasie przygotowywania tej książki nie miał on jednak wystarczającej liczby ratyfikacji,

³²⁶ L. Edwards, M. Veale, *Enslaving the Algorithm...*, *op. cit.*, s. 53.

³²⁷ Zob. P. de Hert, V. Papakonstantinou, *The Council of Europe Data Protection Convention reform: Analysis of the New Text and Critical Comment on Its Global Ambition*, „Computer Law & Security Review” 2014, t. 30, s. 633.

aby wejść w życie³²⁸. *Konwencja 108* jest jedyną prawnie wiążącą umową międzynarodową dotyczącą ochrony danych osobowych i prywatności³²⁹, przyjmującą prawnoczościową optykę w odniesieniu do regulowanych przez nią zagadnień. Podstawą jej przyjęcia jest cel w postaci ochrony prawa do prywatności, uwzględnionego w art. 8 EKPCz³³⁰. Ponadto *Konwencja 108* przewiduje możliwość przystąpienia nie tylko państw członkowskich Rady Europy, lecz również państw niebędących jej członkami³³¹, dzięki czemu tworzy możliwość rozpowszechniania proponowanych w niej standardów ochrony poza Europą.

W swej pierwotnej formie *Konwencja 108* w pewnym stopniu wyprzedzała pojawienie się wyzwań, których regulacji miała być poświęcona. Jej celem było stworzenie podstaw do ochrony danych osobowych w ramach prawa Rady Europy. Zostały w niej sformułowane zasady przetwarzania i wymogi dotyczące jakości danych, m.in. pozyskiwania oraz przetwarzania danych rzetelnie i zgodnie z prawem czy gromadzenia danych dla określonych i usprawiedliwionych celów (art. 5). Wprowadzone zostały, w art. 7, obowiązki dotyczące dbania o bezpieczeństwo danych. Ponadto w *Konwencji 108* znalazły się prawa podmiotu danych, przewidujące w określonych warunkach m.in. uzyskanie możliwości sprostowania lub usunięcia danych jej dotyczących. Położone zostały również fundamenty pod reguły rządzące przepływem danych przez granice. Zgodnie z art. 12 ust. 2 *Konwencji 108* strona nie może, uwzględniając obawy dotyczące ochrony prywatności, zabronić przepływu danych osobowych przez granice na terytorium innej strony lub uzależnia tego przepływu od wydania specjalnego zezwolenia. Skupienie z jednej strony na ochronie praw jednostki, z drugiej zaś dążenie do zagwarantowania możliwości swobodnego przepływu danych jest charakterystycznym elementem europejskiego podejścia do prób regulacji tego zagadnienia do dziś. Świadczy o tym chociażby pełny tytuł RODO: *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.*

³²⁸ Wymóg ratyfikacji przez wszystkie państwa strony *Konwencji 108*, lub wejście w życie 11 października 2023 r., o ile protokół zostanie ratyfikowany przez co najmniej 38 państw. Aktualne dane na temat ratyfikacji: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223>, dostęp: 1.04.2021.

³²⁹ Zob. S. Kierkegaard, N. Waters, G. Greenleaf, L.A. Bygrave, I. Lloyd, S. Saxby, *30 years on: The review of the Council of Europe Data Protection Convention 108*, „Computer Law & Security Review” 2011, t. 27, s. 223. Przyjęta w 2014 r. *Konwencja o cyberbezpieczeństwie i ochronie danych osobowych Unii Afrykańskiej* w czasie przygotowywania książki nie zdążyła wejść w życie, mając 8 z wymaganych 15 ratyfikacji (stan na 18 lipca 2021). <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>, dostęp: 1.04.2021.

³³⁰ Bywa nawet określana jako *spin-off* od art. 8 EKPCz, zob. P. de Hert, V. Papakonstantinou, *op. cit.*, s. 635.

³³¹ Zob. Art. 22 i 23, *Konwencja 108*.

w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych.

Mimo tak pionierskiego charakteru *Konwencji 108*, wśród zawartych w niej przepisów brak jest odniesienia do zautomatyzowanego podejmowania decyzji³³². Zmianę w tym zakresie wprowadza art. 9 zaktualizowanej *Konwencji 108+*³³³. Wśród praw podmiotu danych są wymienione dwa prawa odnoszące się do zautomatyzowanego podejmowania decyzji. Po pierwsze, jest to prawo podmiotu danych do niepodlegania decyzji znacząco na niego wpływającej i opartej wyłącznie na zautomatyzowanym przetwarzaniu danych w sytuacji, w której jego zdanie nie zostało wzięte pod uwagę przy wydawaniu tej decyzji³³⁴. Prawo to nie ma zastosowania w sytuacji, w której wydawanie decyzji jest przewidziane prawem, któremu poddany jest administrator danych (*data controller*) i które przewiduje odpowiednie środki ochrony praw, wolności i uzasadnionych interesów podmiotu danych³³⁵. Drugim prawem dotyczącym zautomatyzowanego podejmowania decyzji jest prawo podmiotu danych do uzyskania na swoje żądanie wiedzy na temat rozumowania stojącego za przetwarzaniem danych, którego wyniki są wobec niego stosowane³³⁶. Według treści wyjaśnień przepisów *Konwencji 108+* powinno ono obejmować informację na temat logiki stojącej za przetwarzaniem danych (*logic underpinning the processing of their data*³³⁷).

Prawa te w dużym stopniu przypominają rozwiązania wprowadzone w RODO w art. 22 oraz opisywane powyżej „prawo do wyjaśnienia”. Podobnie jak w odniesieniu do art. 22 RODO, mogą się pojawić wątpliwości, co należy rozumieć przez wiele pojęć pojawiających się w art. 9 lit. a, np. „znaczącą na niego lub na nią wpływającą” czy „odpowiednie środki ochrony praw”. *Konwencja 108+* nie zawiera bezpośrednich wskazówek w tym zakresie. Wyjaśnienia do treści tych przepisów podkreślają, że zautomatyzowane decyzje objęte treścią art. 9 lit. a muszą być „całkowicie” zautomatyzowane

³³² Co w dokumencie *Application of Convention 108 to the profiling mechanism. Some ideas for the future work of the Consultative Committee* zostało skomentowane jako „dziwne” – zob. Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing Of Personal Data, *Application of Convention 108 to the profiling mechanism. Some ideas for the future work of the Consultative Committee*, T-PD (2008) 01, s. 12.

³³³ Komentarz do treści tych praw, zob. C. de Terwangne, *The work of revision of the Council of Europe Convention 108 for the protection of individuals as regards the automatic processing of personal data*, „International Review of Law, Computers & Technology” 2014, t. 28, nr 2, s. 125–126.

³³⁴ Art. 9 ust. 1 lit. a, *Konwencja 108+*.

³³⁵ Art. 9 ust. 2, *Konwencja 108+*.

³³⁶ Art. 9 ust. 1 lit. c, *Konwencja 108+*.

³³⁷ Rada Europy, *Explanatory Report – CETS 223 – Automatic Processing of Personal Data (Amending Protocol)*, 10 października 2018 r., s. 14.

(w tekście *Konwencji 108+*: *based solely on*; według wyjaśnień: *purely*)³³⁸. Potencjalny zakres sytuacji, w których podmiot danych mógłby powoływać się na prawo do niepodlegania takiej decyzji, jest więc ograniczony. Przypomina to wątpliwości związane z wykładnią użytego w art. 22 RODO sformułowania „opiera się wyłącznie na zautomatyzowanym przetwarzaniu”. *Konwencja 108+* powtarza w tym zakresie treść RODO, a przez to zostaje powielony brak precyzji w oznaczeniu sytuacji, do których odnosi się ten przepis.

W *Konwencji 108+* użyte zostało również nieprecyzyjne sformułowanie, zgodnie z którym podmiot danych ma prawo nie podlegać zautomatyzowanej decyzji, która podjęta zostaje bez wzięcia pod uwagę jego poglądów (*without having his or her views taken into consideration*). Zgodnie z wyjaśnieniami prawo zawarte w art. 9 lit. a obejmuje kwestionowanie wydanej decyzji przez przedstawienie swoich argumentów. Jednocześnie wyjaśnienia do *Konwencji 108+* wprowadzają niejasny wymóg umożliwienia podmiotowi danych wykazania potencjalnych niedokładności w danych osobowych, zanim zostaną one użyte oraz profilu mającego być zastosowanym do jego sytuacji czy innych czynników mogących mieć wpływ na wynik zautomatyzowanej decyzji.

Nie jest zatem jednoznaczne czy podmiotowi danych powinno przysługiwać prawo sprzeciwu wobec decyzji już wydanej, czy wobec tego, co zostało uwzględnione w samych danych, które dopiero miałyby być użyte do wydania decyzji. Chociaż przykłady decyzji podane w wyjaśnieniach, czyli np. odmowa przyznania świadczenia socjalnego czy ocena zdolności kredytowej³³⁹, mogłyby świadczyć o potencjalnie dużej roli praktycznej praw opisanych w art. 9 lit. a, to brak jasności dotyczącej tego, co właściwie prawa te obejmują, może stanowić barierę w stosowaniu postanowień *Konwencji 108+*. Problem ten znowu przypomina wątpliwości, pojawiające się na tle przepisów RODO. Nie jest jasna chronologia, według której podmiot danych ma prawo do sprzeciwu wobec decyzji.

Prawo do wyjaśnienia, wprowadzone w art. 9 lit. c, jest z kolei przedstawione jako niezbędne do korzystania z innych praw podmiotu danych, np. sprzeciwu wobec decyzji czy złożenia skargi do odpowiedniej instytucji³⁴⁰. Sposób jego sformułowania nie pozwala jednak jednoznacznie stwierdzić, jaka jest jego relacja do prawa do niepodlegania zautomatyzowanej decyzji. Wiedza na temat rozumowania stojącego za zautomatyzowanym przetwarzaniem ma być przekazana podmiotowi danych na jego żądanie. Taki sposób ujęcia prawa do wyjaśnienia wskazuje, że raczej niezbędna jest aktywność podmiotu danych, nie zaś uprzednie umożliwienie mu przedstawienia swoich

³³⁸ *Ibidem*, s. 13.

³³⁹ *Ibidem*, s. 13.

³⁴⁰ *Ibidem*, s. 14.

poglądów. Można podejrzewać, że relacja między art. 9 lit. a i art. 9 lit. c mogłaby przybrać następujący kształt: w sytuacji, w której podejmowana jest wobec podmiotu danych zautomatyzowana decyzja, powinna zostać mu przedstawiona możliwość wyrażenia swoich poglądów. Wówczas podmiot danych może zażądać dostępu do przyczyn stojących za propozycją podjęcia wobec niego takiej decyzji. Wykładnia taka pozwoliłaby pogodzić wymóg z art. 9 lit. a z jednoczesnym obowiązkiem zagwarantowania możliwości przewidzianej w art. 9 lit. c. Dodatkowo, na co wskazują wyjaśnienia, podmiot danych powinien mieć możliwość kontroli jakości danych używanych do podejmowania wobec niego zautomatyzowanej decyzji³⁴¹. W żaden sposób te rozwiązania nie odnoszą się jednak do kolektywnego wymiaru zautomatyzowanego podejmowania decyzji, sprowadzając ten problem – podobnie jak robi to RODO – do kwestii jednostkowej.

Prawa uwzględnione w art. 9 mogą być ograniczane na podstawie art. 11 *Konwencji 108+*. Zgodnie z art. 11 ust. 1 ograniczenia muszą być przewidziane w prawie, chronić esencję podstawowych praw i wolności, stanowić środek niezbędny i proporcjonalny w demokratycznym społeczeństwie oraz chronić interesy wymienione w treści art. 11. Katalog zawarty w art. 11 ust. 1 lit. a jest otwarty i wymienia: bezpieczeństwo narodowe, obronność, bezpieczeństwo publiczne, istotne interesy gospodarcze i finansowe państwa, niezawisłość i bezstronność sędziowską oraz prewencję, dochodzenie i ściganie przestępczości, a także wykonywanie kar za przestępstwa³⁴². Przepis ten pełni zatem funkcję podobną do art. 23 RODO. Ponadto art. 11 uwzględnia również możliwość ograniczania praw podmiotu danych ze względu na konieczność ochrony praw i wolności innych. W odniesieniu do art. 9 przewidziane są również możliwości wprowadzania ograniczeń w związku z koniecznością archiwizowania danych w interesie publicznym do prowadzenia badań naukowych i historycznych oraz do celów statystycznych. Ograniczenia muszą być przewidziane w prawie, a także nie może istnieć ryzyko naruszenia praw i wolności podmiotów danych.

Wprowadzenie możliwości powoływania się na tak wiele przesłanek w celu ograniczenia prawa do niepodlegania zautomatyzowanym decyzjom może znacząco obniżyć poziom ochrony jednostek, zwłaszcza w związku z zautomatyzowanym podejmowaniem decyzji wprowadzanym w ramach sektora publicznego. Wiele sfer, w których zautomatyzowane podejmowanie decyzji jest implementowane i może tworzyć niemożliwe do zweryfikowania wątpliwości co do jego zgodności z ogólnym zakazem dyskryminacji, objętych zostało katalogiem z art. 11 *Konwencji 108+*. W świetle takiego sposobu sformułowania zakazu zautomatyzowanego podejmowania decyzji

³⁴¹ *Ibidem*, s. 13.

³⁴² Pelen katalog uwzględniony w art. 11 ust. 1 lit. a, *Konwencja 108+*.

w *Konwencji 108+* dużą rolę może odegrać konieczność wykazania, że ograniczenia praw jednostek są proporcjonalne i niezbędne w demokratycznym społeczeństwie. Mimo ogólnego sformułowania praw jednostek w zakresie zautomatyzowanego podejmowania decyzji w *Konwencji 108+* oraz wprowadzenia możliwości ich ograniczania może ona odegrać istotną rolę jako akt rozpowszechniający chociażby minimalne, to jednak wspólne standardy ochrony praw podmiotów danych.

2.3. Podsumowanie

Celem tego rozdziału było wskazanie, czy na tle obecnej regulacji zautomatyzowanego podejmowania decyzji w prawie europejskim istnieją rozwiązania prawne, które odnoszą się w adekwatny sposób do zagrożeń związanych z brakiem przejrzystości zautomatyzowanego podejmowania decyzji. W rozdziale wykazałam, że interpretacja przepisów RODO dotyczących zautomatyzowanego podejmowania decyzji nastręcza wielu trudności i tym samym potwierdziłam konieczność poszukiwania innych rozwiązań regulacyjnych, które mogłyby wspierać ochronę praw jednostek w wypadku stosowania takich metod podejmowania decyzji.

Wśród postulatów wysuwanych przez badaczy znajduje się konieczność sprecyzowania wielu pojęć pojawiających się w treści art. 22 i 13–15³⁴³. Istotną będzie w tym zakresie rola orzecznictwa TSUE, które może dostarczyć wielu niespodzianek co do rozumienia terminów użytych w RODO. Zanim to jednak nastąpi, państwa członkowskie – korzystając z szerokiego marginesu swobody pozostawionego im przez przepisy RODO – wprowadzają różnorakie rozwiązania w ramach krajowych porządków prawnych odnoszących się do ochrony danych osobowych.

Wskazane i poddane analizie możliwości wprowadzania wyjątków, a także brak jednolitej interpretacji, czym są środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, mogą prowadzić – i prowadzą – do rozbieżności między państwami członkowskimi w poziomie ochrony podmiotów danych. Istotnym elementem rozwiązań włączonych do RODO są możliwości wprowadzania zautomatyzowanego podejmowania decyzji za sprawą prawa krajowego państw członkowskich. Zautomatyzowane decyzje, podejmowane na podstawie krajowych rozwiązań prawnych, mogą znaleźć uzasadnienie, opierając się na wyjątkach przewidzianych w art. 22. Jednocześnie jednak to w stosunku do nich w art. 22

³⁴³ Pięć z ośmiu rekomendacji sformułowanych przez Wachter, Mittelstadta i Floridgo zaczyna się od sformułowania *Clarify...*, zob. S. Wachter, B. Mittelstadt, L. Floridi, *op. cit.*, s. 97–99.

brak sformułowanego wprost w RODO katalogu „środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą”.

Podobne zarzuty można sformułować wobec rozwiązań proponowanych w *Konwencji 108+*: wprowadzane przez nią rozwiązania również pozostają na wysokim poziomie ogólności i dopuszczają wiele wyjątków. Przykłady obejmują brak jasności co do tego, jak rozumieć „oparcie wyłącznie na zautomatyzowanym przetwarzaniu” pojawiające się w opisie prawa przewidzianego w art. 9 lit. a czy „znaczący wpływ” decyzji na jednostkę. Sposób sformułowania praw podmiotu danych w *Konwencji 108+* rodzi również wątpliwości co do tego, kiedy i na jakie prawo jednostka może się powołać, zanim decyzja zostanie podjęta. Czy może nie jest dozwolone podejmowanie decyzji bez uprzedniego zaoferowania jednostce możliwości wyrażenia przez nią opinii na dany temat? Niejasności te ukazują, że w dużym stopniu treść przepisów dotyczących zautomatyzowanego podejmowania decyzji, które pojawiają się w *Konwencji 108+*, powtarza nieprecyzyjne ujęcie zagadnienia w RODO.

Problemem jest również brak rozwiązań – zarówno w RODO, jak i w *Konwencji 108+* – uwzględniających kolektywny wymiar wyzwań tworzonych przez zautomatyzowane podejmowanie decyzji dla praw jednostek. DPIA mogłaby stać się istotnym instrumentem prawnym umożliwiającym testowanie wprowadzanych systemów w świetle wymogów wynikających z zakazu dyskryminacji, a przede wszystkim udostępniania informacji na temat takich systemów. Sposób regulacji tego instrumentu ogranicza jednak jego praktyczne znaczenie i prowadzi do sytuacji, w której pozostaje on wewnętrznym dokumentem przedsiębiorstw lub instytucji. Brak zarówno informacji, które wskazywałyby na korzystanie przez te podmioty z możliwości konsultacji z organami odpowiedzialnymi za ochronę danych osobowych i na stosowanie konsultacji z podmiotami danych. Podobnie, BCR ma marginalne znaczenie dla zwiększania przejrzystości zautomatyzowanego podejmowania decyzji.

Tymczasem zasady dotyczące przetwarzania danych uwzględniane w RODO odwołują się m.in. do przejrzystości. Zgodnie z art. 5 ust. 1 lit. a dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Przejrzystość pojawia się również często w komentarzach doktryny, badaczy, a nawet podmiotów uczestniczących w procesach regulacji zautomatyzowanego podejmowania decyzji jako jeden z elementów niezbędnych do budowy godnych zaufania systemów zautomatyzowanego podejmowania decyzji³⁴⁴. Dlatego możliwość

³⁴⁴ Wybrana literatura i dokumenty analizujące rolę przejrzystości dla rozwoju godnej zaufania technologii: H. Felzmann, E. Fosch Villaronga, Ch. Lutz, A. Tamò-Larrieux, *Transparency You Can Trust: Transparency Requirements for Artificial Intelligence between Legal Norms and Contextual Concerns*, „Big Data & Society” 2019, nr 6(1), s. 1–14; T.Z. Zarsky,

traktowania niektórych systemów zautomatyzowanego podejmowania decyzji, a ściślej – stojących za nimi algorytmów jako informacji publicznej lub dokumentów urzędowych, powinna być rozważona jako uzupełnienie reżimu ochrony praw jednostki odnoszących się do zautomatyzowanego podejmowania decyzji. Skoro postuluje się, a wręcz nakazuje, traktowanie przejrzystości jako jednej z zasad stojących u podstaw przetwarzania danych osobowych³⁴⁵, uzasadnione jest zwrócenie się w stronę prawa, którego rozwojowi przyświeca cel zwiększania poziomu przejrzystości w zakresie wiedzy społeczeństwa o działaniach władz publicznych.

Ponadto przesunięcie akcentu na algorytmy stosowane w ramach zautomatyzowanego podejmowania decyzji pozwala – zgodnie z zapowiedzią sformułowaną we wstępie – przeprowadzić analizę odnoszącą się do systemów zautomatyzowanego podejmowania decyzji niezależnie od tego, w jakim stopniu prowadzą one do zastępowania człowieka w procesach decyzyjnych. O ile jest możliwe, choć niezgodne z prezentowanym powyżej stanowiskiem, że na tle przepisów RODO przeważać zaczęłyby wykładnia, która będzie odnosić art. 22 i art. 13–15 do sytuacji, w których następowaloby całkowite zastąpienie człowieka przez zautomatyzowane rozwiązanie, o tyle problem taki nie występuje w odniesieniu do propozycji traktowania algorytmu jako informacji publicznej, która jest poddana analizie w kolejnych rozdziałach.

Transparent Predictions, „University of Illinois Law Review” 2013, nr 4, s. 1504–1570; F. Pasquale, *Restoring Transparency to Automated Authority*, „Journal on Communication and High Technology Law” 2011, t. 9, s. 235–254; R.H. Weber, *op. cit.*; Komisja, *Biała księga w sprawie sztucznej inteligencji...*, *op. cit.*; European Parliament Research Service, *A governance framework for algorithmic accountability and transparency*, Bruksela 2019 oraz European Parliament Research Service, *Understanding algorithmic decision-making: Opportunities and challenges*, Bruksela 2019.

³⁴⁵ Jak wspominałam: często w parze z rozliczalnością.

Algorytmy stosowane w zautomatyzowanym podejmowaniu decyzji a dostęp do informacji w prawie Rady Europy

3.1. Treść artykułu 10 EKPCz w świetle działalności ONZ w zakresie wolności informacji

Analiza prawa dostępu do informacji jako alternatywnej metody osiągnięcia większej przejrzystości algorytmów używanych do zautomatyzowanego podejmowania decyzji wymaga sięgnięcia do źródeł dyskusji na temat wolności informacji. Historia międzynarodowych inicjatyw dotyczących wolności informacji datuje się od pierwszych lat aktywności ONZ³⁴⁶. Przyczyny, w związku z którymi dostęp do informacji był tak istotny już pod koniec lat 40. XX w., wynikały z kształtowania się dwubiegunowej mapy politycznej, w której realna była konfrontacja między obozem dążącym do realizacji ideałów wiązanych z wolnością słowa a obozem państw, stosujących systemową cenzurę³⁴⁷. Zapoczątkowaną w 1947 r. serię inicjatyw dotyczących wolności informacji i prasy zwieńczyła rezolucja, która przewidywała zwołanie pierwszej w historii³⁴⁸ konferencji Narodów Zjednoczonych w sprawie wolności informacji (*United Nations Conference on Freedom of Information*) w Genewie (marzec–kwiecień 1948 r.³⁴⁹). W ramach konferencji

³⁴⁶ Treściwy przegląd dotyczący inicjatyw związanych z prawem dostępu do informacji przedstawia: D. Banisar, *The Right to Information in the Age of Information*, [w:] *Human Rights in the Global Information Society (Information Revolution and Global Politics)*, red. R.F. Jorgensen, MIT Press, Cambridge–London 2006.

³⁴⁷ Office of the Historian: Department of State, *The United States and the United Nations Conference on Freedom of Information*, Genewa 1948. <https://history.state.gov/historicaldocuments/frus1948v01p1/d189>, dostęp: 1.04.2021.

³⁴⁸ D. Goldberg, *From Sweden to the Global Stage: FOI as European Human Right?*, „Journal of International Media and Entertainment Law” 2016–2017, t. 7, nr 1, s. 10.

³⁴⁹ Losy konferencji oraz opisywanego poniżej art. 17 *Międzynarodowego Paktu Praw Człowieka* (przyjęty ostatecznie jako art. 19 MPPOiP) ciekawie zostały przedstawione

opracowano trzy propozycje konwencji dotyczących wolności informacji: *Konwencji dotyczącej zbierania i międzynarodowego przekazywania wiadomości*, *Konwencji dotyczącej instytucji międzynarodowego prawa do korekty [informacji]* oraz *Konwencji o wolności informacji*³⁵⁰. Wszystkie trzy propozycje konwencji miały z jednej strony pozwolić na ujednoczenie standardów w tych kwestiach, z drugiej strony – w teorii – przyspieszyć proces kodyfikacji m.in. prawa dostępu do informacji. W tym samym czasie toczyły się prace nad MPPOiP, których tok był dość powolny³⁵¹. Wszystkie trzy wypracowane projekty trafiły do Rady Ekonomiczno-Społecznej ONZ, która miała zdecydować o poddaniu ich głosowaniu w Zgromadzeniu Ogólnym ONZ przed otwarciem ich do podpisu dla państw członkowskich. Drogę tę przeszła jedynie *Konwencja o międzynarodowym prawie do korekty*.

Projekt *Konwencji dotyczącej wolności informacji* nie został poddany pod obrady Zgromadzenia Ogólnego ONZ do dzisiaj³⁵². Nieprzyjęcie *Konwencji o wolności informacji* odnoszącej się ściśle do praw dotyczących informacji sprawiło, że zagadnienie prawa dostępu do informacji jest przedmiotem jedynie ogólnych regulacji w ramach prawa międzynarodowego. Zamiast zostać uregulowane w osobnym akcie prawa międzynarodowego, jest ono uwzględniane tylko w pojedynczych artykułach aktów

w artykule Z. Chaffee, Jr., *Legal Problems of Freedom of Information in the United Nations*, „Law & Contemporary Problems”, 1949, t. 14, nr 4, s. 545–583.

³⁵⁰ Projekty tych Konwencji znaleźć można w: ONZ (Rada Ekonomiczno-Społeczna), *United Nations Conference on Freedom of Information* (7th session, 1948, Geneva), E/RES/152(VII), s. 15–27. <https://digitallibrary.un.org/record/212470>, dostęp: 1.04.2021. Projekt Konwencji o wolności informacji został zgłoszony przez brytyjskich delegatów, co do których motywacji tak odnosi się Z. Chaffee: „Piszący nie był w stanie zrozumieć przyczyn, w związku z którymi Brytyjczycy przygotowali ten dokument. Wydał się tak bardzo nieangielski, w tym względzie, że stwierdzał istnienie zasad ogólnych i nie wychodził na przeciw żadnej konkretnej potrzebie, jak robiły to konwencje amerykańska i francuska. To doprowadziło do spekulacji czy rząd laburzystów nie ciągnął Anglii z powrotem w stronę mentalnego nastawienia charakterystycznego dla epoki Wspólnoty Brytyjskiej, tej jedynej epoki w angielskiej historii, kiedy prawa były potrzebne z powodów abstrakcyjnych. Niezależnie od tego, ważne jest, że brytyjska konwencja uzyskała szerokie poparcie na Konferencji od innych kochających-wolność delegatów, została przeważającą większością przyjęta na sesji plenarnej, i wydaje się prawdopodobne, że, kiedy zostanie przedstawiona Zgromadzeniu Ogólnemu, zostanie podpisana przez kilka narodów”. Z. Chaffee, Jr., *op. cit.*, s. 554–555.

³⁵¹ Z. Chaffee, Jr., *op. cit.*, s. 554.

³⁵² *Convention on the International Right of Correction*, 435 U.N.T.S. 191, weszła w życie 24 sierpnia 1962 r. Jej stronami jest 17 państw i pozostaje ona w mocy do dzisiaj. Więcej na temat losów trzech konwencji, zob. T. McGonagle, *The Development of Freedom of Expression and Information within the UN: Leaps and Bounds or Fits and Starts?*, [w:] *The United Nations and Freedom of Expression and Information. Critical Perspectives*, red. T. McGonagle, Y. Donders, Cambridge University Press, Cambridge 2015, s. 10–14.

prawnych dotyczących praw człowieka. Tym samym spadła ranga wolności informacji, która była doceniana przez polityków po II wojnie światowej i przejawiała się w próbie przyjęcia konwencji dotyczącej tego tematu. Poczynając od PDPC, przez MPPOiP, po akty organizacji regionalnych i orzecznictwo ich organów sądowych prawo dostępu do informacji występuje jedynie jako mniej lub bardziej dyskusyjny element zawartych w nich gwarancji. Chociaż treść przepisów dotyczących wolności informacji jest zwykle dość podobna, to występujące różnice obfitują w konsekwencje istotne z punktu widzenia analizy, zwłaszcza w świetle argumentacji opartej na analizie prawno-porównawczej, która pojawia się w orzecznictwie ETPCz dotyczącym prawa dostępu do informacji³⁵³.

Pierwszy, w kategoriach chronologicznych, sposób sformułowania prawa dostępu do informacji w ramach aktów prawnych katalogujących prawa człowieka wiąże się z przyjęciem PDPC. Mimo braku wiążącego prawnie charakteru PDPC pośrednio wywiera znaczny wpływ na standard ochrony praw człowieka, m.in. przez jej wpływ na treść dokumentów międzynarodowych czy powolne przekształcanie się zawartych w niej norm w prawo zwyczajowe³⁵⁴. Zgodnie z jej art. 19: „Każda jednostka ma prawo do wolności poglądów i wypowiedzi; prawo to obejmuje nieskrępowaną wolność posiadania poglądów oraz poszukiwania, otrzymywania i przekazywania informacji oraz idei, wszelkimi środkami i bez względu na granice”³⁵⁵. PDPC wyznaczyła utrzymujący się do dzisiaj trend łączenia w ramach jednego artykułu kwestii wolności słowa oraz prawa dostępu do informacji i traktowania wolności informacji jako elementu wolności słowa³⁵⁶. Stanowiło to odwrót od pierwotnych conceptualizacji relacji między wolnością informacji i wolnością słowa, przy czym to wolność informacji była szerszym pojęciem, w ramach którego miała się mieścić wolność słowa. Pokłosiem takiego sposobu patrzenia na wolność informacji są trudności w uznawaniu jej za istotny element katalogu praw człowieka, widoczne w analizowanym poniżej orzecznictwie ETPCz. Ponadto ogólny sposób sformułowania art. 19 zostawiał przestrzeń do dyskusji dotyczących formy, w której miałyby on znaleźć się w prawnie wiążącym – w przeciwieństwie do PDPC – MPPOiP³⁵⁷.

³⁵³ Opisaną dalej w rozdziale.

³⁵⁴ Zob. W. Czaplinski, A. Wyrozumaska, *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, wyd. 3, C.H. Beck, Warszawa 2014, s. 550.

³⁵⁵ *Powszechna deklaracja praw człowieka*, 10 grudnia 1948, rezolucja Zgromadzenia Ogólnego 217 A; polska wersja językowa: <http://libr.sejm.gov.pl/tek01/txt/onz/1948.html>, dostęp: 1.04.2021.

³⁵⁶ Zob. T. McGonagle, *op. cit.*, s. 6.

³⁵⁷ *Międzynarodowy pakt praw obywatelskich i politycznych* (MPPOiP), Dz.U. 1977 nr 38 poz. 167.

W tym samym czasie co prace nad MPPOiP³⁵⁸ toczyły się negocjacje dotyczące opisanych powyżej trzech projektów konwencji mających dotyczyć wolności informacji. W związku z tym pojawiały się wątpliwości, czy prawo do swobodnego wyrażania opinii w ogóle powinno znaleźć się w *Międzynarodowym pakcie praw obywatelskich i politycznych*, czy może raczej być regulowane za pomocą tych bardziej szczegółowych aktów prawnych. Ostatecznie art. 19 MPPOiP składa się z trzech ustępów. W pierwszym z nich stwierdza się, że każdy człowiek ma prawo do posiadania własnych poglądów. W drugim, częściowo powtarzającym treść PDPC, znalazło się prawo do swobodnego wyrażania opinii. Jako jego część określona została swoboda poszukiwania, otrzymywania i rozpowszechniania wszelkich informacji i poglądów bez względu na granice państwowe. Oznacza to, że swoboda wypowiedzi w MPPOiP bez wątpienia „obejmuje nie tylko wolność otrzymywania i przekazywania informacji i idei, lecz również wolność ich aktywnego poszukiwania czy zdobywania”³⁵⁹. W art. 19 MPPOiP zostały sprecyzowane również środki rozpowszechniania (ustnie, pismem lub drukiem) oraz forma rozpowszechniania (dzieła sztuki, bądź w jakikolwiek inny sposób). Swobodą nowością stanowi ustęp trzeci, który formułuje możliwe – ze względu na odpowiedzialność wynikającą ze swobody wyrażania opinii – ograniczenia. Uzależnia on możliwość wprowadzania ograniczeń od spełnienia dwóch warunków. Po pierwsze, może ono występować jedynie w ustawie oraz, po drugie, w wymienionych w art. 19 celach, tzn. poszanowania praw i dobrego imienia innych (co stanowi wskazówkę dotyczącą potencjalnego konfliktu między ochroną prawa do prywatności a swobodą wyrażania opinii), ochrony bezpieczeństwa państwowego lub porządku publicznego albo zdrowia lub moralności publicznej.

Potwierdzenie wykładni, zgodnie z którą prawo jednostek do otrzymywania informacji będących w posiadaniu państw stanowi immanentną część MPPOiP, znalazło się w decyzji Komitetu Praw Człowieka w sprawie *Toktakunov przeciwko Kirgistanowi*³⁶⁰ z 2011 r. Skarga dotyczyła dostępu do informacji, którego żądało stowarzyszenie Youth Human Rights Group, na

³⁵⁸ Należy podkreślić, że debata nad treścią MPPOiP rozpoczęła się, gdy dobiegała już końca dyskusja dotycząca EKPCz.

³⁵⁹ A. Gliszczyńska-Grabias, *Artykuł 19. Wolność posiadania i wyrażania poglądów*, [w:] *Międzynarodowy Pakt Praw Obywatelskich (Osobistych) i Politycznych. Komentarz*, red. R. Wieruszewski, Wolters Kluwer Polska, Warszawa 2012, s. 468.

³⁶⁰ Komitet Praw Człowieka, Komunikat z dnia 28 marca 2011 r. w sprawie 1470/2006 *Toktakunov przeciwko Kirgistanowi*. W pewnym stopniu do zagadnienia odnosiła się również decyzja Komitetu Praw Człowieka z dnia 7 kwietnia 1999 r. w sprawie 633/1995 *Gauthier przeciwko Kanadzie*. Skarżący – wydawca czasopisma – miał jedynie ograniczony dostęp do łoża prasowej, co zostało uznane za naruszenie jego prawa do poszukiwania, otrzymywania i rozpowszechniania informacji.

temat liczby osób skazanych na śmierć w Kirgistanie od 31 grudnia 2003 r. oraz liczby osób skazanych na śmierć, które były przetrzymywane w systemie penitencjarnym. Dostęp do informacji nie został przyznany ze względu na ich tajny charakter. Postępowanie w ramach kolejnych instancji systemu krajowego potwierdzało zgodność z prawem odmowy opartej na przesłance tajności żądanej informacji. Skarżący zakwestionował tę ocenę, podnosząc, że prawo w Kirgistanie nie przewiduje zakwalifikowania informacji na temat liczby osób skazanych na śmierć jako tajnej, szczególnie zaś regulacje (*by-laws*), które odnoszą się do dostępu do takich informacji, są niedostępne. W związku z tymi argumentami Toktakunov twierdził, że naruszone zostało jego prawo dostępu do informacji (zarówno jako obywatela, jak i jako reprezentanta stowarzyszenia), a także prawo do skutecznej ochrony sądowej w tym zakresie.

Analiza tej sprawy doprowadziła do potwierdzenia przez Komitet Praw Człowieka, że „odniesienie do prawa do «poszukiwania» i do «otrzymywania» «informacji» tak jak włączone do artykułu 19, ustępu 2 Paktu, zawiera prawo jednostki do otrzymania informacji będących w posiadaniu państwa, z wyjątkami dopuszczonymi przez restrykcje uwzględnione w Pakcie”³⁶¹. W decyzji zostało podkreślone, że informacje powinny być udostępniane bez konieczności udowodnienia bezpośredniego lub osobistego zaangażowania w daną kwestię, z wyjątkiem sytuacji, w których są stosowane usprawiedliwione restrykcje. Ponadto Komitet odnotował szczególną rolę mediów i prasy w odniesieniu do prawa dostępu do informacji, przy czym terminy „media” i „prasa” powinny być interpretowane szeroko: za pełniące funkcje mediów i prasy mogą zostać uznane zarówno stowarzyszenia, jak i osoby fizyczne. Kluczowym kryterium uznania danego podmiotu za uprawnionego do żądania dostępu do informacji jest sama funkcja, w ramach której on działa, i fakt, czy służy on realizacji publicznego interesu i uczestnictwa w debacie publicznej³⁶².

Rozważania te są zbliżone do przedstawionej w dalszej części rozdziału argumentacji konstruowanej przez ETPCz, który czerpał inspirację m.in. z decyzji Komitetu Praw Człowieka w sprawie *Toktakunov przeciwko Kirgistanowi*, przedstawiając wykładnię art. 10 EKPCz w zakresie prawa dostępu do informacji. Na art. 10 EKPCz składają się dwa ustępy: pierwszy określa prawa wiążące się z wolnością wyrażania opinii, drugi definiuje możliwe jej ograniczenia, co stanowi o podobieństwie między art. 10 i art. 19 MPPOiP.

³⁶¹ Komitet Praw Człowieka, Komunikat z dnia 28 marca 2011 r. w sprawie 1470/2006, pkt 6.3.

³⁶² „[...] jako taki, może on być uznany za mający [...] specjalną funkcję «watchdoga» w kwestiach odnoszących się do interesu publicznego” – Komitet Praw Człowieka, Komunikat z dnia 28 marca 2011 r. w sprawie 1470/2006, pkt 6.3.

Zasadniczą różnicą między ujęciem zaproponowanym w EKPCz a omówionymi wyżej aktami przygotowanymi w ramach działalności ONZ jest – przede wszystkim – nieobecność jednego czasownika w art. 10 EKPCz. W odróżnieniu do przytaczanych powyżej aktów prawnych sposób sformułowania art. 10 nie uwzględnia „szukania” informacji, lecz jedynie „otrzymywanie i przekazywanie informacji i idei”. Na etapie prac nad EKPCz czasownik *seek* zniknął w brytyjskiej propozycji poprawek do projektu EKPCz, które zostały zgłoszone w marcu 1950 r.³⁶³, chociaż – zgodnie z *travaux préparatoires* – jeszcze wersja procedowana w lutym operowała terminami *seek, receive and impart*³⁶⁴. Chociaż kolejne procedowane wersje artykułu nie zawierały już sformułowania „szukanie”, to zmiana ta nie wzbudzała kontrowersji wśród pracujących nad treścią EKPCz³⁶⁵.

Kontrowersje wzbudziło natomiast sformułowanie „bez ingerencji władz publicznych”, które zostało zaproponowane jako uzupełnienie warunku „bez względu na granice państwowe”. Może to powodować wątpliwości dotyczące odpowiedzialności za ograniczenia wynikające z aktywności niepaństwowych aktorów oraz rozumienia terminu „władza publiczna”³⁶⁶. Podobnie wątpliwości pojawiły się w odniesieniu do niektórych elementów katalogu możliwych ograniczeń, który został sformułowany w ustępie 2. Szczególnie kontrowersyjnym elementem było uwzględnienie „integralności terytorialnej” jako przyczyny możliwych ograniczeń dla wolności informacji i wyrazu³⁶⁷. Ostatecznie katalog przyczyn, które państwa mogą podnosić jako uzasadnienie ograniczania praw związanych ze swobodą wyrazu, jest szerszy niż ten przyjęty w art. 19 MPPOiP i obejmuje: bezpieczeństwo państwowe, integralność terytorialną, bezpieczeństwo publiczne ze względu na konieczność

³⁶³ Jest to spójne z propozycją przedstawioną przez rząd brytyjski w zakresie sposobu sformułowania artykułu dotyczącego wolności informacji na forum ONZ, zob. Rada Europy (*European Commission of Human Rights*), *Preparatory work on article 10 of the European Convention on Human Rights*, DH (56)15 oraz CDH (75)6, s. 8, 10–11. [www.echr.coe.int/LibraryDocs/Travaux/ECHRTravaux-ART10-DH\(56\)15-EN1338895.pdf](http://www.echr.coe.int/LibraryDocs/Travaux/ECHRTravaux-ART10-DH(56)15-EN1338895.pdf), dostęp: 1.04.2021.

³⁶⁴ Śladów odnotowania tej zmiany jako istotnej nie odnalazłam czy to w *travaux préparatoires*, czy też w monumentalnym komentarzu do EKPCz: W.A. Schabas, *op. cit.*, s. 448-450.

³⁶⁵ Problem wykładni przez ETPCz takiego sposobu ujęcia kwestii wolności informacji – w której szukanie informacji jest niezbędne do jej otrzymywania i przekazywania – rozważany jest w dalszej części rozdziału.

³⁶⁶ Tej kwestii jest poświęcona odpowiednia sekcja w dalszej części rozdziału.

³⁶⁷ Zob. Rada Europy (*European Commission of Human Rights*), *Preparatory work on article 10 of the European Convention on Human Rights*, *op. cit.*, s. 13. Integralność terytorialna pojawiła się w artykule z inicjatywy delegacji tureckiej, a utrzymanie jej wiązało się z założeniem, że każde ograniczenia do swobody wyrazu będą podlegać testowi „niezbędności w społeczeństwie demokratycznym” (zob. dalej).

zapobieżenia zakłóceniu porządku lub przestępstwu i ujawnieniu informacji poufnych oraz ochronę zdrowia, moralności, dobrego imienia i praw innych osób, a także zagwarantowanie powagi i bezstronności władzy sądowej.

Treść art. 10 EKPCz, chociaż powstała w wyniku inspiracji wersją przepisów dotyczących wolności słowa i wolności informacji wypracowanych w ramach ONZ, nieco różni się od rozwiązania ostatecznie przyjętego w art. 19 MPPOiP. Prawo poszukiwania – a więc dostępu do – informacji nie jest w EKPCz ujęte wprost. Stwierdzenie jego istnienia wymagało od ETPCz przeprowadzenia skomplikowanej wykładni scharakteryzowanej dalej w rozdziale. Dopiero jej wynikiem jest możliwość stwierdzenia, że w określonych warunkach prawo to stanowi element katalogu praw człowieka uwzględnionych w EKPCz.

3.2. Prawo dostępu do informacji w działalności Rady Europy

Z czasem w ramach działalności Rady Europy zaczęto formułować propozycje, które miały na celu wyjaśnienie wątpliwości dotyczących prawa dostępu do informacji wiążących się z brakiem słowa „poszukiwanie” w treści art. 10 EKPCz³⁶⁸. Aktywność Rady Europy w odniesieniu do prawa dostępu do informacji rozpoczęła się zanim pojawiło się orzecznictwo ETPCz, które w sposób kompleksowy wyjaśnia tę kwestię. Już w 1979 r. Zgromadzenie Parlamentarne Rady Europy przyjęło rekomendację dotyczącą publicznego dostępu do dokumentów rządowych oraz wolności informacji³⁶⁹. Zgromadzenie Parlamentarne odwołało się do decyzji³⁷⁰ podjętej przez Komitet Mini-

³⁶⁸ Treść art. 10 EKPCz: „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 przedsiębiorstw 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 ujawnieniu informacji poufnych lub na zagwarantowanie powagi i bezstronności władzy sądowej”.

³⁶⁹ Zgromadzenie Parlamentarne (Rada Europy), *Recommendation 854 (1979) Access by the public to government records and freedom of information* (Text adopted by the Assembly on 1 February 1979 – 24th Sitting). <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=14888&lang=en>, dostęp: 1.04.2021.

³⁷⁰ „[...] implementuje decyzję podjętą w 1976 aby wprowadzić zapis o prawie do poszukiwania informacji do *Europejskiej konwencji praw człowieka*” – Zgromadzenie Parlamentarne (Rada Europy), *Recommendation 854 (1979)*..., *op. cit.*, pkt 13. Mimo najlepszycych starań nie udało mi się dotrzeć do oryginalnej decyzji, na którą Zgroma-

strów w 1976 r. Odnosiła się ona do wprowadzenia prawa do poszukiwania informacji wyrażonego wprost (*right to seek information*) do treści EKPCz. W rekomendacji z 1979 r. Zgromadzenie Parlamentarne wzywało Komitet Ministrów do podjęcia stosownych działań w tej materii. Jednym z postulatów wymienionych wprost w rekomendacji jest zachęcenie państw członkowskich, które jeszcze tego nie zrobiły, do wprowadzenia systemu wolnego przepływu informacji (*system of freedom of information*). Przez to pojęcie rozumiany jest dostęp do akt rządowych, prawo do szukania i otrzymywania informacji od rządowych agencji i departamentów, prawo do sprawdzania i poprawiania osobistych dokumentów, prawo do prywatności³⁷¹ oraz prawo do szybkiej ścieżki sądowej w tych kwestiach³⁷².

Komitet Ministrów 25 listopada 1981 r. przyjął stosowną rekomendację w tej sprawie³⁷³. Ten prawnie niewiążący dokument wzywał państwa członkowskie do zagwarantowania wszystkim podmiotom podlegającym pod ich jurysdykcję prawa do dostępu na żądanie do informacji będących w posiadaniu władz publicznych innych niż ciała ustawodawcze oraz sędownicze³⁷⁴. Stąd też, w porównaniu z zakresem prawa dostępu do informacji, którego

dzenie Parlamentarne powołuje się w tych Rekomendacjach. W orzeczeniu w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom* można znaleźć również odwołanie do tej kwestii: „Rekomendacja Nr 582 dotycząca mediów komunikacji masowej i praw człowieka przyjęta przez Zgromadzenie Parlamentarne Rady Europy 23 stycznia 1970 r. rekomendowała poinstruowanie Komitetu ekspertów d.s. praw człowieka, aby rozważyli i przygotowali rekomendacje dotyczące: [...] *rozszerzenia wolności informacji zagwarantowanej w artykule 10 Europejskiej konwencji praw człowieka, przez konkluzję w protokole lub w inny sposób, aby uwzględniała ona prawo do poszukiwania informacji (które jest włączone do treści artykułu 19 ust. 2 Międzynarodowego protokołu praw obywatelskich i politycznych Organizacji Narodów Zjednoczonych); powinien również istnieć odpowiedni obowiązek władz publicznych do uczynienia informacji dotyczących interesu publicznego dostępnymi, z uwzględnieniem odpowiednich ograniczeń*”. Wyrok ETPCz z 8 listopada 2016 r. w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, skarga nr 18030/11, pkt 50.

³⁷¹ Okres wypracowywania pierwszych dokumentów z kategorii *soft law* odnoszących się do prawa dostępu do informacji zbiega się w czasie z intensyfikacją prac dotyczących aktów mających na celu wzmocnienie ochrony danych osobowych. Stąd też łączenie tych dwóch kategorii chronionych praw jest uzasadnione nie tylko ich współoddziaływaniem, lecz również toczącą się wówczas debatą na tematy związane zarówno z ochroną danych osobowych i prywatności, jak i prawem dostępu do informacji.

³⁷² Zgromadzenie Parlamentarne (Rada Europy), *Recommendation 854 (1979)*..., *op. cit.*, pkt 13.

³⁷³ Komitet Ministrów (Rada Europy), *Recommendation No. R (81) 19 of the Committee of Ministers to Member States on the Access to Information Held by Public Authorities* (Adopted by the Committee of Ministers on 25 November 1981 at the 340th meeting of the Ministers' Deputies). https://www.access-info.org/wp-content/uploads/Recommendation_81_19.pdf, dostęp: 1.04.2021.

³⁷⁴ Komitet Ministrów (Rada Europy), *Recommendation No. R (81) 19*..., *op. cit.*, pkt I.

promowanie sugerowało Zgromadzenie Parlamentarne, ostateczna forma rekomendacji wprowadza bardziej ograniczony katalog proponowanych działań. Jednocześnie jednak, co godne jest podkreślenia, odnotowane zostaje zalecenie niezależniania dostępu do informacji od konieczności wykazania interesu zależnego od jej otrzymania³⁷⁵.

Rekomendacje te przez długi czas nie przynosiły bezpośrednich rezultatów w postaci przyjęcia zmian w EKPCz. ETPCz już wówczas wydawał się jednak skłaniać ku wykładni, zgodnie z którą – mimo braku sformułowania „poszukiwania” w treści art. 10 – artykuł może stanowić źródło dla uprawnień dotyczących dostępu do informacji. Wskazuje na to następujący fragment obserwacji ETPCz w zakresie dyskusji toczącej się w latach 80. nad projektem Protokołu 6 do EKPCz:

Trybunał uwzględnia, że prawo do otrzymania informacji, zagwarantowane przez artykuł 10 Konwencji, wiąże się z prawem do poszukiwania informacji. Co więcej, wydaje się to ewidentne, dla Trybunału, że takie poszukiwanie informacji (oraz jej otrzymanie i komunikowanie) musi w każdym razie być zagwarantowane środkami prawnymi. Trybunał zauważa również, [...] że prawo do poszukiwania informacji nie wiąże się z żadnym obowiązkiem do jej dostarczenia po stronie władz; jest to prawo do otrzymania (*receive*) informacji, nie zaś prawo do bycia nią obdarowanym (*to be given*)³⁷⁶.

Cytat ten ilustruje jedną z metod, którymi z czasem zaczęły posługiwać się ETPCz, aby uzasadnić obecność prawa dostępu do informacji w EKPCz³⁷⁷. Prawo poszukiwania informacji jest niezbędnym elementem gwarancji przewidzianych w art. 10 jako lustrzane odbicie prawa do otrzymania informacji. Bez dostępu do informacji nie jest możliwe jej otrzymanie. Metoda ta jest o tyle wyjątkowa, że idzie o krok dalej niż literalne brzmienie art. 10. W wykładni proponowanej przez ETPCz jest położony nacisk na logiczne konsekwencje uwzględnienia w treści przepisu aspektu „otrzymywania” informacji, mimo braku zmian w treści samej EKPCz postulowanych w wymienionych wyżej dokumentach.

Waga opracowywanych w latach 70. i 80. dokumentów jako źródła wiedzy odnoszącej się do motywacji do rozwoju rozwiązań dotyczących

³⁷⁵ „Dostęp do informacji nie powinien być odmówiony na podstawie nieposiadania przez osobę go żądającą interesu w tej kwestii”. Komitet Ministrów (Rada Europy), *Recommendation No. R (81) 19...*, *op. cit.*, pkt II.

³⁷⁶ Cytat dokumentu Trybunału (81) 76 za: Wyrok ETPCz z 8 listopada 2016 r. w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, skarga nr 18030/11, pkt 51. Wyrok zawiera również przegląd innych dokumentów z tego okresu świadczących o wspólnym stanowisku państw stron konwencji do treści art. 10 EKPCz jako zawierającej „poszukiwanie” informacji.

³⁷⁷ Pozostałe charakteryzuję dalej w rozdziale.

prawa dostępu do informacji wiąże się ponadto z przedstawieniem w nich motywacji stojących za koniecznością zagwarantowania prawa dostępu do informacji. Pozostają one aktualne w świetle współczesnych uwarunkowań technologiczno-gospodarczych. Przykładem są rekomendacje Zgromadzenia Parlamentarnego z 1979 r., które zawierają następujący fragment: „Zważywszy na fakt, że życie publiczne w dzisiejszym społeczeństwie stało się tak skomplikowane i techniczne, że rządowe organy i agencje często generują i posiadają informacje, które nie mogą być osiągnięte z innych źródeł”³⁷⁸. Chociaż można zauważyć, że to, jakie podmioty są w posiadaniu unikatowych informacji, podległo gwałtownej transformacji w ostatnich dekadach, to nie ulega wątpliwości, że poziom skomplikowania i techniczności życia publicznego jedynie się pogłębił. Stąd też, podążając za motywacją wyrażoną w cytowanym akapicie, należy się przyjrzeć krokom, które od lat 80. zostały podjęte w celu zbliżenia tego, jak rozumiana jest treść prawa dostępu do informacji do realiów społeczno-gospodarczych.

Inicjatywą mającą na celu dostosowanie treści prawa dostępu do informacji do szybko zmieniających się technologii informacyjnych było przyjęcie KDOD³⁷⁹. Wejście w życie KDOD zostało uzależnione od osiągnięcia co najmniej 10 ratyfikacji, co nastąpiło w sierpniu 2020 r. W związku z tym datą wejścia w życie KDOD jest 1 grudnia 2020 r.³⁸⁰ Zgodnie z art. 1 ust. 2 lit. b KDOD objęte jej postanowieniami są wszelkie oficjalne dokumenty, czyli: „wszystkie informacje zarejestrowane w dowolnej formie, utworzone lub otrzymane i przechowywane przez władze publiczne”³⁸¹. Tak szeroka definicja dokumentu pozwala stwierdzić, że postanowieniami KDOD powinno do pewnego stopnia być objęte funkcjonowanie władz publicznych w ramach przestrzeni cyfrowej. Pozwala ona również założyć, że w prawie Rady Europy rozróżnienie między dokumentem a informacją teoretycznie opiera się na tym, że dokument obejmuje wszystkie informacje „zarejestrowane w dowolnej formie”. Informacja niezarejestrowana nie będzie zatem spełniała warunku bycia uznaną za dokument. W świetle dalej opisanego orzecznictwa ETPCz dotyczącego prawa dostępu do informacji różnica ta wydaje się jednak jedynie teoretyczna. Orzecznictwo ETPCz mówi o dostępie do informacji „gotowej i dostępnej”. Tym samym w praktyce informacja, aby można się powoływać na prawo dostępu do niej, musi być również zarejestrowana w jakiejś formie. Dość szeroka jest również wprowadzona do

³⁷⁸ Zgromadzenie Parlamentarne (Rada Europy), *Recommendation 854 (1979)*..., *op. cit.*, pkt 3.

³⁷⁹ *Council of Europe Convention on Access to Official Documents (KDOD)*, CETS Nr 205.

³⁸⁰ Informacje na temat ratyfikacji: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/205/signatures?p_auth=en0DTgZ8, dostęp: 1.04.2021.

³⁸¹ Art. 1 ust. 2 lit. b KDOD.

KDOD definicja władzy publicznych, które obejmują władze i administracje na poziomie krajowym, regionalnym i lokalnym, organy ustawodawcze i sądownicze w ramach wykonywanych przez nie funkcji administracyjnych, a także osoby fizyczne i prawne w zakresie, w którym wykonują one władzę administracyjną (art. 1 ust. 2 lit. a(i)). Ponadto państwa mogą notyfikować poszerzenie zakresu rozumienia władz publicznych o kolejne trzy kategorie podmiotów zdefiniowane w artykule³⁸².

Jednocześnie art. 3 KDOD wprowadza katalog możliwych do przywołania przez państwa przyczyn ograniczania dostępu do oficjalnych dokumentów, który jest szerszy niż ten sformułowany w odniesieniu do informacji w art. 10 EKPCz. Zawiera on m.in. interesy handlowe lub inne o charakterze ekonomicznym (art. 3 ust. 1 lit g KDOD), co mogłoby stanowić poważne wyzwanie dla wyważenia z jednej strony interesów chronionych przez państwo, z drugiej zaś prawa dostępu jednostek do dokumentów w zakresie prób otrzymania dostępu do algorytmów jako dokumentów urzędowych. W obszarach potencjalnie szczególnie wrażliwych na wdrażanie zautomatyzowanego podejmowania decyzji, jak np. opieka zdrowotna, pomoc społeczna czy ubezpieczenia społeczne, głównym celem implementacji wdrażanych zautomatyzowanych rozwiązań jest poprawienie efektywności systemu. W związku z tym argument oparty na inwestycjach finansowych poniesionych w związku z wdrażaniem systemu zautomatyzowanego przetwarzania danych (w tym podnoszone w rozdziale pierwszym kwestie ochrony własności intelektualnej i tajemnic handlowych) i na poprawianiu efektywności wydawanych w danym obszarze środków, mógłby w świetle postanowień KDOD być podnoszony do ograniczania dostępu do dokumentów.

KDOD tworzy również wątpliwości w odniesieniu do kwestii, czy prawo do dostępu do oficjalnych dokumentów stanowi, w rozumieniu Rady Europy, samodzielne³⁸³ prawo człowieka, czy jest jedynie narzędziem do realizacji innych uprawnień. Powołując się na fragment raportu towarzyszącego KDOD brzmiący: „Prawo dostępu do informacji do oficjalnych dokumentów jest również kluczowe dla samorozwoju ludzi i egzekwowania fundamentalnych prawa człowieka”³⁸⁴, David Goldberg twierdzi, że prawo dostępu może być rozumiane jedynie jako instrument służący egzekwowania innych praw³⁸⁵.

³⁸² Czyli organy ustawodawcze w zakresie pełnienia przez nie innych funkcji niż administracyjne oraz organy sądownicze w takim samym zakresie oraz osoby fizyczne lub prawne, o ile wykonują funkcje publiczne lub działają ze środków publicznych, zgodnie z prawem krajowym – art. 1 ust. 2 lit. a(ii), KDOD.

³⁸³ W znaczeniu *self-standing*.

³⁸⁴ Rada Europy, *Explanatory Report to the Council of Europe Convention on Access to Official Documents*, 2009, s. 2. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800d3836>, dostęp: 1.04.2021.

³⁸⁵ D. Goldberg, *op. cit.*, s. 13.

Zauważa również, że tak instrumentalne nastawienie Rady Europy wobec prawa dostępu do oficjalnych dokumentów i dostępu do informacji stawiłaby tę organizację w opozycji do perspektywy promowanej przez ONZ czy inne organizacje regionalne³⁸⁶. Prawo dostępu do dokumentów urzędowych i do informacji nie powinno być postrzegane jedynie jako narzędzie realizacji innych praw jednostki. Możliwość pozyskiwania wiedzy na temat działania władz publicznych stanowi samodzielne prawo, które w demokratycznych społeczeństwach powinno być uznawane za jeden z elementów katalogu praw człowieka. Najnowsze orzecznictwo ETPCz w pewnym stopniu, chociaż nie całkowicie, zmierza w kierunku takiego postrzegania prawa dostępu do informacji.

3.3. Prawo dostępu do informacji w orzecznictwie ETPCz

W związku m.in. z niewielką liczbą ratyfikacji KDOD oraz faktem, że jest ona bardzo niedawno przyjętym aktem prawa Rady Europy dotyczącym dostępu

³⁸⁶ Kluczowa w tym zakresie jest działalność OPA. Inicjatywa dotycząca przygotowania projektu dotyczącego *Modelowego międzyamerykańskiego prawa dotyczącego dostępu do informacji publicznej (Model Inter-American Law on Access to Public Information)* powstała w 2009 r., kiedy to Zgromadzenie Ogólne OPA skierowało do Departamentu Prawa Międzynarodowego organizacji prośbę dotyczącą przygotowanie takiego dokumentu. W 2013 r. gotowy był projekt stosownego programu, który Zgromadzenie Ogólne OPA przyjęło rezolucją z 14 czerwca 2016 r. (OPA, *Inter-American Program on Access to Public Information (Adopted at the Second Plenary Session, held on June 14, 2016)*, Resolution AG/RES. 2885 (XLVI-O/16). http://www.oas.org/en/sla/dil/docs/access_to_information_Inter-American_Program.pdf, dostęp: 1.04.2021. Chociaż ta i inne inicjatywy, np. przyjęcie w 2008 r. *Principles on the Right of Access to Information* (OPA, *Principles on the Right of Access to Information*, CJI/RES.147 (LXXIII-O/08). http://www.oas.org/en/sla/dil/docs/CJI-RES_147_LXXIII-O-08_eng.pdf, dostęp: 1.04.2021, są świadectwem zainteresowania OPA tematem, to istotniejszy jest fakt bezpośredniego rozpoznania prawa dostępu do informacji przez Międzamyerykański Trybunał Praw Człowieka. Kluczowe w tej kwestii orzeczenie w sprawie *Claude Reyes i inni przeciwko Chile* wydane zostało w 2006 r. Międzamyerykański Trybunał Praw Człowieka stwierdził w nim wprost, że art. 13 *Ame-rykańskiej konwencji o ochronie praw człowieka* tworzy samodzielne prawo jednostek do dostępu do publicznych informacji: „Trybunał stwierdza, że wprost przewidując prawo do poszukiwania i otrzymywania informacji artykuł 13 Konwencji chroni prawo wszystkich jednostek do żądania dostępu do informacji będących w posiadaniu Państwa, z wyjątkami dopuszczonymi przez ograniczenia wyłożone w Konwencji”. Międzamyerykański Trybunał Praw Człowieka, *Wyrok w sprawie Claude Reyes i inni przeciwko Chile*, 19 września 2006 r., ser. C No. 151, pkt 77). Odpowiedni fragment art. 13 *Ame-rykańskiej konwencji o ochronie praw człowieka* brzmi: „1. Każdy ma prawo do wolności myśli i wypowiedzi. Prawo to obejmuje wolność poszukiwania, otrzymywania i rozpowszechniania wszelkich informacji i poglądów, niezależnie od granic państwowych, ustnie, pismem, drukiem, w postaci dzieła sztuki lub w jakikolwiek inny sposób według własnego wyboru”. *American Convention on Human Rights*, „*Pact of San Jose*”. <https://www.refworld.org/docid/3ae6b36510.html>, dostęp: 1.04.2021 (polska wersja językowa: <http://libr.sejm.gov.pl/tek01/txt/inne/1969a-c1.html>, dostęp: 1.04.2021).

do dokumentów, głównym źródłem, z którego czerpać można wiedzę o tym, czym obecnie jest prawo dostępu do informacji³⁸⁷, pozostają EKPCz oraz relewantne orzecznictwo. W pierwszej fazie aktywności ETPCz dotyczącej tego tematu dominowało stanowisko, zgodnie z którym – przynajmniej w okolicznościach takich jak w rozpatrywanych wówczas sprawach – nie istniała możliwość powołania się na prawo dostępu do informacji. Przekonanie, że art. 10 EKPCz nie może stanowić źródła dla prawa dostępu do informacji, było wynikiem kładzenia nacisku na negatywne obowiązki państw wynikające ze sposobu sformułowania treści artykułu.

Kluczowym orzeczeniem, w którym ETPCz sformułował tezy dotyczące art. 10, podkreślając brak aktywnych obowiązków państwa w zakresie przekazywania informacji, jest wyrok w sprawie *Leander przeciwko Szwecji*. Sprawa dotyczyła prawa jednostki do wglądu w przyczynę, w związku z którymi nie została ona przyjęta do pracy w sektorze publicznym. Zarzuty dotyczyły naruszenia przez Szwecję art. 8 oraz art. 10 EKPCz. Analiza Trybunału wykazała, że uniemożliwienie przez Szwecję dostępu do informacji zebranych o jednostce, na podstawie których nie została ona przyjęta do pracy, spełniało warunki ograniczeń prawa do ochrony prywatności w formie uwzględnionej w EKPCz, czyli było przewidziane prawem oraz niezbędne w demokratycznym społeczeństwie. W odniesieniu do art. 10 natomiast ETPCz odnotował, że:

[P]rawo do wolności otrzymywania informacji zasadniczo zakazuje rządowi wprowadzania ograniczeń w zakresie otrzymywania przez jednostkę informacji, jakich inni pragną lub mogą pragnąć jej udzielić. W okolicznościach, jakie występują w przedmiotowej sprawie, art. 10 nie przyznaje jednostce prawa dostępu do rejestru zawierającego informacje na temat jej osobistej pozycji ani też nie zobowiązuje rządu do przekazania jej takich informacji³⁸⁸.

Podkreślona zostaje tutaj perspektywa, w której art. 10 ma przede wszystkim stanowić o obowiązku powstrzymania się państwa od tworzenia

³⁸⁷ Posługuję się tutaj pojęciem informacji ze względu na fakt, że termin też jest używany w orzecznictwie ETPCz. Jednocześnie, tak jak wspomniałam wyżej, w świetle orzecznictwa ETPCz różnica między informacją a dokumentem, zgodnie z jego definicją uwzględnioną w KDOD, wydaje się nie mieć praktycznego znaczenia. Natomiast w związku z niewielką liczbą ratyfikacji KDOD to prawo dostępu do informacji oparte na art. 10 EKPCz może mieć większe znaczenie, ponieważ jego konkluzje powinny się odnosić do wszystkich państw stron EKPCz.

³⁸⁸ Wyrok ETPCz z 26 marca 1987 r. w sprawie *Leander przeciwko Szwecji*, skarga nr 9248/81, pkt 74. Tłumaczenie tego fragmentu zaczerpnięte jest z polskiej wersji językowej wyciągu z wyroku w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, zob. Wyrok ETPCz z 8 listopada 2016 r. w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, skarga nr 18030/11, pkt 127.

restrykcji w odniesieniu do dostępu do informacji, których inne – w domyśle: jednostki – pragną rozpowszechnić. Posłużenie się sformulowaniem „w okolicznościach, jakie występują w przedmiotowej sprawie” mogło jednak sugerować, że jest możliwa inna wykładnia treści art. 10³⁸⁹.

Sprawa *Leander przeciwko Szwecji* dotyczyła, co należy podkreślić, informacji na temat jednostki i jej indywidualnej, prywatnej sytuacji. Okoliczność ta przesądza o uznaniu jej jako niepodlegającej prawu dostępu do informacji: art. 10 „nie przyznaje jednostce prawa dostępu do rejestru zawierającego informacje na temat jej osobistej pozycji ani też nie zobowiązuje rządu do przekazania jej takich informacji”. Opisywany powyżej związek między wolnością słowa a prawem dostępu do informacji sprawia natomiast, że myślenie o prawie dostępu do informacji powinno być osadzone raczej w kontekście społecznym, w odniesieniu do spraw o dużym znaczeniu dla debaty publicznej.

Stanowisko ETPCz w odniesieniu do dostępu do informacji dotyczących życia prywatnego jednostki zostało potwierdzone w wyroku *Gaskin przeciwko Zjednoczonemu Królestwu*³⁹⁰. Sprawa dotyczyła próby otrzymania informacji przez pana Gaskina na temat jego dzieciństwa, które spędził w rodzinach zastępczych. W wyroku ETPCz przywołał argumentację sformułowaną w sprawie *Leander przeciwko Szwecji*. Podobnie ETPCz postąpił w sprawie *Roche przeciwko Zjednoczonemu Królestwu*³⁹¹, która również dotyczyła dostępu do informacji na temat jednostki. Pan Roche był poddawany w czasie służby wojskowej dla brytyjskiej armii badaniom medycznym, które prowadziły do wystawienia go na działanie toksycznych chemikaliów, o czym nie otrzymał stosownych informacji. Również w tym wypadku ETPCz nie uznał, aby art. 10 miał zastosowanie do takiej sprawy. Wszystkie wymienione orzeczenia dotyczyły kwestii podnoszonych przez jednostki w imię własnego interesu, nie zaś w imię ogólnego interesu publicznego. Stąd też m.in. ETPCz uznał brak naruszenia art. 10 w tych sprawach.

Podobna argumentacja została jednak powtórzona również w orzeczeniu w sprawie *Guerra i inni przeciwko Włochom* z 1998 r. Sprawa dotyczyła

³⁸⁹ Takie stanowisko, interpretujące sformułowanie pojawiające się w wyroku jako zostawiające przestrzeń dla bardziej proaktywnej interpretacji art. 10, odnaleźć można w literaturze: „Słowa «w okolicznościach, jakie występują w przedmiotowej sprawie» sugerują, że mogą mieć miejsce sytuacje, w których pozytywny obowiązek Państwa się pojawia. W orzecznictwie Trybunału nie pojawił się jednak taki przypadek”. W. Hins, D. Voorhoof, *Access to State-Held Information as a Fundamental Right under the European Convention on Human Rights*, „European Constitutional Law Review” 2007, nr 3, s. 118.

³⁹⁰ Wyrok EPTCz z 7 lipca 1989 r. w sprawie *Gaskin przeciwko Zjednoczonemu Królestwu*, skarga nr 10454/83, pkt 50–53.

³⁹¹ Wyrok ETPCz z 19 października 2005 r. w sprawie *Roche przeciwko Zjednoczonemu Królestwu*, skarga nr 32555/96, pkt 170–173.

m.in. braku informacji udostępnionych przez państwo, a dotyczących zagrożenia związanego z działalnością i wypadkami mającymi miejsce w fabryce chemikaliów³⁹². Wydawać by się mogło, że – w przeciwieństwie do spraw bez wątplenia dotyczących ściśle informacji na temat jednostki i tym samym związanych z art. 8 EKPCz chroniącym prywatność – w wypadku sprawy *Guerra i inni przeciwko Włochom* pojawił się element społecznej wagi informacji na temat zagrożeń związanych z działalnością fabryki. Ten element stanu faktycznego sprawy skłonił Europejską Komisję Praw Człowieka do uznania, że brak działań Włoch stanowił naruszenie prawa dostępu do informacji³⁹³. Sprawa została skierowana do ETPCz, który stwierdził, że również w tych okolicznościach art. 10 nie może być odczytywany jako źródło pozytywnych obowiązków państwa związanych z udostępnianiem danych informacji³⁹⁴. Decyzja taka może być odczytywana jako kontrowersyjna, zwłaszcza w świetle konkluzji ETPCz dotyczącej naruszenia art. 8 EKPCz w związku z nieprzekazaniem przez państwo mieszkańcom dotkniętej zanieczyszczeniami miejscowości informacji na temat ryzyka, które fabryka tworzyła dla ich rodzin i życia prywatnego, czyli *de facto* nieprzekazania im informacji³⁹⁵.

Zmiana stanowiska ETPCz nastąpiła w 2006 r. w przełomowym dla prawa dostępu do informacji wyroku w sprawie *Sdružení Jihočeské Matky przeciwko Republice Czeskiej*³⁹⁶. W tej sprawie organizacja pozarządowa zwróciła się do państwa o udostępnienie informacji technicznych odnoszących się do elektrowni atomowej w Czechach. Podjęcie takiej aktywności przez NGO zaowocowało stwierdzeniem ETPCz, że: „w tych warunkach

³⁹² Sprawa toczyła się na podstawie przepisów włoskich implementujących *dyrektywę Rady 82/501/EEC z 24 czerwca 1982 dotyczącą zagrożenia poważnymi awariami w odniesieniu do niektórych rodzajów działalności przemysłowej*, Dz.Urz. WE 1982 L 230, s. 1–18.

³⁹³ Wyrok ETPCz z 19 lutego 1998 r. w sprawie *Guerra i inni przeciwko Włochom*, skarga nr 14967/89, pkt 40.

³⁹⁴ „Że wolność nie może być skonstruowana jako wymuszająca na Państwie, w okolicznościach takich jak w tej sprawie, pozytywne zobowiązania do zbierania i rozprzestrzeniania informacji ze swojej własnej inicjatywy”. Wyrok ETPCz z 19 lutego 1998 r. w sprawie *Guerra i inni przeciwko Włochom*, skarga nr 14967/89, pkt 53.

³⁹⁵ Podobnie, zob. C. Hilson, *Risk and the European Convention on Human Rights: Towards a New Approach*, „Cambridge Yearbook of European Legal Studies” 2009, nr 11, s. 355–356.

³⁹⁶ Wyrok ETPCz z 10 lipca 2006 r. w sprawie *Sdružení Jihočeské Matky przeciwko Republice Czeskiej*, skarga nr 19101/03. Orzeczenie, co może być odczytywane jako symbolicznie znaczące, zostało wydane w tym samym roku, kiedy Międzyamerykański Trybunał Praw Człowieka wydał orzeczenie *Claude Reyes i inni przeciwko Chile*, afirmujące prawo dostępu do informacji jako samodzielne prawo człowieka. Jest to jednak uwaga dotycząca wymiaru symbolicznego rozpoznawania prawa dostępu do informacji, ponieważ wyrok ETPCz wydany został w lipcu, sprawa zaś *Claude Reyes i inni przeciwko Chile* została rozstrzygnięta we wrześniu.

trybunał uznaje, iż odrzucenie tej prośby stanowiło ingerencję w prawo do otrzymywania informacji wnioskującego [...]”³⁹⁷. ETPCz ostatecznie zdecydował, że techniczne informacje nie podlegały obowiązkowi udostępnienia ze strony państwa ze względu na ograniczenia dopuszczone w art. 10 ust. 2 EKPCz. Powołał się przy tym na konieczność zagwarantowania wysokiego poziomu bezpieczeństwa, co może stanowić argument za utrzymaniem tajności informacji technicznych dotyczących elektrowni. Jak odnotował ETPCz, art. 10 nie tworzy absolutnego prawa dostępu do wszystkich szczegółów technicznych. W przeciwieństwie do informacji dotyczących wpływu danej elektrowni na środowisko nie stanowią one kwestii objętej interesem publicznym³⁹⁸.

Mimo to orzeczenie zapoczątkowało możliwość ograniczonego interpretowania art. 10 EKPCz jako zawierającego – ograniczone przedstawionymi przez ETPCz warunkami – prawo do informacji, od którego wyjątki muszą zostać uzasadnione na podstawie art. 10 ust. 2³⁹⁹. Chociaż podtrzymywane jest przekonanie, że art. 10 stanowi głównie źródło negatywnych obowiązków ciążących na państwie (zakaz „ingerencji władz publicznych”), to ewolucja orzecznictwa pozwala stwierdzić, że pod określonymi warunkami może on stanowić również źródło pozytywnych obowiązków ciążących na państwie. Jak optymistycznie odnotowali w 2007 r. Wouter Hins i Dirk Voorhoof:

Przez wiele lat Europejski Trybunał Praw Człowieka miał opory przed takim stwierdzeniem. Jednakże można zauważyć wskazówki pozwalające stwierdzić,

³⁹⁷ *Dans ces conditions, le Tribunal estime que le rejet de cette demande constituait une ingérence dans le droit du requérant de recevoir des informations [...]*. Wyrok ETPCz z 10 lipca 2006 r. w sprawie *Sdružení Jihočeské Matky przeciwko Republice Czeskiej*, skarga nr 19101/03, pkt 1.1. To oraz kolejne tłumaczenia z francuskiego zawdzięczam Annie Blumsztajn, której dziękuję za pomoc.

³⁹⁸ „Sąd uznaje, że art. 10 Konwencji nie może być interpretowany jako gwarantujący absolutne prawo dostępu do wszystkich szczegółów dot. konstrukcji centrali, ponieważ, inaczej niż informacje na temat efektu informacji środowiskowych, te dane nie mogą być uznane za związane z interesem ogółu” (*La Cour estime que l'article 10 de la Convention ne peut être interprété comme garantissant le droit absolu d'accès à tous les détails techniques liés à la construction de la centrale, car, contrairement aux informations sur l'impact des informations environnementales, ces données ne peuvent être d'intérêt général*). Wyrok ETPCz z 10 lipca 2006 r. w sprawie *Sdružení Jihočeské Matky przeciwko Republice Czeskiej*, skarga nr 19101/03, pkt 1.1.

³⁹⁹ Podobnie, zob. „Chociaż ETPCz, w czasie przygotowywania tego tekstu, nie potwierdził istnienia ogólnego prawa dostępu do dokumentów urzędowych lub informacji opartego na art. 10 EKPCz, najnowsze orzecznictwo ETPCz sugeruje, że – w pewnych okolicznościach – art. 10 EKPCz może wspierać prawo dostępu do dokumentów dla tzw. *public watchdogs*”. D. Goldberg, *op. cit.*, s. 19.

że pozycja Trybunału się zmienia. Europejskie prawo dostępu do informacji, powiązane z artykułem 10 EKPCz, staje się rzeczywistością⁴⁰⁰.

Kolejne lata przyniosły kilka wyroków ETPCz, w których ta prognoza częściowo została potwierdzona.

Rozwój orzecznictwa ETPCz w odniesieniu do prawa dostępu do informacji można podzielić na dwie fazy⁴⁰¹. Pierwsza faza, zapoczątkowana wydaniem wyroku w sprawie *Sdružení Jihočeské Matky przeciwko Republice České* w 2006 i trwająca do 2015 r., charakteryzuje się niesystematycznym podejściem do zagadnienia. ETPCz w tym okresie podejmował dopiero próby wypracowania spójnego podejścia do prawa dostępu do informacji. Wydany w 2016 r. wyrok Wielkiej Izby w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom* zapoczątkował fazę, w której analiza zagadnienia prawa dostępu do informacji ma bardziej systematyczny charakter. Orzeczenie dostarczyło nie tylko rozbudowanej analizy przyczyn stojących za możliwością wykładni art. 10 EKPCz jako zawierającego w sobie prawo dostępu do informacji, lecz również było testem pozwalającym określić, czy w danej sprawie możliwe jest powołanie się na prawo dostępu do informacji, który opisuję w dalszej części rozdziału.

3.3.1. Wypracowywanie spójnego podejścia do prawa dostępu do informacji w orzecznictwie ETPCz

Wyroki wydane w latach 2006–2015, począwszy od omówionego wyżej *Sdružení Jihočeské Matky przeciwko Republice České*, wyraźnie ukazują problem z określeniem przez ETPCz, o czym właściwie można mówić na podstawie treści art. 10 EKPCz. Czy zawiera on jedynie wolność wyrazu? Czy powinien być wykładany jako uwzględniający prawo społeczeństwa do otrzymania informacji? Czy raczej prawo mediów, NGO-sów (szerzej: watchdogów⁴⁰²)

⁴⁰⁰ W. Hins, D. Voorhoof, *op. cit.*, s. 114. Warto odnotować, że kwestia dotycząca tego, które orzeczenie *de facto* stanowiło o zmianie w interpretacji prawa dostępu do informacji w ujęciu ETPCz, jest do pewnego stopnia sporna, np. Dariusz Adamski zwraca szczególną uwagę na rolę orzeczenia w sprawie *Társaság a Szabadságjogokért przeciwko Węgrom* jako znaku mającej miejsce zmiany stanowiska ETPCz: zob. D. Adamski, *Approximating a Workable Compromise on Access to Official Documents: the 2011 Developments in the European Courts*, „Common Market Law Review” 2012, nr 49, s. 547–550.

⁴⁰¹ Ewolucję orzecznictwa ETPCz przed wydaniem wyroku w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom* przeprowadził M. Balcerzak, *Rozdział III: Kategoria jawności i prawo do informacji z perspektywy orzecznictwa Europejskiego Trybunału Praw Człowieka*, [w:] *Standardy Europejskie (Jawność i jej ograniczenia, t. XI)*, red. C. Mik, C.H. Beck, Warszawa 2016.

⁴⁰² Zdecydowałam się posługiwać tym pojęciem z kilku powodów. Po pierwsze, jest ono używane w języku polskim. Po drugie, jego tłumaczenia w orzecznictwie ETPCz różnią się, np. w Wyroku ETPCz z 28 listopada 2013 r. w sprawie *Österreichische Vereinigung zur*

do otrzymania informacji w celu jej rozpowszechnienia? Czy może jednak jego treść powinna być odczytywana jako zawierająca samo prawo dostępu do informacji nieobjęte ograniczeniami wynikającymi z tego, kto poszukuje dostępu do danej treści? Analizowane poniżej wyroki dostarczają materiału ukazującego próbę wypracowania przez ETPCz odpowiedzi na te pytania.

W *Társaság a Szabadságjogokért przeciwko Węgrom*⁴⁰³ z 2009 r. ETPCz potwierdził istnienie ograniczonego prawa dostępu do informacji na podstawie art. 10 EKPCz. Sprawa dotyczyła wniosku o dostęp do informacji w postaci skargi do węgierskiego Trybunału Konstytucyjnego złożonego przez NGO. Dostępu do skargi, którą do Trybunału Konstytucyjnego złożył parlamentarzysta, odmówiono ze względu na zawarte w niej dane osobowe. ETPCz odwołał się w wyroku do szczególnej roli pełnionej nie tylko przez prasę, lecz także przez NGO-sy, w zakresie uczestniczenia w debacie publicznej. Przez ograniczenie dostępu do skargi Węgry skorzystały z monopolu informacyjnego, który przyniósł skutek w postaci rzeczywistej cenzury. Uniemożliwiły więc NGO wykonywanie jej funkcji i rozpowszechnianie informacji istotnej dla interesu publicznego. Ograniczenie, na które powołał się węgierski sąd, było co prawda przewidziane w prawie i przywołane w odniesieniu do ochrony jednego z interesów wymienionych w EKPCz, nie było jednak niezbędne w demokratycznym społeczeństwie. Niejako na marginesie ETPCz odnotował – powołując się na *Sdružení Jihočeské Matky przeciwko Republice Czeskiej* – że wykładnia prawa otrzymywania informacji zawartego w art. 10 podlega rozszerzeniu w kierunku uwzględniania również prawa dostępu do informacji⁴⁰⁴.

Z kolei w sprawie *Kenedi przeciwko Węgrom*, również z 2009 r., ETPCz ograniczył się do stwierdzenia, że uniemożliwienie dostępu do oryginalnych dokumentów i źródeł w celu przeprowadzenia badań historycznych stanowiło naruszenie wolności wyrazu i w związku z tym było naruszeniem art. 10 EKPCz⁴⁰⁵, po czym przystąpił do analizowania, czy naruszenie to mogłoby być usprawiedliwione. W związku z tym, że informacje nie zostały udostępnione mimo wyroku węgierskiego sądu nakazującego ich wydanie,

Erhaltung, Stärkung und Schaffung Eines Wirtschaftlich Gesunden Land- und Forst-Wirtschaftlichen Grundbesitzes (ÖVG) przeciwko Austrii, skarga nr 39534/07, pkt 41 pojawia się sformułowanie „organ nadzoru działający w interesie społecznym”, natomiast w Wyroku ETPCz z 8 listopada 2016 r. w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, skarga nr 18030/11, pkt 164: „strażnik interesu publicznego”. Stąd też w celu ujednoczenia nomenklatury postanowiłam pozostać przy terminie „watchdog”.

⁴⁰³ Wyrok ETPCz z 14 kwietnia 2009 r. w sprawie *Társaság a Szabadságjogokért przeciwko Węgrom*, skarga nr 37374/05.

⁴⁰⁴ *Ibidem*, pkt 35.

⁴⁰⁵ Zob. Wyrok ETPCz z 26 maja 2009 r. w sprawie *Kenedi przeciwko Węgrom*, skarga nr 31475/05, pkt 43.

ograniczenie zostało uznane za nieusprawiedliwione. Należy podkreślić, że mimo odwołania się przez ETPCz do wyroku w sprawie *Társaság a Szabadságjogokért przeciwko Węgrom*, w orzeczeniu *Kenedi przeciwko Węgrom* brak bezpośredniego stwierdzenia, że sprawa dotyczy prawa otrzymania informacji lub dostępu do niej.

Następną sprawą, która dotyczyła tego problemu, było *Youth Initiative for Human Rights przeciwko Serbii*⁴⁰⁶ z 2013 r. Orzeczenie dotyczyło złożenia przez serbską organizację pozarządową wniosku o dostęp do informacji dotyczącej tego, ile osób było poddawanych elektronicznemu nadzorowi przez serbskie służby specjalne. Agencja w pierw odmówiła dostępu do informacji, natomiast po decyzji odpowiedniego organu nakazującej jej udostępnienie stwierdziła, że nie jest w posiadaniu takich danych. Jednym z zarzutów podniesionych przez Serbię przed ETPCz był fakt, że art. 10 nie gwarantuje ogólnego prawa dostępu do informacji⁴⁰⁷. W odpowiedzi ETPCz powołał się na *Társaság a Szabadságjogokért przeciwko Węgrom* i stwierdził, że prawo otrzymywania informacji zawiera prawo dostępu do niej. W sprawie *Youth Initiative for Human Rights przeciwko Serbii* organizacja pełniąca funkcje watchdoga i zaangażowana w sprawy związane z interesem publicznym poszukiwała dostępu do informacji w celu jej rozpowszechnienia, w związku z czym art. 10 miał zastosowanie, działanie zaś wbrew decyzji organu krajowego nie mogło stanowić przesłanki pozwalającej uznać ograniczenie dostępu do informacji za zgodne z art. 10 ust. 2 EKPCz.

Podobnie została oceniona przez ETPCz sytuacja w *Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung Eines Wirtschaftlich Gesunden Land- und Forst-Wirtschaftlichen Grundbesitzes (ÖVG) przeciwko Austrii*⁴⁰⁸ również w 2013 r. Sprawa dotyczyła dostępu do decyzji wydawanych przez Regionalną Komisję ds. Obrotu Ziemią w Tyrolu, o dostęp do których wnioskowała organizacja pozarządowa. Komisja odmówiła dostępu do decyzji, powołując się na brak czasu oraz dostępnego personelu, jej decyzję zaś potwierdził wyrok austriackiego Trybunału Konstytucyjnego. W swej analizie ETPCz ponownie odwołał się do szczególnej roli odgrywanej m.in. przez NGO-sy w zakresie uczestnictwa w debacie publicznej oraz przypomniał, że „konsekwentnie uznawał, że opinia publiczna ma prawo dostępu do informacji dotyczących interesu publicznego”⁴⁰⁹. Uznał tym samym, że w analizowanej sprawie doszło do ingerencji w przysługujące skarżącemu prawo do otrzymywania i przekazywania informacji. Opierając się na przesłankach

⁴⁰⁶ Wyrok ETPCz z 25 czerwca 2013 r. w sprawie *Youth Initiative for Human Rights przeciwko Serbii*, skarga nr 48135/06.

⁴⁰⁷ *Ibidem*, pkt 17.

⁴⁰⁸ Wyrok ETPCz z 28 listopada 2013 r. w sprawie *ÖVG przeciwko Austrii*, skarga nr 39534/07, pkt 44.

⁴⁰⁹ *Ibidem*, pkt 33.

umożliwiających państwu powołanie się na ograniczenia praw z art. 10 EKPCz, stwierdził on natomiast, że odmowa nie była niezbędna w demokratycznym społeczeństwie.

W sprawach *Roșiianu przeciwko Rumunii*⁴¹⁰ z 2014 r. oraz *Guseva przeciwko Bułgarii*⁴¹¹ z 2015 r. wnioskodawcy, podobnie jak w wypadku *Kenedi przeciwko Węgrom*, dysponowali z kolei wyrokami sądów krajowych nakazujących udostępnienie im informacji, o które wnioskowali. W sprawie *Roșiianu przeciwko Rumunii* wnioskodawca, z zawodu dziennikarz, powinien otrzymać dostęp do wnioskowanych informacji zgodnie z wyrokami rumuńskiego sądu. Jednocześnie jednak mer, który miał udzielić informacji, unikał wykonania wyroków. ETPCz odnotował, że „zaproszenia do odebrania kserokopii kilku całkowicie różnych dokumentów zawierających informacje mogące podlegać różnym interpretacjom [...] nie mogą w żadnym przypadku zostać uznane za wykonanie wyroku sądu nakazującego udzielenie informacji o charakterze publicznym”⁴¹². Wyrok pośrednio sugeruje, że celowe sabotowanie wyroku sądu przez dostarczanie wyrywkowych i mogących wprowadzać w błąd informacji nie może być uznane za wykonanie wyroku sądu krajowego, który nakazał udostępnienie danych informacji. W związku z brakiem argumentów Rumunii, które przemawiałyby za możliwością powołania się na ograniczenia przewidziane w art. 10 ust. 2 EKPCz, postępowanie mera zostało uznane za naruszenie art. 10.

W sprawie *Guseva przeciwko Bułgarii* wnioskująca o dostęp do informacji była członkinią i reprezentantką stowarzyszenia walczącego o prawa zwierząt. Sam fakt jej działania na rzecz organizacji został uznany za wystarczający, aby stwierdzić, że działała ona jako watchdog, chociaż wniosek o dostęp do informacji złożyła jako osoba fizyczna⁴¹³. Ukazuje to funkcjonalne podejście ETPCz do określania, jakie podmioty powinny być uznawane za szczególnie uprzywilejowane w zakresie żądania dostępu do informacji. Kluczowym kryterium oceny, czy dana osoba lub organizacja powinna być uznana za watchdoga, jest charakter jej działalności, nie zaś formalna nazwa czy forma prawna organizacji. Również w tym wypadku ograniczenie nie zostało uznane za przewidziane w prawie, ze względu na wyroki przemawiające na korzyść wnioskującej oraz na fakt, że bułgarskie prawo nie przewidywało horyzontu czasowego, w jakim informacje powinny zostać udzielone.

⁴¹⁰ Wyrok ETPCz z 24 czerwca 2014 r. w sprawie *Roșiianu przeciwko Rumunii*, skarga nr 27329/06.

⁴¹¹ Wyrok ETPCz z 17 lutego 2015 r. w sprawie *Guseva przeciwko Bułgarii*, skarga nr 6987/07.

⁴¹² Wyrok ETPCz z 24 czerwca 2014 r. w sprawie *Roșiianu przeciwko Rumunii*, skarga nr 27329/06, pkt 66.

⁴¹³ Zob. Wyrok ETPCz z 17 lutego 2015 r. w sprawie *Guseva przeciwko Bułgarii*, skarga nr 6987/07, pkt 55.

Początki orzecznictwa ETPCz uwzględniającego możliwość powoływania się na prawo dostępu do informacji na podstawie art. 10 EKPCz pozwalają zaobserwować powolne tworzenie katalogu kryteriów, które muszą być spełnione w danej sytuacji, aby podlegała ona prawu dostępu do informacji. Charakterystyczny jest przede wszystkim szczególny charakter podmiotów wnioskujących o dostęp do informacji: dziennikarzy, organizacji pozarządowych czy naukowców – czyli, w nomenklaturze ETPCz, watchdogów. ETPCz podkreśla ich rolę w tworzeniu debaty publicznej, która powinna podlegać ochronie w ramach gwarantowania wolności wyrazu. Dlatego też celem wnioskowania o dostęp do informacji, jak podkreśla ETPCz, powinno być jej rozpowszechnianie. Tym samym prawo dostępu do informacji jest traktowane jako logiczna konsekwencja uwzględnienia w treści art. 10 EKPCz prawa do otrzymywania informacji. Z jednej strony prawo do otrzymywania informacji ma społeczeństwo, z drugiej zaś – właśnie jako prawo dostępu do informacji – mają je watchdogi, czyli np. organizacje pozarządowe czy media współtworzące debatę publiczną.

Definicja watchdogów, w świetle orzecznictwa ETPCz, jest szeroka i obejmuje zarówno formalne organizacje, jak i osoby działające na rzecz rozpowszechniania danych informacji. Dlatego też można uznać np. blogerów czy naukowców za jednostki, które pełnią funkcję watchdogów, czyli dążą do dostarczenia informacji istotnych z punktu widzenia debaty publicznej. Podejście takie można skrytykować jako tworzenie „uprzywilejowanego kręgu «publicznych watchdogów»”⁴¹⁴. Jednak funkcjonalne podejście do definiowania watchdogów, pozwalające na uwzględnienie wśród nich nawet jednostek podejmujących działania na rzecz prowadzenia dobrze poinformowanej debaty publicznej, stanowi rodzaj odpowiedzi na ten problem. ETPCz, próbując pogodzić wykładnię art. 10 uwzględniającą obecność w nim prawa dostępu do informacji z orzecznictwem dotyczącym informacji na temat jednostki, podkreśla rolę społecznego znaczenia informacji podlegających pod treść art. 10. Odwoływanie się do funkcji pełnionej przez watchdogi jest elementem tej strategii, różnicującej dostęp do informacji na temat życia jednostki od informacji istotnych z punktu widzenia całego społeczeństwa.

Dokonany przegląd orzecznictwa z lat 2006–2015 ukazuje jednak niejednolite podejście do analizy spraw przez ETPCz. Stałym elementem pozostaje kolejność, w której najpierw stwierdza on, czy dana sytuacja w ogóle mieści się w zakresie zastosowania art. 10, następnie zaś – czy państwo w prawidłowy sposób powołało się na możliwości ograniczania praw z art. 10, czyli czy ograniczenie wynikało z prawa, dotyczyło jednego z interesów chronionych na podstawie art. 10 ust. 2 i czy było niezbędne w demokratycznym

⁴¹⁴ F. Leghe, P. Weismann, *The European Court of Human Rights and Access to Information*, „International Human Rights Law Review” 2014, t. 3, nr 2, s. 313.

społeczeństwie. Niespełnienie choć jednej z tych przesłanek, czyli np. nieproporcjonalność odmowy niespełniająca wymogu niezbędności w demokratycznym społeczeństwie, stanowi wystarczający powód do uznania ingerencji państwa za nieusprawiedliwioną.

Przeanalizowane powyżej wyroki nie doprowadziły do precyzyjnego sformułowania kryteriów, jakie należy uwzględnić w ramach poszczególnych etapów analizy prowadzącej do uznania, czy w danej sytuacji doszło do naruszenia art. 10 EKPCz. Brakowało w nich również jednoznacznego uznania, że treść art. 10 zawiera w sobie prawo dostępu do informacji. ETPCz powoływał się na różne elementy stanów faktycznych danych spraw, np. fakt, że o informacje wnioskuje NGO, badacz lub dziennikarz pełniący funkcję watchdoga czy fakt, że informacje były gotowe i dostępne. Nie utworzył jednak jasnego testu pozwalającego oceniać dane sytuacje. Większą jasność w odniesieniu do tych zagadnień przyniósł wyrok w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, który Marek Antoni Nowicki określa jako „podsumowanie i uporządkowanie tego procesu interpretacyjnego” w odniesieniu do „prawa do wolności otrzymywania informacji”⁴¹⁵. Orzeczenie to można postrzegać jako początek nowego etapu w wykładni ETPCz dotyczącej art. 10 EKPCz, który charakteryzuje możliwość stosowania dwustopniowego testu dotyczącego stwierdzenia, czy w danym wypadku jest uzasadnione powołanie się na prawo dostępu do informacji.

3.3.2. Systematyzacja podejścia do prawa dostępu do informacji w orzecznictwie ETPCz

Wyrok *Magyar Helsinki Bizottság przeciwko Węgrom* z 2016 r. został wydany przez Wielką Izbę ETPCz na kanwie sprawy dotyczącej wniosków o dostęp do informacji, które sformułowała organizacja pozarządowa. Informacje obejmowały dostęp do list obrońców publicznych w poszczególnych jednostkach policji w Węgrzech. Część z jednostek przekazała NGO żądane informacje, dwie odmówiły jednak udostępnienia wykazów. Wyrok sądu pierwszej instancji nakazywał policji udostępnienie żądanych informacji, został jednak zmieniony przez sąd drugiej instancji, a następnie podtrzymany przez węgierski Sąd Najwyższy. Głównym problemem analizowanym w ramach prawa krajowego wydawało się ocenienie, na ile dane osobowe obrońców publicznych mogą być traktowane jako informacje dotyczące urzędników publicznych i, w związku z tym, czy mogą być udostępnione organizacji pozarządowej. Ze strony NGO motywacją do poszukiwania dostępu do informacji były podejrzenia co do zasad przydzielania obrońców publicznych jako potencjalnie

⁴¹⁵ M.A. Nowicki, *Komentarz do Konwencji o ochronie praw człowieka i podstawowych wolności*, [w:] *Wokół Konwencji Europejskiej. Komentarz do Europejskiej Konwencji Praw Człowieka*, op. cit. (do art. 10).

wpływających na ich niezależność. Sprawa stała się pretekstem do kompleksowego uporządkowania linii orzeczniczej ETPCz w odniesieniu do prawa otrzymywania – i z związku z tym dostępu do – informacji.

ETPCz, w świetle braku sformułowania „poszukiwanie” w treści art. 10 EKPCz, uznał za konieczne podanie bardziej rozbudowanego uzasadnienia dotyczącego podstaw, na których opiera się jego wykładnia EKPCz. Wśród kluczowych dla niej zasad ETPCz wskazał konieczność uwzględniania reguł interpretacji przewidzianych w *Konwencji wiedeńskiej o prawie traktatów*⁴¹⁶, czyli „nadanie wyrazom zwykłego znaczenia w ich kontekście i w świetle przedmiotu i celu postanowienia, w którym zostały użyte”⁴¹⁷. Jednocześnie ETPCz zauważył, że wykładnia powinna być oparta na traktowaniu EKPCz jako całości i na konieczności zagwarantowania praktycznej i skutecznej ochrony zagwarantowanych w niej praw⁴¹⁸. Ponadto zdaniem ETPCz konieczne jest osadzenie wykładni EKPCz w ramach szerzej postrzeganej wykładni prawa międzynarodowego, którego jest ona częścią. Dlatego też rozwój konsensusu dotyczącego danych praw w ramach instrumentów międzynarodowych oraz działań państw stron EKPCz powinien być postrzegany jako źródło inspiracji dla ETPCz⁴¹⁹. Natomiast jako jedynie pomocnicze źródło wykładni w tym wypadku ETPCz wskazał prace przygotowawcze nad EKPCz.

Na tle tych uwag dotyczących źródeł, na których powinna się opierać wykładnia EKPCz, została przeprowadzona analiza pytania: „czy i w jakim zakresie można uznać, że prawo dostępu do informacji będących w posiadaniu państwa jako takie wchodzi w zakres «wolności wyrażania opinii» zagwarantowanej na mocy art. 10 Konwencji, niezależnie od faktu, że prawo to nie wynika bezpośrednio z brzmienia tego postanowienia”⁴²⁰. Na uwagę zasługuje posłużenie się przez ETPCz sformułowaniem „prawo dostępu do informacji”. Chociaż jest ono przedstawione jako element wolności wyrażania opinii, zostało bezpośrednio nazwane „dostępem”, nie zaś np. „otrzymaniem”. Tym samym ETPCz przyznał, że wykładnia wymaga wyjścia poza ramy literalnego odczytywania treści art. 10.

Pierwszym krokiem, wykonanym przez ETPCz w celu odpowiedzi na tak sformułowane kluczowe pytanie, jest próba uporządkowania

⁴¹⁶ *Konwencja Wiedeńska o Prawie Traktatów sporządzona w Wiedniu dnia 23 maja 1969 r.*, Dz.U. 1990 nr 74 poz. 439.

⁴¹⁷ Wyrok ETPCz z 8 listopada 2016 r. w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, skarga nr 18030/11, pkt 119.

⁴¹⁸ Czyli wykładnia, która „zapewni traktatowi efektywność”, zob. komentarz na temat reguł interpretacji umów międzynarodowych w W. Czapliński, A. Wyrozumska, *op. cit.*, s. 624.

⁴¹⁹ Zob. Wyrok ETPCz z 8 listopada 2016 r. w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, skarga nr 18030/11, pkt 124.

⁴²⁰ *Ibidem*, pkt 126.

dotychczasowego orzecznictwa. ETPCz stwierdził, że można je podzielić na dwie grupy. W sprawach takich jak *Kenedi przeciwko Węgrom*, *Youth Initiative for Human Rights przeciwko Serbii*, *Roşianu przeciwko Rumunii* oraz *Guseva przeciwko Bułgarii* wyroki były skoncentrowane głównie wokół „rozważań dotyczących prawa krajowego”⁴²¹, a dokładniej – niestosowania się danych instytucji krajowych do wyroków sądów lub organów państw-stron konwencji nakazujących udzielenie dostępu do danych informacji. Z kolei w sprawach *Társaság a Szabadságjogokért przeciwko Węgrom* oraz *ÖVG przeciwko Austrii* ETPCz rozpoznał ograniczone prawo dostępu do informacji jako części wolności wyrażonych w art. 10 EKPCz. O ile w odniesieniu do pierwszej kategorii spraw są one raczej świadectwem podkreślania przez ETPCz konieczności szanowania przez państwa orzeczeń ich własnych sądów, o tyle druga kategoria spraw prowadzi do zmiany we wcześniejszym podejściu ETPCz do prawa dostępu do informacji na podstawie art. 10 EKPCz. Dlatego też wykładnia dokonana w przypadku tych spraw wymaga zdaniem ETPCz wyjaśnienia. Może ona rodzić wątpliwości co do zgodności ze wcześniejszymi twierdzeniami ETPCz przedstawianymi w sprawach takich jak *Leander przeciwko Szwecji* czy *Guerra i inni przeciwko Włochom*.

Dlatego drugim krokiem w analizie ETPCz jest sprecyzowanie argumentów przemawiających za uznaniem ograniczonego prawa dostępu do informacji jako jednego z elementów wolności wyrażania opinii. Po pierwsze, ETPCz umniejszył rolę, jaką w tym wypadku powinno odgrywać powoływanie się na prace przygotowawcze. Nie została przez ETPCz uznana argumentacja wywodząca brak prawa dostępu do informacji z celowego ominięcia słowa „poszukiwania” w treści art. 10, m.in. ze względu na „brak [...] zapisu jakichkolwiek dyskusji związanych z tą zmianą bądź w ogóle jakiejkolwiek debaty na temat poszczególnych elementów składających się na wolność wyrażania opinii”⁴²². ETPCz odwołał się natomiast w tym aspekcie do prac nad projektem Protokołu 6, w czasie których przejawiała się wspólna wola państw-stron EKPCz do uwzględnienia „poszukiwania” jako elementu art. 10. Po drugie, ETPCz powołał się na rozwój prawa państw-stron konwencji oraz prawa międzynarodowego. Wykonawszy analizę porównawczą, uwzględniającą zarówno orzecznictwo innych organów sądowniczych, jak i prawo krajowe państw-stron, ETPCz doszedł do konkluzji, że można mówić o powszechności aktów prawnych regulujących dostęp do informacji i oficjalnych dokumentów⁴²³.

⁴²¹ *Ibidem*, pkt 132.

⁴²² Wyrok ETPCz z 8 listopada 2016 r. w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, skarga nr 18030/11, pkt 135.

⁴²³ „Jak wynika z materiałów dostępnych Trybunałowi dotyczących ustawodawstwa państw członkowskich Rady Europy, że z wszystkich trzydziestu jeden państw członkowskich, w których przeprowadzono ankietę, z wyjątkiem Luksemburga, rozpoznawane jest prawo dostępu do informacji i/lub oficjalnych dokumentów będących w posiadaniu or-

Szeroko zakrojony konsensus w zakresie prawa dostępu do informacji może stanowić argument przemawiający za koniecznością dynamicznej interpretacji EKPCz⁴²⁴. Zważywszy na to, że większość państw europejskich przyjęła ustawodawstwo dotyczące dostępu do informacji publicznej czy oficjalnych dokumentów, można przyjąć, że ETPCz uwzględni prawo dostępu do informacji jako część dorobku w zakresie rozwoju ochrony praw człowieka. Jest to przejaw traktowania EKPCz jako „żyjącego instrumentu”, którego interpretacja powinna być oparta na zbliżaniu treści zawartych w nim artykułów do współczesnych uwarunkowań⁴²⁵.

Na tle tak przedstawionych podstaw wykładni art. 10 EKPCz ETPCz stwierdził, że: „Trybunał nie uważa, by nie było możliwe interpretowanie art. 10 ust. 1 Konwencji jako przepisu obejmującego prawo dostępu do informacji”⁴²⁶. Składnia tego zdania jest świadectwem ostrożnego podejścia ETPCz do rozszerzania wykładni treści EKPCz. ETPCz traktuje przedstawione przez siebie warunki umożliwiające powoływanie się na prawo dostępu do informacji jako kolejny etap rozwoju linii orzeczniczej zapoczątkowanej w sprawie *Leander przeciwko Szwecji*. Dąży on do sprecyzowania konkretnych okoliczności, które mogą umożliwiać powoływanie się na prawo dostępu do informacji, w przeciwieństwie do tych sytuacji, które określał jako uniemożliwiające „w tych okolicznościach” szeroką wykładnię art. 10.

gonów publicznych. Okazuje się również, że w większości państw członkowskich prawo dostępu do informacji i/lub dokumentów jest nie tylko ograniczone do egzekutywy, ale rozszerza się na informacje i/lub dokumenty będące w posiadaniu legislatywy i władzy sądowniczej a nawet posiadanych przez państwa przedsiębiorstw i ciał prywatnych, które wykonują funkcje publiczne i otrzymują znaczne publiczne finansowanie. Wszystkie prawa dotyczące dostępu do informacji wymieniają kategorie informacji, które nie mogą być poddane ograniczeniom w zakresie udostępnienia. Niektóre państwa stosują test interesu publicznego, który wymaga od władz publicznych i ciał nadzorczych uwzględniania bilansowania interesów w zakresie powstrzymywania dostępu do informacji i interesu publicznego stojącego po stronie ich ujawnienia”. Wyrok ETPCz z 8 listopada 2016 r. w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, skarga nr 18030/11, pkt 64.

⁴²⁴ „[...] istnieje szeroko zakrojony konsensus co do potrzeby uznania prawa jednostki do dostępu do informacji będących w posiadaniu państwa z myślą o wsparciu społeczeństwa w formułowaniu poglądów w kwestiach leżących w interesie ogółu”. Wyrok ETPCz z 8 listopada 2016 r. w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, skarga nr 18030/11, pkt 148.

⁴²⁵ „ETPCz wyklada Konwencję w sposób dynamiczny i zorientowany na cel. Trybunał podkreślał, że gwarantowanie praw wymienionych w EKPCz zakłada, że Konwencja jest żywym instrumentem, który jest interpretowany w świetle wymogów współczesnych uwarunkowań”. P. Tiilikka, *Access to Information as a Human Right in the Case Law of the European Court of Human Rights*, „Journal of Media Law” 2013, t. 5, nr 1, s. 85.

⁴²⁶ Wyrok ETPCz z 8 listopada 2016 r. w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, skarga nr 18030/11, pkt 149.

Dlatego też przede wszystkim stara się on kreować podejście, w którym prawo dostępu do informacji jest niezbędne do realizacji przez watchdogi ich prawa do rozpowszechniania informacji oraz prawa społeczeństwa do otrzymywania informacji⁴²⁷.

Artykuł 10 EKPCz nie jest, zdaniem ETPCz, źródłem ogólnego uprawnienia dla jednostki do żądania dostępu do informacji ani źródłem obowiązku rządu do przekazywania informacji⁴²⁸. Prawo to – a w wypadku państwa obowiązek – aktualizuje się w dwóch wypadkach. Po pierwsze, jeśli ujawnienie informacji zostało nakazane prawomocnym wyrokiem sądu krajowego (jak to nastąpiło np. w *Kenedi przeciwko Węgrom*, *Roșianu przeciwko Rumunii* czy *Guseva przeciwko Bułgarii*). Spór nie dotyczy wówczas samego udzielenia dostępu do informacji, ale raczej działań instytucji państwowych, które mimo odpowiedniego wyroku sądu krajowego nie wykonują swojego obowiązku. Ponadto w sprawach takich – w razie poddania ich analizie z perspektywy kryteriów sformułowanych przez ETPCz – państwa nie są w stanie wykazać, że brak udostępnienia danej informacji jest przewidziany w ustawie. Skoro wyrok sądu krajowego nakazuje udostępnienie informacji, trudno twierdzić, że przywoływany przez państwo wyjątek jest uzasadniony. Po drugie, gdy dostęp do informacji ma kluczowe znaczenie dla wykonania przez jednostkę jej prawa do wolności wyrażania opinii, odmowa udzielenia takiego dostępu stanowi ingerencję w to prawo (jak w wypadku *Társaság a Szabadságjogokért przeciwko Węgrom* oraz *ÖVG przeciwko Austrii*). Przedstawione niżej kryteria, które należy uwzględnić w ramach analizy przeprowadzanej w drugim z typów wymienionych sytuacji, pozwalają stwierdzić, czy – mimo braku wyroku sądu krajowego nakazującego udostępnienie informacji – powinna ona zostać udostępniona.

3.4. Warunki powoływania się na prawo dostępu do informacji

Aby sprecyzować, kiedy sytuacja podlega drugiej z wymienionych przez ETPCz kategorii, Trybunał przedstawił kryteria progowe prawa dostępu do

⁴²⁷ *Ibidem*, pkt 152.

⁴²⁸ „Trybunał uważa ponadto, że art. 10 nie przyznaje jednostce prawa dostępu do informacji będących w posiadaniu władzy publicznej ani nie zobowiązuje rządu do przekazania jej takich informacji. Niemniej jednak, jak wynika z powyższej analizy, takie prawo bądź taki obowiązek mogą powstać, po pierwsze, gdy ujawnienie informacji zostało nakazane w drodze prawomocnego orzeczenia sądowego (co nie miało miejsca w przedmiotowej sprawie) oraz po drugie, w okolicznościach, gdy dostęp do informacji ma kluczowe znaczenie dla wykonania przez jednostkę jej prawa do wolności wyrażania opinii, zwłaszcza «wolności otrzymywania i przekazywania informacji» oraz gdy odmowa udzielenia takiego dostępu stanowi ingerencję w to prawo”. Wyrok ETPCz z 8 listopada 2016 r. w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, skarga nr 18030/11, pkt 156.

informacji będących w posiadaniu państwa. Chociaż ETPCz podkreślił konieczność indywidualnej analizy każdej sytuacji oraz określił kryteria pojawiające się w dotychczasowym jego orzecznictwie jako „przykłady kryteriów, jakie należałoby uwzględnić”⁴²⁹, to wymieniony przez niego katalog może być traktowany jako istotny punkt wyjścia do analizy poszczególnych przypadków. W wyroku w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom* kolejno są charakteryzowane: cel występowania o dostęp do informacji, charakter żądanej informacji, funkcja pełniona przez poszukujących informacji oraz wymóg, aby informacja była gotowa i dostępna.

ETPCz, jako pierwszy warunek konieczny do zaistnienia sytuacji, w której możliwe jest powołanie się na prawo dostępu do informacji, podaje konieczność zdefiniowania celu żądania owego dostępu⁴³⁰. ETPCz prezentuje perspektywę, w której to od celu wnioskowania o dostęp zależy, czy dostęp do informacji stanowi warunek niezbędny do korzystania z prawa do otrzymania i rozpowszechniania informacji. Jeśli celem pozyskania informacji jest dalsza aktywność dziennikarska lub inna (w domyśle aktywistyczna lub naukowa) służąca tworzeniu debaty publicznej, dostęp do informacji może zostać uznany za warunek niezbędny do jej dalszego rozpowszechniania – z perspektywy mediów lub NGO-sów oraz otrzymania informacji – z perspektywy społeczeństwa. Kryterium to pozwala odnotować szczególną pozycję organizacji pozarządowych, mediów oraz prasy w odniesieniu do pozyskiwania dostępu do informacji. Zarówno sprawa *Társaság a Szabadságjogokért przeciwko Węgrom*, jak i *ÖVG przeciwko Austrii*, które ETPCz przywołuje jako elementy konstruowania linii orzeczniczej na temat prawa dostępu do informacji, dotyczyły organizacji pozarządowych. NGO-sy formułowały wnioski o dostęp do informacji w celu dalszego ich rozpowszechniania, uniemożliwianie zaś im dostępu do informacji stanowiło przykład korzystania przez państwo z „monopolu informacyjnego”.

Sformułowanie „monopol informacyjny” jest przywoływane przez ETPCz w odniesieniu do dostępu do informacji niezbędnych w celu uczestniczenia w debacie publicznej. Prowadzi on w rzeczywistości do cenzury: „monopol informacyjny w związku z tym staje się rodzajem cenzury”⁴³¹. Ze względu na odmawianie organizacjom pozarządowym czy mediom dostępu do informacji państwo uniemożliwia im pełnienie ich funkcji⁴³². Dlatego też jeśli celem

⁴²⁹ Wyrok ETPCz z 8 listopada 2016 r. w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, skarga nr 18030/11, pkt 157.

⁴³⁰ *Ibidem*, pkt 158–159.

⁴³¹ Wyrok ETPCz z 14 kwietnia 2009 r. w sprawie *Társaság a Szabadságjogokért przeciwko Węgrom*, skarga nr 37374/05, pkt 28.

⁴³² „Trybunał odnalazł w tym zakresie analogie ze swym orzecznictwem dotyczącym wolności prasy, wskazując, że zobowiązany jest on z najwyższą starannością badać każdy przypadek, w którym władze państwowe, posiadając monopol w dziedzinie informacji,

pozyskania danej informacji jest uczestnictwo w debacie publicznej, może ona stanowić przedmiot prawa dostępu do informacji rozumianego zgodnie z art. 10 EKPCz. W wypadku innej wykładni państwa mogłyby bezkarnie ingerować w prawo do rozpowszechniania informacji.

Drugim warunkiem koniecznym do spełnienia w celu powołania się na dostęp do informacji na podstawie art. 10 EKPCz jest kwestia charakteru poszukiwanej informacji⁴³³. Musi ona spełniać warunki sformułowane w teście interesu publicznego. ETPCz podaje przykłady informacji uznanych za spełniające warunki testu w jego dotychczasowym orzecznictwie, opisywanych wyżej w rozdziale, np. skargi złożonej do Trybunału Konstytucyjnego dotyczącej projektu aktu ustawodawczego o istotnym znaczeniu dla ogółu⁴³⁴, danych dotyczących decyzji na temat przeznaczenia ziemi w ramach obrotu nieruchomości⁴³⁵, informacji na temat użycia środków nadzoru elektronicznego⁴³⁶ czy oryginalnych źródeł dokumentowych do prowadzenia badań historycznych⁴³⁷. ETPCz nie podaje ogólnych warunków testu publicznego interesu, formułując jedynie bardziej abstrakcyjny przykład przyczyn możliwych do podania dla uzasadnienia istnienia interesu publicznego:

Taka potrzeba może istnieć na przykład wówczas, gdy ujawnienie zapewni przejrzystość w kwestii prowadzenia spraw publicznych i spraw leżących w interesie społeczeństwa w ujęciu ogólnym i tym samym umożliwi ogółowi społeczeństwa uczestniczenie w zarządzaniu publicznym⁴³⁸.

Jednocześnie ETPCz podkreśla, że spełnienie tego kryterium jest ściśle związane z okolicznościami danej sprawy⁴³⁹.

Trzecim kryterium jest funkcja, jaką pełni jednostka żądająca dostępu do informacji. Podkreślona została już rola mediów i organizacji pozarządowych, jako podmiotów, których działania w zakresie dostępu do informacji mogą

utrudniają danej osobie bądź podmiotowi wykonywanie funkcji organu nadzoru działającego w interesie społecznym”. Wyrok ETPCz z 28 listopada 2013 r. w sprawie *ÖVG przeciwko Austrii*, skarga nr 39534/07, pkt 41.

⁴³³ Zob. Wyrok ETPCz z 8 listopada 2016 r. w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, skarga nr 18030/11, pkt 160–163.

⁴³⁴ Wyrok ETPCz z 14 kwietnia 2009 r. w sprawie *Társaság a Szabadságjogokért przeciwko Węgrom*, skarga nr 37374/05.

⁴³⁵ Wyrok ETPCz z 28 listopada 2013 r. w sprawie *ÖVG przeciwko Austrii*, skarga nr 39534/07.

⁴³⁶ Wyrok ETPCz z 25 czerwca 2013 r. w sprawie *Youth Initiative for Human Rights przeciwko Serbii*, skarga nr 48135/06.

⁴³⁷ Wyrok ETPCz z 26 maja 2009 r. w sprawie *Kenedi przeciwko Węgrom*, skarga nr 31475/05.

⁴³⁸ Wyrok ETPCz z 8 listopada 2016 r. w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, skarga nr 18030/11, pkt 161.

⁴³⁹ *Ibidem*, pkt 162.

stanowiąc emblematiczne przykłady spełniania kryterium roli pełnionej przez jednostkę żądającą dostępu do informacji. Jednocześnie jednak Trybunał podkreśla, że w katalogu osób, które powinny być objęte wysokim poziomem ochrony w odniesieniu do poszukiwania informacji, są badacze akademicki⁴⁴⁰ oraz autorzy publikacji dotyczących kwestii wrażliwych społecznie. Ponadto powinna się ona odnosić również do blogerów i popularnych użytkowników mediów społecznościowych⁴⁴¹. W tym miejscu warto odnotować, że podejście ETPCz oparte nie na ocenie np. formy prawnej danej organizacji, lecz na funkcji, jaką pełni ona lub jednostka w ramach prowadzonej działalności, ma szczególne znaczenie w odniesieniu do głównego przedmiotu zainteresowania analizy. Prawdopodobnie w rzeczywistości to aktywiści internetowi czy *hacktywiści* mogliby w najbardziej skuteczny sposób stanowić narzędzie społecznej kontroli w zakresie systemów wykorzystujących zautomatyzowane podejmowanie decyzji.

Ostatnim podawanym przez ETPCz kryterium jest to, czy informacja jest gotowa i dostępna do udostępnienia⁴⁴². Zgodnie z utrwalonym już orzecznictwem ETPCz państwo nie ma obowiązku aktywnego tworzenia i udostępniania informacji. Kryterium gotowości i dostępności informacji stanowi przedłużenie tego podejścia: państwo nie może zostać zobowiązane do aktywnego przygotowywania informacji, o których udostępnienie zwraca się dany podmiot. Należy podkreślić, że w razie nieposiadania przez daną instytucję żądanych informacji lub niewykonania przez podmiot o nie wnioskujący wysiłku w celu posłużenia się dostępnymi źródłami informacji ETPCz uzna, że kryterium to nie zostało spełnione⁴⁴³. Jednocześnie jednak, jak pokazuje wyrok w sprawie *ÖVG przeciwko Austrii*, kryterium to nie może być przez państwo nadużywane w celu unikania udostępniania informacji. W przypadku powoływania się przez władze krajowe na trudności związane z przekazaniem informacji będące wynikiem praktyki samych władz i decyzji ETPCz odmówił uznania tej okoliczności jako umożliwiającej usprawiedliwienie nieudzielenia informacji.

⁴⁴⁰ Jak np. w orzeczeniu: Wyrok ETPCz z 26 maja 2009 r. w sprawie *Kenedi przeciwko Węgrom*, skarga nr 31475/05.

⁴⁴¹ „Trybunał przypomina, że wysoki poziom ochrony obejmuje również badaczy akademickich [...] i autorów literatury poświęconej sprawom leżącym w interesie publicznym [...]. Trybunał pragnie również zauważyć, że z uwagi na istotną rolę internetu w zwiększaniu dostępu ogółu społeczeństwa do aktualności oraz ułatwianiu rozpowszechniania informacji [...] funkcja blogerów i popularnych użytkowników mediów społecznościowych również może być podobna do roli «strażników interesu publicznego» pod względem ochrony zagwarantowanej na mocy art. 10”. Wyrok ETPCz z 8 listopada 2016 r. w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, skarga nr 18030/11, pkt 168.

⁴⁴² *Ibidem*, pkt 169–170.

⁴⁴³ Zob. Wyrok ETPCz z 7 lutego 2017 r. w sprawie *Bubon przeciwko Rosji*, skarga nr 63898/09.

Jest to szczególnie istotne, zważywszy na rosnący poziom cyfryzacji działalności władz publicznych i administracji publicznej. Można sformułować hipotezę, że z czasem warunek, aby informacja była gotowa i dostępna, będzie odgrywał coraz mniejsze znaczenie w odniesieniu do dostępu do informacji. Podobnie w odniesieniu do zautomatyzowanego podejmowania decyzji. Jedną z przyczyn stawiania głównej hipotezy tej książki jest próba docieczenia, czy istnieje możliwość pozyskania informacji na temat samej struktury systemu służącego do zautomatyzowanego podejmowania decyzji. Dlatego też wymóg ten stanowi w rzeczywistości argument przemawiający za możliwością pozytywnej weryfikacji głównej hipotezy: prawo dostępu do informacji może obejmować jedynie informacje gotowe, taką zaś jest kod komputerowy używany w ramach zautomatyzowanego podejmowania decyzji.

3.5. Warunki powoływania się przez państwa na ograniczenia prawa dostępu do informacji

W odniesieniu do sprawy *Magyar Helsinki Bizottság przeciwko Węgrom* ETPCz uznał, że sformułowane i omówione powyżej warunki umożliwiające powołanie się na prawo dostępu do informacji zostały spełnione. Spełnienie kumulatywne warunków opisanych powyżej nie sprawia jednak, że dana informacja musi podlegać udostępnieniu. Konieczne jest ponadto każdorazowe sprawdzenie, czy państwo nie miało możliwości odmówienia udostępnienia informacji na podstawie art. 10 ust. 2. Zgodnie z treścią artykułu i relevantnym orzecznictwem ETPCz wprowadzenie ograniczeń w odniesieniu do prawa dostępu do informacji wymaga kumulatywnego spełnienia trzech warunków: możliwość ograniczenia musi być zapisana w ustawie, jej celem musi być realizacja jednego z celów wymienionych w katalogu zawartym w art. 10 ust. 2 oraz musi być niezbędna w demokratycznym społeczeństwie. Warunki te są obowiązujące w odniesieniu do wszelkich praw i wolności gwarantowanych w art. 10 EKPCz i w związku z tym stanowiły przedmiot wykładni ETPCz w sprawach dotyczących szeroko postrzeganej wolności wyrazu. Dlatego też w wyroku *Magyar Helsinki Bizottság przeciwko Węgrom* brak ich pogłębionej i abstrakcyjnej analizy. W poniższym opisie posługuję się z związku z tym głównie przykładami z omówionego powyżej orzecznictwa dotyczącego dostępu do informacji, aby jak najdokładniej przedstawić to zagadnienie.

Odnosnie do wymogu, zgodnie z którym ograniczenia muszą być przewidziane w ustawie, ETPCz odwołuje się do ugruntowanych ustaleń w tej kwestii dokonanych w orzecznictwie. W orzeczeniu w sprawie *Kenedi przeciwko Węgrom* wyrażenie to odczytywane jest w świetle refleksji wokół konceptu legalności (*lawfulness*) w EKPCz. Przez pojęcie to należy rozumieć nie tylko umieszczenie możliwych wyjątków w ustawie, lecz również takie jakościowe cechy prawa krajowego jak jego przewidywalność czy ogólne wykluczenie

arbitralności⁴⁴⁴. Przykładem niezgodności z tym wymogiem jest brak warunków dotyczących terminów dostarczenia danej informacji przewidzianych w prawie⁴⁴⁵. Ponadto należy odnotować, że ETPCz podkreśla kompetencje sądów krajowych do wykładni i stosowania prawa krajowego oraz to, że nie jest on właściwym organem do oceny, czy metody stosowane przez państwo są odpowiednie do regulacji danej dziedziny: jego rolą jest jedynie sprawdzenie, czy użyte środki i ich efekty są zgodne z EKPCz⁴⁴⁶. Dlatego też została wyodrębniona przez ETPCz kategoria spraw, w których dostęp do informacji został przyznany przez instytucje krajowe. Jak zaznaczałam powyżej, mogą być one odczytywane jako niespełniające wymogu, aby ograniczenia dostępu do informacji były przewidziane przez prawo. Skoro sądy krajowe przyznały dostęp, zgodnie z prawem krajowym, to powinien on zostać udzielony. Unikanie udostępnienia informacji w takim scenariuszu stanowi zachowanie arbitralne i nie może być uznane za przewidziane ustawą.

Warunek drugi odnosi się do przyczyn, z jakich odmówiono dostępu. Jak już wspomniałam, katalog sformułowany w art. 10 ust. 2 obejmuje: interes 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 ujawnieniu informacji poufnych lub na zagwarantowanie powagi i bezstronności władzy sądowniczej. Przykładem skutecznej próby uzasadnienia ze strony państwa ograniczenia w zakresie dostępu do informacji jest opisywane powyżej orzeczenie *Sdružení Jihočeské Matky przeciwko Republice České*:

Nie można też odrzucić argumentu władz wynikającego z konieczności chronienia zobowiązań kontraktowych i tajemnicy gospodarczej (wymienionych przez konstruktora centrali) oraz z konieczności zagwarantowania bezpieczeństwa instalacji tak by uniknąć ataku z zewnątrz. I tak, kiedy stosowanie prawa do otrzymania informacji może naruszyć prawo innych, naruszyć bezpieczeństwo albo zdrowie publiczne, zakres prawa dostępu do tychże informacji ograniczany jest przez treść ustępu 2 artykułu 10 Konwencji⁴⁴⁷.

Wyjątki wprowadzane w zakresie dostępu do informacji, co stanowi zasadę interpretacyjną, powinny być rozważane w kategoriach propor-

⁴⁴⁴ Wyrok ETPCz z 26 maja 2009 r. w sprawie *Kenedi przeciwko Węgrom*, skarga nr 31475/05, pkt 44.

⁴⁴⁵ Zob. Wyrok ETPCz z 17 lutego 2015 r. w sprawie *Guseva przeciwko Bułgarii*, skarga nr 6987/07, pkt 59.

⁴⁴⁶ Wyrok ETPCz z 8 listopada 2016 r. w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, skarga nr 18030/11, pkt 184.

⁴⁴⁷ *On ne saurait non plus écarter l'argument des autorités tiré de la nécessité de protéger les obligations contractuelles et le secret économique, invoqués par le constructeur de*

cjonalności odnośnie do tego, jakim celom służą⁴⁴⁸. Uszczegółowieniem tego wymogu jest warunek trzeci, czyli niezbędność w demokratycznym społeczeństwie.

Warunek niezbędności w demokratycznym społeczeństwie stanowił przedmiot szczegółowej wykładni ETPCz w opisywanym powyżej orzeczeniu *ÖVG przeciwko Austrii*. Choć wprowadzone ograniczenia były przewidziane przez ustawę oraz uzasadnione jednym z celów przedstawionych w art. 10 ust. 2 (ochroną dobrego imienia i praw innych osób oraz ze względu na zapobieżenie ujawnieniu informacji poufnych), to ETPCz doszedł do wniosku, że nie spełniają one wymogu bycia niezbędnymi w demokratycznym społeczeństwie. Ze względu na wagę argumentacji ETPCz w tej kwestii należy przytoczyć dłuższy fragment orzeczenia:

Podsumowując, Trybunał uznaje, że argumenty przytaczane przez władze krajowe celem uzasadnienia odmowy uznania wniosku skarżącego stowarzyszenia w przedmiocie uzyskania dostępu do decyzji Komisji należy uznać za «istotne», ale nie za «wystarczające». Mimo, iż nie jest zadaniem Trybunału ustalenie, w jaki sposób Komisja mogła i powinna była umożliwić skarżącemu uzyskanie dostępu do podjętych przez siebie decyzji, uznaje on, że całkowita odmowa udzielenia dostępu do jakichkolwiek decyzji *nie spełniała wymogu proporcjonalności* [wyróżnienie – J.M.]. Komisja, która z własnego wyboru sprawowała *monopol informacyjny* [wyróżnienie – J.M.] w odniesieniu do podejmowanych przez siebie decyzji, w omawiany sposób *uniemożliwiła skarżącemu prowadzenie badań* [wyróżnienie – J.M.] w odniesieniu do jednego z dziewięciu austriackich Landów, tzn. Tyrolu, oraz uczestniczenie w znaczącym zakresie w procesie legislacyjnym dotyczącym wprowadzania zmian w treści tyrolskiego prawa obrotu nieruchomościami. Trybunał stwierdza zatem, że ingerencja w przysługujące skarżącemu prawo do wolności wyrażania

la centrale, et de garantir la sécurité de l'installation afin d'éviter une attaque extérieure. En effet, lorsque l'exercice du droit à recevoir des informations peut porter atteinte aux droits d'autrui, à la sûreté publique ou à la santé, l'étendue du droit d'accès aux informations en cause est limitée par le libellé du paragraphe 2 de l'article 10 de la Convention. Wyrok ETPCz z 10 lipca 2006 r. w sprawie *Sdružení Jihočeské Matky przeciwko Republice Czeskiej*, skarga nr 19101/03, pkt 1.1.

⁴⁴⁸ Właśnie pojęcie proporcjonalności pojawia się w wyroku w sprawie *Sdružení Jihočeské Matky przeciwko Republice Czeskiej*: „W takich jak wyżej opisane warunkach i biorąc pod uwagę margines uznania pozostawiony Państwu, nie można stwierdzić, że ingerencja w wolność otrzymywania informacji wnioskującej była nadmierna w stosunku do zamierzonych celów” (*Dans les circonstances de l'espèce et compte tenu de la marge d'appréciation laissée aux Etats, l'on ne saurait donc affirmer que l'ingérence dans la liberté de la requérante de recevoir des informations était disproportionnée par rapport aux buts poursuivis*). Wyrok ETPCz z 10 lipca 2006 r. w sprawie *Sdružení Jihočeské Matky przeciwko Republice Czeskiej*, skarga nr 19101/03, pkt 1.1.

opinii *nie może zostać uznana za niezbędną w społeczeństwie demokratycznym* [wyróżnienie – J.M.]⁴⁴⁹.

Cytat ten obrazuje przykładowe kryteria, jakie mogą zostać użyte w celu oceny, czy dane ograniczenie może zostać uzasadnione jako niezbędne w demokratycznym społeczeństwie. Jego proporcjonalność może być rozważana w świetle kryteriów przedstawionych powyżej w rozdziale: jeśli jego wprowadzenie *de facto* uniemożliwia organizacji pełnienie jej funkcji jako watchdoga i prowadzi do monopolu informacyjnego państwa, może ono zostać uznane za niezgodne z art. 10 ust. 2 EKPCz.

Podobną analizę ETPCz przeprowadził w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*. Choć ograniczenie zostało uznane za przewidziane w prawie i służące ochronie interesów wymienionych w art. 10 ust. 2 EKPCz, nie zostało ono uznane za niezbędne w demokratycznym społeczeństwie. Informacje, o które wnioskował NGO, obejmowały nazwiska obrońców publicznych – uznane przez Węgry za dane osobowe – oraz liczbę przypadków, w których wyznaczono ich na obrońców w określonych jurysdykcjach. Celem miało być sprawdzenie efektywności systemu przydzielania obrońców publicznych. Brak udostępnienia informacji uniemożliwiało organizacji pozarządowej spełnienie jej funkcji i poinformowanie społeczeństwa na temat istotny dla debaty publicznej. Stąd też całkowita odmowa przyznania wnioskowanych informacji, które były jedynie w posiadaniu instytucji publicznych, stanowiła – zdaniem ETPCz – ograniczenie nieproporcjonalne.

Przedstawione powyżej kryteria pozwalają stwierdzić, że w wybranych sytuacjach prawo dostępu do informacji może być postrzegane jako uprawnienie będące częścią treści kryjącej się pod ogólnym sformułowaniem „swoboda wyrazu”, której poświęcony jest art. 10 EKPCz. Do pewnego stopnia można by jednocześnie stwierdzić, że w związku z rozwojem zarówno prawa międzynarodowego w tym aspekcie, jak i przyjmowanych w porządkach krajowych państw stron EKPCz aktów prawnych dotyczących dostępu do informacji, staje się ono samodzielnym prawem. Sformułowanie:

[...] w określonych rodzajach sytuacji i z zastrzeżeniem konkretnych warunków mogą istnieć przekonujące argumenty przemawiające na korzyść interpretacji, zgodnie z którą postanowienie to obejmuje prawo dostępu jednostki do

⁴⁴⁹ Wyrok ETPCz z 28 listopada 2013 r. w sprawie *ÖVG przeciwko Austrii*, skarga nr 39534/07, pkt 47.

informacji będących w posiadaniu państwa i nakłada na państwo obowiązek udzielenia takich informacji⁴⁵⁰

mogłoby świadczyć zarówno o postrzeganiu prawa dostępu do informacji jako części swobody wyrazu, którego podrzędność podkreślona jest przez kryterium pierwsze testu zaproponowanego przez ETPCz, jak i o uznaniu go w ograniczonym stopniu za samodzielne prawo.

Kryteria umożliwiające korzystanie z tego ograniczonego prawa dostępu do informacji wypracowane przez ETPCz tworzą zatem dwustopniowy test. Na pierwszym etapie badane jest spełnienie warunków umożliwiających powołanie się na prawo dostępu do informacji: (1) cel żądania dostępu do informacji; (2) charakter informacji świadczącej o jej wadze dla interesu publicznego; (3) funkcja pełniona przez podmiot żądający dostępu do informacji; oraz (4) sama informacja, która musi być gotowa i dostępna. Drugi etap obejmuje z kolei warunki, pod którymi państwo ma możliwość powołania się na ograniczenia dla prawa dostępu do informacji (art. 10 ust. 2). Takie ograniczenie musi: (1) być przewidziane w prawie⁴⁵¹; (2) służyć ochronie jednego z celów przewidzianych w art. 10 ust. 2; oraz (3) być niezbędne w demokratycznym społeczeństwie. Należy podkreślić, że na każdym etapie kryteria sformułowane w klarowny sposób w orzecznictwie powinny być spełnione kumulatywnie.

Warto zauważyć, że od czasu wydania w 2016 r. wyroku w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom* został on przez ETPCz zastosowany w innych sprawach dotyczących dostępu do informacji, np. w sprawie *Cangi przeciwko Turcji*⁴⁵² z 2019 r. oraz *Studio Monitori i inni przeciwko Gruzji*⁴⁵³ z 2020 r. Jest to potwierdzenie rozpoczęcia nowej fazy w orzecznictwie ETPCz, w której elementy testu wypracowane w ramach *Magyar Helsinki Bizottság przeciwko Węgrom* pozwalają bardziej precyzyjnie oceniać, czy możliwe jest powołanie się na ograniczone prawo dostępu do informacji wynikające z art. 10 EKPCz.

⁴⁵⁰ Wyrok ETPCz z 8 listopada 2016 r. w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, skarga nr 18030/11, pkt 137.

⁴⁵¹ Jak wspomniałam powyżej: ten warunek prowadzi do stwierdzenia, że w sprawach, w których sąd krajowy przyznał dostęp do danych informacji, brak działań zgodnych z takim wyrokiem stanowi naruszenie prawa dostępu do informacji.

⁴⁵² Wyrok ETPCz z 29 stycznia 2019 r. w sprawie *Cangi przeciwko Turcji*, skarga nr 24973/15.

⁴⁵³ Wyrok ETPCz z 30 stycznia 2020 r. w sprawie *Studio Monitori i inni przeciwko Gruzji*, skarga nr 44920/09 i 8942/10.

3.6. Możliwość stosowania prawa dostępu do informacji w stosunku do systemów zautomatyzowanego podejmowania decyzji

Widoczna w orzecznictwie ETPCz trudność pogodzenia z jednej strony niechęci do narzucania państwu w związku z art. 10 jakichkolwiek obowiązków pozytywnych, z drugiej zaś ewidentnie rozszerzana wykładnia w zakresie prawa dostępu do informacji skłaniają do ostrożnego analizowania możliwości stosowania prawa dostępu do informacji do systemów zautomatyzowanego podejmowania decyzji. Dlatego też, nie wykluczając możliwości ewolucji orzecznictwa w kierunku bardziej liberalnego, nastawionego na uznanie prawa dostępu do informacji z mniej dotkliwymi niż opisane powyżej kryteria obstrzeceniami, chciałabym pozostać przy wąskiej, opartej ściśle na przeanalizowanym orzecznictwie interpretacji. Jest ona i tak wystarczająca, aby uzasadnić wagę jaką – nawet tak ograniczone – prawo dostępu do informacji może odegrać jako odmienny od opartego na ochronie danych osobowych sposób uzyskania wyższego stopnia przejrzystości decyzji opartych na zautomatyzowanym przetwarzaniu danych.

Należy podkreślić, że rozważania te odnoszą się jedynie do sytuacji, w której dany system zautomatyzowanego podejmowania decyzji byłby używany w ramach działalności władzy publicznej czy administracji. Jednostka musi mieć możliwość wnioskowania o dostęp do informacji o nim na podstawie przepisów dotyczących dostępu do informacji publicznej. Stanowi to poważne ograniczenie w porównaniu z podejściem prezentowanym w rozdziałach poświęconych perspektywie opartej na ochronie danych osobowych. Jednocześnie jednak propozycja wykorzystania dostępu do informacji, jako alternatywy dla prawa do wyjaśnienia opartego na RODO, może stanowić odpowiedź na wyzwania związane z zautomatyzowanym podejmowaniem decyzji w najbardziej wrażliwych aspektach życia jednostek. Należy zauważyć, że zgodnie z orzecznictwem ETPCz możliwe jest stwierdzenie naruszenia EKPCz przez państwo w związku z czynami popełnionymi przez przedsiębiorstwo prywatne, o ile czyn ten wynika z działania lub zaniechania państwa⁴⁵⁴. Dlatego też w sytuacji, w której np. obsługa danego systemu zautomatyzowanego podejmowania decyzji spoczywałaby na prywatnym przedsiębiorstwie, lecz jednocześnie służyłaby ona realizacji usług publicznych lub czynności związanych z wykonywaniem władzy publicznej, mogłaby ona podlegać

⁴⁵⁴ „Jedynym sposobem na podniesienie naruszenia praw gwarantowanych przez Konwencję (ale nie Konwencji samej w sobie) popełnionego przez prywatne przedsiębiorstwo jest w związku z tym połączenie tego działania z działaniem lub zaniechaniem Państwa, i w związku z tym stwierdzenie, że Państwo jest za nie odpowiedzialne”. M. Florczak-Wątor, *The Role of the European Court of Human Rights in Promoting Horizontal Positive Obligations of the State*, „International and Comparative Law Review” 2017, t. 17, nr 2, s. 43–44.

analizie z punktu widzenia naruszenia EKPCz. Dzięki takiemu ciągłowi argumentacyjnemu byłaby ograniczona możliwość powoływania się państwa na wykonywanie zautomatyzowanego podejmowania decyzji przez podmioty prywatne i, w związku z tym, niemożności udzielenia informacji na ich temat.

W świetle przeanalizowanego orzecznictwa ETPCz dotyczącego dostępu do informacji domaganie się dostępu do algorytmu jako informacji mogłoby opierać się na dwóch sposobach argumentacji. Po pierwsze, powołanie się na art. 10 i argumentowanie zgodnie z wymogami wypracowanymi w orzecznictwie ETPCz co do możliwości powołania się na prawo do informacji. Drugim scenariuszem jest odwołanie do danego prawa gwarantowanego przez EKPCz. Poniżej analizuję obie możliwości. Ponadto przedstawiam analizę dotyczącą relacji między prawem dostępu do algorytmów na podstawie prawa dostępu do informacji a zakazem dyskryminacji w prawie Rady Europy.

3.6.1. Artykuł 10 jako podstawa żądania dostępu do algorytmów służących do zautomatyzowanego podejmowania decyzji

Aby uzasadnić konieczność otrzymania dostępu do algorytmów używanych w ramach zautomatyzowanego podejmowania decyzji na podstawie prawa dostępu do informacji konieczne byłoby wykazanie, że w danej sytuacji spełnione są warunki testu sformułowanego w *Magyar Helsinki Bizottság przeciwko Węgrom*. W zakresie kryterium pierwszego to od okoliczności sprawy zależałoby, czy żądanie danej informacji ma prowadzić do celu poinformowania opinii publicznej i społeczeństwa o sprawie, o której informacja leżałaby w interesie publicznym. Spełnienie tego kryterium w niektórych przypadkach nie nastroczałoby jednak trudności. Zastosowanie zautomatyzowanych systemów podejmowania decyzji miałyby skutki dla całych grup społecznych, więc powinno być możliwe wystąpienie z wnioskiem o uzyskanie informacji ich dotyczących w celu przekazania poczynionych na ich podstawie ustaleń członkom danej społeczności czy społeczeństwu. Jednocześnie cel ten nie mógłby zostać spełniony bez pozyskania dostępu, co może być postrzegane jako nadużywanie przez państwo monopolu informacyjnego.

W zakresie kryterium drugiego nie powinno stanowić problemu udowodnienie, że charakter informacji o zautomatyzowanym podejmowaniu decyzji leży w zakresie sytuacji, w których możliwe byłoby stosowanie art. 10. Wdrażanie zautomatyzowanych rozwiązań w sferach tak istotnych dla życia publicznego jak sądownictwo, opieka zdrowotna czy pomoc społeczna pozwala zakładać, że wiedza o tym, jak działają algorytmy warunkujące dostęp do tych usług, powinna leżeć w interesie publicznym. Wynika to np. z założenia przyświecającego całej analizie, tj. że zautomatyzowane podejmowanie decyzji może prowadzić do niezgodności działania państw z zakazem dyskryminacji. W takim ujęciu informacja o sposobie działania

danego systemu stanowiłaby element konieczny do poinformowania o tym społeczeństwa. Jednocześnie istniałaby możliwość wykazania, że systemy takie naruszałyby inne prawa jednostek, np. w związku ze sposobem przetwarzania w nich danych czy prawem do sprawiedliwego sądu. Taki scenariusz przewidywałby, że prawo dostępu do informacji mogłoby stanowić narzędzie weryfikacji potencjalnych naruszeń innych praw w stosunku do całych grup społecznych, a nawet całej społeczności – a tym samym byłoby w interesie publicznym ujawnienie rządzących nim mechanizmów.

W zakresie kryterium trzeciego, podobnie jak pierwszego, spełnienie go zależałoby od okoliczności sprawy. Jednocześnie szeroki katalog aktorów wymienianych w orzecznictwie ETPCz, który uwzględni NGO, media, prasę, naukowców, blogerów, a nawet osoby istotne z punktu widzenia działalności w ramach mediów społecznościowych, mógłby prowadzić do stosunkowo łatwego wpisywania się podmiotów w ramy dotyczące tego kryterium. Dotychczasowe doświadczenia, chociażby odnośnie do opisanego powyżej śledztwa ProPubliki na temat programu COMPAS czy działań Fundacji e-Państwo oraz Sieci Obywatelskiej Watchdog Polska w zakresie próby otrzymania algorytmu, na którym bazuje SLPS⁴⁵⁵, jak również działania Panoptykonu prowadzone w celu otrzymania dostępu do informacji na temat sposobu determinowania rodzaju pomocy udzielanej bezrobotnym⁴⁵⁶, pokazują aktywność organizacji pozarządowych w tym obszarze. Organizacje i jednostki zajmujące się prawami człowieka w sferze cyfrowej byłyby w stanie wykazać, że pełnią one funkcję istotną z punktu widzenia informowania społeczeństwa o zagadnieniach związanych z zautomatyzowanym podejmowaniem decyzji. Co więcej, zważywszy na możliwą niewielką aktywność innych podmiotów zajmujących się tematyką praw cyfrowych – np. wyspecjalizowanych agencji czy instytucji państwowych – to watchdogi mogłyby być postrzegane jako podmiot najbardziej aktywny na polu informowania o zagrożeniach związanych z dyskryminacyjnym stosowaniem nowych technologii.

⁴⁵⁵ Zob. S. Gregorczyk-Abram, M. Wawrykiewicz, A. Owczarska, *Entliczek, pentliczek...? Czyli System Losowego Przydziału Spraw w sądach powszechnych*, „Oko.press”, 15 stycznia 2018 r. <https://oko.press/entliczek-pentliczek-system-losowego-przydzialu-spraw-sadach-powszechnych/>, dostęp: 1.04.2021.

⁴⁵⁶ Panoptykon uzyskał dostęp do *Kwestionariusza do profilowania pomocy dla osób bezrobotnych* oraz zasad jego oceniania: <https://panoptykon.org/wiadomosc/jakie-pytania-zawiera-kwestionariusz-profilowania-bezrobotnych>, dostęp: 1.04.2021, oraz artykuł J. Niklas, *Co zawiera algorytm służący do profilowania w urzędach pracy?*, 20 września 2018 r. oraz towarzyszące mu dokumenty: <https://panoptykon.org/wiadomosc/co-zawiera-algorytm-sluzacy-do-profilowania-w-urzedach-pracy>, dostęp: 1.04.2021. WSA przychylił się do interpretacji Fundacji, zgodnie z którą kwestionariusz i zasady oceniania go stanowią informację publiczną, zob. Wyrok WSA w Warszawie, II SAB/Wa 1012/15, 5 kwietnia 2016 r.

W celu zweryfikowania kryterium czwartego, czyli gotowości i dostępności informacji, pytaniem, jakie należałoby postawić, jest: czy system zautomatyzowanego podejmowania decyzji może być uznany za informację? Zgodnie z definicją podaną w pierwszym rozdziale z technicznego punktu widzenia jest on algorytmem lub algorytmami. Algorytm z kolei, zgodnie ze swym oryginalnym znaczeniem, to łańcuch poleceń, który jest „skończoną, abstrakcyjną, efektywną i złożoną strukturą kontroli”⁴⁵⁷, która powinna prowadzić do „osiągnięcia danego celu pod danymi warunkami”⁴⁵⁸. Dlatego też uzasadnione jest rozważanie systemów zautomatyzowanego podejmowania decyzji jako informacji. Są one przede wszystkim tekstem. Kolejne pytanie brzmi czy algorytmy te są gotowe i dostępne dla władz publicznych do udostępnienia? Odwoływanie się do prawa dostępu do samego kodu komputerowego pozwala stwierdzić, że nie byłoby potrzebne generowanie nowej informacji. Nawet jeśli kod ten jest przygotowywany i rozwijany przez zewnętrznego dostawcę, sam fakt, że pełni on zadania należące do sfery obowiązków władz publicznych, powinien być uznany jako argument za traktowaniem go jako informacji publicznej. Niezależnie od tego, który z podmiotów zaangażowanych we wdrażanie zautomatyzowanego podejmowania decyzji w rzeczywistości jest w posiadaniu nośnika, na którym ten kod jest utrwalony, jak długo używany jest on do wykonywania zadań ciążących na władzach publicznych, powinien mieścić się on w ramach informacji podlegających pod treść art. 10 EKPCz.

Możliwość wglądu w sam algorytm – właśnie w takiej postaci, w jakiej jest używany w systemach zautomatyzowanego podejmowania decyzji – jest przyczyną uzasadniającą stwierdzenie, że prawo dostępu do informacji mogłoby stanowić tzw. wyjaśnienie stawiające w centrum model w opozycji do oferowanego przez RODO wyjaśnienia stawiającego w centrum jednostkę. Przykładami ilustrującymi tę zasadniczą różnicę w efektach zastosowania prawa dostępu do informacji w przeciwieństwie do regulacji z zakresu ochrony danych osobowych mogą służyć opisywane już powyżej systemy zautomatyzowanego podejmowania decyzji. Tabela ukazuje przykładowe scenariusze, w których wnioskowanie o dostęp do informacji mogłoby spełniać warunki testu sformułowanego przez ETPCz. W odróżnieniu od podejścia opartego na przepisach RODO, zagwarantowanie dostępu do informacji o samym systemie zautomatyzowanego podejmowania decyzji mogłoby ułatwić systemową ocenę wiarygodności algorytmów jako, rzekomo, bezstronnych narzędzi. Rozważana byłaby nie indywidualna sytuacja jednostki, lecz systemowe działanie danego programu zautomatyzowanego podejmowania decyzji.

⁴⁵⁷ R.K. Hill, *op. cit.*, s. 44.

⁴⁵⁸ *Ibidem*, s. 47.

Tabela: Analiza spełniania kryteriów testu sformułowanego przez ETPCz w potencjalnym przypadku wnioskowania o dostęp do informacji na temat systemu zautomatyzowanego podejmowania decyzji używanego do oceny możliwości ponownego popełnienia przestępstwa przez daną jednostkę (przykład 1) oraz wnioskowania o dostęp do informacji na temat systemu zautomatyzowanego podejmowania decyzji używanego do przydzielania spraw sędziom (przykład 2)

Kryterium	Przykład 1: System zautomatyzowanego podejmowania decyzji używany do oceny możliwości ponownego popełnienia przestępstwa przez daną jednostkę	Przykład 2: System losowego przydziału spraw
1. Cel żądania dostępu do informacji	Udostępnienie opinii publicznej informacji dotyczących systemu zautomatyzowanego podejmowania decyzji, któremu poddawane są liczne jednostki (ocena całokształtu funkcjonującego systemu)	Udostępnienie opinii publicznej informacji dotyczących systemu zautomatyzowanego podejmowania decyzji (ocena całokształtu funkcjonującego systemu), możliwość weryfikacji niezależności sędziów przez wgląd w zasady przydziału spraw
2. Charakter informacji (interes publiczny)	Informacje na temat potencjalnie dyskryminacyjnego charakteru zautomatyzowanego podejmowania decyzji (informacje niezbędne dla debaty publicznej i udostępniane w interesie publicznym), mającego wpływ na sytuację wielu osób	Informacje na temat np. odstępowania od decyzji wydanych przez system zautomatyzowanego podejmowania decyzji, manipulacji wynikami losowań (informacje niezbędne dla debaty publicznej i udostępniane w interesie publicznym)
3. Funkcja pełniona przez żądających informacji	Organizacja działająca w zakresie pomocy więźniom	Organizacja działająca w zakresie obrony niezależności sędziowskiej lub prodemokratycznych aktywistów
4. Gotowa i dostępna informacja	Algorytm służący do zautomatyzowanego podejmowania decyzji (kod komputerowy)	Algorytm służący do zautomatyzowanego podejmowania decyzji (kod komputerowy)

Sytuacje te wydają się w pewnym stopniu prawdopodobne, z punktu widzenia uwzględniającego jedynie pierwszy etap testu. Pojawia się pytanie, na ile ETPCz byłby skłonny uznać ograniczenia dla swobody dostępu do informacji, które zostałyby odnośnie do tych rozwiązań wprowadzone w ustawie i których użycie byłoby uzasadnione jednym z celów podanych w art. 10 ust. 2 EKPCz. Najważniejszym elementem związanym ze spełnieniem przez państwa warunków stawianych przez ETPCz byłaby ocena, czy dane ograniczenie było niezbędne w demokratycznym społeczeństwie. Rozważając przykład SLPS, gdyby niemożność otrzymania informacji na temat jego algorytmów była określona prawem, można by się zastanawiać,

czy jego działanie służy realizacji bezstronności władzy sądowej czy wręcz odwrotnie, szkodzi jej. W kolejnym kroku można by postawić pytanie, czy ograniczenie dostępu do informacji na temat jego działania jest konieczne w demokratycznym społeczeństwie, czy wręcz przeciwnie: informacje o nim są niezbędne do funkcjonowania demokratycznego społeczeństwa.

Na wyraźne podkreślenie zasługuje różnica jakościowa, którą jest podejście do zautomatyzowanego podejmowania decyzji jako przedmiotu mogącego podlegać prawu dostępu do informacji na podstawie art. 10 EKPCz w zestawieniu z możliwościami traktowania dostępu do informacji, w tym np. systemów zautomatyzowanego podejmowania decyzji, jako instrumentu korzystania z innych praw przez jednostki. W pierwszym wypadku kluczowym celem jest zdobycie przez organizację lub jednostkę działającą dla dobra danej grupy informacji na temat sposobu traktowania tej grupy. Kolektywny charakter potencjalnej dyskryminacji przez zautomatyzowane sposoby podejmowania decyzji lepiej koresponduje z tym podejściem niż ze ściśle indywidualistyczną perspektywą prezentowaną w prawie ochrony danych osobowych. Jest ono holistyczną odpowiedzią skoncentrowaną na samym modelu wdrożonego rozwiązania, nie na danej, jednostkowej decyzji. Tym samym może stanowić bardziej adekwatną odpowiedź na wyzwania tworzone przez nowe technologie. Ponadto wprowadzenie swoistego reprezentanta danej grupy mogłoby prowadzić do przewyciężenia przeszkód wynikających np. z niskiego poziomu kompetencji cyfrowych jednostek. Wspecjalizowane w danej działalności organizacje pozarządowe czy aktywiści mogliby stanowić rodzaj tłumacza wdrażanych technologii⁴⁵⁹.

Istotnym czynnikiem wpływającym na możliwość traktowania algorytmów jako informacji podlegającej prawu dostępu do informacji jest to, czy przestrzeń cyfrowa postrzegana jest jako osobna rzeczywistość, czy jako jeden z elementów kształtujących fizyczny świat. Aby umożliwić weryfikowanie ich działania, konieczne jest zrozumienie, że w niektórych przypadkach mają one wpływ na życie jednostek równorzędny z wpływem aktów prawnych. Jak opisane zostało w rozdziale pierwszym: kod staje się prawem. Prawo zaś powinno być dostępne dla jednostek, które są poddane jego działaniu. Tym samym konieczne jest przyjęcie perspektywy, w której – w odniesieniu przynajmniej do części algorytmów wdrażanych w miejsce przepisów – standardem stałoby się ich publikowanie. Takie sytuacje mogłyby się jednak odnosić jedynie do części stosowanych zautomatyzowanych rozwiązań.

⁴⁵⁹ Co do pewnego stopnia przypomina analizowane w rozdziale poświęconym ochronie danych osobowych w Unii Europejskiej rozwiązanie zawarte w art. 80 RODO, które umożliwia reprezentację jednostki organizacjom aktywnym w polu ochrony danych osobowych i wolności związanych z ochroną danych osobowych.

Ponadto zrozumienie algorytmów wymaga kompetencji, które nie są powszechne w społeczeństwie. Dlatego też możliwość traktowania ich jako informacji, o których rozprzestrzenianie wiedzy stanowi element realizacji wolności wyrazu i wolności informacji, jest tak istotne dla możliwości weryfikowania ich potencjalnie dyskryminacyjnego charakteru. Odwracając tok analizy ETPCz, można by stwierdzić, że umożliwienie watchdogom badania i informowania o problemach wiążących się z wdrażaniem zautomatyzowanego podejmowania decyzji jest niezbędne w demokratycznym społeczeństwie. W sytuacjach, w których zautomatyzowane podejmowanie decyzji zastępuje akty prawne lub ma wpływ na to, jak są stosowane, brak przejrzystości skutkuje brakiem dostępu jednostki do reguł, zgodnie z którymi oceniane jest jej postępowanie. Można by rozważyć, czy w demokratycznym społeczeństwie byłaby do przyjęcia sytuacja, w której np. zasady przydziału spraw sędziom byłyby zależne wyłącznie od Ministra Sprawiedliwości i od jego – niezdefiniowanych w akcie prawnym i nieznanych nikomu – preferencji. Analogicznie, wątpliwości może budzić sytuacja, w której zasady te są sformułowane w postaci algorytmu, za który odpowiada Ministerstwo Sprawiedliwości i do którego nikt inny nie ma dostępu.

Sam fakt zapisu danych reguł postępowania w postaci kodu komputerowego nie powinien być decydujący dla uznawania, czy zasady w nim sformułowane mają być znane obywatelom czy nie. Kluczowe powinno być raczej kryterium wpływu na sytuację danych jednostek i grup. Dlatego, jak zaznaczałam w rozdziale pierwszym, można postulować, że jeśli kod komputerowy zastępuje przepisy, wymogi dotyczące jego publikacji powinny być takie same jak w przypadku aktów prawnych. Natomiast kiedy odgrywa rolę podobną lub analogiczną do aktu prawnego lub np. wspiera stosowanie prawa, uzasadnione jest traktowanie go jako informacji, która powinna być udostępniana na podstawie prawa dostępu do informacji.

3.6.2. Prawo dostępu do informacji jako narzędzie do korzystania z innych praw

Zautomatyzowane podejmowanie decyzji może mieć wpływ na realizację praw takich jak prawo do rzetelnego sądu czy prawo do prywatności. W świetle orzecznictwa ETPCz możliwe jest rozważenie traktowania prawa dostępu do informacji jako instrumentu koniecznego do realizacji innych praw. Wyrokiem, w którym nastąpiło uznanie braku informacji za naruszenie prawa do prywatności i ochrony życia rodzinnego jest opisana powyżej sprawa *Guerra i inni przeciwko Włochom*. W wyroku tym ETPCz nie stwierdził naruszenia art. 10 EKPCz. Jednocześnie jednak brak informacji został uznany za naruszenie prawa do ochrony prywatności chronionego art. 8 EKPCz. Ponadto potwierdzenie stanowiska przemawiającego za możliwością traktowania prawa dostępu do informacji jako środka umożliwiającego ochronę innych

praw można znaleźć również w doktrynie⁴⁶⁰. Zdaniem Päivi Tiilikkiej może ono być również postrzegane jako element niezbędny do realizacji innych praw uwzględnionych w EKPCz, np. prawa do życia, do sprawiedliwego sądu czy do prywatności. Możliwości te zasługują na uwagę w świetle obszarów wdrażania rozwiązań opartych na zautomatyzowanym podejmowaniu decyzji oraz sposobu naruszania tych praw.

Rola informacji w odniesieniu do prawa do życia została przez ETPCz podniesiona w wyroku w sprawie *Karandja przeciwko Bułgarii*⁴⁶¹. Sprawa dotyczyła śmierci syna skarżącej poniesionej z ręki policjanta. Jednym z argumentów przytoczonych przez ETPCz przemawiających za tym, że wystąpiło naruszenie art. 2 EKPCz, był fakt, że „przez ponad dwa lata organy prowadzące dochodzenie nie zapoznały wnioskodawcy z wynikami śledztwa”⁴⁶². Występują zatem sytuacje, w których dostęp do informacji warunkuje możliwość stwierdzenia naruszenia przez państwo prawa do życia. Przykładem sytuacji, w której informacja na temat działania zautomatyzowanego podejmowania decyzji byłaby konieczna do wykazania naruszenia przez państwo art. 2 EKPCz, mogłoby być użycie systemów do wspierania decyzji np. policji. Hipotetyczna sytuacja, w której działanie policji oparte byłoby na zautomatyzowanym podejmowaniu decyzji – np. interwencja w miejscu wskazanym przez algorytm – przyniosłoby skutki w postaci postrzelenia osoby obecnej w tym miejscu. Brak informacji dotyczących podstaw wydawanej decyzji, która mogłaby skutkować uszczerbkiem na zdrowiu lub śmiercią, mógłby być odczytywany jako naruszenie prawa do życia. Ponadto policja mogłaby argumentować za słusnością działań podjętych przez nią na podstawie sugestii algorytmu – jednostka zaś nie miałaby możliwości weryfikacji takiej informacji, ponieważ byłaby pozbawiona wiedzy na temat podstaw decyzji wydanej przez system zautomatyzowanego podejmowania decyzji.

W odniesieniu do związku między art. 6 a dostępem do informacji dotychczasowe orzecznictwo ETPCz głównie odnosi się do kwestii dostępu do informacji dotyczących postępowania sądowego. Przykładem jest orzeczenie w sprawie *Shapovalov przeciwko Ukrainie*. Sprawa dotyczyła dziennikarza, który żądał dostępu do informacji dotyczących wyborów prezydenckich w Ukrainie. Zarzuty stawiane Ukrainie dotyczyły naruszenia art. 6 i art. 10 EKPCz. W odniesieniu do prawa do rzetelnego procesu sądowego ETPCz

⁴⁶⁰ „Zgodnie z orzecznictwem, prawo do otrzymania informacji oparte może być na artykule 2 EKPCz (prawo do życia), artykule 6 (gwarantującym prawo do sądu), artykule 8 (chroniącym prawo do prywatności i życia rodzinnego) oraz artykule 10 (chroniącym wolność wyrazu)”. P. Tiilikka, *op. cit.*, s. 79

⁴⁶¹ Wyrok ETPCz z 7 października 2010 r. w sprawie *Karandja przeciwko Bułgarii*, skarga nr 69180/01.

⁴⁶² *Ibidem*, pkt 67.

stwierdził, że: „Trybunał uznaje prawo dostępu do poszczególnych dokumentów, które stanowi część wolności wyrazu, jako prawo obywatelskie w świetle artykułu 6 ust. 1 Konwencji”⁴⁶³. Stąd też trudności w skorzystaniu z drogi sądowej w zakresie dostępu do informacji zostały uznane za naruszenie art. 6 EKPCz. Jednocześnie ETPCz nie przychylił się do argumentacji dziennikarza, zgodnie z którą władze ukraińskie naruszyły art. 10. Trybunał doszedł m.in. do wniosku, że działania dziennikarza nie były ograniczone w zakresie informowania o nieprawidłowościach, które zaobserwował i których doświadczył. ETPCz stwierdził zatem, że chociaż trudności w dochodzeniu swoich praw dotyczących dostępu do dokumentu stanowiły przeszkodę dla realizacji prawa do rzetelnego procesu, to nie stanowiły one naruszenia prawa dostępu do informacji.

Sprawa *Shapovalov przeciwko Ukrainie* rzuca istotne światło na zagadnienie zautomatyzowanego podejmowania decyzji i jego wpływu na prawa gwarantowane przez art. 6 EKPCz. ETPCz podkreślił w niej, że warunkiem skuteczności prawa dostępu do sądu jest „jasna, praktyczna możliwość zakwestionowania czynu stanowiącego ingerencję w jej prawa”⁴⁶⁴. Pytanie, jakie można postawić, brzmi: czy wdrażanie systemów zautomatyzowanego podejmowania decyzji nie utrudnia korzystania z prawa dostępu do sądu? Jeśli argumentacja jednostki miałaby dotyczyć zautomatyzowanego podejmowania decyzji, bez jednoczesnego dostępu do wiedzy na temat zasad ich podejmowania, trudno stwierdzić, aby mogła ona skutecznie kwestionować czyny stanowiące ingerencję w jej prawa.

Przykładem sytuacji, które ukazują charakter tego problemu, jest posługiwanie się wynikami zautomatyzowanego podejmowania decyzji (często opartego na eksperymentalnych technologiach) jako dowodami w postępowaniach karnych⁴⁶⁵. Oskarżony nie ma możliwości praktycznego zakwestionowania przedstawionych dowodów, ponieważ nie wie nawet, na jakim podstawie został wskazany jako oskarżony. Innym przykładem mogłoby być wdrażanie systemów, takich jak np. COMPAS, służących do określenia w danej skali poziomu możliwości, że jednostka popełni kolejne przestępstwo. Przetwarzane przez algorytm wyniki ankiety prowadzą do zakwalifikowania jednostki do jednej z grup o mniejszym lub większym – teoretycznie – ryzyku recydywy. Jak wykazało śledztwo dziennikarskie przeprowadzone

⁴⁶³ Wyrok ETPCz z 31 lipca 2012 r. w sprawie *Shapovalov przeciwko Ukrainie*, skarga nr 5835/05, pkt 49.

⁴⁶⁴ *Ibidem*, pkt 53.

⁴⁶⁵ Zob. V. Eidelman, *Secret Algorithms Are Deciding Criminal Trials and We're Not Even Allowed to Test Their Accuracy*, ACLU, 15 września 2017 r. <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/secret-algorithms-are-deciding-criminal-trials-and>, dostęp: 1.04.2021.

przez organizację ProPublica⁴⁶⁶, algorytm prowadzi do systemowej dyskryminacji osób o innym niż biały kolorze skóry oraz kobiet.

Te przykłady używania zautomatyzowanego podejmowania decyzji, zaczerpnięte ze Stanów Zjednoczonych, wydają się nie do pogodzenia ze standardami ochrony prawnoczłowieczej ustanowionymi w orzecznictwie ETPCz. W perspektywie opartej na postrzeganiu dostępu do informacji jako warunku niezbędnego do realizacji prawa do rzetelnego sądu można podejrzewać, że jednostka mogłaby domagać się dostępu do informacji, jaki wynik wykazał w stosunku do niej algorytm oraz ewentualnie na jakich podstawach wynik ten się opierał. Do takiego spojrzenia na zautomatyzowane podejmowanie decyzji niezbędne jest traktowanie tego podejmowania decyzji jako narzędzia podlegającego ocenie z punktu widzenia wypracowanych w orzecznictwie standardów. Zważywszy na opisane w rozdziale pierwszym skłonności do stronniczości i wydawania dyskryminacyjnych werdyktów wykazywane przez algorytmy, jak najbardziej uzasadnione wydaje się ostrożne podejście do stosowania nowych technologii w obszarze ochrony sądowej i dążenie do zagwarantowania ich przejrzystości. To przejrzystość jest podstawowym warunkiem umożliwiającym weryfikację sposobów ich działania.

Ponadto w art. 6 EKPCz pojawia się sformułowanie „niezawisły i bezstronny sąd”. Można postawić pytanie: czy SLPS wprowadzany w Polsce prowadzi do zwiększenia bezstronności sądów? Czy odwrotnie: fakt, że jego działanie pozostaje wielką niewiadomą, może stanowić pole nadużyć⁴⁶⁷? Brak wiarygodnej odpowiedzi na te pytania ukazuje wagę dostępu do informacji na temat zautomatyzowanego podejmowania decyzji. Można sobie wyobrazić dwie drogi weryfikacji „bezstronności” SLPS. Jedną opartą na prawie dostępu do informacji jako części prawa do rzetelnego procesu, kiedy to w konkretnej sprawie (lub sprawach) zostałyby podniesione, że w wyniku losowania np. sędziów rozstrzygających sprawy osób protestujących przeciwko władzy niezwykle często wylosowywani zostają sędziowie nominowani przez obecną władzę, która SLPS wdrożyła. Drugą byłoby z kolei oparcie argumentacji na art. 10 i próba wykazania np. przez organizację pomagającą protestującym, że dostęp do samego algorytmu jest niezbędnym elementem weryfikacji, czy SLPS stanowi narzędzie sprzyjające niezawisłości i bezstronności sędziów.

Na uwagę zasługuje również relacja między art. 8 i art. 10 EKPCz. Z jednej strony mogą zaistnieć sytuacje, kiedy prawo do prywatności jest

⁴⁶⁶ J. Angwin, J. Larsona, S. Mattu, L. Kirchner, *op. cit.*

⁴⁶⁷ Por. M. Matczak, *op. cit.*; S. Gregorczyk-Abram, M. Wawrykiewicz, A. Owczarska, *op. cit.* oraz K. Izdebski, *Algorithms of Fairness*, „Medium” 15 lutego 2018 r. <https://medium.com/fundacja-epa%C5%84stwo/algorithms-of-fairness-2a30c2f93622>, dostęp: 1.04.2021.

powoływane jako argument przemawiający za odmówieniem dostępu do informacji, jak wystąpiło to np. w *Társaság a Szabadságjogokért przeciwko Węgrom*. Z drugiej strony możliwe jest zastosowanie art. 8 jako narzędzia prowadzącego do zdobycia dostępu do informacji. Przykładem takiej sytuacji było opisywane powyżej orzeczenie w sprawie *Guerra i inni przeciwko Włochom*. Chociaż ETPCz nie stwierdził naruszenia art. 10 przez brak rozpowszechniania przez państwo informacji dotyczących skutków funkcjonowania fabryki chemikaliów, to odnotował naruszenie art. 8 przez brak wystarczającej informacji, która była niezbędna do ochrony życia prywatnego i rodzinnego członków lokalnej społeczności.

Warto rozważyć, czy same algorytmy służące do zautomatyzowanego podejmowania decyzji, w związku z ich potencjalną dyskryminacyjnością oraz faktem, że oparte są na przetwarzaniu danych osobowych, nie mogłyby stanowić informacji koniecznej do zweryfikowania faktu naruszenia prawa do prywatności. Zagadnienie to odsyła do szerszego problemu różnicy między dostępem do informacji opartym na art. 10 a informacją jako środkiem umożliwiającym realizację innych praw. O ile w pierwszym przypadku informacja musi mieć wymiar społeczny i być istotna dla debaty publicznej, o tyle kiedy jest postrzegana jako element innych praw, dotyczy raczej sytuacji jednostki. Dlatego też możemy zakładać, że w związku z ochroną prywatności jednostka mogłaby argumentować, że zautomatyzowane podejmowanie decyzji zastosowane wobec niej miało dyskryminacyjny charakter, i starać się uzyskać wiedzę dotyczącą jej konkretnej sytuacji. Rozwiązanie to jest bliskie opisanym w rozdziale drugim wyjaśnieniom przewidzianym w RODO. Natomiast kiedy watchdog wnioskuje o DPIA czy o sam algorytm używany w systemie zautomatyzowanego podejmowania decyzji wdrożonym w obszarze pomocy społecznej po to, aby go następnie przeanalizować i opublikować, to korzysta on z art. 10 i dąży do przeprowadzenia wyjaśnienia opartego na modelu.

Wspólne dla opisanych możliwości przywoływania prawa dostępu do informacji jako środka do realizacji innych praw jest pytanie: czy korzystanie z dostępu do informacji jako środka umożliwiającego realizację innych praw mogłoby wiązać się z nałożeniem na państwo obowiązków informacyjnych? Orzecznictwo ETPCz nie pozwala na stwierdzenie, że na podstawie art. 10 państwo może być obciążone jakimikolwiek czynnymi obowiązkami w zakresie samodzielnego informowania obywateli. W wyroku *Guerra i inni przeciwko Włochom* brak aktywności ze strony państwa w zakresie informowania o zagrożeniach został jednak uznany za naruszenie art. 8 EKPCz. Sugeruje to, że w sytuacji, w której prawo dostępu do informacji stanowi element realizacji innych praw, *de facto* obowiązki państwa mogą sięgać dalej, niż kiedy prawo dostępu do informacji oparte jest na art. 10. W przypadku, w którym potencjalne zagrożenia dotyczyłyby całych grup, informowanie

o nich mogłoby przynosić skutek podobny do korzystania przez watchdogi z art. 10. Dla takiej wykładni niezbędna byłaby świadomość tego, jak głęboko wymiar cyfrowy w rzeczywistości przenika świat fizyczny i jak silnie algorytmy mogą determinować sytuację prawną jednostek i całych grup.

3.6.3. Prawo dostępu do informacji w świetle zakazu dyskryminacji

W szczególności należy rozważyć możliwość uzyskania dostępu do algorytmów używanych w ramach zautomatyzowanego podejmowania decyzji w świetle charakteru zakazu dyskryminacji w porządku prawnym Rady Europy. Relacja między prawem dostępu do informacji a kwestią zgodności danego zautomatyzowanego sposobu podejmowania decyzji z zakazem dyskryminacji może zostać skonceptualizowana na dwa sposoby.

Po pierwsze, możliwe jest argumentowanie, że przeciwdziałanie brakowi wiedzy na temat danego zautomatyzowanego podejmowania decyzji jest w interesie publicznym i przemawia za koniecznością udzielenia dostępu do danego algorytmu na podstawie art. 10 EKPCz. Potencjał dyskryminacyjny zautomatyzowanego podejmowania decyzji stanowiłby wówczas argument uzasadniający konieczność uzyskania przez daną organizację lub jednostkę dostępu do tej informacji ze względu na trzy przyczyny. Po pierwsze, jej pozyskanie służyłoby interesowi publicznemu i prowadziło do zwiększenia przejrzystości w świetle obaw, jakie można żywić co do potencjalnie dyskryminacyjnego charakteru stosowanego systemu zautomatyzowanego podejmowania decyzji. Po drugie, byłoby niezbędne do wypełniania przez daną organizację swojej roli jako watchdoga. Należy podkreślić, że niezbędnym warunkiem do wszczęcia takiego postępowania byłaby aktywność wynikająca z działalności danej organizacji czy jednostki w zakresie próby uzyskania odpowiedniej informacji od państwa. Po trzecie zaś, państwo w tym zakresie miałoby monopol informacyjny, któremu przeciwdziałanie byłoby możliwe dzięki udzieleniu dostępu do algorytmu.

Drugim sposobem połączenia kwestii potencjalnej dyskryminacyjności zautomatyzowanego podejmowania decyzji z prawem dostępu do informacji są sytuacje, w których pojawiłyby się obawy dotyczące dyskryminacyjnego traktowania jednostki w zakresie jednego z praw gwarantowanych przez EKPCz. W takim scenariuszu dyskryminacyjny charakter wdrożonego rozwiązania stanowiłby element wysuwanej przez jednostkę argumentacji, np. w wyniku używania zautomatyzowanego podejmowania decyzji nastąpiłoby naruszenie jej prawa do rzetelnego procesu w związku ze złamaniem zakazu dyskryminacji, przez wpisane we wdrożony program komputerowy dyskryminacyjne mechanizmy. Dostęp do informacji byłby w takim przypadku niezbędny do wykazania dyskryminacyjnego traktowania w zakresie korzystania z danego prawa.

Na tym tle pojawiają się wątpliwości dotyczące standardu procesowego w zakresie wykazania dyskryminacyjnego traktowania⁴⁶⁸. To właśnie prawo dostępu do algorytmów i innego typu działania mające na celu zwiększenie ich przejrzystości stanowią metody, które umożliwiłyby weryfikację, czy do dyskryminacji dochodzi, czy nie. Chociaż możliwe byłoby wskazywanie na dane świadczące o dyskryminacyjnym traktowaniu, np. na podstawie analiz decyzji wydawanych przez zautomatyzowany system czy przeprowadzanej próby dekompilacji danego programu (czyli *de facto* wykazywanie ich dyskryminacyjnego skutku, jak występowało to np. w przypadku opisywanego programu COMPAS), argumenty takie byłyby znacznie wzmocnione dzięki dostępowi do kodu używanego w ramach danego rozwiązania. Ponadto, odwołując się do przedstawionych w rozdziale pierwszym koncepcji postrzegających kod jako prawo, można by stwierdzić, że w przypadku zautomatyzowanego podejmowania decyzji stosowanego w sektorze publicznym to na instytucjach używających takich rozwiązań powinien ciążyć obowiązek wykazania, że nie mają one dyskryminacyjnego charakteru. Przede wszystkim można wskazać, że – w świetle wdrażania systemów zautomatyzowanego podejmowania decyzji w sektorze publicznym – niezbędne jest przemyślenie sposobów, które gwarantowałyby możliwość weryfikacji niedyskryminacyjności stosowanych rozwiązań.

W związku z tym, że z jednej strony nie wydaje się zasadne domniemywanie dyskryminacyjnego charakteru zautomatyzowanego podejmowania decyzji, z drugiej zaś strony bez odpowiednich zabezpieczeń jednostki są bezbronne w odniesieniu do zautomatyzowanej dyskryminacji, która może występować, najbardziej wskazane wydają się rozwiązania pozwalające na prewencyjne badanie i testowanie wdrażanych rozwiązań. Podejście takie jest proponowane w UE w odniesieniu do zastosowań sztucznej inteligencji wysokiego ryzyka w *Białej księdze w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania*⁴⁶⁹ i opracowanym w ślad za nią wniosku legislacyjnym *Aktu w sprawie SI* z kwietnia 2021 r. Projekt ten odnosi się jednak – potencjalnie – tylko do części zastosowań zautomatyzowanego podejmowania decyzji, które spełniałyby definicyjne kryteria SI zaproponowane w tym wniosku legislacyjnym. Ponadto wdrażanie tych rozwiązań niekoniecznie oznacza, że dostęp do algorytmów stosowanych w zautomatyzowanym podejmowaniu decyzji miałoby szersze grono odbiorców. Proponowane rozwiązania raczej zmiierzają w stronę przeprowadzania samodzielnej oceny stosowanego kodu przez dane przedsiębiorstwa i nadzorczą rolę instytucji publicznych – nie zaś gwarantowanie szerokiego dostępu

⁴⁶⁸ Za zwrócenie uwagi na konieczność nakreślenia tej kwestii dziękuję recenzentce mojej pracy doktorskiej, dr hab. prof. UJ Ninie Półtorak.

⁴⁶⁹ Komisja, *Biała księga w sprawie sztucznej inteligencji...*, *op. cit.*, s. 19–26.

do używanego kodu. Dlatego niezależnie, czy te lub podobne akty prawne zostaną przyjęte, to właśnie prawo dostępu do algorytmów jako informacji mogłoby pozwolić ocenić dyskryminacyjny potencjał wdrażanych rozwiązań i tym samym dostarczać dowodów na potencjalną dyskryminację w razie stosowania danego systemu mimo odkrycia jego dyskryminacyjnego charakteru.

3.7. Podsumowanie

W rozdziale przedstawiona została historia stopniowego wprowadzania prawa dostępu do informacji do katalogu praw człowieka chronionego przez EKPCz. Analiza wykazała, że w związku z brakiem słowa „poszukiwanie” w treści art. 10 EKPCz możliwość wykładni uwzględniającej prawo dostępu do informacji w ramach wolności informacji nie była oczywista. Rozwój orzecznictwa doprowadził jednak do utworzenia katalogu warunków, których spełnienie umożliwia powoływanie się na to prawo. Obejmuje ono sytuacje, w których dostęp został przyznany przez prawomocny wyrok sądu krajowego oraz gdy dostęp do informacji ma kluczowe znaczenie dla wykonania przez organizację czy jednostkę jej prawa do wolności wyrażania opinii, a odmowa udzielenia takiego dostępu stanowi ingerencję w to prawo.

W tych wypadkach konieczne jest spełnienie warunków dwustopniowego testu. Obejmuje on, w swym pierwszym etapie, cztery pozytywne przesłanki, które należy spełnić, aby powoływać się na prawo dostępu do informacji. Po pierwsze, celem żądania dostępu do informacji musi być udostępnienie jej i rozpowszechnienie wiedzy uzyskanej dzięki niej. Wiąże się to z postrzeganiem prawa dostępu do informacji jako logicznej konsekwencji prawa do otrzymywania informacji: aby odbiorcy mogli daną informację uzyskać, musi być ona w pierwotnie otrzymana. Po drugie, charakter informacji musi wiązać się z interesem publicznym. Nie może ona zatem dotyczyć indywidualnej sprawy danej jednostki, lecz musi mieć znaczenie społeczne. Po trzecie, żądający informacji muszą pełnić funkcję watchdog, czyli strażnika interesu publicznego, którego działalność obejmuje uczestnictwo w debacie publicznej. Po czwarte, sama informacja musi być gotowa i dostępna, przy czym jej niedostępność nie może być np. wynikiem polityki prowadzonej przez daną instytucję⁴⁷⁰.

Spełnienie pozytywnych przesłanek testu nie oznacza jednak, że prawo dostępu do informacji powinno być uwzględnione, ponieważ w drugim etapie testu państwo ma możliwość powołania się na przewidziane w art. 10 ust. 2 ograniczenia. Po pierwsze, ograniczenie takie musi być przewidziane w prawie. Po drugie, musi ono służyć ochronie jednego z interesów wymienionych

⁴⁷⁰ Warunek ten zbliża pod względem znaczenia termin „informacja” do terminu „dokument”, który pojawia się w ramach prawa Rady Europy w KDOD.

w EKPCz. Po trzecie, musi być ono niezbędne w demokratycznym społeczeństwie, czyli *de facto* przejść test proporcjonalności. W świetle tak sformułowanych warunków korzystania z prawa dostępu do informacji można wyobrazić sobie sytuacje, w których dostęp do algorytmów spełniałby sformułowane przez ETPCz kryteria.

Ponadto prawo dostępu do informacji może pełnić funkcję instrumentalną w stosunku do innych praw gwarantowanych przez EKPCz, czyli np. prawa do życia, prawa do rzetelnego sądu czy ochrony życia prywatnego. Pozytskane w ten sposób informacje powinny dotyczyć ściśle danej jednostki i jej sytuacji. Stanowiłyby zatem przykład wyjaśnienia skupionego na jednostce. Tymczasem proponowana interpretacja orzecznictwa ETPCz dotyczącego art. 10 powinna być postrzegana raczej jako przykład wyjaśnienia opartego na modelu. Celem pozyskania informacji musiałoby być wyjaśnienie działania samego systemu zautomatyzowanego podejmowania decyzji, nie zaś danej sytuacji, w której został on wykorzystany. Wnioskować o dostęp musiałaby jednostka lub organizacja pełniąca funkcję watchdoga, której intencją byłoby informowanie społeczeństwa o sposobie działania zautomatyzowanego podejmowania decyzji, co wynika ze szczególnej roli przypisywanej watchdogom w orzecznictwie ETPCz dotyczącym art. 10 EKPCz. W ten sposób możliwe byłoby spełnienie kryteriów warunkujących dostęp do informacji w ramach wykładni EKPCz dokonanej przez ETPCz.

Argumentem przemawiającym za wykładnią prawa dostępu do informacji, która w określonych sytuacjach powinna obejmować algorytmy używane w ramach zautomatyzowanego podejmowania decyzji, jest pełniona przez nie funkcja. Niekiedy jest ona analogiczna do funkcji pełnionej przez akty prawne. Wówczas algorytmy powinny być publikowane zgodnie z odpowiednimi warunkami uznania ich autentyczności w świetle obowiązującego prawa. Często są one jednak wdrażane w obszarach dotyczących np. samego stosowania prawa, nie zaś w miejsce obowiązujących przepisów. Dlatego też prawo dostępu do informacji mogłoby stanowić odpowiedź na wyzwania pojawiające się w związku z poszerzającym się spektrum stosowania zautomatyzowanego podejmowania decyzji. Postrzeganie kodu komputerowego jako *de facto* prawa przemawia za dążeniem do wyznaczania wysokich standardów w zakresie gwarantowania przejrzystości wdrażanych, zautomatyzowanych rozwiązań. Perspektywa ta powinna mieć znaczenie zarówno w ramach analizy wykładni art. 10 EKPCz w kontekście posługiwania się w ramach sektora publicznego zautomatyzowanym podejmowaniem decyzji, jak i w odniesieniu do wdrażania takich rozwiązań w obszarach powiązanych z innymi prawami gwarantowanymi przez EKPCz, np. prawem do sądu. Pozwala ona na dostrzeżenie, że skutki zautomatyzowanego podejmowania decyzji wykraczają poza wpływ na sytuację jednostki i dotyczą raczej całych grup społecznych.

Dostęp do dokumentów i informacji w odniesieniu do algorytmów stosowanych do zautomatyzowanego podejmowania decyzji w prawie UE

4.1. Od prawa dostępu do informacji na temat jednostki do prawa dostępu do dokumentów unijnych

Ograniczenia perspektywy, w której dostęp do danych oparty jest na unijnym prawie ochrony danych osobowych, stanowią argument przemawiający za koniecznością namysłu nad tym, czym obecnie jest dostęp do informacji w prawie UE, a czym mógłby się stać. W artykule *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*⁴⁷¹ przywoływani już Sandra Wachter i Brent Mittelstadt przeanalizowali sprawy, w których TSUE stanął przed problemem oceny, czy dane treści stanowią dane osobowe, czy też nie. Pierwsza z nich, *YS przeciwko Minister voor Immigratie, Integratie en Asiel oraz Minister voor Immigratie, Integratie en Asiel przeciwko M i S*⁴⁷², dotyczyła dostępu do informacji na temat przyczyn stojących za decyzją w sprawie wniosku o wydanie dokumentu pobytowego opartego na przepisach *dyrektywy 95/46*. TSUE stwierdził, że dane odnoszące się do osoby wnioskującej o dokument pobytowy, figurujące w dokumencie administracyjnym przedstawiającym powody przytoczone przez pracownika na poparcie projektu decyzji, oraz dane figurujące w analizie prawnej zawartej w tym dokumencie administracyjnym stanowią „dane osobowe”. Jednocześnie jednak samej analizie nie można zakwalifikować w ten sposób. W związku z tym osoba wnioskująca o dostęp do danych jej dotyczących na

⁴⁷¹ S. Wachter, B. Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, „Columbia Business Law Review” 2019, nr 2, s. 494–620.

⁴⁷² Wyrok Trybunału z dnia 17 lipca 2014 r. w sprawach połączonych C-141/12 i C-372/12, *YS przeciwko Minister voor Immigratie, Integratie en Asiel oraz Minister voor Immigratie, Integratie en Asiel przeciwko M i S*, ECLI:EU:C:2014:2081.

podstawie przepisów chroniących dane osobowe powinna mieć dostęp jedynie do tych fragmentów analizy, które można postrzegać jako dane osobowe.

W drugiej sprawie analizowanej w artykule Wachter i Mittelstadta⁴⁷³ Peter Nowak chciał uzyskać dostęp do arkusza egzaminacyjnego niezdanego przez niego egzaminu wraz z komentarzami naniesionymi przez osobę oceniającą. W tym wypadku TSUE orzekł, że pisemne odpowiedzi udzielone przez osobę przystępującą do egzaminu zawodowego i ewentualne naniesione przez egzaminatora komentarze odnoszące się do tych odpowiedzi stanowią dane osobowe w rozumieniu *dyrektywy 95/46*. Dla Wachter i Mittelstadta sprawy te stanowią ilustrację problematyczności zakresu pojęcia danych osobowych w prawie UE. Zauważają oni, że o ile w sprawach połączonych *YS przeciwko Minister voor Immigratie, Integratie en Asiel oraz Minister voor Immigratie, Integratie en Asiel przeciwko M i S*, opinie, rozumowanie i ocena stojące za decyzją nie są uznawane za dane osobowe, o tyle w przypadku sprawy *Peter Nowak przeciwko Data Protection Commissioner* już tak⁴⁷⁴.

Sprawy te pokazują również, jak ograniczone jest prawo dostępu oparte na przepisach dotyczących ochrony danych osobowych. Wyroki TSUE pozwalają podejrzewać, że podobne rozbieżności mogłyby pojawić się w ocenie sytuacji, w których kwestia dostępu do danych osobowych wystąpiłaby na tle zautomatyzowanego podejmowania decyzji. Czy można wyobrazić sobie, że na podstawie przepisów dotyczących dostępu do danych osobowych jednostka mogłaby otrzymać znaczące informacje na temat samego systemu zautomatyzowanego podejmowania decyzji? Ewentualny dostęp mógłby raczej objąć jedynie jej indywidualną sytuację i jej indywidualne wyjaśnienie. Tymczasem – jak wyjaśniam w rozdziale pierwszym – zjawiska wiążące się z zautomatyzowanym podejmowaniem decyzji mają inherentny wymiar kolektywny. Decyzja dotycząca wydania dokumentu pobytowego będąca wynikiem zastosowania systemu zautomatyzowanego podejmowania decyzji jest nie tylko decyzją indywidualną. Jest ona również świadectwem, jak działają mechanizmy determinujące sposób działania tego systemu, które obejmują wszystkie decyzje wydawane z jego użyciem.

Tym samym warto zastanowić się, czy – w razie implementacji przez instytucje unijne i państwa członkowskie systemów zautomatyzowanego podejmowania decyzji – na przybliżone powyżej stany faktyczne nie można by spojrzeć z innej perspektywy, stawiającej w centrum prawo dostępu do dokumentów i informacji. Zastąpienie urzędników oceniających wnioski o zezwolenie na pobyt czy egzaminy zautomatyzowanymi systemami może rodzić pytania o uzasadnienie nie tylko tej jednej, konkretnej,

⁴⁷³ Wyrok Trybunału z dnia 20 grudnia 2017 r. w sprawie C-434/16, *Peter Nowak przeciwko Data Protection Commissioner*, ECLI:EU:C:2017:994.

⁴⁷⁴ Zob. S. Wachter, B. Mittelstadt, *A Right to Reasonable Inferences...*, *op. cit.*, s. 537.

kwestionowanej decyzji, lecz także o legitymizację całego zautomatyzowanego systemu. To on, a nie tylko dane osobowe jednostki, staje się tym elementem potencjalnego stanu faktycznego, do którego dostęp może ułatwić zrozumienie również indywidualnej decyzji.

W związku z tym problematyka dostępu do dokumentów i informacji w odniesieniu do zautomatyzowanego podejmowania decyzji w prawie UE wymaga analizy dwóch zagadnień. Pierwszym jest próba oceny, do jakiego stopnia prawo dostępu do dokumentów unijnych – w formie, jaką przybrało na przestrzeni ostatnich niemal trzech dekad w prawie UE – może odpowiadać na wyzwania związane z zautomatyzowanym podejmowaniem decyzji. Analiza tego problemu ma głównie walor teoretyczny. Systemy zautomatyzowanego podejmowania decyzji są wprowadzane obecnie raczej na poziomie krajowym czy nawet lokalnym. Rozwój systemów używanych w zakresie ochrony granic w Unii Europejskiej jest jednak przykładem, że również ona staje się aktywnym aktorem w zakresie wdrażania systemów zautomatyzowanego podejmowania decyzji⁴⁷⁵. Niewykluczone jest, że wraz z rozpowszechnianiem się tego typu rozwiązań będą one coraz częściej używane również na poziomie polityk realizowanych przez UE. O możliwości takiej świadczy chociażby uwzględnienie w art. 24 *rozporządzenia 2018/1725* norm dotyczących zautomatyzowanego podejmowania decyzji o treści tożsamej z art. 22 RODO.

Odpowiedź na pytanie, czy na podstawie przepisów obecnie regulujących zasady dostępu do dokumentów można wyobrazić sobie potraktowanie systemu służącego do zautomatyzowanego podejmowania decyzji jako dokumentu podlegającego prawu dostępu do dokumentów, prowadzi do drugiego zagadnienia istotnego dla tematu analizy. Jest ona punktem wyjścia do scharakteryzowania relacji między prawem dostępu do dokumentów a prawem dostępu do informacji. W razie przyjęcia wykładni art. 11 KPP zgodnej z wykładnią art. 10 EKPCz prawo do informacji miałyby zastosowanie w odniesieniu do działań państw członkowskich w zakresie, w jakim stosują one prawo UE. Stanowiłoby to odwrót od dotychczasowej logiki stojącej za unijnymi regulacjami dotyczącymi prawa dostępu do dokumentów. Zwiastunem możliwości zmiany stanowiska UE w odniesieniu do uznawania prawa dostępu do informacji za prawo podstawowe jest treść *dyrektywy 2019/1024*. W jej motywie 5⁴⁷⁶ znajduje się sformułowane wprost stwierdzenie, że dostęp

⁴⁷⁵ Zob. A. Napieralski, *Collecting Data at EU Smart Borders: Data Protection Challenges of the New Entry/Exit System*, „Recht & Gesellschaft” 2019, nr 2, s. 199–209; A. Napieralski, *Right to Appeal and Copyright – Challenging Automated Decisions at EU Borders*, „ipCompetence” 2018, t. 20, s. 20–24.

⁴⁷⁶ Oczywiście niewiążący prawnie charakter motywów powinien stanowić wskazówkę nakazującą powściągliwość w stosunku do potencjalnego wpływu wzmianki zawartej w *dyrektywie 2019/1024*. Niemniej również jej przepisy wywołują zastanowienie co do

do informacji jest jednym z praw podstawowych. Treść motywu odsyła do KPP i jest wyjątkowym w prawie unijnym świadectwem postrzegania wolności otrzymywania i przekazywania informacji oraz idei bez ingerencji władz publicznych i bez względu na granice państwowe jako części prawa do wolności wypowiedzi.

4.1.1. Ramy prawne dotyczące prawa dostępu do dokumentów unijnych

Początki wprowadzania regulacji dotyczących dostępu do dokumentów⁴⁷⁷ w UE wiążą się z próbą przyjmowania środków mających zaradzić deficytowi demokracji. Wprowadzenie zasad dotyczących dostępu do dokumentów instytucji miało służyć zbliżaniu UE do jej obywateli, o czym świadczy dołączona do TUE *Deklaracja nr 17 dotycząca prawa dostępu do informacji*⁴⁷⁸. Zgodnie z nią „jawność procesu decyzyjnego umacnia demokratyczny charakter instytucji i zaufanie publiczne do administracji”. Prawo dostępu do informacji miało stanowić narzędzie służące realizacji założeń stojących u podstaw reformy ówczesnych Wspólnot Europejskich. Treść deklaracji zobowiązała ponadto Komisję do przygotowania do 1993 r. raportu na temat prawa dostępu do informacji. Waga dostępu do informacji została podkreślona również przez Radę Europejską w deklaracji *Wspólnota blisko swoich obywateli*⁴⁷⁹ w Birmingham w październiku 1992 r. i w konkluzjach przyjętych

kwestii prawa dostępu do informacji, jego charakteru i zakresu w prawie UE – co analizuję pod koniec rozdziału.

⁴⁷⁷ Jak zauważa Roy W. Davies, przed Traktatem z Maastricht można było zaobserwować w prawie wspólnotowym istnienie prawa dostępu do akt jako elementu prawa do rzetelnego procesu. Wiąże się ono jednak ściśle z daną sprawą i sytuacją, tym samym nie można go utożsamiać w żaden sposób z prawem dostępu do dokumentów czy prawem dostępu do informacji. Zob. R.W. Davies, *Access to Documents: a Constitutional Right or a General Principle of Law?*, „Irish Jurist New Series” 2004, t. 39, s. 60. Podobnie zob. M. Riekkinen, M. Suksi, *Access to Information and Documents as a Human Right*, Institute for Human Rights/Åbo Akademi University, Turku-Åbo 2015, s. 69–70. Kompleksowy opis historii rozwoju prawa dostępu do dokumentów (a pierwotnie: informacji), zob. L. Rossi, P. Vinagre e Silva, *Public Access to Documents in the EU*, Hart Publishing, Oxford–Portland 2017, s. 9–38; D. Adamski, *Prawo do informacji o działaniach władz publicznych Unii Europejskiej*, C.H. Beck, Warszawa 2011, s. 32–49. Ponadto podobne wyliczenia dokumentów przyjętych w związku z dostępem do informacji przez instytucje wspólnotowe zawiera wiele orzeczeń dotyczących dostępu do dokumentów, np. Wyrok Sądu pierwszej instancji z dnia 19 lipca 1999 w sprawie T-14/98, *Heidi Hautala przeciwko Radzie Unii Europejskiej*, ECLI:EU:T:1999:157, pkt 1–6; Wyrok Sądu pierwszej instancji z dnia 19 marca 1998 r. w sprawie T-83/96, *Gerard van der Wal przeciwko Komisji Wspólnot Europejskich*, ECLI:EU:T:1998:59, pkt 1–3.

⁴⁷⁸ *Treaty on European Union – Declaration on the right of access to information*, Dz.Urz. WE 1992 C 191, s. 101.

⁴⁷⁹ Rada Europejska, *Conclusions of the Birmingham European Council (A Community close to its citizens)*, Bull. EC 10-1992, pkt I.8, s. 9.

w Edynburgu w grudniu 1992 r.⁴⁸⁰, w których to Rada Europejska zachęcała do kontynuacji wysiłków dotyczących tego tematu.

Komisja, zobowiązana treścią *deklaracji nr 17* do przygotowania raportu na temat prawa dostępu do informacji, przedstawiła 5 maja 1993 r. Radzie, PE i Komitetowi Ekonomiczno-Społecznemu wyniki porównawczej ankiety dotyczącej dostępu do dokumentów w państwach członkowskich i innych wybranych państwach⁴⁸¹. Niecały miesiąc później Komisja opublikowała *komunikat 93/C 166/04* dotyczący otwartości we Wspólnocie⁴⁸². Kilka tygodni później Rada Europejska podczas szczytu w Kopenhadze zachęciła Komisję i Radę do dalszych prac „opartych na zasadzie zagwarantowania obywatelom najszerszego dostępu do informacji”⁴⁸³. Zwiększeniem wszystkich tych aktywności było przyjęcie przez Radę i Komisję *Kodeksu postępowania dotyczącego publicznego dostępu do dokumentów Rady i Komisji*⁴⁸⁴.

Kodeks, chociaż nie był prawnie wiążącym aktem⁴⁸⁵, wyznaczył standard realizacji prawa dostępu do dokumentów. Zasadą miał stać się najszerszy możliwy dostęp do dokumentów będących w posiadaniu Komisji i Rady⁴⁸⁶. Na podstawie Kodeksu kolejno Rada i Komisja przyjęły decyzje regulujące dostęp do dokumentów. Instytucje obrały jednak odmienne strategie w stosunku do tego wyzwania. Komisja włączyła w art. 1 *decyzji 94/90*⁴⁸⁷ treść Kodeksu jako element decyzji oraz przyjęła w niej odpowiednie zasady proceduralne dotyczące dostępu do jej dokumentów.

⁴⁸⁰ Rada Europejska, *Conclusions of the Edinburgh European Council (Openness and Transparency)*, Bull. EC 12-1992, pkt I.5, s. 10. Zob. M. O'Neill, *The Right of Access to Community-Held Documentation as a General Principle of EC Law*, „European Public Law” 1998, t. 4, nr 3, s. 409.

⁴⁸¹ Komisja Wspólnot Europejskich, *Communication 93/C 156/05 on public access to the institutions' documents*, Dz.Urz. WE 1993 C 156, s. 5.

⁴⁸² Komisja Wspólnot Europejskich, *Communication 93/C 166/04 on openness in the Community*, Dz.Urz. WE 1993 C 166, s. 4.

⁴⁸³ Rada Europejska, *Conclusions of the Copenhagen European Council (A Community close to its citizens)*, Bull. EC 6-1993, pkt I.22, s. 15–16.

⁴⁸⁴ *Code of Conduct concerning public access to Council and Commission documents* (Kodeks), Dz.Urz. WE 1993 L 340, s. 41.

⁴⁸⁵ Co potwierdzone zostało w: Wyrok Trybunału z dnia 30 kwietnia 1996 r. w sprawie C-58/94, *Królestwo Niderlandów przeciwko Radzie Unii Europejskiej*, ECLI:EU:C:1996:171, pkt 27.

⁴⁸⁶ „Wszyscy (*the public*) będą mieli najszerszy możliwy dostęp do dokumentów będących w posiadaniu Komisji i Rady” – Kodeks.

⁴⁸⁷ *Decyzja 94/90/EWWG, WE, Euratom w sprawie dostępu do dokumentów*, Dz.Urz. WE 1994 L 46, s. 58 (zmieniona następnie przez: *Decyzja Komisji z 19 września 1996 zmieniającą decyzję 94/90/EWWG, WE, Euratom z 8 lutego 1994 w sprawie dostępu do dokumentów* (96/657/Euratom, EWWG, WE), Dz.Urz. WE 1996 L 247, s. 45.

Rada natomiast przyjęła decyzję⁴⁸⁸ w formie powtarzającej zapisy przyjęte w Kodeksie⁴⁸⁹. Ponadto decyzja Rady została przyjęta na podstawie prawnej umożliwiającej jej przyjmowanie reguł proceduralnych⁴⁹⁰, co stało się przedmiotem skargi o stwierdzenie nieważności zainicjowanej przez Królestwo Niderlandów.

Sprawa ta pokazuje fundamentalny spór dotyczący postrzegania kwestii dostępu do dokumentów w prawie UE. Z jednej strony można na niego patrzeć jako na kwestię dotyczącą głównie instytucji: to ich zasad działania dotyczą normy odnoszące się do udostępniania dokumentów i to według tej logiki wydawała się postępować Rada. Z drugiej strony, jak starało się wykazać Królestwo Niderlandów, prawo dostępu do dokumentów może być postrzegane jako przede wszystkim prawo jednostki do otrzymania informacji na temat działania instytucji. Wyrok Trybunału jest próbą połączenia tych dwóch stanowisk. Podkreśla on, że w związku z brakiem relewantnego aktu ustawodawczego, który regulowałby dostęp do dokumentów instytucji wspólnotowych, instytucje są zmuszone przyjmować środki o charakterze wewnętrznym, aby sprostać wymogom zasady dobrej administracji⁴⁹¹. Jednocześnie zauważa on, że fakt wywierania przez *decyzję 93/731* skutków prawnych wobec osób trzecich nie stoi w sprzeczności z jej wewnętrznym charakterem⁴⁹². Tym samym pośrednio i w ograniczonym stopniu Trybunał rozpoznał prezentowane przez Królestwo Niderlandów stanowisko pozwalające postrzegać dostęp do dokumentów jako kwestię, w której istotne są również uprawnienia jednostek.

Kodeks oraz przyjęte na jego podstawie decyzje stały się bazą dla orzecznictwa Sądu oraz Trybunału dotyczącego dostępu do dokumentów⁴⁹³. Jed-

⁴⁸⁸ *Decyzja 93/731/WE w sprawie dostępu do dokumentów Rady*, Dz.Urz. WE 1993 L 340, s. 43.

⁴⁸⁹ Na temat tych różnic, zob. D. Curtin, H. Meijers, *Access to European Union Information: An Element of Citizenship and a Neglected Constitutional Right*, [w:] *The European Union and Human Rights*, red. N.A. Neuwahl, A. Rosas, Brill, Haga 1995, s. 91.

⁴⁹⁰ Zob. D. Curtin, H. Meijers, *Access to European Union Information...*, *op. cit.*, s. 91 oraz Wyrok Trybunału z dnia 30 kwietnia 1996 r. w sprawie C-58/94, *Królestwo Niderlandów przeciwko Radzie Unii Europejskiej*, ECLI:EU:C:1996:171.

⁴⁹¹ Wyrok Trybunału z dnia 30 kwietnia 1996 r. w sprawie C-58/94, *Królestwo Niderlandów przeciwko Radzie Unii Europejskiej*, ECLI:EU:C:1996:171, pkt 37.

⁴⁹² *Ibidem*, pkt 38.

⁴⁹³ Listę spraw sprzed przyjęcia *rozporządzenia 1049/2001* można znaleźć w tekście: S. Peers, *The New Regulation on Access to Documents: A Critical Analysis*, „Yearbook of European Law” 2001, t. 21, nr 1, s. 388. Kompleksowy przegląd orzecznictwa dotyczącego dostępu do dokumentów w prawie UE, zob. L. Rossi, P. Vinagre e Silva, *op. cit.*; D. Adamski, *Prawo do informacji...* oraz J. Heliskoski, P. Leino, *Darkness at the Break of Noon: the Case Law on Regulation No. 1049/2001 on Access to Documents*, „Common Market Law Review” 2006, t. 43, s. 735–781. W dalszej części rozdziału odwołuję się jedynie do orzeczeń istotnych z punktu widzenia tematu.

nocześnie prawo dostępu do dokumentów stawało się coraz bardziej obecne w kolejnych przyjmowanych wersjach traktatów. Po pierwsze, TUE⁴⁹⁴ zrewidowany przez Traktat z Amsterdamu wprost odwołuje się do zasady otwartości⁴⁹⁵, formułując zasadę, zgodnie z którą „decyzje są podejmowane tak otwarcie jak to możliwe i tak blisko obywateli jak to możliwe”⁴⁹⁶. Po drugie, Traktat z Amsterdamu bezpośrednio sformułował prawo dostępu do dokumentów dla każdego obywatela Unii oraz każdej osoby fizycznej lub prawnej mającej miejsce zamieszkania lub siedziby w państwie członkowskim⁴⁹⁷. Instytucjami objętymi zakresem tej regulacji miały być Parlament Europejski, Rada i Komisja, zasady zaś dostępu do dokumentów miały być określone przez Radę w terminie do dwóch lat od wejścia w życie Traktatu z Amsterdamu⁴⁹⁸. Ponadto każda z instytucji wymienionych w artykule została zobowiązana do wypracowania własnych zasad dotyczących dostępu do jej dokumentów. Po trzecie, w Traktacie z Amsterdamu uwzględniono osobny przepis odnoszący się do Rady⁴⁹⁹. Kładł on nacisk na konieczność zagwarantowania dostępu do dokumentów w odniesieniu do sytuacji, w których Rada pełniła funkcję prawodawczą. Uwzględnienie tych norm wśród przepisów rangi traktatowej stanowiło niewątpliwie wzmocnienie pozycji prawa dostępu do dokumentów w prawie pierwotnym UE.

Efektom zmian wprowadzonych w odniesieniu do prawa dostępu do dokumentów w Traktacie z Amsterdamu było przyjęcie – zgodnie z wpisaniem w Traktat zapowiedzią – *rozporządzenia 1049/2001*⁵⁰⁰, kompleksowo ujmującego sposób regulacji kwestii dostępu do dokumentów w prawie UE. Mimo podjętych prób nowelizacji aktu obowiązuje on – w chwili przygotowywania książki – w swej pierwotnej formie. Jak zauważają Leonor Rossi i Patricia Vinagre de Silva, może to być dowodem „adekwatności rozwiązań przyjętych w *rozporządzeniu 1049/2001* lub znakiem, że raz zgodziwszy się na przyjęcie

⁴⁹⁴ Art. 1 TUE (w Traktacie z Amsterdamu: art. 1 ust. 4, *Traktat z Amsterdamu*, Dz.Urz. WE 1997 C 340, s. 1–144).

⁴⁹⁵ Zob. dalej w rozdziale.

⁴⁹⁶ Art. 1 TUE (w Traktacie z Amsterdamu: art. 1 ust. 4, *Traktat z Amsterdamu*, Dz.Urz. WE 1997 C 340, s. 1–144).

⁴⁹⁷ Art. 255, *Traktat ustanawiający Wspólnotę Europejską (wersja skonsolidowana, Amsterdam)*, Dz.Urz. UE 2006 C 321E (w Traktacie z Amsterdamu: art. 2 ust. 45, *Traktat z Amsterdamu*, Dz.Urz. WE 1997 C 340, s. 1–144. Polskie tłumaczenie, zob. D. Adamski, *Prawo do informacji...*, s. 38–39 – przypis).

⁴⁹⁸ W ramach procedury wspóldecydowania.

⁴⁹⁹ Art. 207 ust. 3 *Traktat ustanawiający Wspólnotę Europejską (wersja skonsolidowana, Amsterdam)*, Dz.Urz. UE 2006 C 321E (w Traktacie z Amsterdamu: art. 2 ust. 39(3), *Traktat z Amsterdamu*, Dz.Urz. WE 1997 C 340, s. 1–144).

⁵⁰⁰ *Rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji* (rozporządzenie 1049/2001), Dz.Urz. WE 2001 L 145, s. 43–48.

rozporządzenia instytucje nie są w stanie ponownie zgodzić się na dalszą reformę⁵⁰¹.

Brak nowelizacji *rozporządzenia 1049/2001* nie oznacza jednak, że stan prawny dotyczący dostępu do dokumentów w prawie UE nie zmienił się od niemal 20 lat. Przyjęcie Traktatu z Lizbony oraz nadanie mocy prawnej KPP w znaczący sposób wpłynęły na zakres i wagę prawa dostępu do dokumentów w UE. Po pierwsze, art. 15 TFUE rozszerzył katalog instytucji objętych prawem dostępu do dokumentów urzędowych na każdą instytucję, organ lub jednostkę organizacyjną UE⁵⁰². Po drugie, do treści art. 15 została wprowadzona w ust. 1 zasada otwartości. Po trzecie, art. 42 KPP potwierdza status prawa każdego obywatela Unii i każdej osoby fizycznej lub prawnej mającej miejsce zamieszkania lub statutową siedzibę w państwie członkowskim do dostępu do dokumentów instytucji, organów i jednostek organizacyjnych Unii jako prawa podstawowego. W ciągu niecałych 30 lat od pierwszych inicjatyw dotyczących prawa dostępu do dokumentów zostało ono podniesione do rangi traktatowej oraz uwzględnione w akcie kodyfikującym prawa podstawowe⁵⁰³.

4.1.2. Prawo dostępu do dokumentów unijnych jako narzędzie służące demokracji

Rozwój prawa dostępu do dokumentów jest odbiciem politycznych i instytucjonalnych procesów występujących w ostatnich trzech dekadach w Europie. Nie ulega wątpliwości, że prawo dostępu do dokumentów jest silnie nacechowane politycznie. Decyzje o tym, co należy lub można upubliczniać, a co powinno zachować tajny charakter, to jeden ze środków wpływania na debatę publiczną. Wymogi dotyczące przejrzystości działania władz publicznych są formułowane w ramach prawnych ustanawianych we współczesnych

⁵⁰¹ L. Rossi, P. Vinagre e Silva, *op. cit.*, s. 31.

⁵⁰² Przy czym zgodnie z art. 15 ust. 3 TFUE.: „Trybunał Sprawiedliwości Unii Europejskiej, Europejski Bank Centralny i Europejski Bank Inwestycyjny podlegają niniejszemu ustępowi jedynie w wykonywaniu swoich funkcji administracyjnych”.

⁵⁰³ Uwzględnienie prawa dostępu do dokumentów w KPP może być postrzegane jako świadectwo podniesienia jego rangi: „Umieszczenie prawa dostępu do dokumentów w Karcie potwierdza fundamentalne znaczenie tego prawa, które musi być przestrzegane przez instytucje unijne oraz państwa członkowskie wykonujące prawo unijne”. *Karta Praw Podstawowych Unii Europejskiej. Komentarz, op. cit.*, s. 2 (do art. 42). Na temat zmiany zakresu zastosowania prawa dostępu do dokumentów w związku z uwzględnieniem go w KPP, zob. dalej w rozdziale. Ponadto w kontekście uwzględnienia dostępu do dokumentów jako prawa podstawowego warto podkreślić zarówno pozycję europejskiego Ombudsmana w *rozporządzeniu 1049/2001* w związku z uwzględnieniem w art. 8 rozporządzenie możliwości złożenia skargi u rzecznika praw obywatelskich w razie wydania przez instytucję decyzji odmawiającej całkowicie lub częściowo dostępu do dokumentów, jak i jego aktywność w tej materii, zob. publikacja autorstwa unijnego RPO w latach 2003–2013: N. Diamandouros, *Openness and Access to Documents*, „European State Aid Law Quarterly” 2008, nr 4, s. 654–658.

systemach demokratycznych. Jak pokazuje przykład list poparcia dla kandydatów do neo-KRS, ograniczanie możliwości dostępu do informacji jest jednym z przejawów erozji demokracji. Z kolei próby jego wprowadzania w UE były przejawem wysiłków mających na celu budowanie bardziej demokratycznych mechanizmów na poziomie instytucji unijnych.

Sama historia wprowadzania prawa dostępu do dokumentów do prawa UE wiąże się ze ściśle politycznym wymiarem integracji. Po pierwsze, przegrane referendum w Danii w 1992 r. dotyczące rewizji traktatów (tj. Traktatu z Maastricht) stało się przyczyną zwrotu w stronę aktywności mających zwiększyć przejrzystość działań unijnych⁵⁰⁴. Następnie zaś akcesja w 1995 r. do Wspólnot państw o silnej tradycji otwartego rządu – Finlandii i Szwecji – wzmocniła grupę państw członkowskich mających wysokie oczekiwania w zakresie działań ukierunkowanych na osiągnięcie wyższego poziomu otwartości instytucji wspólnotowych⁵⁰⁵. Po drugie, przywoływane powyżej dokumenty unijne wprost odwołują się do politycznego wymiaru dostępu do informacji i dokumentów jako elementu procesu „demokratyzacji” i „zbliżania Unii do jej obywateli”. Po trzecie, charakter prawa dostępu do dokumentów jako ściśle powiązanego z wymiarem politycznym integracji potwierdza przegląd literatury i orzecznictwa. Pojęcia pojawiające się we unijnych dokumentach z początku lat 90. XX w. dotyczących dostępu do informacji wyznaczyły obowiązujący w pewnym stopniu do dzisiaj trend w orzecznictwie i doktrynie. Dostęp do informacji jest łączony z takimi pojęciami, jak: przejrzystość (*transparency*)⁵⁰⁶, demokracja⁵⁰⁷, otwartość (*openness*)⁵⁰⁸, legitymizacja⁵⁰⁹, rozliczalność (*accountability*)⁵¹⁰, dobre rządy (*good governance*)⁵¹¹

⁵⁰⁴ D. Adamski, *Prawo do informacji...*, s. 34.

⁵⁰⁵ *Ibidem*, s. 36.

⁵⁰⁶ Na przykład *Treaty on European Union – Declaration on the right of access to information*, Dz.Urz. WE 1992 C 191, s. 101.

⁵⁰⁷ *Ibidem*.

⁵⁰⁸ Na przykład Komisja Wspólnot Europejskich, *Communication 93/C 166/04 on openness in the Community...* czy art. 15, TFUE.

⁵⁰⁹ Na przykład motyw 2, *rozporządzenie 1049/2001* – w polskiej wersji językowej *legitymizacja* tłumaczone jest jako „prawowitość”. W orzecznictwie tłumaczone bywa jako „legitymizacja” (Wyrok Trybunału z dnia 17 października 2013 r. w sprawie C-280/11 P, *Rada Unii Europejskiej przeciwko Access Info Europe*, ECLI:EU:C:2013:671, pkt 32) lub „legitymizacja” (np. pkt 13 w tym samym wyroku) – jak widać, niekiedy nawet w tym samym orzeczeniu.

⁵¹⁰ Na przykład motyw 2, *rozporządzenie 1049/2001*. Na temat tego pojęcia w kontekście UE, zob. np. E. Fisher, *The European Union in the Age of Accountability*, „Oxford Journal of Legal Studies” 2004, t. 24, nr 3, s. 495–515.

⁵¹¹ Na przykład art. 15, TFUE. Na temat tego pojęcia w kontekście UE zob. np.: F. Weiss, S. Steiner, *Transparency as an Element of Good Governance in the Practice of the EU and the WTO: Overview and Comparison*, „Fordham International Law Journal” 2006, t. 30, nr 5, s. 1545–1586.

czy partycypacja⁵¹². Nagromadzenie używanych w odniesieniu do prawa dostępu do dokumentów pojęć odnoszących się do sfery wartości prowadzi do zaciemnienia znaczenia powiązań między tymi terminami. Jednocześnie jednak próba rekonstrukcji relacji między terminami opisującymi przyczyny stojące za rozwojem prawa dostępu do dokumentów ma potencjał naświetlenia normatywnej treści przepisów dotyczących tego zagadnienia.

Prawo dostępu do dokumentów może być postrzegane jako jeden z elementów służących realizacji zasady przejrzystości i zasady otwartości. Relacja między tymi dwiema zasadami nie jest jasna, ponieważ często są one wymieniane „jednym tchem”, ale – za Alberto Alemanno – można podejrzewać, że zasada otwartości powinna być rozumiana szerzej, jako akcentująca konieczność podejmowania przez instytucje unijne proaktywnych działań⁵¹³ (np. publikacja informacji na temat ich aktywności). W świetle takiej interpretacji prawo dostępu do dokumentów służy zasadzie przejrzystości, ponieważ jest ono uzależnione od aktywności obywateli, nie zaś samych instytucji. Ponadto jest ono pośrednio elementem wdrażania zasady otwartości, ponieważ zakres udostępnianych przez instytucje informacji ma wpływ na zakres potencjalnego korzystania z prawa dostępu do dokumentów (np. wnioskowanie o dostęp do dokumentów może być niepotrzebne, skoro zostały one opublikowane przez daną instytucję). Prawo dostępu do dokumentów w żaden sposób nie może być jednak postrzegane jako wyczerpujące treść zasady otwartości czy przejrzystości⁵¹⁴. Jest ono jednym z elementów ich urzeczywistniania. Podobną relację można zaobserwować w odniesieniu do partycypacji. Dostęp do dokumentów jest jedną z form uczestnictwa obywateli w życiu politycznym wspólnoty obok np. udziału w wyborach czy inicjatywy obywatelskiej.

Zasady przejrzystości, otwartości i partycypacji są najbardziej i bezpośrednio związane z prawem dostępu do dokumentów. Za ich pośrednictwem są realizowane kolejne wartości związane z dostępem do informacji, czyli rozliczalność i legitymizacja. Relację taką potwierdza orzecznictwo TSUE, np. w sprawie *Królestwo Szwecji i Maurizio Turco przeciwko Radzie Unii Europejskiej*⁵¹⁵ TSUE zauważył, że „przejrzystość (*transparency*) przyczynia się do tego, by przydać większej legitymizacji w oczach europejskich obywateli

⁵¹² Na przykład art. 15, TFUE. W polskich wersjach językowych pojawia się również tłumaczenie „uczestnictwo”.

⁵¹³ A. Alemanno, *Unpacking the Principle of Openness in EU Law: Transparency, Participation and Democracy*, „European Law Review” 2014, t. 39, nr 1.

⁵¹⁴ Zob. P. Settembri, *Transparency and the EU Legislator: Let He Who Is without Sin Cast the First Stone*, „Journal of Common Market Studies” 2005, t. 43, nr 3, s. 641 oraz przywołana tam literatura.

⁵¹⁵ Wyrok Trybunału z dnia 1 lipca 2008 r. w sprawach połączonych C-39/05 P oraz C-52/05 P, *Królestwo Szwecji i Maurizio Turco przeciwko Radzie Unii Europejskiej*, ECLI:EU:C:2008:374.

i zdobyć ich większe zaufanie”⁵¹⁶, a także wpływa na „korzyści płynące [...] ze wzmoczonej przejrzystości, czyli większego uczestnictwa obywateli w procesie podejmowania decyzji, a także większej legitymizacji, skuteczności i rozliczalności (*accountability*) administracji względem obywateli w systemie demokratycznym”⁵¹⁷.

Cytaty te pokazują również, co stoi na szczycie tej układanki złożonej z zasad, których realizacji służy prawo dostępu do dokumentów: demokracja, a dokładniej liberalna demokracja w rozumieniu nadanym jej zgodnie z koncepcją dobrych rządów. Taką hierarchię potwierdzają dokumenty i akty prawne wydawane przez instytucje unijne⁵¹⁸, orzecznictwo⁵¹⁹ oraz doktryna⁵²⁰. Prawo dostępu do dokumentów jest jednym z narzędzi, którymi posłużono się, aby realizować postulat demokratyzacji UE w duchu zachodnioeuropejskich i skandynawskich standardów⁵²¹. Stało się ono niezbędnym

⁵¹⁶ *Ibidem*, pkt 58.

⁵¹⁷ *Ibidem*, pkt 45. Tak samo m.in.: Wyrok Trybunału z dnia 17 października 2013 r. w sprawie C-280/11 P, *Rada Unii Europejskiej przeciwko Access Info Europe*, ECLI:EU:C:2013:671, pkt 32; Wyrok Trybunału z dnia 3 lipca 2014 r. w sprawie C-350/12 P, *Rada Unii Europejskiej przeciwko Sophie in 't Veld*, ECLI:EU:C:2014:2039, pkt 53; Wyrok Sądu z dnia 18 września 2015 r. w sprawie T-395/13, *Samuli Miettinen przeciwko Radzie Unii Europejskiej*, ECLI:EU:T:2015:648, pkt 20; Wyrok Sądu z dnia 7 lutego 2018 r. w sprawie T-851/16, *Access Info Europe przeciwko Komisji Europejskiej*, ECLI:EU:T:2018:69, pkt 27.

⁵¹⁸ Począwszy od *deklaracji nr 17* po art. 15 TFUE.

⁵¹⁹ Na przykład odwołując się bezpośrednio do *deklaracji nr 17* (np. Wyrok Sądu pierwszej instancji z dnia 17 czerwca 1998 r. w sprawie T-174/95, *Svenska Journalistförbundet przeciwko Radzie Unii Europejskiej*, ECLI:EU:T:1998:127, pkt 1) czy przez odnotowanie wagi prawa dostępu do dokumentów dla demokracji przez powołanie się na *rozporządzenie 1049/2001* (np. Wyrok Trybunału z dnia 6 marca 2003 r. w sprawie C-41/00 P, *Interporc Im- und Export GmbH przeciwko Komisji Wspólnot Europejskich*, ECLI:EU:C:2003:125, pkt 39).

⁵²⁰ Na przykład „Przejrzystość administracji publicznej jest kluczowa w demokratycznym społeczeństwie. Szeroki dostęp do informacji na temat kwestii będących w ogólnym interesie pozwala obywatelom mieć adekwatny obraz stanu społeczeństwa, w którym żyją, i formułować o nim krytyczne opinie”. W. Hins, D. Voofhoof, *Access to State-Held Information as a Fundamental...*, *op. cit.*, s. 114; czy Pierpaolo Settembri, który stwierdza: „Podsumowując, istnieje kontinuum informacja-odpowiedzialność-demokracja”. P. Settembri, *op. cit.*, s. 641; czy M.E. de Leeuw, *Openness in the legislative process in the European Union*, „*European Law Review*” 2007, t. 32, nr 3, s. 296 oraz K. Lenaerts, *The Principle of Democracy in the Case Law of the European Court of Justice*, „*International and Comparative Law Quarterly*” 2013, t. 62, s. 300 – *passim*.

⁵²¹ Nawet Peter Dyrberg, który opisuje historyczne uwarunkowania rozwoju prawa dostępu do informacji w Szwecji, aby ukazać, że niekoniernie prawo to stanowiło element ustroju demokratycznego uznawany powszechnie jako niezbędny, a jego rozwój był efektem specyficznych relacji między administracją a władzą ustawodawczą w Szwecji, ostatecznie przedstawia argument, zgodnie z którym w „skomplikowanych współczesnych społeczeństwach z ogromnym sektorem publicznym władza ustawodawcza nie jest w stanie na co dzień monitorować administracji i dlatego klasyczny model [w którym to legislatura

elementem gwarancji przejrzystości, otwartości i partycypacji – a tym samym odpowiedzialności i legitymizacji instytucji, zgodnie z demokratycznym charakterem UE.

4.1.3. W poszukiwaniu charakteru prawa dostępu do dokumentów w prawie UE

Już wspomniany powyżej wyrok w sprawie *Królestwo Niderlandów przeciwko Radzie* potwierdzał, że decyzja przyjęta przez Radę w celu uregulowania zasad dostępu do jej dokumentów może tworzyć prawa dla osób trzecich. Tym samym charakter tego zagadnienia jako czysto wewnętrznego i proceduralnego został pośrednio zakwestionowany. Jednocześnie nie została podana w wątpliwość przez TSUE podstawa prawna, na której Rada oparła wydaną przez siebie decyzję. W tym świetle na uwagę zasługuje weryfikowana przez Deirdre Curtin hipoteza, zgodnie z którą prawo dostępu do informacji może być postrzegane przez pryzmat obywatelstwa unijnego. W artykule opublikowanym w 1999 r. twierdziła ona, że:

[...] wszyscy obywatele, jako obywatele żyjący w demokracji, są uprawnieni do wiedzy o tym co się robi w ich imieniu i dlatego ta zasada [dostępu do dokumentów – J.M.] powinna znajdować ogólne zastosowanie niezależnie od przyjęcia danych środków prawnych w zakresie postępowań sądowych⁵²².

Następnie autorka wskazała na związek między prawem dostępu do dokumentów a np. wolnością wyrazu, starając się argumentować za koniecznością postrzegania prawa dostępu do dokumentów przez pryzmat praw podstawowych. Jednocześnie przyznawała ona, że ówczesny sposób regulacji prawa dostępu do dokumentów nie świadczy o takim postrzeganiu tego prawa w UE.

Hipoteza Curtin przedstawia istniejący w doktrynie problem w zakresie analizy rozwoju prawa dostępu do dokumentów w prawie UE, mianowicie próby oceny, czy uzasadniona i na jakich podstawach byłaby interpretacja prawa dostępu do dokumentów jako prawa podstawowego stanowiącego zasadę ogólną prawa unijnego wynikającą z dorobku orzeczniczego ETPCz

nadzorowała administrację – J.M.] musi zostać zrewidowany” oraz stwierdzając, że „dobre działająca demokracja jest zależna od obywateli i debaty opartej na faktach”. P. Dyrberg, *Accountability and Legitimacy: What is the Contribution of Transparency*, [w:] *Accountability and Legitimacy in the European Union*, red. A. Arnulf, D. Wincott, Oxford University Press, Oxford 2002, s. 82.

⁵²² D.M. Curtin, *The fundamental principle of open decision-making and EU (political) citizenship*, [w:] *Legal Issues of the Amsterdam Treaty*, red. D. O’Keeffe, P. Twomey, Hart Publishing, Oxford 1999, s. 73–74.

oraz tradycji konstytucyjnych państw członkowskich⁵²³. Argumentacja przemawiająca za taką wykładnią opierała się na trzech spostrzeżeniach⁵²⁴. Po pierwsze, prawo dostępu do dokumentów powinno być postrzegane jako prawo podstawowe ze względu na jego niezbędność dla demokracji. W tym duchu prawo dostępu do dokumentów powinno być traktowane jako element zawartej w art. 1 TUE zasady otwartości⁵²⁵ i demokracji⁵²⁶, stanowiąc jednocześnie sposób na nadanie tym abstrakcyjnym zasadom treści normatywnej. Po drugie, prawo dostępu do dokumentów może być postrzegane jako niezbędne z punktu widzenia innych praw podstawowych, przede wszystkim wolności wyrazu i dostępu do informacji⁵²⁷. Po trzecie, w orzecznictwie została odnotowana obecność trendu w porządkach prawnych państw członkowskich dotyczącego traktowania prawa dostępu jako zasady konstytucyjnej lub wprowadzonej w ustawodawstwie⁵²⁸.

Mimo tych spostrzeżeń TSUE raczej jest powściągliwy w zakresie uznania prawa dostępu do dokumentów jako zasady ogólnej. Można odnieść wrażenie, że z punktu widzenia przynajmniej części doktryny orzecznictwo dotyczące prawa dostępu do dokumentów to pula straconych szans na „podkreślenie charakteru jawności i dostępu do dokumentów jako praw

⁵²³ Przegląd autorów za i przeciw uznawaniu dostępu do dokumentów za zasadę ogólną prawa UE, zob. U. Öberg, *EU Citizen's Right to Know: The Improbable Adoption of a European Freedom of Information Act*, „Cambridge Yearbook of European Legal Studies” 1999, t. 2, s. 314.

⁵²⁴ Magdalena Elisabeth de Leeuw pisze o dwóch sposobach argumentacji – opierając się na odwołaniu do niezbędności dla demokracji oraz dla innych praw podstawowych, zob. M.E. de Leeuw, *Case C-41/00 P, Interporc Im- und Export GmbH v. Commission of the European Communities, judgment of 6 March 2003*, [2003] ECR I-02125; *Case T-76/02, Mara Messina v. Commission of the European Communities, judgment of 17 September 2003*, nyr; *Case T-47/01, Co-Frutta Soc. Coop. Rl v. Commission of the European Communities, judgment of 16 October 2003*, nyr., „Common Market Law Review” 2004, t. 41, s. 271. W artykule Michaela O’Neilla z kolei pojawia się dodatkowo interpretacja oparta na wspólnych zasadach konstytucyjnych państw członkowskich, i to za jego rozumowaniem podążam w tym podrozdziale, zob. M.O’Neill, *op. cit.*, s. 418–430.

⁵²⁵ O rozwoju tej zasady i nabieraniu przez nią treści normatywnej, zob. A. Alemanno, O. Stefan, *Openness at the Court of Justice of the European Union: Toppling a Taboo*, „Common Market Law Review” 2014, t. 51, s. 103.

⁵²⁶ Zob. M.P. Broberg, *Access to documents: a general principle of Community law?*, „European Law Review” 2002, t. 27, nr 2, s. 204.

⁵²⁷ O problemie relacji między prawem dostępu do dokumentów a prawem dostępu do informacji – zob. dalej w rozdziale.

⁵²⁸ Wyrok Trybunału z dnia 30 kwietnia 1996 r. w sprawie C-58/94, *Królestwo Niderlandów przeciwko Radzie Unii Europejskiej*, ECLI:EU:C:1996:171, pkt 34. W tym duchu na ten temat, zob. M.E. de Leeuw, *Case C-41/00 P, Interporc Im- und Export GmbH v. Commission of the European Communities...*, *op. cit.*, s. 268–274.

podstawowych o wielkiej wadze konstytucyjnej”⁵²⁹. Podobnie w odniesieniu do zasady przejrzystości odmówienie jej statusu zasady ogólnej skutkuje wykluczeniem możliwości „traktowania przejrzystości jako źródła prawa pierwotnego, przez pryzmat którego po pierwsze interpretowane powinny być akty prawa pochodnego oraz, po drugie, na podstawie którego podnosić można by zarzut nieważności działań instytucji i organów Unii wtedy, gdy sprzeczne byłyby one z wymogami przejrzystości”⁵³⁰.

Z związku z powściągliwością TSUE w odniesieniu do tego zagadnienia motorem napędzającym rozwój charakteru prawa dostępu do dokumentów – a za jego pośrednictwem również zasady przejrzystości – w prawie unijnym były zmiany zachodzące na poziomie prawa pierwotnego. To w wyniku aktywności związanych z rewizjami traktatów stanowiących UE prawo dostępu do dokumentów stało się częścią katalogu praw uwzględnionych w KPP jak również było w coraz szerszym zakresie wprowadzane do traktatów⁵³¹. Rozwój prawa dostępu do dokumentów jest świadectwem prób demokratyzacji UE i sprecyzowania aksjologicznego wymiaru integracji europejskiej.

4.1.4. Zbieżność aksjologiczna między prawem dostępu do dokumentów a zasadami prawa ochrony danych osobowych

Zasady, których realizacji służyć ma prawo dostępu do dokumentów, są w pewnym stopniu tożsame z zasadami ustanawiającymi horyzont aksjologiczny regulacji dotyczących ochrony danych osobowych. W katalogu zasad zawartych w art. 5 RODO pojawia się m.in. przejrzystość przetwarzania danych osobowych oraz rozliczalność, czyli odpowiedzialność administratora za wykazanie przestrzegania zasad wymienionych w art. 5 ust. 1. Wymóg przejrzystości przetwarzania podnoszony jest również w dokumentach dotyczących wpływu technologii nazywanych sztuczną inteligencją na wykorzystywanie danych osobowych⁵³². Zwrócenie uwagi na konieczność zagwarantowania, aby zasada przejrzystości odnosiła się nie tylko do informacji udostępnianych na temat przetwarzania danych osobowych jednostce, lecz także do analizy systemów używanych do przetwarzania danych, jest krokiem w stronę zbliżenia tego, jak rozumiana jest przejrzystość w odniesieniu

⁵²⁹ P. Leino, *Case C-64/05 P, Kingdom of Sweden v. Commission of the European Communities and Others, Judgment of the European Court of Justice (Grand Chamber) of 18 December 2007*, nyr, „Common Market Law Review” 2008, t. 45, s. 1486.

⁵³⁰ D. Adamski, *Prawo do informacji...*, s. 51.

⁵³¹ W tym duchu zob. E.H. Van Coller, *Transparency and Access to Documents: A General Principle of European Community Law*, „De Jure” 2006, t. 39, nr 1, s. 168.

⁵³² Zob. Komisja, *Biała księga w sprawie sztucznej inteligencji...*, op. cit., s. 23–24 oraz art. 13 i Tytuł IV: *Obowiązki w zakresie przejrzystości w odniesieniu do określonych systemów sztucznej inteligencji w Akcie w sprawie SI*.

do ochrony danych osobowych, do jej rozumienia w zakresie prawa dostępu do dokumentów.

Pogłębianie poziomu dyskusji na temat roli odgrywanej przez dane osobowe we współczesnym świecie sprzyja odnotowaniu relacji między tym, jak przetwarzane są dane, i demokracją. Wykorzystywanie zautomatyzowanego podejmowania decyzji w marketingu politycznym stało się przyczynkiem dla prób zrozumienia wpływu nowych technologii opartych na analizie danych na procesy demokratyczne. Wiedza o tym, w jaki sposób systemy zautomatyzowanego podejmowania decyzji działają – czyli ich przejrzystość – jest jednym z elementów niezbędnych do zagwarantowania ich zgodności z demokratycznymi procedurami. Stąd częściowa zbieżność zasad, których realizacji ma służyć prawo dostępu do dokumentów i które kształtują warunki przetwarzania danych osobowych zgodnie z europejskimi standardami, może stanowić argument za możliwością rozważenia systemów zautomatyzowanego podejmowania decyzji jako dokumentów podlegających prawu dostępu w świetle prawa UE. Przejrzystość przetwarzania jest zagadnieniem istotnym nie tylko z punktu widzenia podmiotu danych i ochrony jego praw, np. prawa do niedyskryminacyjnego traktowania, lecz również z punktu widzenia całego społeczeństwa, kiedy stawką jest np. ważność wyborów czy referendum.

W celu rozważenia możliwości postrzegania kolektywnego wymiaru wpływu zautomatyzowanego podejmowania decyzji jako przemawiającego za uznaniem wagi dostępu do samych algorytmów opartym na prawie dostępu do dokumentów unijnych niezbędne jest określenie treści tego prawa w prawie UE.

4.2. Treść prawa dostępu do dokumentów unijnych w prawie UE

W przeciwieństwie do kwestii wzmacniania statusu prawa dostępu do dokumentów w prawie UE, orzecznictwo TSUE odegrało natomiast ważną rolę w odniesieniu do wykładni samej treści prawa dostępu do dokumentów. To w orzecznictwie można odnaleźć odpowiedzi na pytania dotyczące wyjaśnienia, jak należy rozumieć termin „dokument”, do jakich sfer działalności instytucji unijnych odnosi się prawo dostępu do dokumentów i jak należy rozumieć od niego wyjątki – którym jest poświęcony ten podrozdział.

4.2.1. Konceptualizacja relacji prawa dostępu do dokumentów unijnych i prawa dostępu do informacji w UE

Opisana powyżej historia rozwoju prawa dostępu do dokumentów w prawie UE ukazuje brak spójności pojęciowej obecny od początku dyskusji nad tą kwestią na forum wspólnotowym. Sformułowanie „dostęp do informacji” zostało na etapie prac prowadzonych na początku lat 90. przez Komisję

zastąpione terminem „dostęp do dokumentów” i w tej formie stało się przedmiotem unijnych regulacji zarówno na poziomie traktatów, jak i w *rozporządzeniu 1049/2001*. Jak staram się wykazać poniżej, mimo szerokiej definicji dokumentu w prawie UE⁵³³, koncentracja na dostępie do dokumentów, nie zaś dostępie do informacji, jest – w związku z opisanym rozwojem orzecznictwa ETPCz – znacząca z punktu widzenia treści normatywnej analizowanych praw.

Zgodnie z art. 3 lit. a *rozporządzenia 1049/2001* dokument to „wszelkie treści bez względu na nośnik (zapisane na papierze, przechowywane w formie elektronicznej czy jako dźwięk, nagranie wizualne czy audiowizualne) dotyczące kwestii związanych z polityką, działalnością i decyzjami mieszczącymi się w sferze odpowiedzialności tych instytucji”. Należy zauważyć, że definicja ta uległa rozszerzeniu w stosunku do swojej pierwotnej formy zawartej w Kodeksie, w świetle której dokumentem był „każdy pisany tekst, niezależnie od medium, na którym został zapisany, który zawiera istniejące dane i jest w posiadaniu Rady lub Komisji”⁵³⁴. Obecnie jako dokument traktowana może być właściwie każda treść, jak długo jest ona zapisana na określonym nośniku – czy to fizycznym, czy w formie elektronicznej. Warunkiem niezbędnym do uznania danej treści za dokument jest fakt jej utrwalenia. Jak stwierdził Sąd w wyroku *Julien Dufour przeciwko Europejskiemu Bankowi Centralnemu* na tle definicji dokumentu w *decyzji 2004/258/WE* dotyczącej dostępu publicznego do dokumentów EBC⁵³⁵: „mowa jest o treści utrwalonej, którą po jej stworzeniu można odtworzyć lub z którą można się zapoznać. Zatem elementy nieutrwalone nie stanowią dokumentów, nawet jeśli są znane EBC”⁵³⁶. Ryzyko, że „istotne informacje zostaną zapisane w formie wypadającej z tej kategorii [dokumentu – J.M.]”⁵³⁷ pozostaje jednak aktualne. Jak wskazałam powyżej, konieczne jest utrwalenie danej informacji. Jeśli jest ona np. jedynie przekazywana ustnie i nie zostanie zapisana, nie można uwzględnić jej jako przedmiotu podlegającego prawu dostępu do dokumentów.

⁵³³ Szczegółowe omówienie definicji dokumentu w prawie unijnym, zob. L. Rossi, P. Vinagre e Silva, *op. cit.*, s. 89–125.

⁵³⁴ Sekcja *General Principle* w: Kodeks.

⁵³⁵ *Decyzja Europejskiego Banku Centralnego z dnia 4 marca 2004 r. w sprawie publicznego dostępu do dokumentów Europejskiego Banku Centralnego (EBC/2004/3)* (decyzja 2004/258/WE), Dz.Urz. UE 2004 L 80, s. 42–44. Uwagi TSUE przedstawione na tle *decyzji 2004/258/WE* zasługują na uwzględnienie w związku z faktem, że definicje dokumentu w tej decyzji i w *rozporządzeniu 1049/2001* są właściwie tożsame.

⁵³⁶ Wyrok Sądu z dnia 26 października 2011 r. w sprawie T-436/09, *Julien Dufour przeciwko Europejskiemu Bankowi Centralnemu*, ECLI:EU:T:2011:634, pkt 88.

⁵³⁷ P. Keller, *European and International Media Law. Liberal Democracy, Trade, and the New Media*, Oxford University Press, Oxford 2011, s. 293.

Ponadto rozszerzeniu uległ katalog podmiotów, w których posiadaniu mogą być dokumenty, do których dostęp powinien być udzielony w związku z uwzględnieniem w art. 15 TFUE wszystkich instytucji, organów i jednostek organizacyjnych UE. Na podkreślenie zasługuje fakt, że *rozporządzenie 1049/2001* doprowadziło do odejścia od zasady autorstwa. W jej świetle instytucje nie mogły udzielać dostępu do dokumentów, które sporządzone zostały przez stronę trzecią⁵³⁸. Teoretycznie w wyniku przyjęcia *rozporządzenia 1049/2001* zasada autorstwa została usunięta z prawa UE⁵³⁹. Obecnie zgodnie z treścią art. 2 ust. 3 *rozporządzenia 1049/2001* prawo dostępu do dokumentów dotyczy dokumentów „przechowywanych przez instytucje, tj. dokumentów sporządzanych lub otrzymywanych przez nie i pozostających w ich posiadaniu, na wszystkich obszarach działalności Unii Europejskiej”. Odnosi się ono zatem również do tych dokumentów, które znalazły się w posiadaniu instytucji UE, chociaż zostały stworzone np. przez instytucje państw członkowskich. Tym samym drugorzędne – chociaż, jak wykazuję dalej w rozdziale, nie całkowicie pozbawione znaczenia – staje się pytanie, kto dokument przygotował. Kluczowe dla możliwości żądania dostępu do niego jest natomiast, aby: (1) był on w formie zarejestrowanej na jakimkolwiek medium, (2) był w posiadaniu unijnych instytucji oraz (3) dotyczył kwestii związanych z polityką, działalnością i decyzjami mieszczącymi się w sferze odpowiedzialności tych instytucji. Tym samym mogłoby się wydawać, że zakres znaczeniowy pojęcia „dokument” w prawie UE jest relatywnie szeroki.

Mimo szerokiego ujęcia znaczenia „dokumentu” taki sposób określenia przedmiotu prawa dostępu do dokumentów generuje jednak możliwe rozbieżności interpretacyjne między prawem dostępu do dokumentów a prawem dostępu do informacji. Częściowo problem ten został zauważony w orzeczeniu w sprawie *Rada UE przeciwko Heidi Hautala*⁵⁴⁰. Sprawa dotyczyła fińskiej europarlamentarzystki, która zwróciła się do Rady z wnioskiem o dostęp do dokumentów dotyczących unijnych kryteriów eksportu broni. Rada odmówiła jej dostępu do raportu dotyczącego tego zagadnienia, powołując się na wyjątek, uwzględniony w art. 4 ust. 1 *decyzji Rady 93/731/WE*, dotyczący możliwości powołania się na interes publiczny w postaci relacji z państwami trzecimi w celu uzasadnienia odmowy dostępu

⁵³⁸ Na ten temat zob. M.E. de Leeuw, *Case C-41/00 P, Interporc Im- und Export GmbH v. Commission of the European Communities...*, *op. cit.*, s. 274–279.

⁵³⁹ Chociaż art. 4 ust. 5 daje możliwość państwom członkowskim w zakresie ograniczenia dostępu do dokumentów od nich pochodzących – art. 4 ust. 5: „Państwo Członkowskie może zażądać od instytucji nieujawniania dokumentu pochodzącego od tego Państwa Członkowskiego bez jego uprzedniej zgody” – *rozporządzenie 1049/2001*. O kontrowersjach związanych z tym zagadnieniem dalej w rozdziale.

⁵⁴⁰ Wyrok Trybunału z dnia 6 grudnia 2001 r. w sprawie C-353/99 P, *Rada Unii Europejskiej przeciwko Heidi Hautala*, ECLI:EU:C:2001:661.

do dokumentu. W wyroku Sądu stwierdzono, że *decyzja 93/731* nie nakazuje Radzie rozważenia, czy możliwe jest udzielenie częściowego dostępu do dokumentów. Jednocześnie nie zakazuje ona wprost postąpienia w ten sposób⁵⁴¹. Następnie Sąd powołał się kolejno na ogólną zasadę mówiącą o jak najszerszym dostępie do dokumentów i konieczność wykładni wyjątków od niej w sposób ścisły. Powołując się na zasadę proporcjonalności, stwierdził on, że cel w postaci ochrony interesu publicznego w odniesieniu do stosunków międzynarodowych mógłby zostać osiągnięty poprzez usunięcie przez Radę tych fragmentów raportu, które mogłyby skutkować szkodą dla tego interesu. Sąd zastrzegł jednocześnie, że gdyby analiza raportu i usuwanie z niego fragmentów mogących zaszkodzić chronionemu interesowi okazały się nadmiernie pracochłonne⁵⁴², Rada powinna wyważyć między interesem w postaci publicznego dostępu do dokumentów a ochroną dobrej administracji. Ostateczną konkluzją Sądu była konieczność – w związku z wykładnią *decyzji 93/731* w świetle zasady prawa do informacji (*the principle of the right to information*) oraz zasady proporcjonalności – sprawdzenia przez instytucję, czy możliwy jest częściowy dostęp do informacji, które nie są objęte wyjątkiem.

Twierdzenie Sądu, że prawo dostępu do dokumentów stanowi *de facto* prawo do informacji, i w związku z tym Rada powinna była rozważyć częściowy dostęp do dokumentu, stało się przedmiotem apelacji wniesionej przez Radę do Trybunału. Trybunał stwierdził, że błędne jest twierdzenie, jakoby *decyzja 93/731* odnosiła się jedynie do dokumentów, nie zaś do informacji w nich zawartych⁵⁴³. Ponadto Trybunał stwierdził, że odmówienie dostępu do informacji zawartych w danym dokumencie, które nie są objęte wyjątkami przewidzianymi w *decyzji 93/731*, ograniczałoby skuteczność prawa dostępu do dokumentów. Potwierdzona została konieczność wykładni wyjątków w świetle zasady proporcjonalności oraz wyważenia interesów między dostępem do dokumentów a dobrą administracją. Trybunał nie uznał za konieczne – w świetle przedstawionych ustaleń – by odnieść się do argumentów podniesionych przez Radę i rząd Hiszpanii, dotyczących błędnego oparcia wyroku przez Sąd na istnieniu zasady dostępu do informacji.

⁵⁴¹ Wyrok Sądu pierwszej instancji z dnia 19 lipca 1999 r. w sprawie T-14/98, *Heidi Hautala przeciwko Radzie Unii Europejskiej*, ECLI:EU:T:1999:157, pkt 78.

⁵⁴² „W szczególnych wypadkach, gdyby ilość dokumentów lub fragmentów, które należałoby usunąć, skutkowało nieracjonalną ilością pracy administracyjnej koniecznej do wykonania, Rada mogłaby dokonać wyważenia interesów publicznego dostępu do tych fragmentów i ciężaru pracy wywołanego przez konieczność wykonania tych czynności”. Wyrok Sądu pierwszej instancji z dnia 19 lipca 1999 r. w sprawie T-14/98, *Heidi Hautala przeciwko Radzie Unii Europejskiej*, ECLI:EU:T:1999:157, pkt 86.

⁵⁴³ Wyrok Trybunału z dnia 6 grudnia 2001 r. w sprawie C-353/99 P, *Rada Unii Europejskiej przeciwko Heidi Hautala*, ECLI:EU:C:2001:661, pkt 23.

Apelacja Rady została odrzucona jedynie na podstawie stwierdzenia, że Rada była zobowiązana dokonać analizy możliwości udzielenia częściowego dostępu do informacji niechronionych wyjątkami przewidzianymi w *decyzji 93/731*.

Orzeczenia Sądu i Trybunału w sprawach *Heidi Hautala przeciwko Radzie i Rada przeciwko Heidi Hautali* są do pewnego stopnia rewolucyjne w zakresie problemu definiowania terminu „dokument” w prawie unijnym. Jednym z ich pośrednich efektów było wprowadzenie regulacji dostępu częściowego do art. 4 ust. 6 *rozporządzenia 1049/2001*⁵⁴⁴. Podchodząc jednak do nich – mimo to – sceptycznie, należy zauważyć, że Sąd wprost uznał istnienie zasady prawa do informacji⁵⁴⁵, ale Trybunał nie skorzystał z możliwości odniesienia się do tego zagadnienia. Nie została więc zakwestionowana sama istota prawa dostępu do dokumentów w prawie unijnym: pozostaje ono zależne od istnienia dokumentu. Zmiana, którą wprowadziło orzeczenie *Rada przeciwko Heidi Hautala*, odnosi się do zawartości dokumentu. Prawo dostępu do dokumentów obejmuje nie dokument w formie, w jakiej jest on w posiadaniu danej instytucji, lecz – przez ów dokument – do informacji, które w nim się znajdują.

Aktualny pozostaje również problem odnotowany w doktrynie⁵⁴⁶ różnicy między prawem dostępu do dokumentów a prawem dostępu do informacji w kontekście rozróżnienia między porządkami prawnymi państw członkowskich w zestawieniu z unijnym. W ramach relacji między prawem dostępu do dokumentów a prawem dostępu do informacji należy odnotować węższy zakres pierwszego z wymienionych praw⁵⁴⁷. Dlatego też z perspektywy obywateli państw członkowskich o silnej tradycji otwartego rządu i szerokiego postrzegania dostępu do informacji koncentracja na dostępie do dokumentów może być postrzegana jako błąd. Przykładem takiego stanowiska jest komentarz Päivi Leino w odniesieniu do analizy przedstawionej w wyroku *Rada*

⁵⁴⁴ „Jeśli wyjątki dotyczą jedynie części tego dokumentu, pozostałe części dokumentu powinny być ujawnione” – art. 4 ust. 6, *rozporządzenie 1049/2001*.

⁵⁴⁵ Zob. D.M. Curtin, *Citizens' Fundamental Right of Access to EU Information: an Evolving Digital Passepartout?*, „Common Market Law Review” 2000, t. 37, s. 14.

⁵⁴⁶ Na przykład Bart Driessen, który wymienia elementy wchodzące w skład przejrzystości na poziomie UE, w tym m.in. osobno publiczny dostęp do dokumentów i publiczny dostęp do informacji. Zob. B. Driessen, *Transparency in EU Institutional Law. A Practitioner's Handbook. Second, Completely Revised Edition*, Kluwer Law International, Alphen aan den Rijn 2012, s. 4.

⁵⁴⁷ Zob. o posłużeniu się terminem dokumentu w prawie Wspólnot Europejskich: „Tak sformułowany obowiązek był więc węższy niż wynikający z ustawodawstwa większości państw europejskich (np. Szwecji i Finlandii), gdzie obywatelom przyznaje się «prawo do informacji»”. M. Szwarc, *Zasady wglądu do dokumentów instytucji Wspólnot Europejskich*, „Państwo i Prawo” 2001, z. 11, s. 70 czy D.M. Curtin, *Citizens' Fundamental Right of Access to EU Information: an Evolving Digital Passepartout?*, *op. cit.*, s. 16.

przeciwko Heidi Hautali. Nieco złośliwie zauważa ona, że uwzględnianie pracochłonności analizy dotyczącej tego, które elementy danego dokumentu powinny być wyjęte spod zakresu wyjątku przywoływanego przez instytucje i powoływanie się przy tym na interes w postaci dobrej administracji jest – z jej skandynawskiej perspektywy – „nieco dziwne”⁵⁴⁸.

4.2.2. Relacja między prawem dostępu do dokumentów w prawie UE a prawem dostępu do informacji w orzecznictwie ETPCz – nieobecny art. 11 KPP

Problematyczne jest również porównanie wykładni prawa dostępu do dokumentów w prawie unijnym z tym, jaką ewolucję przeszło prawo dostępu do informacji w orzecznictwie ETPCz⁵⁴⁹. Opisany proces uznawania przez ETPCz tego, że art. 10 EKPCz powinien być interpretowany jako zawierający prawo dostępu do informacji, pozostaje niezauważony przez TSUE. Zawartość art. 11 KPP, którego treść wykładana powinna odpowiadać prawom uwzględnionym w art. 10 EKPCz, mogłaby być postrzegana jako element gwarantowania prawa dostępu do informacji w prawie UE. Zgodnie z art. 52 ust. 3 KPP przepis art. 11 „ma mieć takie samo znaczenie i zakres jak ten, który wynika z art. 10 EKPCz”⁵⁵⁰. Tymczasem zasada ta nie znajduje odzwierciedlenia w wykładni art. 11 KPP proponowanej przez TSUE.

W orzecznictwie TSUE i w opiniach rzeczników generalnych odwołania do przełomowego orzecznictwa ETPCz dotyczącego art. 10 EKPCz, opisywanego w rozdziale trzecim w odniesieniu do zagadnienia prawa dostępu do dokumentów i informacji⁵⁵¹, pojawiły się cztery razy⁵⁵², tj.: dwukrotnie

⁵⁴⁸ P. Leino, *Case C-353/99 P, Council v. Heidi Hautala, judgment of the Full Court of 6 December 2001, nyr, appeal against the judgment of the Court of First Instance of 19 July 1999 in Case T-14/98, Hautala v. Council, [1999] II-2489*, „Common Market Law Review” 2002, t. 39, s. 631–632.

⁵⁴⁹ Zagadnienie to jest analizowane w: D. Adamski, *Rozdział II: Unijne modele regulacji jawności i jej ograniczeń oraz ich wpływ na systemy krajowe*, [w:] *Standardy europejskie (Jawność i jej ograniczenia, t. XI)*, red. C. Mik, C.H. Beck, Warszawa 2016.

⁵⁵⁰ *Karta Praw Podstawowych Unii Europejskiej. Komentarz, op. cit.*, s. 4 (do art. 11).

⁵⁵¹ TSUE odwoływał się do np. wyroku ETPCz w sprawie *Magyar Helsinki Bizottság* w kontekście wpływu NGO na życie publiczne, zob. Wyrok Trybunału z dnia 18 czerwca 2020 r. w sprawie C-78/18, *Komisja Europejska przeciwko Węgrom*, ECLI:EU:C:2020:476 czy opinia rzecznika generalnego Eleanor Sharpston przedstawiona w dniu 12 października 2017 r. w sprawie C-664/15, *Protect Natur-, Arten- und Landschaftschutz Umweltorganisation przeciwko Bezirkshauptmannschaft Gmünd*, ECLI:EU:C:2017:760.

⁵⁵² Do czasu redakcji przeze mnie treści tego rozdziału w czerwcu 2020 r. Poszukiwanie odpowiednich spraw przeprowadziłam przez sprawdzenie m.in. następujących kombinacji wyszukiwań w Curii: (1) ‘article 10 of the ECHR’ ‘access to information’; (2) ‘Magyar Helsinki Bizottság’; (3) ‘Társaság a Szabadságjogokért’; (4) ‘Sdružení Jihočeské Matky’; (5) ‘Youth Initiative for Human Rights’; (6) ‘Article 10’ ‘article 11’ ‘charter’ ‘ECHR’ ‘access to information’. Analogiczne wyszukiwanie przeprowadziłam w lipcu

w opiniach rzeczników generalnych⁵⁵³ oraz dwukrotnie w treści wyroków Sądu⁵⁵⁴. Ze względu na tak skromny zbiór dokumentów sądowych poruszających to zagadnienie warto zwrócić uwagę na wszystkie wzmianki dotyczące relacji między art. 11 KPP i orzecznictwem ETPCz dotyczącym art. 10 EKPCz. Opinia rzecznika generalnego Michała Bobeka w sprawie *KE przeciwko Patrickowi Breyerowi* dotyczyła decyzji Komisji w sprawie wniosku o dostęp do dokumentów złożonego przez Patricka Breyera odnoszących się do transpozycji przez Austrię *dyrektywy 2006/24/WE* oraz do pism procesowych złożonych przez Republikę Austrii w ramach sprawy C-189/09 między Komisją Europejską a Austrią, która zakończyła się wydaniem wyroku w dniu 29 lipca 2010 r.⁵⁵⁵ Sąd uznał, że decyzja Komisji oparta na argumentach, zgodnie z którym pisma nie wchodziły w zakres *rozporządzenia 1049/2001*, była błędna. Komisja, w odwołaniu od wyroku Sądu, argumentowała, że art. 15 ust. 3 akapit 4 TFUE zakazuje prawodawcy Unii rozciągania prawa dostępu do dokumentów instytucji na dokumenty mające związek z działalnością orzeczniczą TSUE⁵⁵⁶.

Rzecznik generalny w swojej opinii odwołał się do wyroku w sprawie *Társaság a Szabadságjogokért przeciwko Węgrom*⁵⁵⁷ ze względu na fakt, że wyrok ETPCz odnosił się do dostępu do informacji dotyczących postępowania sądowego. Rzecznik generalny stwierdził, że:

Trybunał podlega zasadzie otwartości, która znajduje zastosowanie także do jego działalności orzeczniczej. Wolność otrzymywania informacji, gwarantowana na gruncie art. 11 ust. 1 [K]arty i podlegająca wykładni poprzez art. 52 ust. 3

2021 r. i nie przyniosło ono nowych wyników, które miałyby znaczenie dla zagadnień omawianych w książce.

⁵⁵³ Opinia rzecznika generalnego Michała Bobeka przedstawiona w dniu 21 grudnia 2016 r. w sprawie C-213/15 P, *Komisja przeciwko Patrickowi Breyerowi*, ECLI:EU:C:2016:994 oraz opinia rzecznika generalnego Juliane Kokott przedstawiona w dniu 8 września 2009 r. w sprawie C-139/07 P, *Komisja Wspólnot Europejskich przeciwko Technische Glaswerke Ilmenau GmbH*, ECLI:EU:C:2009:520.

⁵⁵⁴ Wyrok Sądu z dnia 23 stycznia 2017 r. w sprawie T-727/15, *Association Justice & Environment, z.s. przeciwko Komisji Europejskiej*, ECLI:EU:T:2017:18 oraz Wyrok Sądu z dnia 29 listopada 2012 r. w sprawie T-590/10, *Gabi Thesing i Bloomberg Finance LP przeciwko Europejskiemu Bankowi Centralnemu*, ECLI:EU:T:2012:635.

⁵⁵⁵ Wyrok Trybunału z dnia 29 lipca 2010 r. w sprawie C-189/09, *Komisja Europejska przeciwko Republice Austrii*, ECLI:EU:C:2010:455.

⁵⁵⁶ Wyrok Trybunału z dnia 18 lipca 2017 r. w sprawie C-213/15 P, *Komisja przeciwko Patrickowi Breyerowi*, ECLI:EU:C:2017:563.

⁵⁵⁷ Opinia rzecznika generalnego Michała Bobeka przedstawiona w dniu 21 grudnia 2016 r. w sprawie C-213/15 P, *Komisja przeciwko Patrickowi Breyerowi*, ECLI:EU:C:2016:994, pkt 88.

karty i art. 10 konwencji o ochronie praw człowieka przez ETPC, także wyraźnie sugeruje większy stopień otwartości⁵⁵⁸.

Odwołanie do orzeczenia ETPCz stanowiło punkt wyjścia do szerszych rozważań dotyczących problemu otwartości sądów. Treść rozważań rzecznika generalnego nie została jednak odzwierciedlona w wyroku Trybunału. Co prawda odwołał się on do „otwartości”, jednak w treści orzeczenia brak nawiązania do aktywności ETPCz w zakresie problematyki dostępu do informacji.

Podobnie stało się w wypadku postępowania w sprawie *Komisja przeciwko Technische Glaswerke Ilmenau GmbH*⁵⁵⁹, w którym odwołanie do orzecznictwa ETPCz odegrało jeszcze bardziej marginalną rolę. Opinia rzeczniczki generalnej Juliane Kokott odsyła do wyroków w sprawach *Társaság a Szabadságjogokért przeciwko Węgrom* oraz *Kenedi przeciwko Węgrom* jedynie w przypisie nr 18, w nawiązaniu do art. 42 KPP. Użyte w nim zostało sformułowanie, zgodnie z którym art. 10 EKPCZ: „obejmuje także prawo dostępu do informacji [...], w przypadku gdy te informacje są niezbędne dla wolności wyrażania opinii”⁵⁶⁰. Rzeczniczka nie odwołała się przy tej okazji do art. 11 KPP. Co więcej, w przypisie uwzględniła również odwołania do starszego orzecznictwa ETPCz (m.in. w sprawie *Leander przeciwko Szwecji czy Guerra i inni przeciwko Włochom*), w pewien sposób symbolicznie umniejszając rolę zmiany linii orzeczniczej ETPCz w tej kwestii. W swoim wyroku w sprawie *Komisja Wspólnot Europejskich przeciwko Technische Glaswerke Ilmenau GmbH* Trybunał w żaden sposób nie nawiązał do orzecznictwa ETPCz.

Ciekawszego materiału dostarcza wyrok Sądu w sprawie *Association Justice & Environment, z.s. przeciwko Komisji Europejskiej*. Sprawa dotyczyła wniosku stowarzyszenia Association Justice & Environment o dostęp do dokumentów dotyczących postępowania toczącego się przeciwko Czechom w zakresie stosowania *Dyrektywy Parlamentu Europejskiego i Rady 2008/50/WE z dnia 21 maja 2008 r. w sprawie jakości powietrza i czystszej powietrza dla Europy*⁵⁶¹. W swoim wniosku stowarzyszenie wskazało na istnienie nadrzędnego interesu publicznego, w postaci ochrony jakości

⁵⁵⁸ *Ibidem*, pkt 90.

⁵⁵⁹ Wyrok Trybunału z dnia 29 czerwca 2010 r. w sprawie C-139/07 P, *Komisja Europejska przeciwko Technische Glaswerke Ilmenau GmbH*, ECLI:EU:C:2010:376.

⁵⁶⁰ Przypis 18 (do punktu 47), opinia rzecznika generalnego Juliane Kokott przedstawiona w dniu 8 września 2009 r. w sprawie C-139/07 P, *Komisja Wspólnot Europejskich przeciwko Technische Glaswerke Ilmenau GmbH*, ECLI:EU:C:2009:520.

⁵⁶¹ *Dyrektywa Parlamentu Europejskiego i Rady 2008/50/WE z dnia 21 maja 2008 r. w sprawie jakości powietrza i czystszej powietrza dla Europy*, Dz.Urz. UE 2008 L 152, s. 1–44.

powietrza oraz ochrony zdrowia, który przemawiał za udostępnieniem żądanych dokumentów. Komisja odrzuciła zarówno pierwszy wniosek stowarzyszenia, jak i wniosek potwierdzający, opierając się na wyjątku z art. 4 ust. 2 *rozporządzenia 1049/2001* dotyczącego ochrony celów kontroli, śledztw i audytu⁵⁶². Nie zgodziła się ona również z argumentem, jakoby istniał nadrzędny interes publiczny, który uzasadniałby odstępianie od wyjątku.

W swojej skardze do Sądu stowarzyszenie przywołało jako argument przemawiający za anulowaniem decyzji Komisji m.in. orzecznictwo dotyczące art. 10 EKPCz. W tym świetle w skardze pojawiło się odwołanie do art. 11 KPP jako chroniącego wolność wyrazu, a zatem również wolność otrzymywania informacji. Argumenty przedstawione przez stowarzyszenie za zmianą linii orzeczniczej TSUE w zakresie wykładni dotyczącej warunków powoływania się na nadrzędny interes publiczny nie spotkały się z uznaniem Sądu. Sąd potwierdził, że art. 11 KPP powinien być postrzegany jako odpowiadający art. 10 EKPCz⁵⁶³. Zauważył jednak, że do czasu przystąpienia UE do EKPCz Konwencja nie stanowi aktu prawnego formalnie włączonego do prawa unijnego⁵⁶⁴. Choć zgodnie z art. 52 ust. 3 KPP „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”, to orzecznictwo TSUE podkreśla, że tożsamość wykładni znaczenia i zakresu tych praw nie może jednocześnie naruszać autonomii prawa UE i TSUE⁵⁶⁵.

Ten krytycznie nastawiony do potencjalnego wpływu orzecznictwa ETPCz na wykładnię TSUE *passus* kończy akapit stwierdzający, że przywołane przez stowarzyszenie Association Justice & Environment orzecznictwo ETPCz nie jest istotne dla sprawy toczącej się przed Sądem. Sąd stwierdził, że po pierwsze, żadne z orzeczeń nie dotyczyło dostępu do informacji w ramach otoczenia regulacyjnego porównywalnego do tego opartego na *rozporządzeniu 1049/2001*. Po drugie zaś, żadne z przywoływanych przez stronę

⁵⁶² W wypadku drugiej decyzji, odwołując się do ogólnego domniemania dotyczącego nieujawniania dokumentów postępowania w sprawie uchybienia zobowiązaniom państwa członkowskiego na etapie poprzedzającym wniesienie skargi – zob. Wyrok Sądu z dnia 23 stycznia 2017 r. w sprawie T-727/15, *Association Justice & Environment, z.s. przeciwko Komisji Europejskiej*, ECLI:EU:T:2017:18, pkt 6.

⁵⁶³ Wyrok Sądu z dnia 23 stycznia 2017 r. w sprawie T-727/15, *Association Justice & Environment, z.s. przeciwko Komisji Europejskiej*, ECLI:EU:T:2017:18, pkt 70.

⁵⁶⁴ *Ibidem*, pkt 71.

⁵⁶⁵ *Ibidem*, pkt 72 i przywołane tam orzecznictwo: Wyrok Trybunału z dnia 15 lutego 2016 r. w sprawie C-601/15 PPU, *J.N. przeciwko Staatssecretaris van Veiligheid en Justitie*, ECLI:EU:C:2016:84, pkt 47 oraz Wyrok Trybunału z dnia 28 lipca 2016 r. w sprawie C-294/16 PPU, *JZ przeciwko Prokuraturze Rejonowej Łódź-Śródmieście*, ECLI:EU:C:2016:610, pkt 50.

postępowania orzeczeń „nie dotyczyło odmowy dostępu do dokumentów w celu ochrony celów śledztwa, a w szczególności ochrony atmosfery niezbędnej poufności na etapie poprzedzającym wniesienie skargi”⁵⁶⁶. Na podstawie m.in. tych przyczyn Sąd odmówił uznania argumentów dotyczących EKPCz i KPP przedstawionych przez stowarzyszenie.

Ostatnia sprawa, w której przywołane zostało orzecznictwo ETPCz na temat dostępu do informacji, *Gabi Thesing i Bloomberg Finance LP przeciwko Europejskiemu Bankowi Centralnemu*, dotyczyła sporu między dziennikarką a EBC. Gabi Thesing – jako dziennikarka Bloomberg Finance LP – chciała uzyskać dostęp do dwóch dokumentów dotyczących sytuacji finansowej Grecji. Odmowa EBC opierała się na odwołaniu do ochrony interesu publicznego w postaci polityki gospodarczej UE i Grecji oraz ochrony wewnętrznych procedur decyzyjnych i konsultacji EBC, a także – w odniesieniu do drugiego z dokumentów – na ochronie interesów handlowych osób fizycznych lub prawnych⁵⁶⁷.

Sąd w tym wypadku podjął się bardziej szczegółowej analizy w celu wykazania, z jakiej przyczyny przywołane przez stronę orzecznictwo ETPCz dotyczące art. 10 nie jest istotne z punktu widzenia rozpatrywanej przez niego sprawy⁵⁶⁸. Na przykład w odniesieniu do sprawy *Kenedi przeciwko Węgrom* Sąd wykazuje, że analizowane tam ograniczenie nie było przewidziane w prawie – podczas gdy w sprawie *Gabi Thesing i Bloomberg Finance LP przeciwko Europejskiemu Bankowi Centralnemu* było. W wypadku sprawy *Társaság a Szabadságjogokért przeciwko Węgrom* Sąd powołuje się z kolei na różnicę w stanie faktycznym, który w tym przypadku dotyczył problemu danych osobowych zawartych w żądanej informacji. Sprawa rozpatrywana przez Sąd – w jego argumentacji – nie dotyczyła natomiast tego problemu.

Opisane sprawy ukazują niechęć TSUE do uznania prawa dostępu do informacji zgodnego z wykładnią ETPCz jako wiążącego w świetle praw UE. Sam fakt ich niewielkiej liczebności świadczy o ignorowaniu zmiany w wykładni EKPCz, która dokonała się w czasie ostatniej dekady opisanej w poprzednim rozdziale. Natomiast te wzmianki, które pojawiły się w opiniach rzeczników generalnych oraz orzeczeniach Sądu, nie odnoszą się do samej esencji problemu różnicy między prawem dostępu do dokumentów a prawem do informacji. TSUE bazuje na proceduralnym postrzeganiu prawa

⁵⁶⁶ Wyrok Sądu z dnia 23 stycznia 2017 r. w sprawie T-727/15, *Association Justice & Environment, z.s. przeciwko Komisji Europejskiej*, ECLI:EU:T:2017:18, pkt 73.

⁵⁶⁷ Odpowiednio art. 4 ust. 1 lit. a, art. 4 ust. 3 oraz art. 4 ust. 2 akapit 1, *decyzja 2004/258/WE*.

⁵⁶⁸ Ponieważ orzecznictwo TSUE dotyczące „autonomii prawa UE” w świetle relacji między EKPCz a KPP pojawiło się w 2016 r., to przyczyną stojącą za większym wysiłkiem w celu udowodnienia braku relewantności orzecznictwa ETPCz dla sprawy może być niemożność odwołania się do tego argumentu.

dostępu do dokumentów. Brak w nim miejsca na optykę pozwalającą spojrzeć na dostęp do dokumentów jako problem związany z wolnością wyrazu i jako narzędzie gwarantujące możliwości prowadzenia debaty publicznej.

Świadectwem takiej wykładni jest brak dostrzeżenia szczególnej roli, jaką mogą mieć do odegrania watchdogi⁵⁶⁹. Zważywszy na fakt, że stronami dwóch postępowań przed Sądem, w których pojawiły się nawiązania do orzecznictwa ETPCz, były organizacja pozarządowa oraz dziennikarka, zaskakujący jest brak odwołania w wyrokach do twierdzeń ETPCz dotyczących specjalnej pozycji organizacji pozarządowych i mediów w odniesieniu do korzystania z prawa do informacji – przy jednoczesnym odnotowywaniu ich wagi dla debaty publicznej⁵⁷⁰. W przeciwieństwie do orzecznictwa ETPCz, TSUE nie odnotowuje wagi, jaką działalność NGO lub dziennikarki może mieć dla jakości debaty publicznej, oraz pomija w swej analizie fakt, że żądane przez nich informacje miałyby być udostępnione społeczeństwu. W wykładni TSUE prawo dostępu do informacji jest raczej prawem jednostki wnioskującej o dostęp do dokumentu niż prawem społeczeństwa do bycia poinformowanym o danych faktach.

Za stanowiskiem takim stoi przywiązanie do konieczności ochrony autonomii prawa UE kosztem zgodności wykładni KPP z wykładnią EKPCz. Szczególnie problematyczne w tym świetle jest powoływanie się przez Sąd na fakt, że ograniczenie analizowane w wyroku *Gabi Thesing i Bloomberg Finance LP przeciwko Europejskiemu Bankowi Centralnemu* było przewidziane w prawie. Zgodnie z wykładnią ETPCz wprowadzane wobec prawa do informacji ograniczenia powinny m.in. być niezbędne w demokratycznym społeczeństwie, który to wymóg Sąd ignoruje w swojej analizie⁵⁷¹. Wybiórcze traktowanie warunków umożliwiających powołanie się na prawo dostępu do informacji sformułowanych przez ETPCz wprowadza interpretacyjne zamieszanie i pośrednio kwestionuje autonomiczność prawa UE, którą TSUE chce chronić.

Podsumowując, należy uznać, że brakuje przesłanek pozwalających stwierdzić, że TSUE jest na dobrej drodze do rozpoznania prawa do informacji jako odrębnego od prawa dostępu do dokumentów. Wytyczne dotyczące wykładni KPP zawarte w samej jej treści – w świetle orzecznictwa ETPCz – nakazują podejrzewać, że prawo do informacji powinno być postrzegane

⁵⁶⁹ Przedstawione w tym miejscu w odniesieniu do prawa dostępu do dokumentów urzędowych uwagi dotyczą ściśle analizowanych spraw. Kompleksowa analiza pozycji NGO w prawie UE, zob. P. Staszczuk, *A Legal Analysis of NGOs and European Civil Society*, Kluwer Law International, Alphen aan den Rijn 2019.

⁵⁷⁰ Zob. Wyrok Trybunału z dnia 18 czerwca 2020 r. w sprawie C-78/18, *Komisja Europejska przeciwko Węgrom*, ECLI:EU:C:2020:476, pkt 79.

⁵⁷¹ Szerzej o tym problemie w podrozdziale dotyczącym wyjątków od prawa dostępu do dokumentów w prawie UE.

jako element art. 11 KPP. TSUE nie podejmuje jednak wysiłku w zakresie dokonania kompleksowego zestawienia wykładni art. 10 EKPCz zaproponowanej przez ETPCz i prezentowanego przez siebie podejścia do prawa dostępu do dokumentów. Stan taki jest tym bardziej niezrozumiały, że TSUE wydaje się przyznawać, że wolność otrzymywania informacji jest chroniona na mocy art. 11 ust. 1 KPP⁵⁷². Odmawia on jednak wykonania kolejnego kroku, zgodnego z wykładnią rozwiniętą przez ETPCz, czyli przyznania, że prawo do otrzymywania informacji powinno być odczytywane jako źródło prawa dostępu do informacji. Wrywkowe odnośnienie się do poszczególnych elementów analizy przeprowadzanej w orzecznictwie przez ETPCz świadczy o przedkładaniu przez TSUE autonomii prawa unijnego ponad gwarantowanie ochrony praw podstawowych w zakresie i na poziomie proponowanym przez ETPCz. Informacja, w rozumieniu promowanym przez TSUE, jest niczym więcej niż elementem dokumentu.

Waga potencjalnego wzmocnienia interakcji między wykładnią prawa dostępu przez ETPCz i prawa dostępu do dokumentów urzędowych przez TSUE wynika z dwóch przyczyn. Po pierwsze, w odniesieniu do istniejących w prawie UE regulacji dotyczących dostępu do dokumentów urzędowych instytucji unijnych uwzględnienie art. 11 KPP jako gwarantującego prawo dostępu do informacji mogłoby się przyczynić do szerokiej wykładni przepisów dotyczących dostępu do dokumentów. Prawo dostępu do informacji w tym kontekście stanowiłoby tło aksjologiczne dla wykładni prawa unijnego i mogłoby prowadzić np. do bardziej zdecydowanej kontroli stosowania wyjątków obligatoryjnych, które – w świetle prawa dostępu do informacji – nie powinny występować. Według wykładni art. 10 EKPCz każdy wyjątek od prawa dostępu do informacji powinien spełniać warunek niezbędności w demokratycznym społeczeństwie, co kłóci się z ideą wyjątków obligatoryjnych. Tym samym mocniejsze osadzenie wykładni prawa UE dotyczącego prawa dostępu do dokumentów urzędowych w ramach tworzonych przez ewoluujące orzecznictwo ETPCz dotyczące prawa dostępu do informacji mogłoby przyczynić się do poszerzenia zakresu praw gwarantowanych przez KPP i ujednolicenia podejścia ETPCz z tym, które prezentuje TSUE⁵⁷³.

Po drugie, wpływ uznania istnienia prawa dostępu do informacji opartego na art. 11 KPP mógłby prowadzić do uznania, że w zakresie stosowania prawa UE przez państwa członkowskie prawo dostępu do informacji stanowi

⁵⁷² Na przykład Wyrok Trybunału z dnia 22 stycznia 2013 r. w sprawie C-283/11, *Sky Österreich GmbH przeciwko Österreichischer Rundfunk*, ECLI:EU:C:2013:28, pkt 51; Wyrok Trybunału z dnia 22 grudnia 2008 r. w sprawie C-336/07, *Kabel Deutschland Vertrieb und Service GmbH & Co. KG przeciwko Niedersächsische Landesmedienanstalt für privaten Rundfunk*, ECLI:EU:C:2008:765, pkt 33 (odesłanie do EKPCz).

⁵⁷³ Wskazane również w świetle tego, w jaki sposób relację między EKPCz i KPP charakteryzuje sama KPP – zob. art. 52 ust. 2 KPP.

prawo podstawowe chronione przez KPP. Argumentem przemawiającym za taką wykładnią jest sposób określenia relacji między wykładnią EKPCz i KPP w samej Karcie oraz sposób określenia w KPP jej zakresu stosowania. Skutek ten byłby ponadto istotny w kontekście opisywanych w rozdziale pierwszym zagrożeń generowanych przez zautomatyzowane podejmowanie decyzji dla przejrzystości i zakazu dyskryminacji. W świetle wyzwań tworzonych przez stosowanie nowych technologii zautomatyzowanej dla zakazu dyskryminacji dostęp do informacji może być postrzegany jako niezbędny warunek możliwości stwierdzenia, czy dyskryminacja ma miejsce, czy nie. Ze względu na fundamentalny charakter zakazu dyskryminacji dla prawa unijnego możliwość weryfikacji dyskryminacyjności zautomatyzowanego podejmowania decyzji stosowanego przez państwa członkowskie jest kluczowym problemem, któremu prawo UE będzie musiało sprostać.

4.2.3. Algorytm jako dokument w prawie UE w świetle koncepcji kodu jako prawa

W związku z postrzeganiem informacji jako elementu dokumentu w prawie UE kluczowa jest próba odpowiedzi na pytanie, czy algorytmy używane w systemach zautomatyzowanego podejmowania decyzji mogłyby zostać uznane za dokument. W tym celu warto odwołać się do wyroku Sądu w sprawie *Julien Dufour przeciwko Europejskiemu Bankowi Centralnemu*⁵⁷⁴. Dotyczyła ona doktoranta, który złożył do EBC wnioski o dostęp do informacji w postaci sprawozdań tej instytucji dotyczących rekrutacji i mobilności jego personelu oraz do „baz danych, którymi posłużono się do przeprowadzenia analiz statystycznych w sprawozdaniach”⁵⁷⁵. EBC udzielił mu częściowego dostępu do sprawozdań oraz oddalił wnioski o dostęp do baz, argumentując, że nie są one objęte definicją dokumentu zawartą w *decyzji 2004/258/WE*⁵⁷⁶, a także, że nie istnieje żaden samoistny dokument, który mógłby zostać udostępniony skarżącemu w odpowiedzi na jego wnioski⁵⁷⁷.

W ramach postępowania przed Sądem EBC przedstawił wiele argumentów odnoszących się do cech technicznych używanych przez siebie systemów

⁵⁷⁴ Wyrok Sądu z dnia 26 października 2011 r. w sprawie T-436/09, *Julien Dufour przeciwko Europejskiemu Bankowi Centralnemu*, ECLI:EU:T:2011:634.

⁵⁷⁵ *Ibidem*, pkt 4.

⁵⁷⁶ Zgodnie z art. 3 lit. a decyzji 2004/58: „«dokument» i «dokument EBC» oznacza wszelkie treści bez względu na nośnik (utrwalone na papierze lub przechowywane w formie elektronicznej, bądź też jako nagranie dźwiękowe, wizualne lub audiowizualne) stworzone lub będące w dyspozycji EBC i dotyczące kwestii związanych z jego polityką, działalnością lub decyzjami, jak również dokumenty pochodzące z Europejskiego Instytutu Walutowego (EIW) oraz Komitetu Prezesów banków centralnych Państw Członkowskich Europejskiej Wspólnoty Gospodarczej (Komitet Prezesów)”.

⁵⁷⁷ Wyrok Sądu z dnia 26 października 2011 r. w sprawie T-436/09, *Julien Dufour przeciwko Europejskiemu Bankowi Centralnemu*, ECLI:EU:T:2011:634, pkt 5.

informatycznych oraz aspektów organizacyjnych dotyczących baz danych, m.in. kwestii korzystania z oprogramowania dostarczanego przez prywatną firmę czy usuwania wyników po 24 miesiącach i możliwości uzyskania do nich płatnego dostępu od dostawcy oprogramowania. Argumentacja taka jest symptomatyczna w świetle opisanych w rozdziale pierwszym zagadnień dotyczących braku przejrzystości systemów zautomatyzowanego podejmowania decyzji. Odwoływanie się do faktu, że dane oprogramowanie jest dostarczane przez zewnętrznego usługodawcę, czy do warunków, na jakich umożliwia on korzystanie z danego programu, mogłoby stanowić argument również w sprawach związanych z zautomatyzowanym podejmowaniem decyzji. Należy podkreślić, że problemy te nie są *de facto* wyzwaniem technicznymi. Są one wynikiem rozwiązań prawnych i organizacyjnych, nie zaś ograniczeniem wynikającym ze specyfiki technologii. Podnoszenie tych argumentów nie stanowiło w związku z tym próby zrozumienia, czym są bazy danych i jak należy je postrzegać w świetle definicji dokumentu w prawie UE.

Próbie oceny tego zagadnienia podjął Sąd, który swoją analizę rozpoczął od zainspirowania się definicją baz danych zaczerpniętą z art. 1 ust. 2 *dyrektywy 96/9/WE* w sprawie ochrony prawnej baz danych⁵⁷⁸, po czym odniósł cechy charakterystyczne baz danych do definicji dokumentu z *decyzji 2004/258/WE*. Konkluzją Sądu było, po pierwsze, że:

[...] pojęcie bazy danych nie obejmuje wyłącznie zbioru danych zawartych w bazie, ale również środki techniczne, w które jest ona wyposażona, które pozwalają na uporządkowanie tych danych w sposób systematyczny lub metodyczny, a także ich precyzyjne i indywidualne pobieranie⁵⁷⁹.

Po drugie, Sąd przeprowadził analizę, w ramach której sprawdzał, czy zbiory danych, zawarte w bazie danych, spełniają warunki z definicji dokumentu. Sąd stwierdził, że zbiory danych zawarte w bazie mogą być traktowane jako dokument, m.in. ze względu na fakt, że dla uznania danej treści za dokument nie ma znaczenia np. jej długość ani to, czy jest zrozumiała. Następnie Sąd doszedł do wniosku, że w sprawie nie było konieczne ustalenie, czy baza danych EBC może „jako taka” stanowić przedmiot wniosku o dostęp złożonego na podstawie *decyzji 2004/258/WE*⁵⁸⁰. Ponadto Sąd

⁵⁷⁸ *Dyrektywa 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r. w sprawie ochrony prawnej baz danych* (dyrektywa 96/9/WE), Dz.Urz. WE 1996 L 77, s. 20–28. Definicja brzmi: „[...] zbiór niezależnych utworów, danych lub innych materiałów uporządkowanych w sposób systematyczny lub metodyczny, indywidualnie dostępnych środkami elektronicznymi lub innymi sposobami”.

⁵⁷⁹ Wyrok Sądu z dnia 26 października 2011 r. w sprawie T-436/09, *Julien Dufour przeciwko Europejskiemu Bankowi Centralnemu*, ECLI:EU:T:2011:634, pkt 95.

⁵⁸⁰ *Ibidem*, pkt 183.

stwierdził, że wniosek o dostęp nie może dotyczyć utworzenia nowego dokumentu („uporządkowanych według planu, który nie występuje w rzeczowej bazie danych”⁵⁸¹).

Granica między dokumentem istniejącym a nowym w kontekście informacji znajdujących się w bazach danych została przez TSUE określona w wyroku w sprawie *Reiner Typke przeciwko Komisji Europejskiej*⁵⁸². Stwierdził on, że:

W tych okolicznościach wszelkie informacje, które mogą być pozyskane z elektronicznej bazy danych w ramach jej powszedniego użytkowania za pomocą zaprogramowanych narzędzi wyszukiwania, winny być uznane za dokumenty istniejące, nawet jeśli informacje te nie były dotąd wyświetlane w takiej formie albo nie były wcześniej przedmiotem wyszukiwania przez pracowników instytucji⁵⁸³.

Dlatego w odniesieniu do treści baz danych jako dokumentów istniejących najważniejszą rolę odgrywa specyfika techniczna bazy danych i pozyskiwanie z niej dokumentów oparte na zasadzie najszerszego możliwego dostępu. Operacja taka – wyszukiwanie danych i tworzenie z nich dokumentu – traktowana jest jako udzielanie dostępu do dokumentu istniejącego. W sytuacji, w której wymagane byłoby poświęcenie „istotnego nakładu pracy”, aby pozyskać odpowiednie dane, postępowanie takie byłoby potraktowane jako tworzenie nowego dokumentu⁵⁸⁴. TSUE wydaje się w tym kontekście przyjmować perspektywę użytkownika bazy danych, nie zaś osoby odpowiedzialnej za jej tworzenie czy zarządzanie nią⁵⁸⁵. Wykorzystanie narzędzi wyszukiwania dostępnych w bazie może również być postrzegane jako forma dostępu częściowego⁵⁸⁶.

⁵⁸¹ *Ibidem*, pkt 152 oraz 149.

⁵⁸² Wyrok Trybunału z dnia 11 stycznia 2017 r. w sprawie C-491/15 P, *Reiner Typke przeciwko Komisji Europejskiej*, ECLI:EU:C:2017:5, pkt 30–49. Rozumowanie dotyczące informacji z baz danych powtórzone w: Wyrok Sądu z dnia 27 listopada 2019 r. w sprawie T-31/18, *Luisa Izuzquiza i Arne Semsrott przeciwko Europejskiej Agencji Straży Granicznej i Przybrzeżnej (Frontex)*, ECLI:EU:T:2019:815, pkt 50–54.

⁵⁸³ Wyrok Trybunału z dnia 11 stycznia 2017 r. w sprawie C-491/15 P, *Reiner Typke przeciwko Komisji Europejskiej*, ECLI:EU:C:2017:5, pkt 37.

⁵⁸⁴ „[...] wszelkie informacje, których uzyskanie wymaga bądź zmiany organizacji elektronicznej bazy danych, bądź zmiany narzędzi wyszukiwania rzeczywiście dostępnych w celu pozyskiwania informacji, należy uznać za nowy dokument”. Wyrok Trybunału z dnia 11 stycznia 2017 r. w sprawie C-491/15 P, *Reiner Typke przeciwko Komisji Europejskiej*, ECLI:EU:C:2017:5, pkt 40.

⁵⁸⁵ „Niemniej jednak programowanie i zarządzanie informatyczne takimi bazami danych nie należy do czynności wykonywanych w ramach bieżącego użytkowania przez końcowych użytkowników”. Wyrok Trybunału z dnia 11 stycznia 2017 r. w sprawie C-491/15 P, *Reiner Typke przeciwko Komisji Europejskiej*, ECLI:EU:C:2017:5, pkt 36.

⁵⁸⁶ W orzeczeniu Sąd przypomniał również o obowiązku instytucji – w tym wypadku EBC – w zakresie pomocy we wskazaniu posiadanych przez instytucję dokumentów „które

Orzecznictwo TSUE może stanowić podstawę dla rozważenia jak, w razie konieczności stwierdzenia, czy algorytm lub program komputerowy używany do zautomatyzowanego podejmowania decyzji jest dokumentem, hipotetycznie przebiegłaby analiza tego problemu. Po pierwsze, należałoby zastanowić się nad tym, czym jest program komputerowy. W związku z brakiem jego definicji legalnej w prawie UE⁵⁸⁷ należałoby spróbować poszukać innych źródeł umożliwiających ocenę charakteru prawnego programów komputerowych. Pewną możliwością byłoby odwołanie się do objęcia go ochroną analogiczną do utworów literackich w *Konwencji berneńskiej o ochronie dzieł literackich i artystycznych z dnia 9 września 1886 r.*⁵⁸⁸ i na podstawie tego postrzeżenia stwierdzenie, że jak długo jest on utrwalony na nośniku, może on spełniać warunki definicji dokumentu w prawie UE. Program komputerowy mógłby być określony jako tekst.

W odniesieniu do programu komputerowego problemem mógłby się wydawać również jego wysoki poziom skomplikowania i rozbudowania. Jednak, jak wskazał Sąd w orzeczeniu *Julien Dufour przeciwko Europejskiemu Bankowi Centralnemu*, definicja dokumentu w prawie UE nie zawiera kryterium długości („wielkość, długość, waga lub sposób prezentacji treści są pozbawione znaczenia przy ustalaniu, czy treść tę rzeczona definicja obejmuje, czy nie”⁵⁸⁹). W razie uznania programu komputerowego za tekst bez znaczenia byłyby więc jego poziom skomplikowania czy długość. Nie byłaby również problematyczna konieczność utworzenia nowego dokumentu. Dostęp do kodu komputerowego mógłby obejmować gotowe rozwiązania zapisane na nośniku. W związku z faktem, że program komputerowy musi być utrwalonym na nośniku tekstem, można zatem bronić twierdzenia, że może on być postrzegany jako dokument w świetle unijnej definicji tego terminu.

Ponadto program taki musiałby – zgodnie z wymogami sformułowanymi w ramach definicji dokumentu z *rozporządzenia 1049/2001* – dotyczyć kwestii związanych z polityką, działalnością i decyzjami mieszczącymi się w sferze odpowiedzialności instytucji, do których kierowany byłby wniosek. Zważywszy na fakt, że byłyby one – hipotetycznie – instytucjami używającymi

są analogiczne do dokumentów objętych wnioskiem o dostęp lub które mogą zawierać część lub całość informacji poszukiwanych przez wnioskodawcę”. Wyrok Sądu z dnia 26 października 2011 r. w sprawie T-436/09, *Julien Dufour przeciwko Europejskiemu Bankowi Centralnemu*, ECLI:EU:T:2011:634, pkt 31.

⁵⁸⁷ Nie została ona zawarta w *dyrektywie 2009/24/WE*.

⁵⁸⁸ *Konwencja berneńska o ochronie dzieł literackich i artystycznych z dnia 9 września 1886 r., przejrzana w Berlinie dnia 13 listopada 1908 r. i w Rzymie dnia 2 czerwca 1928 r. (ratyfikowana zgodnie z ustawą z dnia 5 marca 1934 r.)* (konwencja berneńska), Dz.U. 1935 nr 84 poz. 515.

⁵⁸⁹ Wyrok Sądu z dnia 26 października 2011 r. w sprawie T-436/09, *Julien Dufour przeciwko Europejskiemu Bankowi Centralnemu*, ECLI:EU:T:2011:634, pkt 93.

zautomatyzowanego podejmowania decyzji, również to kryterium zostałoby spełnione.

To, co mogłoby natomiast stanowić barierę w odniesieniu do dostępu do kodu używanego w ramach systemów zautomatyzowanego podejmowania decyzji, to próby udzielania dostępu częściowego. W odniesieniu do programów komputerowych byłby on raczej pozbawiony sensu. Udostępnienie jedynie części informacji zawartych w kodzie jako tekście mogłoby prowadzić do nieporozumień dotyczących działania danego programu np. w razie udostępnienia informacji na temat rodzaju kryteriów uwzględnianych przy zautomatyzowanym podejmowaniu decyzji, bez informacji o przypisanych im wagach oraz podstawach wyliczania zmiennych. Problem dostępu częściowego jest jednak drugorzędny w stosunku do głównej konkluzji, zgodnie z którą – na tle samej definicji dokumentu w prawie UE – można wyjść z założenia, że program komputerowy służący do zautomatyzowanego podejmowania decyzji mógłby zostać uznany za dokument.

Argumentem przemawiającym za możliwością postrzegania programu komputerowego służącego do zautomatyzowanego podejmowania decyzji jako dokumentu jest również nacisk kładziony przez TSUE na dostęp do dokumentów związanych z procesem ustawodawczym. Zgodnie z teoriami zarysowanymi w rozdziale pierwszym można zaobserwować wpływ zautomatyzowanego podejmowania decyzji na prawo. Z jednej strony, algorytmy mogą do pewnego stopnia zastępować akty prawne, kiedy np. przepisy regulujące daną kwestię jedynie odsyłają do systemów informatycznych, które mają za zadanie pełnić funkcję dotychczas regulowaną bezpośrednio w przepisach. Z drugiej strony, algorytmy mogą być wykorzystywane jako narzędzie – przynajmniej teoretycznie – usprawniające proces podejmowania decyzji na podstawie regulacji, lecz w zautomatyzowany sposób. Oba te mechanizmy mogą być postrzegane jako elementy wpływające na działalność legislacyjną.

Należy podkreślić, że to właśnie dostępowi do dokumentów dotyczących ustawodawczej sfery aktywności instytucji TSUE przypisuje szczególne znaczenie⁵⁹⁰. W kluczowym orzeczeniu o dostępie do opinii Służby Prawnej Rady dotyczącej projektu dyrektywy Rady ustanawiającej minimalne normy określające przyjmowanie osób ubiegających się o azyl w państwach członkowskich, *Królestwo Szwecji i Maurizio Turco przeciwko Radzie*⁵⁹¹, TSUE wprost stwierdził, że otwartość⁵⁹² „pozwalająca na to, by rozbieżności między szeregiem punktów widzenia były poddane otwartej debacie, przyczynia się

⁵⁹⁰ Zob. P. Leino, *Just a Little Sunshine in the Rain: the 2010 Case Law of the European Court of Justice on Access to Documents*, „Common Market Law Review” 2011, t. 48, s. 1249.

⁵⁹¹ Wyrok Trybunału z dnia 1 lipca 2008 r. w sprawach połączonych C-39/05 P i C-52/05 P, *Królestwo Szwecji i Maurizio Turco przeciwko Radzie Unii Europejskiej*, ECLI:EU:C:2008:374.

⁵⁹² Z niejasnych przyczyn tłumaczona w polskiej wersji wyroku jako „jawność”.

do tego, by przydać większej legitymizacji w oczach europejskich obywateli i zdobyć ich większe zaufanie”⁵⁹³. Argumentacja TSUE została oparta m.in. na motywie 6 *rozporządzenia 1049/2001*, w którym znajduje się stwierdzenie, że szerszy dostęp do dokumentów powinien być udzielony w przypadkach, gdy instytucje sprawują władzę ustawodawczą⁵⁹⁴. TSUE stwierdził, że należy porównać zagrożenie dla interesu w postaci ochrony niezależności Służby Prawnej Rady i interesu publicznego w postaci zwiększenia przejrzystości i otwartości procesu legislacyjnego i demokratycznych uprawnień obywateli UE⁵⁹⁵. Konkluzją orzeczenia jest m.in. stwierdzenie, że, co do zasady, *rozporządzenie 1049/2001* zobowiązuje instytucję do ujawniania opinii Służby Prawnej Rady, co stanowiło odwrócenie poglądu prezentowanego w tej sprawie przez Sąd.

Sprawa *Królestwo Szwecji i Maurizio Turco przeciwko Radzie Unii Europejskiej* przedstawia mechanizm, zgodnie z którym TSUE wpisuje dostęp do dokumentów w szersze zagadnienie legitymizacji procedury legislacyjnej i możliwości swoistej kontroli działań ustawodawczych UE przez jej obywateli. Stanowisko to zostało potwierdzone przez TSUE w wyroku w sprawie *Rada Unii Europejskiej przeciwko Access Info Europe*⁵⁹⁶, w którym Trybunał potwierdził, że z zasady dokumenty dotyczące procesu legislacyjnego powinny być udostępniane, wyjątki zaś stosowane ściślej⁵⁹⁷. Stanowisko to jest aprobowane przez doktrynę, która podkreśla, że „jawność ustawodawstwa jest kluczowa dla [...] demokracji”⁵⁹⁸ – zarówno w jej bezpośredniej, jak i reprezentacyjnej formie. Dostęp do informacji na temat procesów

⁵⁹³ Wyrok Trybunału z dnia 1 lipca 2008 r. w sprawach połączonych C-39/05 P i C-52/05 P, *Królestwo Szwecji i Maurizio Turco przeciwko Radzie Unii Europejskiej*, ECLI:EU:C:2008:374, pkt 59.

⁵⁹⁴ Motyw 6 wspomina również o konieczności jednoczesnego zachowania skuteczności procesu podejmowania przez te instytucje decyzji – zob. motyw 6, *rozporządzenie 1049/2001* oraz Wyrok Trybunału z dnia 1 lipca 2008 r. w sprawach połączonych C-39/05 P i C-52/05 P, *Królestwo Szwecji i Maurizio Turco przeciwko Radzie Unii Europejskiej*, ECLI:EU:C:2008:374, pkt 46.

⁵⁹⁵ Wyrok Trybunału z dnia 1 lipca 2008 r. w sprawach połączonych C-39/05 P i C-52/05 P, *Królestwo Szwecji i Maurizio Turco przeciwko Radzie Unii Europejskiej*, ECLI:EU:C:2008:374, pkt 67–68.

⁵⁹⁶ Wyrok Trybunału z dnia 17 października 2013 r. w sprawie C-280/11 P, *Rada Unii Europejskiej przeciwko Access Info Europe*, ECLI:EU:C:2013:671, pkt 33. Szczegółowe omówienie tej sprawy, zob. S. Lea, P.J. Cardwell, *Transparency Requirements in the Course of a Legislative Procedure: Council v. Access Info Europe*, „European Public Law” 2015, nr 21(1), s. 61–80.

⁵⁹⁷ Zob. V. Abazi, M. Hillebrandt, *The legal limits to confidential negotiations: Recent case law developments in Council transparency: Access Info Europe and In ‘t Veld*, „Common Market Law Review” 2015, t. 52, s. 845.

⁵⁹⁸ D. Curtin, P. Leino, *In Search of Transparency for EU Law-Making: Trilogues on the Cusp of Dawn*, „Common Market Law Review” 2017, t. 54, s. 1680.

legislacyjnych jest inherentną częścią systemów, które stawiają w centrum rządu prawa, ponieważ „odnosi się ona do źródeł i uzasadnień dla prawa samego w sobie”⁵⁹⁹.

Takie postrzeganie tworzenia prawa trafnie podsumowuje cytat z opinii rzecznika generalnego Edra Cruza Villalóna w sprawie *Rada Unii Europejskiej przeciwko Access Info Europe*:

„Legislacja” jest z definicji działaniem ustawodawczym, które w społeczeństwie demokratycznym można prowadzić jedynie poprzez procedury o charakterze publicznym i w tym znaczeniu „przejrzystym”. W inny sposób nie można by uchwalić „ustawy” będącej wyrażeniem woli tych, których ma ona dotyczyć, co jest fundamentem jej legalności jako niepodważalnego mandatu. W demokracji przedstawicielskiej, co ma miejsce w Unii, wiedza o procedurze ustawodawczej powinna być dostępna dla obywateli, bowiem w inny sposób nie mogliby oni pociągnąć swoich przedstawicieli do odpowiedzialności politycznej, do czego mają prawo na podstawie mandatu wyborczego⁶⁰⁰.

Zważywszy na znaczenie, jakie TSUE przykłada do przejrzystości prawodawstwa, można podejrzewać, że w razie konieczności oceny używania zautomatyzowanego podejmowania decyzji w sposób mający na celu zastąpienie nim ustawodawstwa TSUE mógłby okazać się krytycznie nastawiony wobec takich działań. Niezbędne do podejścia ujmującego stosowanie zautomatyzowanego podejmowania decyzji jako *de facto* prawodawstwa byłoby odnotowanie, że kod komputerowy odgrywa rolę zbliżoną do prawa. Gdyby TSUE przyjął w swojej analizie perspektywę stawiającą w centrum pytanie o konsekwencje stosowania zautomatyzowanego podejmowania decyzji dla jednostek, mógłby on zbliżyć się do wniosku, że technologia staje się prawem i jej stosowanie wpływa na sytuację jednostki w sposób analogiczny do tego, jak w przypadku oceny jej sytuacji opartej na przepisach. Perspektywa taka miałaby potencjał doprowadzenia do stawiania wobec technologii wymogów w zakresie przejrzystości podobnych do tych, jakie są stosowane wobec ustawodawstwa. Jednym z nich mógłby być nacisk na konieczność zagwarantowania dostępu do dokumentów – np. kodu komputerowego czy założeń przyświecających automatyzacji i przekładaniu na kod komputerowy danych przepisów – w okolicznościach, w których zautomatyzowane podejmowanie decyzji zastępuje lub wchodzi w interakcję z sytuacjami regulowanymi aktem prawnym.

⁵⁹⁹ D. Curtin, H. Meijers, *The Principle Of Open Government In Schengen And The European Union: Democratic Retrogression?*, „Common Market Law Review” 1995, t. 32, s. 391.

⁶⁰⁰ Opinia rzecznika generalnego Edra Cruza Villalóna przedstawiona w dniu 16 maja 2013 r. w sprawie C-280/11 P, *Rada Unii Europejskiej przeciwko Access Info Europe*, ECLI:EU:C:2013:325, pkt 63.

Problem, jaki mógłby się pojawić, to formalistyczne podejście do oceny, co konstytuuje akt prawny. W razie obrania stanowiska, zgodnie z którym działanie ustawodawcze musi być związane z procedurą ustawodawczą w rozumieniu TFUE⁶⁰¹, materialny wymiar zautomatyzowanego podejmowania decyzji jako formy działalności legislacyjnej miałby marginalne znaczenie. Jedynie perspektywa, w której kluczowy staje się rzeczywisty wpływ danego systemu zautomatyzowanego podejmowania decyzji na prawa jednostki, pozwoliłaby uwzględnić prawotwórczy charakter technologii i, co za tym idzie, jej w rzeczywistości ustawodawczy charakter. W przypadku bardziej teleologicznej wykładni formuły „sprawowanie władzy ustawodawczej” mogłyby się jednak pojawić inne problemy, np. wykazanie, że zautomatyzowane podejmowanie decyzji rzeczywiście stanowi formę utajnionego tworzenia prawa, nie zaś np. czynność czysto administracyjną. Zważywszy na formalistyczne podejście TSUE do prawa dostępu do dokumentów urzędowych, raczej nie jest możliwe, aby przyjęta została wykładnia kładąca nacisk na funkcje rzeczywiście pełnione przez zautomatyzowane podejmowanie decyzji. Problematyczne mogłoby również okazać się wykazanie, że dana sytuacja, w której stosowane jest zautomatyzowane podejmowanie decyzji, nie powinna być postrzegana jako przyporządkowana do kategorii uznawanych za wyjątki od prawa dostępu do dokumentów w prawie UE.

4.3. Wyjątki od prawa dostępu do dokumentów unijnych w prawie UE

Już na tle stanu prawnego obowiązującego w wyniku przyjęcia Kodeksu oraz decyzji Rady i Komisji Sąd uznał zasadę „najszerzego możliwego dostępu” jako wyznaczającą granice zastosowania prawa dostępu do dokumentów⁶⁰², od której wyjątki muszą być ściśle interpretowane⁶⁰³. Reżim prawny dotyczący dostępu do dokumentów w UE oparty na *rozporządzeniu 1049/2001* wprowadza w art. 4 trzy typy wyjątków oraz, dodatkowo, uprawnienia stron trzecich dotyczące konsultacji lub możliwości żądania zgody na udostępnienie dokumentu.

⁶⁰¹ Taka sugestia pojawia się w: Wyrok Sądu z dnia 7 lutego 2018 r. w sprawie T-851/16, *Access Info Europe przeciwko Komisji Europejskiej*, ECLI:EU:T:2018:69, pkt 106: „W niniejszym przypadku należy przypomnieć, że sporne dokumenty nie zostały sporządzone w ramach procedury ustawodawczej w rozumieniu traktatu FUE”.

⁶⁰² Wyrok Sądu pierwszej instancji z dnia 6 lutego 1998 r. w sprawie T-124/96, *Interporc Im- und Export GmbH przeciwko Komisji Wspólnot Europejskich*, ECLI:EU:T:1998:25, pkt 49. Zob. również: S. Peers, *op. cit.*, s. 389.

⁶⁰³ Nie zajmuję się rozwojem problematyki wyjątków od dostępu do dokumentów w prawie UE czy bardziej szczegółowo tym zagadnieniem – odpowiednia literatura na ten temat to, m.in. L. Rossi, P. Vinagre e Silva, *op. cit.*, s. 126–140 czy D. Adamski, *Prawo do informacji...*, s. 129–298.

Pierwszy typ wyjątków można określić mianem wyjątków obligatoryjnych. Zgodnie z art. 4 ust. 1 *rozporządzenia 1049/2001* „instytucja odmówi dostępu do dokumentów”, których ujawnienie naruszałoby ochronę interesu publicznego dotyczącego bezpieczeństwa publicznego, kwestii obronnych i wojskowych, stosunków międzynarodowych oraz finansowej, monetarnej czy ekonomicznej polityki Wspólnoty lub państwa członkowskiego. Dodatkowo art. 4 ust. 1 odnosi się również do ochrony interesu o charakterze raczej prywatnym, mianowicie prywatności i integralności osoby fizycznej. Katalog zwykłych wyjątków fakultatywnych z kolei został sformułowany w art. 4 ust. 2⁶⁰⁴. Katalog ten obejmuje ochronę interesów handlowych osoby fizycznej lub prawnej, w tym własności intelektualnej, postępowania sądowego lub porady prawnej oraz celu kontroli, śledztwa czy audytu. W odniesieniu do tych wyjątków *rozporządzenie 1049/2001* przewiduje konieczność sprawdzenia, czy za ujawnieniem nie przemawia przeważający interes publiczny.

Ponadto zgodnie z art. 4 ust. 3 *rozporządzenia 1049/2001*, w sytuacji, w której dostęp do dokumentu sporządzonego przez instytucję do celów wewnętrznych lub otrzymanego przez instytucję odnosi się do spraw, w przypadku których decyzja nie została wydana, możliwe jest nieudzielenie dostępu. Warunkiem koniecznym do nieudzielenia dostępu jest w tej sytuacji powiązanie ujawnienia dokumentu z poważnym naruszeniem procesu podejmowania decyzji przez tę instytucję. Również w tym wypadku dokument może zostać ujawniony, jeśli przemawia za tym interes publiczny. Ustęp 3 odnosi się również do dostępu do dokumentu zawierającego opinie do wykorzystania wewnętrznego jako część rozważań i konsultacji wstępnych w obrębie rzeczonoj instytucji. Dostęp do niego nie zostanie udzielony nawet po podjęciu decyzji, jeśli ujawnienie takiego dokumentu poważnie naruszyłoby proces podejmowania decyzji przez tę instytucję. Również w tym wypadku może on zostać udzielony, jeśli za ujawnieniem przemawia interes publiczny. Wyjątki z art. 4 ust. 3 można nazwać, za Dariuszem Adamskim, wyjątkami fakultatywnymi kwalifikowanymi⁶⁰⁵.

Wspólną cechą wykładni wszystkich wyjątków jest konieczność ich interpretacji w sposób ścisły. W związku z tym, jak zauważył Andrzej Wasilewski, po pierwsze, konieczne jest tłumaczenie wszelkich wątpliwości, jakie mogą się pojawić, na korzyść dostępu do dokumentu. Po drugie, niezbędne jest

⁶⁰⁴ Pojęcia tego używa D. Adamski, zob. D. Adamski, *Prawo do informacji...*, op. cit., s. 200. Tymczasem L. Rossi i P. Vinagre e Silva określają je jako „wyjątki obowiązkowe z (nowym) testem równoważenia” (*mandatory with a (new) balancing test*) – zob. L. Rossi, P. Vinagre e Silva, *op. cit.*, s. 142.

⁶⁰⁵ Ze względu na fakt, że nie wydają się one kluczowe na tle analizy algorytmów używanych do zautomatyzowanego podejmowania decyzji jako dokumentów, nie są one omówione dalej.

zbadanie każdego z dokumentów lub kategorii dokumentów przed wydaniem decyzji odmawiającej dostępu do dokumentów i wykazanie rzeczywistego zagrożenia dla chronionego prawnie interesu. Po trzecie zaś, konieczne jest rozważenie możliwości udzielenia częściowego dostępu do tych fragmentów żądanych dokumentów, które nie są objęte wyjątkiem⁶⁰⁶. Obowiązek wykazania, że wyjątek powinien mieć zastosowanie, ciąży na instytucji⁶⁰⁷.

Odrębnym zagadnieniem, będącym w ograniczonej formie kontynuacją zasady autorstwa rządzącej dostępem do dokumentów w prawie UE przed przyjęciem *rozporządzenia 1049/2001*, jest art. 4 ust. 4 i 5. W art. 4 ust. 4 został wprowadzony wymóg konsultacji ze stroną trzecią w celu dokonania oceny możliwości zastosowania wyjątku dotyczącego dokumentów stron trzecich. Konsultacje nie muszą być przeprowadzone w razie braku wątpliwości, czy dokument będzie ujawniony, czy nie. Rozwiązanie to jest bardziej otwarte na możliwości ujawniania dokumentów stron trzecich niż w przypadku stosowania zasady autorstwa. Nie uzależnia ono ujawnienia dokumentu od wyniku konsultacji, a nawet umożliwia ich brak. Inaczej jest jednak w sytuacji, w której dokument pochodzi od państwa członkowskiego. Zgodnie z art. 4 ust. 5 państwo członkowskie może zażądać od instytucji nieujawniania dokumentu bez uzyskania uprzedniej zgody od tego państwa członkowskiego. W literaturze można odnaleźć interpretację takiego rozwiązania jako przyznanie państwom członkowskim prawa weta w stosunku do udostępniania pochodzących od nich dokumentów⁶⁰⁸.

Tak radykalne twierdzenie nie znalazło jednak potwierdzenia w orzecznictwie TSUE, który w sprawach *Szwecja przeciwko Komisji*⁶⁰⁹ oraz *IFAW przeciwko Komisji* stwierdził, że wykładnia art. 4 ust. 5 powinna być dokonywana w świetle wyjątków z ust. 1–3 tego artykułu. W związku z tym rola państwa członkowskiego ogranicza się do uczestniczenia w podejmowaniu decyzji przez instytucję: „uprzednia zgoda państwa członkowskiego [...] jest podobna nie tyle do dyskrecjonalnego prawa weta, ile do pewnego rodzaju zgodnej opinii na temat braku podstaw do zastosowania wyjątków przewidzianych

⁶⁰⁶ Zob. A. Wasilewski, *Prawo dostępu do dokumentów instytucji Unii Europejskiej*, „Europejski Przegląd Sądowy” 2006, nr 11, s. 9–10.

⁶⁰⁷ Zob. S. Peers, *op. cit.*, s. 397–398.

⁶⁰⁸ Zob. M.E. de Leeuw, *The Regulation on public access to European Parliament, Council and Commission documents in the European Union: are citizens better off?*, „European Law Review” 2003, t. 28, nr 3, s. 337.

⁶⁰⁹ Wyrok Trybunału z dnia 18 grudnia 2007 r. w sprawie C-64/05 P, *Królestwo Szwecji przeciwko Komisji Wspólnot Europejskich i innym*, ECLI:EU:C:2007:802, pkt 76 oraz Wyrok Trybunału z dnia 21 czerwca 2012 r. w sprawie C-135/11 P, *IFAW Internationaler Tierschutz-Fonds gmbH przeciwko Komisji Europejskiej*, ECLI:EU:C:2012:376, pkt 58.

w ust. 1–3⁶¹⁰. Państwo członkowskie ma zatem obowiązek uzasadnić swoją opinię, opierając się na przepisach *rozporządzenia 1049/2001*, a w razie braku odpowiedniego uzasadnienia instytucja dokonuje analizy sytuacji i decyduje o przyznaniu lub nieprzyznaniu dostępu⁶¹¹.

W pewien sposób podobne jest rozwiązanie wprowadzone wobec dokumentów sensytywnych⁶¹². Dla ich ujawnienia, zgodnie z ust. 3, potrzebna jest zgoda instytucji, która je stworzyła. Ponadto art. 9 określający warunki udzielania dostępu do dokumentów sensytywnych jest wprost powiązany z art. 4. Po pierwsze, definicja dokumentów sensytywnych odsyła do art. 4, przez stwierdzenie, że jako dokumenty sensytywne są postrzegane takie, które chronią podstawowe interesy państw członkowskich w obszarach objętych art. 4 ust. 1 lit. a, a mianowicie w obszarze bezpieczeństwa publicznego, obrony i spraw wojskowych. Po drugie, odmowa dostępu musi być uzasadniona w sposób, który nie szkodzi interesom chronionym w art. 4. W związku z takim sposobem sformułowania i wykładni art. 4 ust. 5 oraz art. 9 – powiązanych z treścią art. 4 ust. 1–3 – tym większa jest rola wyjaśnienia pojęć i mechanizmów stosowanych w związku z wyjątkami od dostępu do dokumentów określonymi w *rozporządzeniu 1049/2001*.

4.3.1. Wyjątki obligatoryjne

W związku ze stosowaniem wyjątków obligatoryjnych można było zaobserwować pewną niespójność orzecznictwa⁶¹³ w zakresie standardów kontroli sądowej nad ich stosowaniem. Przykładem podejścia opartego na tzw. standardzie minimalnym był wyrok w opisywanej już powyżej sprawie *Hautala przeciwko Radzie*⁶¹⁴. Zgodnie z tym podejściem instytucjom została pozostawiona dyskrejonalna władza w zakresie analizy przesłanek przemawiających za odmową dostępu do dokumentu, a kontrola sądowa ograniczała się do

⁶¹⁰ Wyrok Trybunału z dnia 18 grudnia 2007 r. w sprawie C-64/05 P, *Królestwo Szwecji przeciwko Komisji Wspólnot Europejskich i innym*, ECLI:EU:C:2007:802, pkt 76.

⁶¹¹ Zob. A. Arnall, *Court of Justice, Joined Cases C-39/05 P & C-52/05 P, Sweden and Turco v. Council, judgment of the Grand Chamber of 1 July 2008, not yet reported*, „Common Market Law Review” 2009, t. 46, s. 1231.

⁶¹² Zgodnie z definicją z art. 9 ust. 1 są to: „dokumenty pochodzące od instytucji lub utworzonych przez nie agencji, z Państw Członkowskich, państw trzecich lub Organizacji Międzynarodowych, zaklasyfikowane jako «TRÈS SECRET/TOP SECRET», «SECRET» lub «CONFIDENTIEL» zgodnie z przepisami obowiązującymi w danej instytucji, które chronią podstawowe interesy Państw Członkowskich w obszarach objętych art. 4 ust. 1 lit. a), a mianowicie w obszarze bezpieczeństwa publicznego, obrony i spraw wojskowych” – *rozporządzenie 1049/2001*.

⁶¹³ Zob. D. Adamski, *Prawo do informacji...*, *op. cit.*, zwłaszcza s. 134–145.

⁶¹⁴ Podobnie również Wyrok Sądu pierwszej instancji z dnia 12 lipca 2001 r. w sprawie T-204/99, *Olli Mattila przeciwko Radzie Unii Europejskiej i Komisji Wspólnot Europejskich*, ECLI:EU:T:2001:190.

przestrzegania zasad postępowania i uzasadnienia, materialnej prawdziwości stanu faktycznego i braku oczywistych błędów w ocenie i nadużycia władzy. Z kolei w sprawie *Kuijer przeciwko Radzie*⁶¹⁵ Sąd zdecydował się „zanalizować racjonalność poszczególnych twierdzeń Rady”⁶¹⁶. Tym samym standard kontroli został podniesiony w celu merytorycznej oceny argumentów przywoływanych przez instytucję. Nie była to jednak decyzja, która wówczas w sposób klarowny zapoczątkowałaby nową linię orzeczniczą⁶¹⁷.

Źródłem zmiany, jaką można natomiast odnotować w najnowszym orzecznictwie dotyczącym dostępu do dokumentu, była kwestia korzystania przez Sąd i Trybunał z możliwości wglądu do dokumentów, których dotyczy spór. Problem ten okazał się przełomowy dla zagadnienia kontroli stosowania wyjątków obligatoryjnych z *rozporządzenia 1049/2001*. Zagadnienie to w pierw był analizowane przez Trybunał na tle możliwości powołania się na wyjątki z art. 4 ust. 1–3 przez państwo członkowskie na podstawie art. 4 ust. 5. W sprawie *IFAW Internationaler Tierschutz-Fonds gGmbH przeciwko Komisji Europejskiej* Trybunał zauważył, że – aby Sąd mógł dokonać oceny *in concreto* zasadności decyzji odmawiającej dostępu do dokumentu – konieczne jest zapoznanie się z dokumentem, którego dotyczy spór⁶¹⁸. Dopiero zapoznanie się z nim pozwala przeprowadzić kontrolę zgodności z prawem zaskarżonej decyzji odmawiającej do niego dostępu. Stąd też można stwierdzić, że w wyroku zostało wskazane, że Sąd ma obowiązek przeprowadzić merytoryczną analizę spornych dokumentów. Nie może on ograniczyć

⁶¹⁵ Wyrok Sądu pierwszej instancji z dnia 7 lutego 2002 r. w sprawie T-211/00, *Aldo Kuijer przeciwko Radzie Unii Europejskiej*, ECLI:EU:T:2002:30.

⁶¹⁶ D. Adamski, *Prawo do informacji...*, *op. cit.*, s. 144 i przywołana tam literatura.

⁶¹⁷ W kolejnych decyzjach dotyczących wyjątków z art. 4 ust. 1 TSUE odwoływał się raczej do standardu minimalnego kontroli, stawiając jako podstawę wydawanych wyroków: Wyrok Sądu pierwszej instancji z dnia 26 kwietnia 2005 r. w sprawach połączonych T-110/03, T-150/03 oraz T-405/03, *Jose Maria Sison przeciwko Radzie Unii Europejskiej*, ECLI:EU:T:2005:143 oraz Wyrok Trybunału z dnia 1 lutego 2007 r. w sprawie C-266/05 P, *Jose Maria Sison przeciwko Radzie Unii Europejskiej*, ECLI:EU:C:2007:75; Wyrok Sądu pierwszej instancji z dnia 25 kwietnia 2007 r. w sprawie T-264/04, *WWF European Policy Programme przeciwko Radzie Unii Europejskiej*, ECLI:EU:T:2007:114 – z orzeczeń analizowanych przez D. Adamskiego, *op. cit.*, s. 145–168.

⁶¹⁸ Wyrok Trybunału z dnia 21 czerwca 2012 r. w sprawie C-135/11 P, *IFAW Internationaler Tierschutz-Fonds gGmbH przeciwko Komisji Europejskiej*, ECLI:EU:C:2012:376, pkt 70–76. Podobnie, instytucja ma obowiązek zidentyfikowania dokumentów, których dotyczy wniosek, aby z jednej strony uzasadnić ewentualną odmowę ich udostępnienia oraz umożliwić Sądowi kontrolę zastosowania tego wyjątku („Ponadto należy wskazać, że zidentyfikowanie w zaskarżonej decyzji dokumentów objętych wnioskiem o udzielenie dostępu jest konieczne, by umożliwić Sądowi sprawowanie kontroli i ustalenie, czy Komisja zasadnie przyjęła, że żądane dokumenty należały do postępowania EU Pilot”). Wyrok Sądu z dnia 28 maja 2020 r. w sprawie T-701/18, *Liam Campbell przeciwko Komisji Europejskiej*, ECLI:EU:T:2020:224, pkt 63–66.

się do ściśle proceduralnej perspektywy i zaufania twierdzeniom instytucji, która jest w posiadaniu dokumentów, o dostęp do których toczy się spór. Pogląd ten został wzmocniony w wyroku *Ivan Jurašinić przeciwko Radzie*, w którym Trybunał orzekł, że w razie twierdzenia przez skarżącego, że wyjątek z art. 4 nie ma zastosowania do dokumentu, o który wnioskuje, Sąd jest „oczywiście zobowiązany nakazać przedstawienie tego dokumentu i zbadać go z poszanowaniem ochrony sądowej przysługującej temu skarżącemu”⁶¹⁹. Jedyne zapoznanie się z dokumentem, zgodnie z orzeczeniem Trybunału, pozwala *in concreto* ocenić, czy instytucja mogła zgodnie z prawem odmówić dostępu do dokumentu.

W wyniku tej zmiany standard kontroli sądowej dotyczącej decyzji instytucji o stosowaniu wyjątków z art. 4 ust. 1 został podniesiony. Jednocześnie Trybunał nie zrezygnował całkowicie z twierdzeń dotyczących uprawnień dyskrecjonalnych instytucji w zakresie stosowania wyjątków z art. 4 ust. 1. Można więc zaobserwować z jednej strony pogłębienie poziomu analizy spornych dokumentów w ramach postępowań sądowych, z drugiej zaś odwoływanie się do kryteriów opartych na standardzie minimalnym w celu uzasadnienia wyroku. Przykładem stosowania takiej kompilacji obu strategii są odpowiednio orzeczenie Sądu⁶²⁰ i Trybunału⁶²¹ w sprawach *Sophie in 't Veld przeciwko Radzie* oraz *Rada przeciwko Sophie in 't Veld*.

Sophie in 't Veld, europarlamentarzystka, zwróciła się z wnioskiem o dostęp do opinii służb prawnych Rady dotyczącej zalecenia Komisji dla Rady w kwestii upoważnienia do rozpoczęcia negocjacji między UE a USA w celu zawarcia umowy międzynarodowej o udostępnieniu departamentowi danych z komunikatów finansowych w ramach zapobiegania terroryzmowi. Rada powołała się na wyjątek dotyczący interesu publicznego w dziedzinie stosunków międzynarodowych, twierdząc, że ujawnienie informacji mogłoby zaszkodzić negocjacjom oraz prowadziłoby do udostępnienia drugiej stronie informacji na temat stanowiska UE. Sąd, wydając wyrok, zapoznał się ze spornym dokumentem i zauważył, że „analiza prawna dokonana w tym dokumencie zawiera pewne ustępy mające związek z celami, jakie Unia zamierza osiągnąć w negocjacjach, w szczególności dlatego, że poruszone są w nim kwestie dotyczące swoistej treści planowanej umowy”⁶²². Na podstawie przeprowadzonej analizy Sąd stwierdził, że z wyjątkiem tych fragmentów

⁶¹⁹ Wyrok Trybunału z dnia 28 listopada 2013 r. w sprawie C-576/12 P, *Ivan Jurašinić przeciwko Radzie Unii Europejskiej*, ECLI:EU:C:2013:777, pkt 27.

⁶²⁰ Wyrok Sądu z dnia 4 maja 2012 r. w sprawie T-529/09, *Sophie in 't Veld przeciwko Radzie Unii Europejskiej*, ECLI:EU:T:2012:215.

⁶²¹ Wyrok Trybunału z dnia 3 lipca 2014 r. w sprawie C-350/12 P, *Rada Unii Europejskiej przeciwko Sophie in 't Veld*, ECLI:EU:C:2014:2039.

⁶²² Wyrok Sądu z dnia 4 maja 2012 r. w sprawie T-529/09, *Sophie in 't Veld przeciwko Radzie Unii Europejskiej*, ECLI:EU:T:2012:215, pkt 35.

żądanego dokumentu, które dotyczą swoistej treści planowanej umowy i mogą spowodować ujawnienie strategicznych celów, do których osiągnięcia zmierza Unia w negocjacjach, Rada nie wykazała, w jaki sposób szerszy dostęp do dokumentu mógłby konkretnie i rzeczywiście naruszyć interes publiczny w dziedzinie stosunków międzynarodowych⁶²³.

Wyrok Sądu jest połączeniem podejścia opartego na merytorycznej analizie działania instytucji i zastosowania standardu minimalnego. Wykorzystując wiedzę pozyskaną w wyniku analizy racjonalności twierdzeń Rady, Sąd ostatecznie powołuje się na brak odpowiedniego uzasadnienia odmowy – czyli argument odwołujący się do kryteriów oceny stosowanych w ramach standardu minimalnego. Wyrok Trybunału, będący rezultatem odwołania Rady od wyroku Sądu, jest z kolei bardziej zachowawczy. Wprost przywołany zostaje model kontroli oparty na standardzie minimalnym⁶²⁴, a wyrok Sądu został wpisany w schemat kontroli ograniczonej do uzasadnienia spornej decyzji⁶²⁵.

Dalszy rozwój orzecznictwa może obrać kierunek nastawiony na drobiazgową analizę spornych dokumentów, jak np. w orzeczeniu Sądu w sprawie *Access Info Europe przeciwko Komisji Europejskiej*⁶²⁶ z lutego 2018 r. Sprawa dotyczyła dostępu do opinii prawnych lub analiz na temat zgodności z prawem unijnym i prawem międzynarodowym umowy między UE a Turcją o readmisji osób przebywających nielegalnie oraz działań UE i państw członkowskich podejmowanych w związku z umową między państwami UE a Turcją w kwestii uchodźców. Odmowa ich ujawnienia na podstawie art. 4 ust. 1 była motywowana koniecznością ochrony stosunków międzynarodowych. Wyrok ten pokazuje ciągłość dyskrecjonalnej władzy instytucji w tym aspekcie z jednoczesnym obowiązkiem przedstawienia przez instytucje uzasadnienia, które wykazuje konkretny, rzeczywisty i dający się racjonalnie przewidzieć – a nie jedynie hipotetyczny – charakter⁶²⁷ możliwych naruszeń chronionych w art. 4 ust. 1 interesów publicznych.

Jednocześnie jednak podniósł się standard kontroli sądowej nad stosowaniem wyjątków obligatoryjnych. Sam sposób sformułowania tezy wyroku świadczy o zmianie w rozstrzyganiu sporów dotyczących dostępu do

⁶²³ *Ibidem*, pkt 58.

⁶²⁴ Wyrok Trybunału z dnia 3 lipca 2014 r. w sprawie C-350/12 P, *Rada Unii Europejskiej przeciwko Sophie in 't Veld*, ECLI:EU:C:2014:2039, pkt 63.

⁶²⁵ *Ibidem*, pkt 68.

⁶²⁶ Wyrok Sądu z dnia 7 lutego 2018 r. w sprawie T-851/16, *Access Info Europe przeciwko Komisji Europejskiej*, ECLI:EU:T:2018:69.

⁶²⁷ Wyrok Trybunału z dnia 3 lipca 2014 r. w sprawie C-350/12 P, *Rada Unii Europejskiej przeciwko Sophie in 't Veld*, ECLI:EU:C:2014:2039, pkt 52 i 64; Wyrok Sądu z dnia 7 lutego 2018 r. w sprawie T-851/16, *Access Info Europe przeciwko Komisji Europejskiej*, ECLI:EU:T:2018:69, pkt 37 i przytoczone tam orzecznictwo.

dokumentów. Sąd odniósł się do konkretnych fragmentów zdań zawartych w dokumentach, o które wniosek złożyło Access Info Europe⁶²⁸. Tym samym nacisk został położony już nie tylko na proceduralne elementy postępowania zgodnie ze standardem minimalnym, lecz również na treść spornych dokumentów, zgodnie z postulatem analizy i kontroli rozumowania stojącego za decyzjami instytucji. Taki kierunek rozwoju linii orzeczniczej TSUE jest słuszny, jeśli na zagadnienie dostępu do dokumentów spojrzeć z perspektywy ogólnej zasady mającej na celu zagwarantowanie jak najszerszego dostępu. Kontrola sądowa, biorąca pod uwagę nie tylko aspekty proceduralne, lecz także treść dokumentów, jest niezbędna do powstrzymywania instytucji przed nadużywaniem przewidzianych w *rozporządzeniu 1049/2001* wyjątków i wyważeniem między interesami zasługującymi na ochronę zgodnie z przepisami rozporządzenia a interesem społeczeństwa w postaci informacji na temat danych kwestii.

4.3.2. Wyjątki fakultatywne

Przedstawiając w orzeczeniu w sprawie *Turco przeciwko Radzie* kolejność kroków, które powinny być wykonane przez instytucję w celu podjęcia decyzji o powołaniu się na wyjątek fakultatywny, TSUE wymienia trzy elementy⁶²⁹. Po pierwsze, instytucja – w wypadku sprawy *Turco* Rada – powinna upewnić się, że żądany dokument należy do kategorii uwzględnionych w wyjątkach (np. jest poradą prawną). Po drugie, stwierdzić, czy ujawnienie tego dokumentu naruszyłoby wartość chronioną przez wyjątki, przy czym ryzyko tego naruszenia musi dać się w rozsądny sposób przewidzieć. Po trzecie, instytucja powinna dokonać analizy ukierunkowanej na zbadanie, czy interes publiczny przemawiający za udostępnieniem dokumentu przeważa nad chronioną przez wyjątki wartością. Należy podkreślić, że ciężar dowodu wskazującego na to, że wyjątek powinien nie mieć zastosowania w związku z przeważającym interesem publicznym, ciąży na stronie żądającej dostępu do dokumentu⁶³⁰. Instytucje nie są zobowiązane z urzędu analizować możliwości istnienia interesu publicznego przemawiającego za ujawnieniem dokumentu, lecz

⁶²⁸ Podobnie dokładną analizę przeprowadzono w: Wyrok Sądu z dnia 27 listopada 2019 r. w sprawie T-31/18, *Luisa Izuzquiza i Arne Semsrott przeciwko Europejskiej Agencji Straży Granicznej i Przybrzeżnej (Frontex)*, ECLI:EU:T:2019:815 dotyczącym wyjątku odnoszącego się do bezpieczeństwa publicznego.

⁶²⁹ Wyrok Trybunału z dnia 1 lipca 2008 r. w sprawach połączonych C-39/05 P oraz C-52/05 P, *Królestwo Szwecji i Maurizio Turco przeciwko Radzie Unii Europejskiej*, ECLI:EU:C:2008:374, pkt 37–47 i 50.

⁶³⁰ Zob. S. de Abreu Ferreira, *The Fundamental Right of Access to Environmental Information in the EC: A Critical Analysis of WWF-EPO v. Council*, „Journal of Environmental Law” 2007, t. 19, nr 3, s. 405 oraz B. Driessen, *The Council of the European Union and access to documents*, „European Law Review” 2005, t. 30, nr 5, s. 681.

jednocześnie nie jest to zabronione. Analiza wyjątków objętych art. 4 ust. 3 powinna przebiegać w podobny sposób, uwzględniając jedynie konieczność poważnego naruszenia chronionych przez wyjątek wartości⁶³¹.

Głównym problemem prawnym pojawiającym się w odniesieniu do wyjątków fakultatywnych jest konieczność stwierdzenia, czym jest nadrzędny interes publiczny. Zgodnie z obserwacją Rossi i Vinagre e Silvy wymogi dotyczące identyfikacji odpowiedniego nadrzędnego interesu publicznego doprowadziły do – jak na razie – niemal nieuznawania przez TSUE istnienia takiego interesu⁶³². Warto jednak zauważyć, że zgodnie z orzecznictwem nadrzędny interes publiczny, który mógłby uzasadniać ujawnienie dokumentu, niekoniecznie musi się różnić od zasad stanowiących podstawę *rozporządzenia 1049/2001*⁶³³, czyli zasad otwartości i przejrzystości. W praktyce okazuje się, że właśnie realizacja tych zasad czasami jest uznawana przez TSUE za interes publiczny zasługujący na ochronę⁶³⁴. Może on być jednak przywoływany w związku z innym interesem publicznym jako narzędzie niezbędne do jego ochrony. Przykładem takiego instrumentalnego postrzegania dostępu do dokumentów jest traktowanie go jako elementu niezbędnego do sprawdzenia, czy dany akt prawny został przyjęty zgodnie z prawem⁶³⁵.

4.3.3. Wyjątki od prawa dostępu do dokumentów w odniesieniu do problematyki zautomatyzowanego podejmowania decyzji

Tak nikłe możliwości wykazania istnienia interesu publicznego, który przeważać powinien nad ochroną wartości uwzględnionych jako wyjątki fakultatywne, mogą stanowić poważne ograniczenie uzyskania dostępu do kodu programów komputerowych służących do zautomatyzowanego podejmowania decyzji. Potencjalne sytuacje próby pozyskania dostępu do takich dokumentów raczej stanowiłyby przedmiot postępowania ze względu na odmowę dostępu w wyniku powołania się przez instytucję na art. 4 ust. 2. Wyjątki obligatoryjne, z wyjątkiem specyficznych sytuacji, które mogłyby odnosić się

⁶³¹ Zob. zestawienie wykonane przez L. Rossi, P. Vinagre e Silva, *op. cit.*, s. 144.

⁶³² L. Rossi, P. Vinagre e Silva, *op. cit.*, s. 159 – publikacja Rossi i Vinagre e Silvy obejmuje przegląd orzecznictwa do końca 2015 r. (s. V).

⁶³³ Wyrok Sądu z dnia 7 lutego 2018 r. w sprawie T-851/16, *Access Info Europe przeciwko Komisji Europejskiej*, ECLI:EU:T:2018:69, pkt 104 i przywołane tam orzecznictwo.

⁶³⁴ Zob. L. Rossi, P. Vinagre e Silva, *op. cit.*, s. 159 oraz Wyrok Trybunału z dnia 1 lipca 2008 r. w sprawach połączonych C-39/05 P oraz C-52/05 P, *Królestwo Szwecji i Maurizio Turco przeciwko Radzie Unii Europejskiej*, ECLI:EU:C:2008:374, pkt 67.

⁶³⁵ Zob. „zasady przejrzystości, otwartości, demokracji i partycypacji, podniesione przez wnioskodawcę i potwierdzone przez TSUE jako przeważający interes publiczny, nie są celem samym w sobie. Łączą się one z innymi interesami, między którymi ochrona legalności ustawodawstwa zajmuje wysokie miejsce”. D. Adamski, *How Wide Is “The Widest Possible”? Judicial Interpretation of the Exceptions to the Right of Access to Official Documents Revisited*, „Common Market Law Review” 2009, t. 46, s. 538.

do bezpieczeństwa publicznego⁶³⁶ lub polityki ekonomicznej, niekoniecznie wydają się główną potencjalną przeszkodą do otrzymania dostępu do kodu jako dokumentu.

Tymczasem wyjątki fakultatywne, zwłaszcza dotyczące ochrony interesów handlowych osoby fizycznej lub prawnej oraz opinii prawnych, z dużym prawdopodobieństwem mogłyby być podnoszone w sprawach dotyczących systemów zautomatyzowanego podejmowania decyzji. Przede wszystkim wiąże się to z opisaną w rozdziale pierwszym ochroną własności intelektualnej odnoszącą się do programów komputerowych. Można wyobrazić sobie sytuację, w której instytucje powołują się na niemożność udostępnienia kodu jako dokumentu ze względu na fakt, że jest on chroniony na podstawie przesłanki mówiącej o interesie handlowym usługodawcy, który jedynie umożliwia instytucji korzystanie z danego programu do zautomatyzowanego podejmowania decyzji. W takiej sytuacji kluczowy byłby element analizy mający na celu wykazanie istnienia przeważającego interesu publicznego, który mógłby umożliwić ujawnienie dokumentu będącego przedmiotem sporu. Z kolei w sytuacji, w której to twórcy kodu wnosiliby o zastosowanie tego wyjątku, to na nich ciążyłby obowiązek przedstawienia odpowiednich argumentów, na co wskazuje orzecznictwo TSUE dotyczące stosowania wyjątku dotyczącego interesów handlowych⁶³⁷.

Zgodnie z przedstawionym wyżej rozumowaniem możliwa byłaby próba argumentacji wskazująca na pełnienie przez zautomatyzowane podejmowanie decyzji funkcji zbliżonych do prawa. W świetle połączenia argumentów opartych na dostępie do dokumentów dotyczących procesu ustawodawczego oraz odnoszących się do zasady przejrzystości i otwartości można by próbować uzasadnić konieczność uzyskania dostępu do kodu. Możliwość taka jest uzależniona przede wszystkim od doceniania wagi otwartości kodu dla możliwości sprawowania demokratycznej kontroli nad wprowadzanymi rozwiązaniami technologicznymi, które w rzeczywistości pełnią funkcję prawa. Dostrzeżenie, że jego dostępność powinna być traktowana jako argument

⁶³⁶ Na przykład systemy mające wspierać działania w zakresie prewencji przestępczości mogłyby być potraktowane jako objęte wyjątkiem z zakresu bezpieczeństwa publicznego.

⁶³⁷ „[...] osobie, która wnosi o zastosowanie jednego z tych wyjątków przez instytucję, organ lub jednostkę organizacyjną Unii, do których ma zastosowanie wspomniane rozporządzenie, spoczywa obowiązek przedstawienia w stosownym czasie odpowiednich wyjaśnień instytucji, organowi lub jednostce organizacyjnej, o których mowa”. Wyrok Trybunału z dnia 22 stycznia 2020 r. w sprawie C-175/18 P, *PTC Therapeutics International Ltd przeciwko Europejska Agencja Leków (EMA)*, ECLI:EU:C:2020:23, pkt 95. Tak samo w: Wyrok Trybunału z dnia 22 stycznia 2020 r. w sprawie C-178/18 P, *MSD Animal Health Innovation GmbH i Intervet International BV przeciwko Europejska Agencja Leków (EMA)*, ECLI:EU:C:2020:873, pkt 94-96 i Wyrok Trybunału z dnia 29 października 2020 r. w sprawie C-576/19 P, *Intercept Pharma Ltd i Intercept Pharmaceuticals Inc. przeciwko Europejska Agencja Leków (EMA)*, ECLI:EU:C:2020:873, pkt 52-53.

przemawiający za istnieniem przeważającego interesu publicznego, warunkuje uznanie istnienia konieczności odstąpienia od zastosowania wyjątków fakultatywnych przez instytucje.

Ponadto w świetle potencjalnej dyskryminacji występującej w przypadku stosowania zautomatyzowanego podejmowania decyzji można by próbować dodatkowo odnieść się do zakazu dyskryminacji jako kolejnego interesu publicznego, którego ochrona powinna przeważać nad ochroną interesów handlowych. Nawiązując do argumentacji przedstawionej w rozdziale pierwszym, należy podkreślić, że zautomatyzowane podejmowanie decyzji może opierać się na mechanizmach inherentnie dyskryminujących. Brak wglądu w kod komputerowy używany w stosowanych systemach zautomatyzowanego podejmowania decyzji prowadzi do uniemożliwienia weryfikacji zasad, zgodnie z którymi odbywa się przyporządkowywanie jednostek do grup poddanych danemu sposobowi traktowania. Niejawność systemów zautomatyzowanego podejmowania decyzji jest więc przeszkodą do oceny ich zgodności z zakazem dyskryminacji. W razie dostrzeżenia, że zakaz dyskryminacji mógłby być traktowany jako przeważający interes publiczny, zagwarantowanie dostępu do kodu komputerowego używanego w ramach zautomatyzowanego podejmowania decyzji jako do dokumentu byłoby narzędziem wspomagającym argumentację za niepodleganiem danej sytuacji wyjątkom fakultatywnym od ogólnej zasady jak najdalej idącej otwartości.

Problem, jaki mógłby się pojawić w razie traktowania kodu komputerowego jako dokumentu, wiąże się ze specyfiką kodu jako tekstu. Udzielenie do niego np. dostępu częściowego mogłoby spowodować więcej konfuzji niż wsparcia w zrozumieniu zasad działania używanego rozwiązania. Można jednocześnie argumentować, że tym istotniejsze byłoby udostępnianie całości kodu jako rozwiązania umożliwiającego kompleksowe zbadanie np. w jaki sposób on działa, czy zastosowane w nim rozwiązania mogą mieć charakter dyskryminacyjny i czy jego wdrożenie może prowadzić do dyskryminacji.

Barierą dostępu do kodu używanego w ramach zautomatyzowanego podejmowania decyzji mogłoby również okazać się podejście TSUE opierające się na perspektywie użytkownika danego systemu informatycznego. W odniesieniu do baz danych TSUE stawia granicę „istniejących dokumentów” tak daleko, jak daleko sięgają kompetencje użytkownika bazy do wyszukiwania w niej danych, bez nadmiernego nakładu pracy. Postawienie w podobny sposób sprawy w odniesieniu do kodu komputerowego *de facto* uniemożliwiłoby domaganie się do niego dostępu.

Problematyczna jest również możliwość kontroli przez Sąd lub Trybunał treści kodu jako dokumentu. O ile w odniesieniu do tradycyjnych tekstów pisanych może być ona oceniana jako element postępu w postrzeganiu roli kontroli sądowej dotyczącej dostępu do dokumentów, o tyle trudno sobie wyobrazić analogiczną sytuację dotyczącą kodu. Przewrotnie można

stwierdzić, że jest to istotny argument przemawiający za koniecznością udostępniania treści kodu komputerowego używanego w ramach zautomatyzowanego podejmowania decyzji: w razie przyjęcia, że zautomatyzowane decyzje pełnią w rzeczywistości funkcje prawa, niepokojąca byłaby sytuacja, w której organ sądowiczy nie byłby w stanie zrozumieć, zgodnie z jakimi mechanizmami funkcje te pełni kod komputerowy. W takiej sytuacji ani jednostka podlegająca decyzji wydanej na podstawie zautomatyzowanego podejmowania decyzji nie byłaby w stanie zweryfikować, czy działanie takiego kodu jest np. zgodne z zakazem dyskryminacji, ani organ sądowiczy, przed którym mogłaby próbować dochodzić swoich praw. Dostęp do kodu jako dokumentu mógłby natomiast umożliwić weryfikację jego sposobu działania przez ekspertów, debatę publiczną na temat zastosowanych w nim rozwiązań, publikację informacji na jego temat w mediach i tym samym – potencjalnie – uświadomienie podlegającym jego działaniu jednostkom norm, które są wobec nich stosowane.

Podsumowując, można stwierdzić, że istnieje możliwość potraktowania kodu będącego zapisem systemu zautomatyzowanego podejmowania decyzji jako dokumentu w rozumieniu prawa UE. Hipotetycznie, w razie istnienia możliwości powoływania się przez daną instytucję na wyjątki fakultatywne, istnieje również możliwość argumentowania za dostrzeżeniem i udowodnieniem obecności przeważającego interesu publicznego, przemawiającego za koniecznością ujawnienia jego treści. Kluczem do rozstrzygnięcia tego typu sprawy na korzyść przejrzystości byłoby np. wykazanie bezpośredniego związku między systemem zautomatyzowanego podejmowania a ustawodawstwem. Po pierwsze, należałoby wskazać, że w danej sytuacji zautomatyzowane podejmowanie decyzji jest *de facto* prawem i ma dla jednostki skutki prawne. Po drugie, w niektórych sytuacjach⁶³⁸ można by odwołać się do orzecznictwa TSUE dotyczącego braku mocy wiążącej aktów prawnych, które nie zostały opublikowane, w zakresie, w jakim zmierzają one do nałożenia obowiązków na jednostki⁶³⁹, jeśli w rozważanej sytuacji zautomatyzowane podejmowanie decyzji miałyby takie skutki. Również prawdopodobne jest uzyskanie dostępu do dokumentów przygotowywanych w ramach procesu wdrażania systemu zautomatyzowanego podejmowania decyzji albo przynajmniej części zawartych w nich informacji.

Można by również rozważyć scenariusz, w którym – w przeciwieństwie do tego, jaka zwykle zachodzi relacja między dostępem do dokumentów

⁶³⁸ Mam tu na myśli wspomniane w rozdziale pierwszym sytuacje, w których kod komputerowy wdrażany jest w miejsce przepisów.

⁶³⁹ Zob. Wyrok Trybunału z dnia 10 marca 2009 r. w sprawie C-345/06, *Gottfried Heinrich*, ECLI:EU:C:2009:140, pkt 63 oraz jego krytyczne omówienie: M. Bobek, *Case C-345/06, Gottfried Heinrich, Judgment of the Court of Justice (Grand Chamber) of 10 March 2009, not yet reported*, „Common Market Law Review” 2009, t. 46, s. 2077–2094.

a ochroną danych osobowych⁶⁴⁰ – przeważający interes publiczny odnosiłby się właśnie do ochrony danych osobowych jako dobra zasługującego na ochronę i prowadzącego do niezastosowania wyjątków fakultatywnych. W świetle opisanych w książce rozwiązań wprowadzonych w RODO, powtórzonych w *rozporządzeniu 2018/1725*, dotyczących kwestii dostępu do wyjaśnień podstaw stojących za zautomatyzowanym podejmowaniem decyzji, można by próbować argumentować, że dostęp do kodu lub dokumentów powinien zostać uzasadniony przez interes publiczny w postaci kolektywnego wymiaru ochrony danych osobowych. Stanowiłoby to formę opisywanego w rozdziale pierwszym wyjaśnienia bazującego na modelu i uzupełnienie koncentrujących się na ochronie praw indywidualnych jednostki rozwiązań opisanych w rozdziale drugim nazywanych prawem do wyjaśnienia. Dokumenty pozyskane w ten sposób mogłyby pomóc zrozumieć sam system podejmowania decyzji w sposób zautomatyzowany, nie zaś jedynie indywidualny przypadek dotyczący danej osoby.

4.3.4. Porównanie konstrukcji wyjątków od prawa dostępu do dokumentów unijnych w prawie UE z konstrukcją wyjątków od prawa do informacji w orzecznictwie ETPCz

Rozważone w tym miejscu scenariusze zakładają, że z dużym prawdopodobieństwem udostępnienie dokumentów dotyczących zautomatyzowanego podejmowania decyzji wiązałoby się z koniecznością uzasadnienia istnienia przeważającego interesu publicznego przemawiającego za ich ujawnieniem. Jest to wynik analizy opartej na dotychczasowym podejściu do problematyki dostępu do dokumentów w prawie UE oraz jeden z kluczowych elementów odróżniających sposób myślenia o dostępie do dokumentów w prawie unijnym od stanowiska przedstawianego przez ETPCz w odniesieniu do dostępu do informacji. Konstrukcja wyjątków w orzecznictwie ETPCz, zgodnie z analizą przedstawioną w rozdziale trzecim, opiera się na następujących krokach: najpierw jest sprawdzane, czy sytuacja spełnia pozytywne warunki,

⁶⁴⁰ Czyli problemu związanego z możliwością udostępniania znajdujących się w dokumencie danych osobowych – kluczowe orzeczenie dla tego zagadnienia to Wyrok Trybunału z dnia 29 czerwca 2010 r. w sprawie C-28/08, *Komisja Europejska przeciwko The Bavarian Lager Co. Ltd.*, ECLI:EU:C:2010:378. Przykładowe artykuły dotyczące tej kwestii, zob. H. Kranenborg, *Access to Documents and Data Protection in the European Union: On the Public Nature of Personal Data*, „Common Market Law Review” 2009, t. 45, s. 1079–1114; D. Adamski, *How Wide Is “The Widest Possible”?*..., *op. cit.*, s. 527–529. Analiza relacji między prawem dostępu do dokumentów i informacji a ochroną danych osobowych i pośrednim wpływem regulacji na poziomie UE na krajowe porządki prawne w zakresie dostępu do informacji i dokumentów, zob. G. Sibiga, I. Małobęcka-Szwast, *Relacje prawa do informacji publicznej oraz prawa do ochrony danych osobowych w świetle ogólnego rozporządzenia o ochronie danych (RODO)*, „Monitor Prawniczy” 2019, nr 22 (dodatek specjalny: Polskie przepisy o ochronie danych osobowych), s. 60–73.

które mogą prowadzić do obowiązku udzielenia danych informacji. Następnie jest przeprowadzany test dotyczący warunków, które powinny być spełnione kumulatywnie, aby państwo mogło powołać się na dozwolone wyjątki.

Z tej przyczyny przedstawiona powyżej argumentacja Sądu w sprawie *Gabi Thesing i Bloomberg Finance LP przeciwko Europejskiemu Bankowi Centralnemu* może być postrzegana jako jedynie częściowo prawidłowa. Sam fakt, że dane ograniczenie jest przewidziane w prawie, nie jest w oczach ETPCz wystarczającym argumentem za odmówieniem dostępu do informacji. Po pierwsze, konieczne jest oparcie wyjątków na jednej z podstaw wymienionych w art. 10 ust. 2 EKPCz. W tym świetle wątpliwości może rodzić sam fakt szerszego katalogu interesów, których ochrona stanowi podstawę możliwości odmówienia dostępu do dokumentu, sformułowanego w *rozporządzeniu 1049/2001* w stosunku do tego, który zawarty został w art. 10 EKPCz. Należy zauważyć, że art. 11 KPP w ogóle nie uwzględnia możliwości ograniczenia praw w nim zawartych. Tym samym wyraźna staje się różnica między tym, jak sformułowane zostało prawo dostępu do dokumentów w prawie UE, a tym, jak brzmi prawo dostępu do informacji w orzecznictwie ETPCz. W odniesieniu do prawa dostępu do dokumentów – zgodnie z art. 15 ust. 3 TFUE – możliwe jest wprowadzanie ograniczeń rozporządzeniem przyjętym w ramach zwykłej procedury ustawodawczej. Gdyby TSUE był gotowy uznać istnienie prawa dostępu do informacji na podstawie treści art. 11 KPP, sam katalog powodów, w związku z którymi można by je ograniczać, nie powinien być szerszy niż ten, który uwzględniony jest w art. 10 EKPCz.

Po drugie, zgodnie z orzecznictwem ETPCz i z argumentacją Sądu w sprawie *Gabi Thesing i Bloomberg Finance LP przeciwko Europejskiemu Bankowi Centralnemu* ograniczenia dotyczące prawa dostępu do informacji muszą być przewidziane w ustawie. Odwołanie przez Sąd do tej kwestii stanowiło przykład przeniesienia warunków dotyczących prawa dostępu do informacji na rozumowanie dotyczące prawa dostępu do dokumentów. Jednocześnie jest ono zgodne z art. 15 ust. 3 TFUE i wymogiem zawarcia warunków korzystania z prawa dostępu do dokumentów i ograniczeń tego prawa w rozporządzeniu. Warunek ten jest wspólny prawu dostępu do dokumentów w prawie UE i prawu dostępu do informacji w orzecznictwie ETPCz.

Po trzecie, zgodnie z orzecznictwem ETPCz dotyczącym prawa dostępu do informacji niezbędne jest wykazanie przez państwo, że ograniczenie jest „konieczne w demokratycznym społeczeństwie”. Tymczasem w prawie UE dotyczącym dostępu do dokumentów nacisk jest położony raczej na uzasadnienie ze strony wnioskodawcy, które ukazywałoby nadrzędny interes publiczny mogący stanowić podstawę odstąpienia od wyjątku. Mimo konieczności uzasadniania decyzji ciążącej na unijnych instytucjach, ostatecznie to wnioskodawca musi wykazać, dlaczego udzielenie dostępu do dokumentu jest istotne, aby możliwe było odstąpienie od stosowania wyjątku. Tymczasem

w świetle orzecznictwa ETPCz to raczej państwo musi wykazać, że udzielenie dostępu do informacji jest niemożliwe. Ponadto test zaproponowany przez ETPCz nie uwzględnia możliwości stosowania wyjątków obligatoryjnych. Możliwość wykazania, że dane ograniczenie nie jest niezbędne w demokratycznym społeczeństwie, przynajmniej teoretycznie, powinna pozwolić w każdej sytuacji podważyć zgodność z prawem ograniczeń wprowadzanych przez państwo. Tymczasem unijne prawo dostępu do dokumentów jest pod tym względem bardziej restrykcyjne.

4.4. Dostęp do dokumentów i informacji w prawie UE w świetle zautomatyzowanego podejmowania decyzji w państwach członkowskich

Regulacje unijne są bardziej restrykcyjne również w porównaniu z prawem dostępu do dokumentów i informacji niektórych państw członkowskich. Kluczowym przykładem ilustrującym ten stan rzeczy jest wyrok w sprawie *Svenska Journalistförbundet przeciwko Radzie Unii Europejskiej*⁶⁴¹. Dotyczyła ona wniosku o dostęp do tych samych 20 dokumentów skierowanego przez Szwedzkie Stowarzyszenie Dziennikarzy do władz szwedzkich oraz do Rady. Władze szwedzkie udzieliły dostępu do 18 dokumentów, podczas gdy Rada jedynie do dwóch. Sprawa ta pokazuje, że problemy wiążące się z poziomem otwartości promowanym głównie przez państwa skandynawskie i poziomem otwartości promowanym na poziomie UE znacznie utrudniają dyskusję na temat wypracowania wspólnych standardów w tym zakresie⁶⁴². Mimo to prawo dotyczące dostępu do dokumentów – a właściwie „informacji sektora publicznego” – zostało w pewnym stopniu zharmonizowane⁶⁴³. Obecnie problematykę tę reguluje *dyrektywa 2019/1024*.

⁶⁴¹ Wyrok Sądu pierwszej instancji z dnia 17 czerwca 1998 r. w sprawie T-174/95, *Svenska Journalistförbundet przeciwko Radzie Unii Europejskiej*, ECLI:EU:T:1998:127.

⁶⁴² Zob. I. Österdahl, *Case T124/96, Interporc Imund Export GmbH v. Commission, Judgment of 6 February 1998*, [1998] ECR II0231; *Case T83/96, Gerard van der Wal v. Commission, Judgment of 19 March 1998*, [1998] ECR II0545; *Case T174/95, Svenska Journalistförbundet v. Council of the European Union, Judgment of 17 June 1998*, [1998] ECR II2289, „Common Market Law Review” 1999, t. 36, s. 1075.

⁶⁴³ Wpierw za sprawą *dyrektywy 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego*, Dz.Urz. UE 2003 L 345, s. 90–96 (polskie wydanie specjalne: rozdz. 13, t. 32, s. 701–707), zmienionej następnie *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 publicznego*, Dz.Urz. UE 2013 L 175, s. 1–8. Omówienie zagadnienia dostępu do informacji sektora publicznego na tle stanu prawnego sprzed nowelizacji dyrektywy w 2019 r., zob. M. Van Eechoud, K. Janssen, *Rights of Access to Public Sector Information*, „Masaryk University Journal of Law and Technology” 2012, t. 6, nr 3, s. 471–500.

4.4.1. Dyrektywa 2019/1024 w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego a zautomatyzowane podejmowanie decyzji

Przyjęcie *dyrektywy 2019/1024* jest wynikiem spostrzeżenia, że w obliczu rozwoju gospodarki cyfrowej dotychczasowe regulacje odnoszące się do dostępu do informacji sektora publicznego nie są wystarczające⁶⁴⁴. Celem przyjęcia dyrektywy było, zgodnie z art. 1, propagowanie wykorzystywania otwartych danych i stymulowania innowacji w produktach i usługach, a jej przedmiotem jest regulacja ponownego wykorzystywania istniejących dokumentów będących w posiadaniu organów sektora publicznego i przedsiębiorstw publicznych państw członkowskich.

Treść *dyrektywy 2019/1024* jest istotna dla tematu analizy przede wszystkim ze względu na bezpośrednie odniesienie do możliwości uznawania programu komputerowego za dokument. Zgodnie z motywem 30 definicja „dokumentu” nie ma obejmować programów komputerowych, chociaż państwa członkowskie mogą rozszerzyć jej zakres stosowania na programy komputerowe. Treść definicji terminu „dokument”, podana w art. 2 ust. 6⁶⁴⁵, nie zawiera jednak takiego stwierdzenia. Jest ona zasadniczo powtórzeniem definicji dokumentu znanej z *rozporządzenia 1049/2001*, ze zmianą w postaci uwzględnienia wprost możliwości dostępu częściowego. Skoro motyw dyrektywy przewiduje możliwość traktowania programu komputerowego jako dokumentu, można stwierdzić, że zasadniczo możliwe jest, w świetle definicji dokumentu w prawie unijnym, traktowanie programu komputerowego jako dokumentu. Świadczy o tym również zawarcie wyłączenia tej kategorii dokumentów z definicji zawartej w *dyrektywie 2019/1024*. Ich wyłączenie wprost może być odczytywane jako świadectwo możliwości traktowania programów komputerowych jako dokumentów w razie braku takiego wyłączenia⁶⁴⁶.

⁶⁴⁴ Zob. motywy 1–13, a zwłaszcza 10–12, *dyrektywa 2019/1024*.

⁶⁴⁵ Dokument oznacza: „a) dowolną treść niezależnie od jej nośnika (papier lub forma elektroniczna lub zapis dźwiękowy, wizualny bądź audiowizualny); lub b) dowolną część tej treści” – art. 2 ust. 6, *dyrektywa 2019/1024*.

⁶⁴⁶ Na przykład w uzasadnieniu projektu ustawy transponującej dyrektywę w Polsce czytamy: „Z kolei ograniczenie prawa do ponownego wykorzystywania w zakresie informacji sektora publicznego stanowiących program komputerowy (art. 6 ust. 4 pkt 7) jest zgodne z rozumieniem definicji „dokumentu” przyjętej na gruncie dyrektywy 2019/1024/UE. Zgodnie z motywem 30 preambuły dyrektywy definicja „dokumentu” wskazana w art. 2 pkt 6 nie obejmuje programów komputerowych. Jednocześnie jednak państwa członkowskie mogą rozszerzyć zakres stosowania dyrektywy na programy komputerowe. Stąd w art. 10 ust. 5 projektu ustawy wskazano możliwość udostępniania lub przekazywania przez podmioty zobowiązane do ponownego wykorzystywania kodów źródłowych lub innych elementów programów komputerowych opracowanych w ramach realizacji zadań publicznych”. *Uzasadnienie do projektu ustawy z dnia o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego z 29 czerwca 2021 r.*, Druk nr 1338, Warszawa,

Kolejnym istotnym dla omawianych tu problemów elementem *dyrektywy 2019/1024* jest chaos pojęciowy w zakresie określenia, czym są dokument, informacja i dane. Chociaż wszystkie wersje językowe dyrektywy mają w tytule słowo oznaczające „informację”⁶⁴⁷, to pojęcie to nie pojawia się w art. 1 dyrektywy opisującym jej przedmiot i zakres zastosowania. W art. 1 ust. 1, który określa zakres zastosowania dyrektywy, są wymienione dokumenty będące w posiadaniu organów sektora publicznego państw członkowskich, dokumenty będące w posiadaniu przedsiębiorstw publicznych należących do wymienionych w dyrektywie kategorii oraz dane badawcze. Z kolei ust. 2, który wymienia kategorie, do których dyrektywa nie ma zastosowania, w jedenastu na dwanaście przypadków posługuje się terminem „dokument”⁶⁴⁸.

Termin „informacja” nie jest również definiowany w art. 2 *dyrektywy 2019/1024*. Tym samym można podejrzewać, że jest on używany jako pojęcie bardziej ogólne i abstrakcyjne, które zawiera wszystkie elementy opisane jako przedmiot regulacji w dyrektywie. O takiej interpretacji świadczy również uwzględnienie w motywie 5 dyrektywy odesłania do art. 11 KPP jako podstawy istnienia prawa podstawowego w postaci „dostępu do informacji”. Interpretacja taka jest odwróceniem optyki, w której informacja jest traktowana jako element dokumentu. W świetle *dyrektywy 2019/1024* to ona staje się głównym pojęciem opisującym prawa jednostek dotyczące dostępu do informacji sektora publicznego w państwach członkowskich.

Ponadto na podkreślenie zasługuje włączenie do dokumentów objętych zakresem zastosowania dyrektywy kategorii dokumentów będących w posiadaniu przedsiębiorstw publicznych⁶⁴⁹. Jest to wynikiem rozpoznania, że wyłączenie przedsiębiorstw publicznych z zakresu stosowania przepisów dotyczących ponownego wykorzystania informacji sektora publicznego prowadzi do niskiej dostępności dokumentów produkowanych przy realizacji usług świadczonych w interesie ogólnym⁶⁵⁰. Jednoczesne uwzględnienie w *dyrektywie*

29 czerwca 2021 r., s. 27. <https://orka.sejm.gov.pl/Druki9ka.nsf/0/057A8FFDE2C50C-63C12587040037BD25/%24File/1338.pdf> dostęp: 17.07.2021.

⁶⁴⁷ Według mojej najlepszej wiedzy.

⁶⁴⁸ Ust. 2 lit. g mówi o „logach, herbach i symbolach” – art. 1 ust. 2 lit. g, *dyrektywa 2019/1024*.

⁶⁴⁹ Są to następujące kategorie przedsiębiorstw publicznych: „(i) prowadzą działalność w obszarach określonych w dyrektywie 2014/25/UE; (ii) działają w charakterze podmiotów świadczących usługi publiczne zgodnie z art. 2 rozporządzenia (WE) nr 1370/2007; (iii) działają w charakterze przewoźników lotniczych wykonujących obowiązki użyteczności publicznej zgodnie z art. 16 rozporządzenia (WE) nr 1008/2008; lub (iv) działają w charakterze armatorów Wspólnoty wykonujących zobowiązania z tytułu świadczenia usług publicznych zgodnie z art. 4 rozporządzenia (EWG) nr 3577/92” – art. 1 ust. 1 lit. b, *dyrektywa 2019/1024*.

⁶⁵⁰ Zob. motyw 24, *dyrektywa 2019/1024*.

2019/1024 bardzo szerokiego katalogu kategorii dokumentów wyłączonych z zakresu stosowania dyrektywy może prowadzić do ograniczenia w praktyce znaczenia nowej regulacji.

Z niemal całkowitą pewnością można założyć, że treść motywu 30 *dyrektywy 2019/1024* wprost wykluczy możliwość traktowania systemów służących do zautomatyzowanego podejmowania decyzji wykorzystywanych przez państwa członkowskie z zakresu jej stosowania. Mimo braku mocy prawnie wiążącej motywów uwzględnienie takiego rozwiązania w treści *dyrektywy 2019/1024* prawdopodobnie byłoby wzięte pod uwagę przez TSUE w razie ewentualnego sporu dotyczącego wykładni dyrektywy. Tym samym dyrektywa nie będzie miała praktycznego znaczenia dla problemu zautomatyzowanego podejmowania decyzji. Wyjątkiem będą państwa, które zdecydują się traktować programy komputerowe jako dokumenty, co może doprowadzić do stworzenia różnych poziomów ochrony w różnych państwach członkowskich i tym samym – w pewnym stopniu – zaprzepaścić wysiłki dążące do unifikacji regulacji dotyczących zautomatyzowanego podejmowania decyzji na podstawie prawa ochrony danych osobowych. *Dyrektywa 2019/1024* jest jednak pierwszym krokiem do rozpoznania prawa dostępu do informacji jako prawa podstawowego uwzględnionego w KPP, co pośrednio może mieć istotny wpływ na zwiększenie przejrzystości w odniesieniu do systemów zautomatyzowanego podejmowania decyzji.

4.4.2. Prawa podstawowe a dostęp do informacji o zautomatyzowanym podejmowaniu decyzji

W świetle wskazanej powyżej wzmianki na temat prawa do informacji zawartego w art. 11 KPP warto spróbować rozważyć możliwe konsekwencje rozwoju orzecznictwa TSUE w kierunku uznawania prawa dostępu do informacji jako inherentnie obecnego w treści tego przepisu. Ze względu na zakres zastosowania KPP uznanie prawa do informacji jako części art. 11 mogłoby wpłynąć na włączenie państw członkowskich do grona podmiotów objętych jego oddziaływaniem. Zgodnie z zakresem zastosowania KPP w razie uznania istnienia prawa dostępu do informacji powinno być ono traktowane jako wiążące państwa członkowskie w zakresie, w jakim stosują one prawo unijne. Stanowiłoby to istotną zmianę w stosunku do reżimu opartego na art. 15 TFUE (i znajdującego odzwierciedlenie w art. 42 KPP), który dotyczy jedynie dostępu do dokumentów udzielanego przez instytucje, organy i jednostki organizacyjne UE.

Taka wykładnia KPP umożliwiłaby ponadto niejako pomocnicze traktowanie prawa dostępu do informacji jako narzędzia realizacji innych praw gwarantowanych jednostkom w prawie unijnym. Tym samym przedmiotem potencjalnego sporu mógłby być nie sam dostęp do dokumentów na podstawie *dyrektywy 2019/1024*, lecz dostęp do dokumentu w postaci programu

komputerowego jako narzędzie realizacji np. unijnego prawa antydyskryminacyjnego⁶⁵¹. W razie wdrażania przez państwa członkowskie systemów zautomatyzowanego podejmowania decyzji w obszarach objętych unijnymi dyrektywami antydyskryminacyjnymi można wyobrazić sobie sytuację, w której pojawiłyby się wątpliwości dotyczące zgodności zastosowanych rozwiązań technologicznych z wymogami prawnymi wynikającymi z dyrektyw. Możliwość dostępu do kodu będącego podstawą do podejmowanych w sposób zautomatyzowany decyzji byłaby kluczowym aspektem badania tej niezgodności.

Hipotetycznym przykładem mógłby być system zautomatyzowanego podejmowania decyzji wdrożony na poziomie krajowym, który wspierałby procesy rekrutacyjne dotyczące nauczycieli, czyli element wchodzący w zakres regulowanego przez prawo unijne dostępu do zatrudnienia. Zasady działania systemu, do którego dostęp byłby wykupiony od prywatnego przedsiębiorcy, byłyby utajnione. Ogólnie dostępne byłyby wytyczne dotyczące poziomu kwalifikacji niezbędnego do kandydowania na dane stanowiska. Po kilku miesiącach od wdrożenia systemu okazałoby się, że na stanowiskach kierowniczych nie została zatrudniona ani jedna kobieta, na stanowiskach zaś obejmujących naukę na najwcześniejszych etapach edukacji – ani jeden mężczyzna. Dodatkowo pojawiłyby się wątpliwości dotyczące dyskryminacji na tle pochodzenia, ponieważ system nie rekomendowałby osób, których nazwiska sugerowałyby, że są innej narodowości niż obywatele państwa, które ów system wdrożyło. Ministerstwo odpowiedzialne za wdrożenie systemu utrzymywałoby, że jest on bardziej bezstronny niż procesy rekrutacyjne, które występowały wcześniej. Przedsiębiorstwo odpowiedzialne za kod używany w ramach systemu zautomatyzowanego podejmowania decyzji opublikowałoby ulotkę, w której powoływałoby się na fakt, że używa wysoce zaawansowanych technologii informatycznych w tworzonych przez siebie rozwiązaniach. Ponadto utrzymywałoby ono, że kod został napisany zgodnie z wytycznymi otrzymanymi od ministerstwa.

W takiej sytuacji dostęp do kodu byłby warunkiem koniecznym do oceny, czy państwo członkowskie postępuje zgodnie z prawem UE. W świetle przepisów regulujących dostęp do dokumentów w prawie unijnym możliwość uzyskania dostępu do kodu w takiej sytuacji jest marginalna. Przede wszystkim musiałby on być w posiadaniu instytucji unijnych. Ponadto państwo członkowskie mogłoby wyrazić sprzeciw wobec udostępnienia go, który

⁶⁵¹ Rozważania na temat związków między zasadą przejrzystości a równym traktowaniem głównie na tle zamówień publicznych, zob. S. Prechal, M. de Leeuw, *Dimensions of Transparency: The Building Blocks for a New Legal Principle?*, „Review of European Administrative Law” 2007, nr 1, s. 57–61. Autorki stawiają w tekście m.in. hipotezę dotyczącą możliwości rozszerzenia zasady przejrzystości na inne aspekty prawa UE (s. 60).

mógłby zostać uwzględniony przez instytucję unijną. Prawdopodobnie istniałaby również konieczność wykazania nadrzędnego interesu publicznego przemawiającego za jego udostępnieniem. Natomiast w razie wykładni art. 11 KPP zgodnej z wykładnią art. 10 EKPCz sytuacja przedstawiałaby się nieco inaczej. W związku z zakresem stosowania KPP możliwe byłoby powołanie się na prawo dostępu do informacji wynikające z faktu, że sytuacja objęta byłaby zakresem zastosowania prawa unijnego przez państwo członkowskie. Dostęp do kodu stanowiłby narzędzie realizacji praw uwzględnionych w unijnych przepisach antydyskryminacyjnych. Dostęp do kodu mógłby być przedstawiany jako konieczny w związku z brakiem innej możliwości weryfikacji zgodności z unijnym prawem zachowania państwa i tego, w jaki sposób traktowane są jednostki.

Opór TSUE przed uznaniem prawa dostępu do informacji za prawo podstawowe jest tym bardziej niezrozumiałe, że wydaje się ono spełniać wszelkie przesłanki pozwalające uznać je za zasadę ogólną. Prawo dostępu do informacji jest obecne w większości konstytucji lub innych wysokiej rangi aktach prawnych państw członkowskich. Jest ono również rozpoznawane przez ETPCz jako jeden z elementów praw gwarantowanych przez EKPCz⁶⁵². Co więcej, ma ono ogromne znaczenie dla weryfikacji stosowania prawa oraz działania władz publicznych przez zewnętrzne podmioty (media, organizacje pozarządowe). Stąd też wskazane wydawałoby się docenienie jego znaczenia przez TSUE jako organu sądowiczego organizacji opierającej się na tworzeniu i stosowaniu wspólnych rozwiązań prawnych. Ponadto ignorowanie znaczenia dostępu do informacji oznacza utrudnianie realizacji innych praw i zasad prawa UE, np. zakazu dyskryminacji. Wraz z rozpowszechnianiem się stosowania zautomatyzowanego podejmowania decyzji konieczność sięgnięcia po środki prawne zwiększające przejrzystość takich systemów będzie stawała się coraz bardziej paląca. Uznanie, że prawo dostępu do informacji jako prawo podstawowe jest jedną z zasad ogólnych prawa UE, mogłoby wzmocnić mechanizmy chroniące przed zautomatyzowaną, algorytmiczną dyskryminacją.

4.4.3. Dostęp do dokumentów jako element wartości unijnych

W świetle aksjologii przyświecającej wprowadzaniu regulacji dotyczących dostępu do dokumentów w prawie UE na rozważenie zasługuje ponadto scenariusz odwołujący się do zasady demokracji. Historycznie prawo dostępu do dokumentów było w prawie unijnym rozwijane jako element demokracji charakteru unijnych procedur i instytucji. Odwrócenie tej logiki nakazuje postawić pytanie, czy prawo dostępu do dokumentów może być

⁶⁵² Zob. *The Laws of Transparency in Action. A European Perspective*, red. D.C. Dragos, P. Kovač, A.T. Marseille, Palgrave Macmillan, Cham 2019.

potraktowane jako element wartości wchodzących w zakres art. 2 TUE. Skoro Unia opiera się m.in. na wartościach poszanowania demokracji i państwa prawnego, a dostęp do dokumentów jest jednym ze sposobów realizacji zasady demokracji, wartości zaś – w tym poszanowania demokracji i państwa prawnego – są wspólne państwu członkowskiemu, to czy brak realizacji prawa dostępu do dokumentów może być traktowany jako naruszenie wartości unijnych przez państwo członkowskie?

Pytanie to może wydawać się daleko idącą hipotezą. Kiedy jednak rozważy się je w świetle konkretnych możliwości używania systemów zautomatyzowanego podejmowania decyzji, może ono być potraktowane jako bardziej realistyczny scenariusz. Po pierwsze, może się pojawić już wspomniany problem zastępowania przepisów przez odwołania do systemów zautomatyzowanego podejmowania decyzji. Mechanizm taki może rodzić wątpliwości w świetle demokratycznych procedur tworzenia prawa. Dotychczasowe doświadczenia w zakresie prób pociągnięcia państw członkowskich do odpowiedzialności za naruszenia wartości z art. 2 ukazują praktyczną niewykonalność takiego scenariusza. Barięą jest chociażby zróżnicowanie standardów dotyczących procedur legislacyjnych czy rozwiązań instytucjonalnych między państwami członkowskimi⁶⁵³.

Zastępowanie elementów aktów prawnych odesłaniami do informatycznych systemów zautomatyzowanego podejmowania decyzji nie wydaje się jednak wystarczająco ewidentnym i radykalnym problemem w świetle naruszenia takich wartości jak rządy prawa czy demokracja. Prawdopodobnie, aby zaalarmować unijne instytucje, państwo członkowskie musiałoby posunąć się do próby wdrożenia systemu tak dalece odbiegającego od europejskich norm dotyczących ochrony prywatności i danych osobowych, jak np. rozwiązania, które przypominałyby chińskie eksperymenty z *Social Credit System*, czyli próbę wprowadzania kompleksowego systemu oceniającego poszczególne zachowania jednostki i na podstawie analizy danych determinującego jej możliwości korzystania np. z danych usług.

Po drugie, mogą się pojawić konkretne sfery powiązane bezpośrednio z unijnymi wartościami, w których stosowanie zautomatyzowanego podejmowania decyzji będzie tworzyło możliwość kwestionowania ich zgodności z prawem UE. Przykładem takiego obszaru może być skuteczna ochrona prawna. Zgodnie z orzecznictwem TSUE istnieje związek między zasadą skutecznej ochrony prawnej z art. 19 TUE a niezależnością sądownictwa⁶⁵⁴.

⁶⁵³ Poziom zróżnicowania modeli europejskiej demokracji liberalnej jest jednym z najczęściej pojawiających się argumentów w odniesieniu do ukazywania słabości prób tworzenia wspólnych standardów w tym zakresie, zob. J.W. Muller, *Defending Democracy within the EU*, „Journal of Democracy” 2013, t. 24, nr 2, s. 138.

⁶⁵⁴ Na przykład Wyrok Trybunału z dnia 27 lutego 2018 r. w sprawie C-64/16, *Associação Sindical dos Juízes Portugueses przeciwko Tribunal de Contas*, ECLI:EU-

W orzecznictwie jest podkreślana konieczność zagwarantowania, że zasady rządzące organizacją krajowych sądów, jako sądów unijnych, np. składem organu czy sposobem wyboru jego członków, gwarantują ich niezawisłość i bezstronność. TSUE podkreśla, że państwa członkowskie są zobowiązane przestrzegać zasad „pozwalających wykluczyć, w przekonaniu uczestników postępowania, wszelką uzasadnioną wątpliwość co do niezależności tego organu od czynników zewnętrznych oraz neutralności w odniesieniu do sprzecznych ze sobą interesów”⁶⁵⁵. Aby dany organ był uznany za niezawisły, a zatem za sąd w rozumieniu unijnym i w związku z tym za spełniający wymogi związane z zagwarantowaniem skutecznej ochrony prawnej, państwo członkowskie musi spełnić te wymogi w odniesieniu do zasad rządzących organizacją systemu sądownictwa.

Tymczasem rozwijanie systemów mających wspierać sędziów w wydawaniu wyroków i systemów mających na celu przydzielanie sędziom spraw mogą wywoływać wątpliwości w zakresie tego, czy używanie systemów zautomatyzowanego podejmowania decyzji w sądownictwie nie stoi w sprzeczności z poszanowaniem niezależności sądownictwa i tym samym skutecznej ochrony prawnej. Można zastanawiać się, czy wdrażanie systemu zautomatyzowanego przydzielania spraw sędziom w państwie, co do którego istnieją poważne wątpliwości w zakresie zgodności działań jego rządu z wartościami unijnymi, nie tworzy zagrożenia dla niezależności sądownictwa. W związku z tajnym charakterem zasad stojących za podejmowanymi przez system informatyczny decyzjami nie ma możliwości weryfikacji jego rzeczywistej obiektywności. Dostęp do kodu używanego w ramach systemu mógłby – w takiej sytuacji – stanowić element niezbędny do sprawdzenia zgodności działań państwa członkowskiego z unijnymi wartościami.

4.5. Podsumowanie

Dotychczasowa perspektywa przyjmowana w odniesieniu do dostępu do dokumentów instytucji unijnych stoi w sprzeczności ze sposobem postrzegania prawa do informacji w najnowszym orzecznictwie ETPCz dotyczącym tej kwestii. Mimo ewolucji unijnego prawa pierwotnego i wtórnego w zakresie dostępu do dokumentów trudno stwierdzić, aby zaczął on być postrzegany jako element szerszej kwestii dostępu do informacji. Wbrew

:C:2018:117 czy Wyrok Trybunału z dnia 25 lipca 2018 r. w sprawie C-216/18 PPU, LM, ECLI:EU:C:2018:586. Problem ten analizę w artykule J. Mazur, *Automated Decision-Making Systems as a Challenge for Effective Legal Protection in European Union Law*, „European Law Review” 2021, t. 46, nr 2, s. 194–210.

⁶⁵⁵ Zob. Wyrok Trybunału z dnia 25 lipca 2018 r. w sprawie C-216/18 PPU, LM, ECLI:EU:C:2018:586 i cytowane tam orzecznictwo, pkt 66.

odesłaniom do zasad przejrzystości i otwartości, dotychczasowe orzecznictwo TSUE jest raczej świadectwem dominacji formalistycznej wykładni przepisów *rozporządzenia 1049/2001* i odpowiednich decyzji instytucji regulujących dostęp do ich dokumentów. Szczególnie wyraźnym przykładem rozbieżności między strategią TSUE a orzecznictwem ETPCz jest sam sposób łączenia zagadnienia dostępu do dokumentów urzędowych z treścią art. 42 KPP przy jednoczesnym marginalizowaniu wpływu najnowszej wykładni ETPCz dotyczącej art. 10 EKPCz, która powinna być odczytywana jako mająca wpływ na sposób rozumienia treści art. 11 KPP. W orzecznictwie TSUE można zaobserwować brak systematyzacji relacji między treścią prawa dostępu do dokumentów urzędowych a treścią prawa dostępu do informacji. Przejawia się on m.in. w sposobie formułowania rozważań dotyczących wyjątków od prawa dostępu do dokumentów w prawie UE w zestawieniu z możliwościami ograniczenia prawa do informacji zgodnymi z wykładnią art. 10 EKPCz.

Biorąc pod uwagę samą definicję dokumentu w prawie UE, traktowanie programu komputerowego używanego do zautomatyzowanego podejmowania decyzji właśnie jako dokumentu jest możliwe do uzasadnienia. Ponadto perspektywa, w której zautomatyzowane podejmowanie decyzji może być potraktowane jako *de facto* działalność legislacyjna, może dostarczyć argumentów za dążeniem do uzyskania wyższego stopnia przejrzystości i otwartości używanych w jego ramach rozwiązań informatycznych. Byłoby to zgodne z funkcjonalnym podejściem do analizy tego, jaką rolę odgrywa zautomatyzowane podejmowanie decyzji, zastępujące niekiedy przepisy. Można jednak wyrazić obawę, że formalistyczna, pozytywistyczno-prawna perspektywa podchodzenia do tego, czym jest akt prawny, zgodnie z którą np. akt ustawodawczy musi zostać przyjęty w procedurze ustawodawczej, uniemożliwiłaby TSUE analizę kodu komputerowego jako elementu tworzącego lub współtworzącego akt prawny. Tymczasem wychodząc z realistyczno-prawnego punktu widzenia, można by stwierdzić, że kluczowe do oceny, czy dany akt powinien być postrzegany jako akt prawny, są np. skutki, jakie wywołuje on dla jednostki. Wówczas kształtowanie jej sytuacji prawnej (np. w zakresie możliwości korzystania z danych usług publicznych lub warunków, na jakich możliwe jest korzystanie z nich) przemawiałoby za uznaniem algorytmów stosowanych w ramach zautomatyzowanego podejmowania decyzji właśnie jako aktów prawnych. Dodatkowo problemy mogą pojawić się w związku z tym, jakiego rodzaju wyjątki mogą być przywoływane w kontekście takich spraw przez unijne instytucje. Konieczność wykazania stojącego za ujawnieniem przeważającego interesu publicznego może stanowić poważną trudność w ramach postępowań dotyczących ewentualnego pozyskania dostępu do programu komputerowego jako dokumentu instytucji unijnej.

Przesłanką pozwalającą formułować ostrożne przewidywania dotyczące ewentualnej zmiany postrzegania prawa dostępu do dokumentów w prawie UE jest motyw 5 *dyrektywy 2019/1024*, w którym pojawia się odesłanie do treści art. 11 KPP oraz zawarcie w treści dyrektywy możliwości traktowania kodu komputerowego jako dokumentu. W razie uwzględnienia go w przyszłym orzecznictwie TSUE hipoteza Carol Harlow, zgodnie z którą w prawie unijnym dostęp do informacji jest postrzegany raczej jako prawo jednostki, nie zaś jako publiczne prawo do wiedzy⁶⁵⁶, może stracić na aktualności. Podążenie za stanowiskiem, zgodnie z którym dostęp do dokumentów jest częścią praw związanych z wolnością wyrazu, może pozwolić na potraktowanie tego zagadnienia jako problemu nie tyle jednostkowego, ile raczej społecznego. W odniesieniu jednak do samego zautomatyzowanego podejmowania decyzji przepisy dyrektywy nie przyniosą raczej żadnych zmian, ze względu na zawarcie w treści jej motywów wyłączenia programów komputerowych z zakresu znaczeniowego pojęcia „dokument”.

Ponadto *dyrektywa 2019/1024* dotyczy ponownego dostępu do informacji sektora publicznego państw członkowskich, nie zaś dokumentów będących w posiadaniu instytucji unijnych. Z jednej strony, można podejrzewać, że potencjalny rozwój orzecznictwa TSUE na jej tle, który uwzględniałby pojawiające się w niej stwierdzenie o prawie dostępu do informacji jako prawie podstawowym, mógłby mieć wpływ również na wykładnię przepisów dotyczących prawa dostępu do dokumentów instytucji. Z drugiej strony, można również wyobrazić sobie sytuację, w której TSUE rozdziela kwestię prawa dostępu do informacji dotyczącego działań państw członkowskich od prawa dostępu do dokumentów instytucji, organów i jednostek organizacyjnych UE zawartego w art. 42 KPP. Zważywszy na dotychczasową niechęć TSUE do uznania istnienia zasady ogólnej w postaci dostępu do informacji w prawie UE, trudno podejrzewać, aby to on miał stać się *spiritus movens* w zakresie rozszerzania wykładni przepisów prawa unijnego dotyczących prawa dostępu do dokumentów – a potencjalnie – prawa dostępu do informacji.

Motywacją zmiany stanowiska TSUE mogłoby być dostrzeżenie, że zautomatyzowane podejmowanie decyzji może pełnić w rzeczywistości funkcję analogiczną do prawa lub nawet zastępować akty prawne. Zauważenie, że prawo unijne może być obchodzone za sprawą przekładania go na kod komputerowy, np. przez wdrażanie dyskryminacyjnych mechanizmów ukrytych w czarnej skrzynce technologii, powinno przyczynić się do rozwoju wyższych

⁶⁵⁶ Zob. C. Harlow, *Freedom of Information and Transparency as Administrative and Constitutional Rights*, „Cambridge Yearbook of European Legal Studies” 1999, t. 2, s. 299–300.

standardów w zakresie dążenia do przejrzystości nowych technologii. Nieprzejrzystość zautomatyzowanego podejmowania decyzji może stanowić zagrożenie dla samych fundamentów integracji europejskiej. Dlatego nawet instrumentalne traktowanie prawa dostępu do informacji jako ściśle środka niezbędnego do realizacji innych praw gwarantowanych przez UE, mogłoby stanowić ważny krok do kształtowania środowiska cyfrowego opartego na unijnych wartościach.

Wnioski końcowe

1. Prawo ochrony danych osobowych jako niewystarczający instrument do ochrony przed brakiem przejrzystości zautomatyzowanego podejmowania decyzji

Przeprowadzona analiza pozwoliła wykazać, że zautomatyzowane podejmowanie decyzji może być postrzegane jako mechanizm oddziałujący na sposób tworzenia i stosowania prawa. Zastępowanie ludzi lub wspomaganie ich w ramach procesów decyzyjnych przez algorytmy ma wpływ na poziom przejrzystości podjętej decyzji. Wprowadzanie w akta prawnych odwołań do systemów informatycznych, które zastępują normy prawne regulujące daną kwestię, prowadzi do jeszcze dalej idącego cedowania funkcji pełnionej przez prawo na rozwiązania technologiczne. Wdrożone w ten sposób rozwiązanie nie tylko determinuje sytuację poszczególnych jednostek, lecz również w rzeczywistości tworzy ramy regulacyjne.

Rozwiązania wykorzystujące zautomatyzowane podejmowanie decyzji mogą być postrzegane jako zjawisko mające wpływ na sytuację prawną nie tylko jednostek, lecz także całych grup. Jest to wynik posługiwania się w ramach zautomatyzowanego podejmowania decyzji analizą danych i algorytmami, które opierają się na przyporządkowywaniu jednostki do danej grupy i w wyniku tego podporządkowania podejmowaniu wobec niej danej decyzji. Kryteria, jakie są wykorzystywane w tym procesie, mogą mieć charakter dyskryminujący. Problemem jest jednak nie tylko fakt, że technologie mogą być dyskryminacyjne. Na podstawowym poziomie problemem jest już sam brak możliwości weryfikacji, czy są one, czy nie są dyskryminacyjne. Wiele przeszkód uniemożliwia dostęp do algorytmów stojących za

wdrażanymi przez państwa i podmioty prywatne rozwiązaniami wykorzystującymi zautomatyzowane podejmowanie decyzji.

Brak przejrzystości zautomatyzowanego podejmowania decyzji jest zagadnieniem, któremu miały przeciwdziałać przepisy RODO. Ich celem miała być ochrona praw jednostki w związku z zautomatyzowanym podejmowaniem decyzji. Są one jednak dość niejasne, a ich interpretacja różni się między państwami członkowskimi. Zakaz stosowania zautomatyzowanego podejmowania decyzji uwzględniony w art. 22 RODO jest obwarowany wyjątkami umożliwiającymi *de facto* jego powszechne stosowanie. Przepisy wprowadzające „prawo do wyjaśnienia” są na tyle nieprecyzyjne, że ich rzeczywisty wpływ na możliwość weryfikacji przez jednostkę przyczyn stojących za podjętą wobec niej decyzją jest ograniczony. Dotychczasowe stosowanie RODO w Polsce również ilustruje brak znaczenia rozwiązań, które mogłyby być odczytywane jako próba spojrzenia na zautomatyzowane podejmowanie decyzji z perspektywy grup poddawanych jego stosowaniu, np. w czasie przygotowywania książki nie pojawiły się informacje o skutecznie przeprowadzonych konsultacjach DPIA. Podobne zarzuty można sformułować wobec *Konwencji 108+*, która nie dość, że jest równie nieprecyzyjna jak RODO, to – w czasie przygotowywania książki – nie weszła jeszcze w życie.

Stąd też uzasadniona jest konkluzja, że przepisy z zakresu prawa ochrony danych osobowych nie stanowią wystarczającej odpowiedzi na wyzwania pojawiające się w związku z rozpowszechnianiem się stosowania zautomatyzowanego podejmowania decyzji. Problem braku adekwatnych rozwiązań prawnych dla zautomatyzowanego podejmowania decyzji jest szczególnie istotny w świetle zakazu dyskryminacji w prawie europejskim. Zautomatyzowane podejmowanie decyzji prowadzi do wyników, które można odbierać jako dyskryminację ze względu na chronione przesłanki. Mechanizmy te, stosowane w obszarach objętych regulacjami unijnymi, powinny być traktowane jako wyzwanie dla unijnego zakazu dyskryminacji. Natomiast w związku z charakterem zakazu dyskryminacji w EKPCz dla wykazania potencjalnej dyskryminacyjności zautomatyzowanych systemów podejmowania decyzji konieczne byłoby, aby dotyczyły one praw ujętych w EKPCz. Stąd też wątpliwości mogą powodować m.in. zastosowania zautomatyzowanego podejmowania decyzji w sposób mogący mieć wpływ na prawo jednostki do rzetelnego procesu sądowego.

Na problem ten można patrzeć, z jednej strony, z perspektywy jednostki. Wydana wobec niej decyzja może być kwestionowana jako dyskryminacyjna. Podejście takie nie jest jednak adekwatne dla charakteru wyzwań wynikających z dyskryminacyjnych mechanizmów, które mogą być wpisane w systemy zautomatyzowanego podejmowania decyzji. Wprowadzanie w sektorze publicznym zautomatyzowanego podejmowania decyzji w miejsce uprzednich

regulacji prawnych czyni potencjalną dyskryminację nieprzejrystą. Nie byłaby zgodna z zakazem dyskryminacji sytuacja, w której przepisy przewidywałyby dostosowywanie rodzaju pomocy społecznej udzielanej jednostce, uwzględniając m.in. kryterium jej płci. Tymczasem jest możliwe, że algorytm używany do automatyzacji procesu udzielania pomocy społecznej traktowałby takie kryterium jako znaczące. Informacja o takim sposobie kształtowania kryteriów podejmowania decyzji nie byłaby jednak – w przypadku stosowania systemu zautomatyzowanego podejmowania decyzji – możliwa do uzyskania bez wglądu w sposób działania stojącego za nim algorytmu. Dlatego też, z drugiej strony, na zagadnienie zautomatyzowanej dyskryminacji należy patrzeć z perspektywy wzmacniania mechanizmów dyskryminacyjnych w związku z nieprzejrystą instytucjonalizacją stosowania zautomatyzowanego podejmowania decyzji.

Z tych przyczyn należy uznać, że zautomatyzowane podejmowanie decyzji tworzy wyzwania dla zakazu dyskryminacji w prawie europejskim, którym sprostanie powinno opierać się m.in. na dążeniu do zwiększenia poziomu przejrzystości algorytmów. Jednym ze sposobów na zwiększenie poziomu przejrzystości zautomatyzowanego podejmowania decyzji jest traktowanie algorytmów jako informacji podlegającej prawu dostępu do informacji publicznej lub dokumentów urzędowych.

2. Algorytmy stosowane w zautomatyzowanym podejmowaniu decyzji jako informacja publiczna w świetle orzecznictwa ETPCz i TSUE

Główna hipoteza, czyli twierdzenie, że algorytmy używane w ramach zautomatyzowanego podejmowania decyzji w sektorze publicznym mogą być uznane za informację publiczną, została zweryfikowana jako prawdziwa w odniesieniu do wykładni prawa dostępu do informacji przez ETPCz. Choć zakres informacji możliwych do uzyskania na podstawie art. 10 EKPCz musi być postrzegany jako ograniczony, w ściśle określonych sytuacjach prawo dostępu do informacji powinno umożliwiać traktowanie algorytmów używanych w ramach zautomatyzowanego podejmowania decyzji jako informacji podlegającej prawu dostępu do informacji. Dotyczy to zarówno warunków, jakie muszą zostać spełnione w odniesieniu do ubiegania się o informację, jak i możliwości wprowadzania ograniczeń w prawie dostępu do informacji, które przewiduje art. 10 ust. 2 EKPCz. Ponadto w ramach weryfikacji głównej hipotezy należy odnotować, że zgodnie z orzecznictwem ETPCz dostęp do informacji stanowić może element niezbędny do realizacji innych praw zawartych w EKPCz, np. prawa do życia, do rzetelnego procesu lub prawa do prywatności i ochrony życia rodzinnego. Zważywszy na fakt, że zautomatyzowane podejmowanie decyzji może mieć wpływ na sytuację

jednostki pod względem korzystania z tych praw, możliwa jest konceptualizacja prawa dostępu do informacji jako elementu niezbędnego do korzystania z tych właśnie praw gwarantowanych przez EKPCz.

Odmienne przedstawiają się konkluzje dotyczące weryfikacji głównej hipotezy w odniesieniu do prawa UE. Po pierwsze, należy oddzielić zautomatyzowane podejmowanie decyzji, o którym informacje byłyby w posiadaniu unijnych instytucji, organów i jednostek organizacyjnych, od tego, które pozostawałoby całkowicie w gestii państw członkowskich. W wypadku tego pierwszego typu sytuacji możliwe jest stwierdzenie, że algorytmy używane do zautomatyzowanego podejmowania decyzji zostałyby potraktowane jako dokumenty w świetle prawa unijnego. Rozwój prawa dostępu do dokumentów urzędowych w UE doprowadził do stosowania szerokiej definicji dokumentu. Stąd też – jak długo zautomatyzowane podejmowanie decyzji stosowane byłoby przez podmioty, które objęte są unijnymi regulacjami dotyczącymi dostępu do dokumentów, możliwe jest wyobrażenie sobie konieczności udostępnienia informacji na ich temat w trybie wniosku o dostęp do dokumentów urzędowych.

W wypadku zautomatyzowanego podejmowania decyzji stosowanego przez państwa członkowskie prawo unijne w bardzo ograniczonym stopniu może prowadzić do uznania algorytmów za informację lub dokumenty podlegające prawu dostępu do informacji lub dokumentów urzędowych. Wynika to m.in. z rozbieżności między postrzeganiem tych praw przez TSUE i ETPCz. TSUE traktuje prawo dostępu do informacji jedynie jako element prawa dostępu do dokumentów urzędowych, którego zakres w prawie UE jest ograniczony do unijnych instytucji, organów i jednostek organizacyjnych na zasadach przewidzianych w odpowiednich aktach prawa UE. Odmawia on natomiast wykładni art. 11 KPP – wbrew wykładni odpowiadającego mu art. 10 EKPCz – uznającej prawo dostępu do informacji jako część praw związanych z wolnością wyrazu i prawem do otrzymywania oraz rozpowszechniania informacji. Strategia ta prowadzi do bardzo ograniczonego zakresu prawa dostępu do dokumentów urzędowych w prawie UE. Pojawiają się jednak sygnały zwiastujące możliwość zmiany w tym zakresie. Unijna dyrektywa dotycząca dostępu do danych sektora publicznego wprost stwierdza – chociaż w niewiążącym prawnie motywie – że dostęp do informacji jest prawem podstawowym i zawiera odwołanie do art. 11 KPP. Ponadto fakt, że przewiduje ona wprost – również w motywie – wyłączenie programów komputerowych z definicji dokumentu, może być odczytywany jako sygnał potwierdzający, że definicja dokumentu w prawie UE powinna uwzględniać możliwość traktowania programów komputerowych jako dokumentów.

Podsumowując, należy stwierdzić, że możliwe jest traktowanie niektórych algorytmów używanych w zautomatyzowanym podejmowaniu decyzji

stosowanym w ramach sektora publicznego jako informacji podlegającej prawu dostępu do informacji w świetle jego wykładni dokonywanej przez ETPCz. Możliwe jest również traktowanie algorytmów używanych do zautomatyzowanego podejmowania decyzji stosowanego przez instytucje, organy i jednostki organizacyjne UE jako dokumentu podlegającego prawu dostępu do dokumentów urzędowych zgodnie z jego wykładnią dokonywaną przez TSUE. Brak jednocześnie podstaw, aby obecnie, w świetle ostrożnej i sprzecznej z wykładnią ETPCz interpretacją prawa dostępu do informacji dokonywaną przez TSUE, zakładać, aby algorytmy stosowane do zautomatyzowanego podejmowania decyzji przez państwa członkowskie mogły podlegać prawu dostępu do informacji. Wykładnia taka nie jest zgodna z tym, jak określa relację między EKPCz i orzecznictwem ETPCz a KPP i jej wykładnią sama KPP. W świetle przepisów KPP jej art. 11 powinien być odczytywany jako źródło ograniczonego prawa dostępu do informacji, które powinno przysługiwać jednostkom w zakresie, w jakim państwa członkowskie stosują prawo UE. Zwłaszcza w świetle wyzwań, które zautomatyzowane podejmowanie decyzji tworzy dla zakazu dyskryminacji w prawie UE, błędem jest niedostrzeganie roli, jaką mogłoby odegrać prawo dostępu do informacji jako środek prawny umożliwiający weryfikację, czy dane rozwiązanie jest, czy nie jest dyskryminacyjne.

3. Rola przejrzystego zautomatyzowanego podejmowania decyzji w gwarantowaniu zgodności działań państw członkowskich z wartościami UE

Opór TSUE przed uznaniem prawa dostępu do informacji za istotny element katalogu praw podstawowych jest problematyczny w świetle relacji między zasadami i wartościami, których realizacji ma ono służyć, i kierunkiem, w jakim poszła europejska integracja. Historycznie prawo dostępu do informacji, z czasem zmienione na prawo dostępu do dokumentów, miało odgrywać rolę narzędzia demokratyzującego UE. Było ono postrzegane jako jeden z instrumentów, które miały wpływać na wyższy poziom przejrzystości procesów decyzyjnych, otwartości instytucji czy uczestnictwa obywateli w życiu politycznym. Jednak współcześnie UE nie tylko ma ambicję demokratyzować siebie samą, ale również wymagać od państw członkowskich, aby postępowaly one zgodnie z wartościami takimi jak właśnie demokracja i praworządność.

Wśród wielu problemów związanych z egzekwowaniem, aby państwa członkowskie działały w zgodzie z tymi wartościami, powinien zostać odnotowany wpływ nowych technologii na przejrzystość procedur, a tym samym na ich demokratyczność. Począwszy od przypadków tak oczywistych jak personalizowanie przekazu politycznego w ramach kampanii wyborczych, przez

programy mające na celu przewidywanie prawdopodobieństwa występowania zachowań przestępczych w danych dzielnicach na podstawie analizy danych, po stosowanie algorytmów w miejsce przepisów określających przydzielenie spraw sędziom, zautomatyzowane podejmowanie decyzji ma wpływ na funkcjonowanie demokratycznych systemów politycznych. O ile nie byłoby słuszne stwierdzenie, że każdy system zautomatyzowanego podejmowania decyzji narusza wartości demokratycznego państwa prawa, o tyle uzasadniona jest wątpliwość, czy jakikolwiek system zautomatyzowanego podejmowania decyzji wdrażany w sektorze publicznym, którego zasady działania pozostają niejawne i nie podlegają niczyjej kontroli, może być postrzegany jako działający w zgodzie z tymi zasadami. Dlatego też wdrażanie przez państwa członkowskie UE rozwiązań wykorzystujących zautomatyzowane podejmowanie decyzji w obszarach objętych zakresem prawa unijnego powinno być przedmiotem zainteresowania unijnych instytucji jako potencjalnie niezgodne z unijnymi wartościami. Konsekwencja w zakresie wymagania od państw członkowskich działania zgodnie z wartościami wyrażonymi w art. 2 TUE wymaga dostrzeżenia, że naruszenia tych wartości mogą być efektem działań podejmowanych w sferze cyfrowej.

4. Neutralność technologiczna i dynamiczna wykładnia vs postulatory *de lege ferenda*

Kiedy rozpoczynałam prace nad tą książką, głosy mówiące o konieczności zwiększenia poziomu przejrzystości zautomatyzowanego podejmowania decyzji podnoszone były głównie przez aktywistów i naukowców. Natomiast gdy kończyłam jej przygotowywanie, Komisja Europejska opublikowała projekt *Aktu w sprawie SI*, w którym m.in. formułuje propozycje wymogów, jakie powinny spełnić algorytmy i dane, na których są one trenowane, aby mogły być uznane za zgodne z prawem. Można to odczytywać jako pozytywną zmianę w zakresie kształtowania dyskursu dotyczącego regulacji nowych technologii i wzrostu świadomości decydentów politycznych co do tego, jaką rolę mogą one odgrywać w odniesieniu do praw jednostki i kształtowania uwarunkowań systemowych, w których jednostki funkcjonują. Jednocześnie pokazuje to, z jak powolnym procesem mamy do czynienia.

Dlatego też postulatory *de lege ferenda*, jakkolwiek nie odmawiam im wagi i również je formułuję, są drugorzędne w stosunku do głównego wniosku z przeprowadzonej analizy. Jest nim możliwość wykładni istniejących przepisów w sposób umożliwiający zwiększenie poziomu przejrzystości zautomatyzowanego podejmowania decyzji, który prowadziłby do weryfikacji, na ile jest ono zgodne z zakazem dyskryminacji. Tak jak TSUE, wbrew dominującej i mylnej narracji o gospodarce współdzielenia, zauważył, że Uber powinien być traktowany jako usługa w dziedzinie transportu, tak analogicznie można

by odnotować, że zautomatyzowane podejmowanie decyzji i algorytmy w nim używane bywają niczym innym jak prawem.

Wykładni takiej może sprzyjać nastawienie ETPCz do zasad wykładni EKPCz. Zgodnie z jego orzecnictwem istnieje konieczność: „interpretacji Konwencji i stosowania jej w sposób, który zagwarantuje prawom w niej zawartym wymiar praktyczny i efektywny, a nie tylko teoretyczny i iluzoryczny [podkreślenie – J.M.]”⁶⁵⁷. W związku z rozwojem technologicznym oraz możliwością prób wdrażania zautomatyzowanego podejmowania decyzji w coraz to kolejnych płaszczyznach życia dążenie do większej przejrzystości systemów zautomatyzowanego podejmowania decyzji, które mogą dotyczyć sfer działalności państwa, może stanowić element stosowania EKPCz w sposób praktyczny i efektywny. Jak pokazują losy *Konwencji o wolności informacji* opisywane na początku rozdziału trzeciego, przyjmowanie nowych aktów prawa międzynarodowego może obfitować w niespodzianki i opóźnienia. Stąd też hipoteza, która pozwala skorzystać z obowiązujących rozwiązań – przez ich neutralną technologicznie interpretację – do realizacji celów, którym przyjęcie tych aktów prawnych miało służyć, wychodzi naprzeciw duchowi orzecnictwa ETPCz podkreślającego konieczność traktowania EKPCz jako żyjącego instrumentu.

Z kolei postawa TSUE wobec wykładni regulacji w świetle rozwoju nowych technologii charakteryzuje się ambiwalencją. Z jednej strony można przywołać przykłady kreatywności interpretacji, np. skutkującej rozwojem prawa do bycia zapomnianym. Z drugiej zaś strony, w odniesieniu do prawa dostępu do informacji, TSUE nie jest gotowy uznać jego istnienia. W sytuacji rozwoju „gospodarki informacyjnej” czy „społeczeństwa informacyjnego” ignorowanie istnienia praw odnoszących się wprost do „informacji” jest dość niepokojącą tendencją orzecniczą. Tym samym rola, jaką prawo to mogłoby odgrywać w odniesieniu do zwiększania poziomu przejrzystości zautomatyzowanego podejmowania decyzji, zależy od rozwoju inicjatyw ustawodawczych na poziomie UE, które wprost formułowałyby przepisy dotyczące takiej możliwości.

Ze względu na specyfikę kompetencji UE w zakresie regulacji zasad udzielania dostępu do informacji publicznej przez państwa członkowskie postulatory dotyczące tego zagadnienia należy rozbić na dwa rodzaje. Po pierwsze, na poziomie UE można dążyć do rozszerzania zakresu regulacji takich jak np. *dyrektywa 2019/1024*. Jest to przykład przyjmowania perspektywy, w której prawo dostępu do informacji i do dokumentów urzędowych jest traktowane jako element niezbędny do tworzenia rynku wewnętrznego. Dążenie do uwzględniania wprost w tego typu aktach prawnych

⁶⁵⁷ Przeglądu orzecnictwa, w którym pojawia się odwołanie do tego wymogu dokonuje A. Schabas, *op. cit.*, s. 33.

możliwości traktowania programów komputerowych używanych do zautomatyzowanego podejmowania decyzji jako dokumentu znajduje uzasadnienie w możliwości dyskryminacji ze względu na miejsce pochodzenia wynikającej ze sposobu ich napisania. Sam fakt uwzględnienia możliwości traktowania programów komputerowych jako dokumentu przez państwa w ramach transpozycji dyrektywy świadczy o możliwości uczynienia z takiego podejścia przedmiotu regulacji samej dyrektywy, nie zaś możliwości pozostawionej w gestii państw członkowskich.

Po drugie, możliwe i pożądane jest wprowadzanie regulacji dotyczących wymogów publikacji informacji na temat wdrażanych rozwiązań opartych na zautomatyzowanym podejmowaniu decyzji. Podobnie do obowiązków państw w zakresie komunikacji społeczeństwu informacji dotyczących skutków wywieranych przez dane przedsięwzięcia na środowisko, UE mogłaby podejmować inicjatywy w zakresie zobowiązania państw do publikacji informacji dotyczących wdrażanych w środowisku cyfrowym rozwiązań wykorzystujących zautomatyzowane podejmowanie decyzji. Przykładem regulacji idącej w tym kierunku jest DPIA. Niestety, ze względu na zbyt miękki charakter przepisów wprowadzonych w RODO, DPIA jest jedynie narzędziem wykorzystywanym wewnątrz. Z kolei propozycje zawarte w *Akcie w sprawie SI* są na tak wczesnym etapie debaty nad nimi, że trudno ocenić, w jakim stopniu mogą one przysłużyć się zwiększaniu możliwości społeczeństwa w zakresie pozyskiwania wiedzy o systemach zautomatyzowanego podejmowania decyzji. Wprowadzanie obowiązków w zakresie przeprowadzania i publikacji ocen skutków dla ochrony danych czy z punktu widzenia ochrony praw człowieka (HRIA) leży w kompetencjach UE i tego typu wymogi mogłyby – i powinny – stać się standardem⁶⁵⁸. Ponadto państwa członkowskie powinny być zobowiązane do publikacji kodu źródłowego używanego w systemach zautomatyzowanego podejmowania decyzji wdrażanych w sektorze publicznym w sytuacjach, w których kod ten zastępuje przepisy. Chociażby ze względu na fakt, że rozwiązania takie mogą naruszać zakaz dyskryminacji, państwa powinny aktywnie wykazywać, że wdrażane systemy zautomatyzowanego podejmowania decyzji nie stanowią systemowego naruszenia prawa UE.

Wprowadzanie takich wymogów jest pożądane i możliwe z punktu widzenia kompetencji UE. Zanim jednak staną się one przedmiotem ewentualnych regulacji, konieczna jest dalsza rewizja myślenia o nowych technologiach i roli, jaką odgrywają one we współczesnym społeczeństwie. Świadomość znaczenia ich przejrzystości jest warunkiem niezbędnym zarówno dla wykładni

⁶⁵⁸ O roli audytowania systemów zautomatyzowanego podejmowania decyzji, zob. J. Mökander, J. Morley, M. Taddeo, L. Floridi, *Ethics-Based Auditing of Automated Decision-Making Systems: Nature, Scope, and Limitations*, „Science and Engineering Ethics” 2021, t. 27, artykuł nr 44.

prawa dostępu do informacji w sposób umożliwiający korzystanie z niego w odniesieniu do systemów zautomatyzowanego podejmowania decyzji, jak i dla propozycji regulacyjnych dążących do osiągnięcia ich większej otwartości. Chociaż w odniesieniu do przetwarzania danych rola odgrywana przez zasadę przejrzystości została odnotowana przez jej uwzględnienie w RODO, środki prawne mogące teoretycznie służyć jej realizacji mają głównie charakter dobrowolny, a przez to są w rzeczywistości niemal martwymi przepisami.

5. Komplementarność rozwiązań regulacyjnych dotyczących dostępu do informacji na temat zautomatyzowanego podejmowania decyzji

Charakteryzujący analizę przedstawioną w książce nacisk na przejrzystość algorytmów i ich dostępność dla społeczeństwa oczywiście można krytykować jako niewystarczający do zagwarantowania ich niedyskryminacyjnego charakteru. W żaden sposób nie twierdzę jednak, że inne rozwiązania⁶⁵⁹ nie powinny być wdrażane. Fałszywe byłoby jednak przedstawianie propozycji rozwiązań mających na celu zwiększenie przejrzystości przez gwarantowanie szerokiego dostępu do programów używanych w zautomatyzowanym podejmowaniu decyzji jako konkurencyjnych dla rozwiązań koncentrujących się na dostępie do algorytmów np. dla wyspecjalizowanych agencji czy niezależnych ekspertów⁶⁶⁰. Kiedy zauważy się, że algorytmy zaczynają zastępować prawo, można wykazać absurdalność takiego argumentu przez stwierdzenie, że analogicznie można by wyjść z założenia, że istnienie sądów i Biura Analiz Sejmowych może zastąpić dostęp do aktów prawnych zagwarantowany bezpośrednio jednostce. Logika cedująca możliwość kontroli jedynie na niezależne ciała eksperckie może prowadzić do pytania: dlaczego jednostki miałyby mieć dostęp do aktów prawnych, według których oceniane jest ich postępowanie, skoro istnieją eksperckie ciała odpowiedzialne za analizę tych aktów prawnych? Analogicznie, istnienie eksperckich i niezależnych instytucji w żaden sposób nie musi wykluczać dostępu do algorytmów dla społeczeństwa.

⁶⁵⁹ Propozycję kompleksowego podejścia do wyzwań związanych z zautomatyzowanym podejmowaniem decyzji przedstawili np. J. Cobbe, M. Seng Ah Lee, J. Singh, *Reviewable Automated Decision-Making: A Framework for Accountable Algorithmic Systems*, „Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (FAccT '21)” 2021, Association for Computing Machinery, Nowy Jork, NY, USA, s. 598–609. <https://doi.org/10.1145/3442188.3445921>, dostęp: 18.07.2021.

⁶⁶⁰ Jak przedstawia to np. P.B. de Laat, *Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?*, „Philosophy and Technology” 2018, t. 31, s. 539–540.

Chociaż propozycja traktowania algorytmów jako aktów prawnych może wydawać się zbyt daleko idąca, nie jest ona w rzeczywistości bardziej kontrowersyjna niż przyjmowanie aktów prawnych w lakoniczny sposób odnoszących się do narzędzi informatycznych, które mają wykonywać dane decyzje. Zasadniczą różnicą jest zgodność tych podejść z założeniami, na których opierają się demokratyczne społeczeństwa. Publikowanie algorytmów używanych w ramach sektora publicznego, analogicznie do publikowania aktów prawnych, stanowiłoby realizację zasady takiej jak otwartość, a także mogłoby się przekładać na większą rozliczalność ich pomysłodawców i twórców. Natomiast wdrażanie zautomatyzowanych rozwiązań, które pozostają poza demokratyczną kontrolą, stanowi narzędzie pozwalające na poddawanie jednostek i całych grup traktowaniu opartemu na zasadach, z którymi nie mają one nawet szans się zapoznać.

Instytucje publiczne posługujące się zautomatyzowanym podejmowaniem decyzji zwykle nie udostępniają algorytmów do niego z własnej inicjatywy. Dlatego dostęp do algorytmów używanych w ramach zautomatyzowanego podejmowania decyzji jako do informacji publicznej może stanowić rozwiązanie niezbędne do zagwarantowania większej równowagi w wiedzy na temat zasad ich działania. Rola organizacji społecznych, aktywistów, naukowców czy mediów w analizowaniu sposobów funkcjonowania zautomatyzowanego podejmowania decyzji nie prowadziłyby do większej rozliczalności wdrażanych systemów. Mogłaby jednak ona zwiększać świadomość jednostek na temat sposobu kodowania ich praw i obowiązków oraz rodzaju konsekwencji, jakie mogą wynikać ze stosowanego sposobu oceny ich zachowania. Szczególnie w świetle zagrożeń związanych z powtarzaniem i instytucjonalizacją dyskryminacyjnych mechanizmów za sprawą wdrażania nieprzejrzystych technologii należy stwierdzić, że udzielanie informacji na ten temat – zarówno z własnej inicjatywy, jak i w odpowiedzi na wniosek o dostęp do informacji publicznej – powinno stać się standardem w państwach uważających się za praworządne i demokratyczne.

Bibliografia

Literatura

- Abazi V., Hillebrandt M., *The legal limits to confidential negotiations: Recent case law developments in Council transparency: Access Info Europe and In't Veld*, „Common Market Law Review” 2015, t. 52, s. 825–845.
- Abreu Ferreira S. de, *The Fundamental Right of Access to Environmental Information in the EC: A Critical Analysis of WWF-EPO v. Council*, „Journal of Environmental Law” 2007, t. 19, nr 3, s. 399–408.
- Adamski D., *Approximating a Workable Compromise on Access to Official Documents: the 2011 Developments in the European Courts*, „Common Market Law Review” 2012, nr 49, s. 521–558.
- Adamski D., *How Wide Is “The Widest Possible”? Judicial Interpretation of the Exceptions to the Right of Access to Official Documents Revisited*, „Common Market Law Review” 2009, t. 46, s. 521–549.
- Adamski D., *Prawo do informacji o działaniach władz publicznych Unii Europejskiej*, C.H. Beck, Warszawa 2011.
- Adamski D., *Rozdział II: Unijne modele regulacji jawności i jej ograniczeń oraz ich wpływ na systemy krajowe*, [w:] *Standardy europejskie (Jawność i jej ograniczenia, t. XI)*, red. C. Mik, C.H. Beck, Warszawa 2016.
- Alemanno A., Stefan O., *Openness at the Court of Justice of the European Union: Toppling a Taboo*, „Common Market Law Review” 2014, t. 51, s. 97–139.
- Alemanno A., *Unpacking the Principle of Openness in EU Law: Transparency, Participation and Democracy*, „European Law Review” 2014, t. 39, nr 1, s. 72–90.
- Angwin J., Larsona J., Mattu S., Kirchner L., *Machine Bias. There’s Software Used Across the Country to Predict Future Criminals. And It’s Biased against Blacks*, „ProPublica” 2016. <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing>, dostęp: 1.04.2021.
- Arnulf A., *Court of Justice, Joined Cases C-39/05 P & C-52/05 P, Sweden and Turco v. Council, Judgment of the Grand Chamber of 1 July 2008, Not Yet Reported*, „Common Market Law Review” 2009, t. 46, s. 1219–1238.

- Austin L.M., *Enough About Me: Why Privacy is About Power, not Consent (or Harm)*, [w:] *A World Without Privacy: What Law Can and Should Do?*, red. A. Sarat, Cambridge University Press, Cambridge 2015.
- Balcerzak M., *Rozdział III: Kategoria jawności i prawo do informacji z perspektywy orzecznictwa Europejskiego Trybunału Praw Człowieka*, [w:] *Standardy europejskie (Jawność i jej ograniczenia, t. XI)*, red. C. Mik, C.H. Beck, Warszawa 2016.
- Banisar D., *The Right to Information in the Age of Information*, [w:] *Human Rights in the Global Information Society (Information Revolution and Global Politics)*, red. R.F. Jorgensen, MIT Press, Cambridge–Londyn 2006.
- Barocas S., Selbst A.D., *Big Data's Disparate Impact*, „California Law Review” 2016, t. 104, s. 671–732.
- Barta J., Fajgielski P., Markiewicz R., [w:] *jednak staną się one, Ochrona danych osobowych. Komentarz*, wyd. 6, Wolters Kluwer Polska, Warszawa 2015.
- Bartlett R., Morse A., Stanton R., Wallace N., *Consumer-Lending Discrimination in the FinTech Era*, „NBER Working Paper” 2019, nr 25943.
- Bayamloğlu E., Leenes R., *The 'Rule of Law' Implications of Data-Driven Decision-Making: a Techno-rRegulatory Perspective*, „Law, Innovation and Technology” 2018, t. 10, nr 2, s. 295–313.
- Benoist E., *Collecting Data for the Profiling of Web Users*, [w:] *Profiling the European Citizen. Cross-Disciplinary Perspectives*, red. M. Hildebrandt, S. Gutwirth, Springer, Nowy Jork 2008.
- Bielak-Jomaa E., Lubasz D., red., *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Wolters Kluwer Polska, Warszawa 2017.
- Bing J., *Code, Access and Control*, [w:] *Human Rights in the Digital Age*, red. M. Klang, A. Murray, Routledge–Cavendish, Londyn–Sydney–Portland 2004.
- Binns R., *Algorithmic Accountability and Public Reason*, „Philosophy & Technology” 2018, t. 31, nr 4, s. 543–556.
- Bloch-Wehba H., *Access to Algorithms*, „Fordham Law Review” 2020, t. 88, s. 1265–1314.
- Bobek M., *Case C-345/06, Gottfried Heinrich, Judgment of the Court of Justice (Grand Chamber) of 10 March 2009, Not Yet Reported*, „Common Market Law Review” 2009, t. 46, s. 2077–2094.
- Brkan M., Bonnet G., *Legal and Technical Feasibility of the GDPR's Quest for Explanation of Algorithmic Decisions: of Black Boxes, White Boxes and Fata Morganas*, „European Journal of Risk Regulation” 2020, t. 11, nr 1, s. 18–50.
- Brkan M., *Do Algorithms Rule the World? Algorithmic Decision-Making and Data Protection in the Framework of the GDPR and Beyond*, „International Journal of Law and Information Technology” 2019, t. 27, nr 2, s. 91–121.
- Broberg M.P., *Access to Documents: A General Principle of Community Law?*, „European Law Review” 2002, t. 27, nr 2, s. 193–205.
- Burrell J., *How the Machine “Thinks”: Understanding Opacity in Machine Learning Algorithms*, „Big Data and Society” 2016, t. 3, nr 1, s. 1–12.
- Bygrave L.A., *Automated Profiling Minding The Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, „Computer Law & Security Review” 2001, t. 17, nr 1, s. 17–24.
- Bygrave L.A., *Data Privacy Law. An International Perspective*, Oxford University Press, Oxford 2014.
- Casey B., Farhangi A., Vogl R., *Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise*, „Berkeley Technology Law Journal” 2019, t. 34, s. 143–188.

- Cecere G., Jean C., Le Guel F., Manant M., *STEM and Teens: An Algorithm Bias on a Social Media*, 2018. <https://ssrn.com/abstract=3176168>, dostęp: 1.04.2021.
- Chaffee Z., Jr., *Legal Problems of Freedom of Information in the United Nations*, „Law & Contemporary Problems” 1949, t. 14, nr 4, s. 545–583.
- Chander A., *The Racist Algorithm*, „Michigan Law Review” 2017, t. 115, s. 1023–1045.
- Chłopecki A., *Sztuczna inteligencja – szkice prawnicze i futurologiczne*, C.H. Beck, Warszawa 2018.
- Chomiczewski W., *Profilowanie w ogólnym rozporządzeniu o ochronie danych*, [w:] *Polska i Europejska Reforma Ochrony Danych Osobowych*, red. E. Bielak-Jomaa, D. Lubasz, Wolters Kluwer Polska, Warszawa 2016.
- Cinciarini P., Russo D., Sillitti A., Succi G., *Reverse Engineering: A European IPR Perspective*, „SAC ‘16 Proceedings of the 31st Annual ACM Symposium on Applied Computing” 2016, s. 1498–1503.
- Ciechomska M., *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych*, „Europejski Przegląd Sądowy” 2017, nr 5, s. 37–42.
- Cobbe J., Seng Ah Lee M., Singh J., *Reviewable Automated Decision-Making: A Framework for Accountable Algorithmic Systems*, „Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency (FAccT ‘21)” 2021, Association for Computing Machinery, New York, NY, USA, s. 598–609. <https://doi.org/10.1145/3442188.3445921>, dostęp: 18.07.2021.
- Coller E.H. van, *Transparency and Access to Documents: A General Principle of European Community Law*, „De Jure” 2006, t. 39, nr 1, s. 163–169.
- Cowgill B., Tucker C., *Algorithmic Bias: A Counterfactual Perspective*, „Working Paper: NSF Trustworthy Algorithms” 2017. <http://trustworthy-algorithms.org/whitepapers/Bo%20Cowgill.pdf>, dostęp: 1.04.2021.
- Curtin D.M., *Citizens’ Fundamental Right of Access to EU Information: an Evolving Digital Passepartout?*, „Common Market Law Review” 2000, t. 37, s. 7–41.
- Curtin D.M., *The Fundamental Principle of Open Decision-Making and EU (political) Citizenship*, [w:] *Legal Issues of the Amsterdam Treaty*, red. D. O’Keeffe, P. Twomey, Hart Publishing, Oxford 1999.
- Curtin D., Leino P., *In Search of Transparency for EU Law-Making: Trilogues on the Cusp of Dawn*, „Common Market Law Review” t. 54, s. 1673–1712.
- Curtin D., Meijers H., *Access to European Union Information: An Element of Citizenship and a Neglected Constitutional Right*, [w:] *The European Union and Human Rights*, red. N.A. Neuwahl, A. Rosas, Brill, Haga 1995.
- Curtin D., Meijers H., *The Principle Of Open Government In Schengen And The European Union: Democratic Retrogression?*, „Common Market Law Review” 1995, t. 32, s. 399–442.
- Czapliński W., Wyzomska A., *Prawo międzynarodowe publiczne. Zagadnienia systemowe*, wyd. 3, C.H. Beck, Warszawa 2014.
- Danks D., London A.J., *Algorithmic Bias in Autonomous Systems*, „Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI-17)” 2017. https://www.researchgate.net/profile/Alex_London/publication/318830422_Algorithmic_Bias_in_Autonomous_Systems/links/5a4bb017aca2729b7c893d1b/Algorithmic-Bias-in-Autonomous-Systems.pdf, dostęp: 1.04.2021.
- Datta A., Tschantz M.C., Datta A., *Automated Experiments on Ad Privacy Settings: A Tale of Opacity, Choice, and Discrimination*, „Proceedings on Privacy Enhancing Technologies” 2015, nr 1, s. 92–112.

- Davies R.W., *Access to Documents: a Constitutional Right or a General Principle of Law?*, „Irish Jurist New Series” 2004, t. 39, s. 51–73.
- Diamandouros N., *Openness and Access to Documents*, „European State Aid Law Quarterly” 2008, nr 4, s. 654–658.
- Dmochowska A., Zadrozny M., *Unijna reforma ochrony danych osobowych. Analiza zmian*, C.H. Beck, Warszawa 2016.
- Domańska M., *Zakaz dyskryminacji ze względu na więcej niż jedno zabronione kryterium*, Warszawa 2019.
- Dragos D.C., Kovač P., Marseille A.T., red., *The Laws of Transparency in Action. A European Perspective*, Palgrave Macmillan, Cham 2019.
- Dreyer S., Schulz W., *The General Data Protection Regulation and Automated Decision-making: Will it deliver? Potentials and limitations in ensuring the rights and freedoms of individuals, groups and society as a whole*, Gütersloh 2019. <https://www.hiig.de/publication/the-general-data-protection-regulation-and-automated-decision-making-will-it-deliver-potentials-and-limitations-in-ensuring-the-rights-and-freedoms-of-individuals-groups-and-society-as-a-whole/>, dostęp: 1.04.2021.
- Driessen B., *The Council of the European Union and access to documents*, „European Law Review” 2005, t. 30, nr 5, s. 675–696.
- Driessen B., *Transparency in EU Institutional Law. A Practitioner’s Handbook. Second, Completely Revised Edition*, Kluwer Law International, Alphen aan den Rijn 2012.
- Drożdż A., *Protection of Natural Persons with Regard to Automated Individual Decision-Making in the GDPR*, Kluwer Law International, Alphen aan den Rijn 2020.
- Dyrberg P., *Accountability and Legitimacy: What is the Contribution of Transparency*, [w:] *Accountability and Legitimacy in the European Union*, red. A. Arnull, D. Wincott, Oxford University Press, Oxford 2002.
- Edwards L., Veale M., *Enslaving the Algorithm: From a “Right to an Explanation” to a “Right to Better Decisions”?*, „IEEE Security and Privacy” 2018, t. 16, nr 3, s. 46–54.
- Edwards L., Veale M., *Slave to the Algorithm? Why a ‘Right to an Explanation’ Is Probably Not the Remedy You Are Looking For*, „Duke Law and Technology Review” 2017, t. 16, nr 1, s. 18–84.
- Eechoud M. van, Janssen K., *Rights of Access to Public Sector Information*, „Masaryk University Journal of Law and Technology” 2012, t. 6, nr 3, s. 471–499.
- Eidelman V., *Secret Algorithms Are Deciding Criminal Trials and We’re Not Even Allowed to Test Their Accuracy*, ACLU, 15 września 2017 r. <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/secret-algorithms-are-deciding-criminal-trials-and>, dostęp: 1.04.2021.
- Eubanks V., *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, St Martin’s Press, Nowy Jork 2018.
- Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Wolters Kluwer Polska, Warszawa 2018.
- Felzmann H., Fosch Villaronga E., Lutz Ch., Tamò-Larrieux A., *Transparency You Can Trust: Transparency Requirements for Artificial Intelligence between Legal Norms and Contextual Concerns*, „Big Data & Society” 2019, nr 6(1), s. 1–14.
- Filippi P. de, Hassan S., *Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code*, „First Monday” 2016, t. 21, nr 12. https://www.researchgate.net/publication/311447869_Blockchain_Technology_as_a_Regulatory_Technology_From_Code_is_Law_to_Law_is_Code, dostęp: 1.04.2021.
- Fisher E., *The European Union in the Age of Accountability*, „Oxford Journal of Legal Studies” 2004, t. 24, nr 3, s. 495–515.

- Florczak-Wątor M., *The Role of the European Court of Human Rights in Promoting Horizontal Positive Obligations of the State*, „International and Comparative Law Review” 2017, t. 17, nr 2, s. 39–53.
- François E., *Zakres zastosowania Karty Praw Podstawowych UE*, „Europejski Przegląd Sądowy” 2016, nr 8, s. 19–20.
- Gienas K., *Zabezpieczenia techniczne utworów a dozwolony użytek na tle prawa wspólnotowego i polskiego*, „Europejski Przegląd Sądowy” 2009, nr 12, s. 9–14
- Gillespie T., *The Relevance of Algorithms*, [w:] T. Gillespie, P. Boczkowski, K. Foot, *Media Technologies, Essays on Communication, Materiality, and Society*, MIT Press, Cambridge-Londyn 2014.
- Gliszczyńska-Grabias A., *Artykuł 19. Wolność posiadania i wyrażania poglądów* [w:] *Międzynarodowy Pakt Praw Obywatelskich (Osobistych) i Politycznych. Komentarz*, red. R. Wieruszewski, Wolters Kluwer Polska, Warszawa 2012.
- Goldberg D., *From Sweden to the Global Stage: FOI as European Human Right?*, „Journal of International Media and Entertainment Law” 2016–2017, t. 7, nr 1, s. 1–29.
- Goodman B., *A Step Towards Accountable Algorithms?: Algorithmic Discrimination and the European Union General Data Protection*, „29th Conference on Neural Information Processing Systems (NIPS 2016), Barcelona, Spain” 2016.
- Goodman B., Flaxman S., *European Union Regulations on Algorithmic Decision-Making and a “Right to Explanation”*, „2016 ICML Workshop on Human Interpretability in Machine Learning (WHI 2016)” 2016. <https://arxiv.org/abs/1606.08813>, dostęp: 1.04.2021.
- Grabowski A., *Kumulacja ochrony programu komputerowego prawem autorskim i patentowym, w przypadku udzielenia skutecznego w Polsce patentu europejskiego na wynalazek realizowany przy użyciu programu komputerowego – część I*, „Studia Prawnicze i Administracyjne” 2013, nr 2, s. 51–57.
- Gregorczyk-Abram S., Wawrykiewicz M., Owczarska A., *Entliczek, pentliczek...? Czyli System Losowego Przydziału Spraw w sądach powszechnych*, „Okno.press”, 15 stycznia 2018 r. <https://okno.press/entliczek-pentliczek-system-losowego-prydzialu-spraw-sadach-powszechnych/>, dostęp: 1.04.2021.
- Grzelak A., *Projekt reformy ochrony danych osobowych – czy rzeczywiście powstanie jednolity i spójny system?*, „Kwartalnik Kolegium Ekonomiczno-Społecznego. Studia i Prace” 2014, nr 4, s. 93–125.
- Grzeszczak R., *Władza wykonawcza w systemie Unii Europejskiej*, Stowarzyszenie Absolwentów WPiA UW, Warszawa 2011.
- Hacker P., *Teaching Fairness To Artificial Intelligence: Existing And Novel Strategies Against Algorithmic Discrimination Under EU Law*, „Common Market Law Review” 2018, t. 55, s. 1143–1186.
- Harlow C., *Freedom of Information and Transparency as Administrative and Constitutional Rights*, „Cambridge Yearbook of European Legal Studies” 1999, t. 2, s. 285–302.
- Heliskoski J., Leino P., *Darkness at the Break of Noon: the Case Law on Regulation No. 1049/2001 on Access to Documents*, „Common Market Law Review” 2006, t. 43, s. 735–781.
- Helm P., *Group Privacy in Times of Big Data. A Literature Review*, „Digital Culture and Society” 2016, t. 2, nr 2, s. 137–151.
- Hert P. de, Papanikolaou V., Malgieri G., Beslay L., Sanchez I., *The Right to Data Portability in the GDPR: Towards User-Centric Interoperability of Digital Services*, „Computer Law & Security Review” 2018, t. 34, nr 2, s. 193–203.

- Hert P. de, Papakonstantinou V., *The Council of Europe Data Protection Convention Reform: Analysis of the New Text and Critical Comment on Its Global Ambition*, „Computer Law & Security Review” 2014, t. 30, s. 633–642.
- Hildebrandt M., *A Vision of Ambient Law*, [w:] *Regulating Technologies Legal Futures, Regulatory Frames and Technological Fixes*, red. R. Brownsword, K. Yeung, Hart Publishing, Oxford–Portland 2008.
- Hildebrandt M., *Profiling: From Data to Knowledge The challenges of a crucial technology*, „Datenschutz und Datensicherheit” 2006, t. 30, nr 9, s. 548–552.
- Hildebrandt M., *Smart Technologies and the End(s) of Law. Novel Entanglements of Law and Technology*, Edward Elgar Publishing, Cheltenham 2015.
- Hill R.K., *What an Algorithm Is*, „Philosophy & Technology” 2016, nr 29, s. 35–59.
- Hilson C., *Risk and the European Convention on Human Rights: Towards a New Approach*, „Cambridge Yearbook of European Legal Studies” 2009, nr 11, s. 353–375.
- Hins W., Voofhoof D., *Access to State-Held Information as a Fundamental Right under the European Convention on Human Rights*, „European Constitutional Law Review” 2007, nr 3, s. 114–126.
- Hof S. van der, Lievens E., *The Importance of Privacy by Design and Data Protection Impact Assessments in Strengthening Protection of Children’s Personal Data Under the GDPR*, „Communications Law” 2018, t. 23, nr 1, s. 33–43.
- Izdebski K., *Algorithms of Fairness*, „Medium” 2018. <https://medium.com/fundacja-epa-%C5%84stwo/algorithms-of-fairness-2a30c2f93622>, dostęp: 1.04.2021.
- Jankowska M., *Podmiotowość prawna sztucznej inteligencji?*, [w:] *O czym mówią prawnicy, mówiąc o podmiotowości*, red. A. Bielska-Brodziak, Uniwersytet Śląski, Katowice 2015.
- Janssen H.L., *An approach for a fundamental rights impact assessment to automated decision-making*, „International Data Privacy Law” 2020, t. 10, nr 1, s. 76–106.
- Johnson K., Pasquale F., Chapman J., *Artificial Intelligence, Machine Learning, and Bias in Finance: Toward Responsible Innovation*, „Fordham Law Review” 2019, t. 88, nr 2, s. 499–529.
- Kaminski M.E., *The Right to Explanation, Explained*, „Berkeley Technology Law Journal” 2019, t. 34, nr 1, s. 189–218.
- Kammourieh L., Baar T., Berens J., Letouzé E., Manske J., Palmer J., Sangokoya D., Vinck P., *Group Privacy in the Age of Big Data*, [w:] *Group Privacy. New Challenges of Data Technologies*, red. L. Taylor, L. Floridi, B. van der Sloot, Springer, Cham 2017.
- Kaźmierczak J., *Prawo do przenoszenia danych osobowych – wybrane zagadnienia na tle realizacji nowego uprawnienia przyznanego przez RODO*, „Internetowy Kwartalnik Antymonopolowy i Regulacyjny” 2018, nr 4(7), s. 86–97.
- Keller P., *European and International Media Law. Liberal Democracy, Trade, and the New Media*, Oxford University Press, Oxford 2011.
- Kierkegaard S., Waters N., Greenleaf G., Bygrave L.A., Lloyd I., Saxby S., *30 years on: The review of the Council of Europe Data Protection Convention 108*, „Computer Law & Security Review” 2011, t. 27, s. 223–231.
- Kim T.W., Routledge B.R., *Informational Privacy, A Right to Explanation, and Interpretable AI*, „Conference: IEEE PAC (Privacy-Aware Computing) 2018” 2018. <https://ieeexplore.ieee.org/document/8511831>, dostęp: 1.04.2021.
- Kleinberg J., Ludwig J., Mullainathan S., Sunstein C.R., *Discrimination in the Age of Algorithms*, „Journal of Legal Analysis” 2018, t. 10, s. 113–174.
- Kleinman Z., *Cambridge Analytica: The story so far*, BBC, 21 marca 2018 r. <https://www.bbc.co.uk/news/technology-43465968>, dostęp: 1.04.2021.

- Koops B.-J., *Criteria for Normative Technology: The Acceptability of 'Code as law' in Light of Democratic and Constitutional Values*, [w:] *Regulating Technologies Legal Futures, Regulatory Frames and Technological Fixes*, red. R. Brownsword, K. Yeung, Hart Publishing, Oxford–Portland 2008.
- Korff D., *New Challenges to Data Protection Study – Working Paper No. 2: Data Protection Laws in the EU: The Difficulties in Meeting the Challenges Posed by Global Social and Technical Developments (European Commission DG Justice, Freedom and Security Report)*, 2010. <https://ssrn.com/abstract=1638949>, dostęp: 1.04.2021.
- Kranenborg H., *Access to Documents and Data Protection in the European Union: On the Public Nature of Personal Data*, „Common Market Law Review” 2009, t. 45, s. 1079–1114.
- Kroll J.A., Huey J., Barocas S., Felten E.W., Reidenberg J.R., Robinson D.G., Yu H., *Accountable Algorithms*, „University of Pennsylvania Law Review” 2017, t. 165, s. 633–705.
- Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (EU) 2016/679*, C.H. Beck, Warszawa 2016.
- Kullmann M., *Platform Work, Algorithmic Decision-Making, and EU Gender Equality Law*, „International Journal of Comparative Labour Law and Industrial Relations” 2018, t. 34, nr 1, s. 1–21.
- Kuner Ch., Bygrave L.A., Docksey Ch., red., *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford University Press, Oxford 2020.
- Kuziemski M., Misuraca G., *AI governance in the public sector: Three tales from the frontiers of automated decision-making in democratic settings*, „Telecommunications Policy” 2020, t. 44, nr 6, artykuł nr 101976.
- Laat P.B. de, *Algorithmic Decision-Making Based on Machine Learning from Big Data: Can Transparency Restore Accountability?*, „Philosophy and Technology” 2018, t. 31, s. 525–541.
- Lambrecht A., Tucker C., *Algorithmic Bias? An Empirical Study into Apparent Gender-Based Discrimination in the Display of STEM Career Ads*, 2018. <https://ssrn.com/abstract=2852260>, dostęp: 1.04.2021.
- Lea S., Cardwell P.J., *Transparency Requirements in the Course of a Legislative Procedure: Council v. Access Info Europe*, „European Public Law” 2015, nr 21(1), s. 61–80.
- Leeuw M.E. de, *Case C-41/00 P, Interporc Im- und Export GmbH v. Commission of the European Communities, judgment of 6 March 2003*, [2003] ECR I-02125; *Case T-76/02, Mara Messina v. Commission of the European Communities, judgment of 17 September 2003*, nyr; *Case T-47/01, Co-Frutta Soc. Coop. RI v. Commission of the European Communities, judgment of 16 October 2003*, nyr., „Common Market Law Review” 2004, t. 41, s. 261–280.
- Leeuw M.E. de, *Openness in the legislative process in the European Union*, „European Law Review” 2007, t. 32 nr 3, s. 295–318.
- Leeuw M.E. de, *The Regulation on public access to European Parliament, Council and Commission documents in the European Union: are citizens better off?*, „European Law Review” 2003, t. 28, nr 3, s. 324–348.
- Legg S., Hutter M., *A Collection of Definitions of Intelligence*, [w:] B. Goertzel, P. Wang, *Frontiers in Artificial Intelligence and Applications: Volume 157: Advances in Artificial General Intelligence: Concepts, Architectures and Algorithms*, IOS Press, Amsterdam 2007, s. 17–24.

- Leghe F., Weismann P., *The European Court of Human Rights and Access to Information*, „International Human Rights Law Review” 2014, t. 3, nr. 303–315.
- Lehman-Wilzig S.N., *Frankenstein Unbound: Towards a Legal Definition of Artificial Intelligence*, „Futures” 1981, t. 13, nr 6, s. 442–457.
- Leino P., *Case C-353/99 P, Council v. Heidi Hautala, judgment of the Full Court of 6 December 2001, nyr, appeal against the judgment of the Court of First Instance of 19 July 1999 in Case T-14/98, Hautala v. Council*, [1999] II-2489, „Common Market Law Review” 2002, t. 39, s. 621–632.
- Leino P., *Case C-64/05 P, Kingdom of Sweden v. Commission of the European Communities and Others, Judgment of the European Court of Justice (Grand Chamber) of 18 December 2007, nyr*, „Common Market Law Review” 2008, t. 45, s. 1469–1486.
- Leino P., *Just a Little Sunshine in the Rain: the 2010 Case Law of the European Court of Justice on Access to Documents*, „Common Market Law Review” 2011, t. 48, s. 1215–1252.
- Lenaerts K., *The Principle of Democracy in the Case Law of the European Court of Justice*, „International and Comparative Law Quarterly” 2013, t. 62, s. 271–315.
- Lepri B., Oliver N., Letouzé E., Pentland A., Vinck P., *Fair, Transparent, and Accountable Algorithmic Decision-making Processes. The Premise, the Proposed Solutions, and the Open Challenges*, „Philosophy and Technology” 2018, t. 31, s. 611–627.
- Lessig L., *Code and Other Laws of Cyberspace*, Basic Books, Nowy Jork 1999.
- Lessig L., *Code. Version 2.0*, Basic Books, Nowy Jork 2006.
- Lessig L., *Law Regulating Code Regulating Law*, „Loyola University Chicago Law Journal” 2003, t. 35, s. 1–14.
- Lievens E., Verdoodt V., *Looking for needles in a haystack: Key issues affecting children’s rights in the General Data Protection Regulation*, „Computer Law & Security Review” 2018, t. 34, nr 2, s. 269–278.
- Litwiński P. (red.), P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych: komentarz*, C.H. Beck, Warszawa 2017.
- Lum K., Isaac W., *To predict and serve?*, „Significance” 2016, t. 13, nr 5, s. 14–19.
- Lyon D., red., *Surveillance as Social Sorting Privacy, Risk, and Digital Discrimination*, Routledge, Londyn–Nowy Jork 2003.
- Malgieri G., *Automated decision-making in the EU member States: The right to explanation and other “suitable safeguards” for algorithmic decisions in the EU national legislations*, „Computer Law & Security Review” 2019, t. 35, nr 5, s. 1–26.
- Malgieri G., Comandé G., *Why a Right to Legibility of Automated Decision-Making Exists in the General Data Protection Regulation*, „International Data Privacy Law” 2017, t. 7, nr 4, s. 243–265.
- Maliszewska-Nienartowicz J., *Rozdział I. Pojęcie i źródła europejskiego prawa antydyskryminacyjnego*, [w:] *Prawo antydyskryminacyjne. System prawa Unii Europejskiej*, t. 6, red. J. Maliszewska-Nienartowicz, C.H. Beck, Warszawa 2020.
- Maliszewska-Nienartowicz J., *Rozdział III: Konstrukcja prawna zakazu dyskryminacji oraz prawa do niedyskryminacyjnego traktowania*, [w:] *Prawo antydyskryminacyjne. System prawa Unii Europejskiej*, t. 6, red. J. Maliszewska-Nienartowicz, C.H. Beck, Warszawa 2020.
- Markiewicz R., *Kłopoty z programem źródłowym*, „Zagadnienia Naukoznawstwa” 2015, nr 3(205), s. 311–322.
- Matczak M., *List do Trybunału Sprawiedliwości Unii Europejskiej ws. praworządności w Polsce*, „Archiwum Osiatyńskiego”, 1 czerwca 2018 r. <https://archiwumosiatyńskiego.pl/>

- wpis-w-debacie/list-do-trybunalu-sprawiedliwosci-unii-europejskiej-ws-praworzadnosci-w-polsce, dostęp: 1.04.2021.
- Mazur J., *Automated Decision-Making and the Precautionary Principle in EU Law*, „Baltic Journal of European Studies” 2019, t. 9, nr 4, s. 3–18.
- Mazur J., *Automated Decision-Making Systems as a Challenge for Effective Legal Protection in European Union Law*, „European Law Review” 2021, t. 46, nr 2, s. 194–210.
- Mazur J., *Unia Europejska wobec rozwoju sztucznej inteligencji: proponowane strategie regulacyjne a budowanie jednolitego rynku cyfrowego*, „Europejski Przegląd Sądowy” 2020, nr 9, s. 13–18.
- McCullagh K., *The General Data Protection Regulation: A Partial Success for Children on Social Network Sites?*, [w:] *Data Protection, Privacy and European Regulation in the Digital Age*, red. T. Bräutigam, S. Miittinen, Helsingin yliopiston oikeustieteellinen tiedekunta, Helsinki 2016.
- McGonagle T., *The Development of Freedom of Expression and Information Within the UN: Leaps and Bounds or Fits and Starts?*, [w:] *The United Nations and Freedom of Expression and Information. Critical Perspectives*, red. T. McGonagle, Y. Donders, Cambridge University Press, Cambridge 2015.
- Mednis A., *Prawo ochrony danych osobowych wobec profilowania osób fizycznych*, PRESCOM, Warszawa 2019.
- Mendoza I., Bygrave L.A., *The Right Not to be Subject to Automated Decisions Based on Profiling*, [w:] *EU Internet Law. Regulation and Enforcement*, red. T.-E. Synodinou, P. Jougoux, Ch. Markou, T. Prastitou, Springer, Cham 2017.
- Mitchell T., *The Need for Biases in Learning Generalizations*, „Techreport” 1980. <https://www.semanticscholar.org/paper/The-Need-for-Biases-in-Learning-Generalizations-Mitchell/6cf35ec34efa592f83e3a1b748aea14957fc784a>, dostęp: 1.04.2021.
- Mitchell W.J., *City of Bits Space, Place, and the Infobahn*, MIT Press, Cambridge–Londyn 1996.
- Mittelstadt B.D., Allo P., Taddeo M., Wachter S., Floridi L., *The ethics of algorithms: Mapping the debate*, „Big Data & Society” 2016, t. 3, nr 2, s. 1–21.
- Mittelstadt B., *From Individual to Group Privacy in Big Data Analytics*, „Philosophy and Technology” 2017, t. 30, s. 475–494.
- Mökander J., Morley J., Taddeo M., Floridi L., *Ethics-Based Auditing of Automated Decision-Making Systems: Nature, Scope, and Limitations*, „Science and Engineering Ethics” 2021, t. 27, artykuł nr 44.
- Muller J.W., *Defending Democracy within the EU*, „Journal of Democracy” 2013, t. 24, nr 2, s. 138–149.
- Napieralski A., *Collecting Data at EU Smart Borders: Data Protection Challenges of the New Entry/Exit System*, „Recht & Gesellschaft” 2019, nr 2, s. 199–209.
- Napieralski A., *Right to Appeal and Copyright – Challenging Automated Decisions at EU Borders*, „ipCompetence” 2018, t. 20, s. 20–24.
- Niklas J., *Co zawiera algorytm służący do profilowania w urzędach pracy?*, 2018. <https://panoptykon.org/wiadomosc/co-zawiera-algorytm-sluzacy-do-profilowania-w-urzedach-pracy>, dostęp: 1.04.2021.
- Niklas J., *Problem dyskryminacji automatycznej – uwagi na tle ogólnego rozporządzenia o ochronie danych osobowych*, „Europejski Przegląd Sądowy” 2019, nr 7, s. 4–9.
- Noto La Diega G., *Against the Dehumanisation of Decision-Making – Algorithmic Decisions at the Crossroads of Intellectual Property, Data Protection, and Freedom of Information*, „Journal of Intellectual Property, Information Technology and Electronic Commerce Law” 2018, t. 9, nr 3, s. 3–34.

- Nowicki M.A., *Komentarz do Konwencji o ochronie praw człowieka i podstawowych wolności*, [w:] *Wokół Konwencji Europejskiej. Komentarz do Europejskiej Konwencji Praw Człowieka*, wyd. 7, Wolters Kluwer Polska, Warszawa 2017.
- O'Neil C., *Broń matematycznej zagłady. Jak algorytmy zwiększają nierówność i zagrażają demokracji*, tłum. M. Zieliński, Wydawnictwo Naukowe PWN, Warszawa 2017.
- O'Neill M., *The Right of Access to Community-Held Documentation as a General Principle of EC Law*, „European Public Law” 1998, t. 4, nr 3, s. 403–432.
- Öberg U., *EU Citizen's Right to Know: The Improbable Adoption of a European Freedom of Information Act*, „Cambridge Yearbook of European Legal Studies” 1999, t. 2, s. 303–328.
- Österdahl I., *Case T124/ 96, Interporc Imund Export GmbH v. Commission, Judgment of 6 February 1998*, [1998] ECR II0231; *Case T83/ 96, Gerard van der Wal v. Commission, Judgment of 19 March 1998*, [1998] ECR II0545; *Case T174/ 95, Svenska Journalistförbundet v. Council of the European Union, Judgment of 17 June 1998*, [1998] ECR II2289, „Common Market Law Review” 1999, t. 36, s. 1059–1077.
- Pasquale F., *Restoring Transparency to Automated Authority*, „Journal on Communication and High Technology Law” 2011, t. 9, s. 235–254.
- Pasquale F., *The Black Box Society. The Secret Algorithms That Control Money and Information*, Harvard University Press, Cambridge–Londyn 2015.
- Peers S., *The New Regulation on Access to Documents: A Critical Analysis*, „Yearbook of European Law” 2001, t. 21, nr 1, s. 385–442.
- Podrecki P., red., *Prawo Internetu*, wyd. 2, Lexis Nexis, Warszawa 2007.
- Politou E., Alepis E., Patsakis C., *Forgetting Personal Data and Revoking Consent under the GDPR: Challenges and Proposed Solutions*, „Journal of Cybersecurity” 2018, t. 4, nr 2, s. 1–20.
- Póltorak N., *Zakres związania państw członkowskich Kartą Praw Podstawowych Unii Europejskiej*, „Europejski Przegląd Sądowy” 2014, nr 9, s. 17–28.
- Prechal S., de Leeuw M., *Dimensions of Transparency: The Building Blocks for a New Legal Principle?*, „Review of European Administrative Law” 2007, nr 1, s. 51–62.
- Radoniewicz F., *Ochrona programów komputerowych w prawie UE (cz. I)*, „Europejski Przegląd Sądowy” 2009, nr 3, s. 22–28.
- Radoniewicz F., *Ochrona programów komputerowych w prawie UE (cz. II)*, „Europejski Przegląd Sądowy” 2009, nr 5, s. 24–34.
- Reda J., *When filters fail: These cases show we can't trust algorithms to clean up the internet*, 28 września 2017 r. <https://juliareda.eu/2017/09/when-filters-fail/>, dostęp: 1.04.2021.
- Reidenberg J.R., *Lex Informatica: The Formulation of Information Policy Rules through Technology*, „Texas Law Review” 1997–1998, t. 76, s. 553–593.
- Riekkinen M., Suksi M., *Access to Information and Documents as a Human Right*, Institute for Human Rights/Åbo Akademi University, Turku-Åbo 2015.
- Rossi L., Vinagre e Silva P., *Public Access to Documents in the EU*, Hart Publishing, Oxford–Portland 2017.
- Sakowska-Baryła M., red., *Ogólne rozporządzenie o ochronie danych osobowych: komentarz*, C.H. Beck, Warszawa 2018.
- Sandeen S.K., Mylly U.-M., *Trade Secrets and the Right to Information: A Comparative Analysis of E.U. and U.S. Approaches to Freedom of Expression and Whistleblowing*, „North Carolina Journal of Law & Technology” 2020, t. 21, nr 3, s. 1–61.
- Savin A., *Profiling in the Present and New EU Data Protection Frameworks*, [w:] *Erhvervsretlige emner*, red. P. A. Nielsen, P. K. Schmidt, K. Dyppel Weber, Erhvervsretlige emne, Juridisk Institut CBS, Djof 2015. <https://ssrn.com/abstract=2697531>, dostęp: 1.04.2021.

- Schabas W.A., *The European Convention on Human Rights: a commentary*, Oxford University Press, Oxford 2015.
- Schermer B.W., *The Limits of Privacy in Automated Profiling and Data Mining*, „Computer Law & Security Review” 2011, t. 27, nr 1, s. 45–52.
- Schiek D., *A New Framework on Equal Treatment of Persons in EC Law? Directives 2000/43 EC, 2000/78/EC and 2002/??/EC changing Directive 76/207/EEC in context*, „European Law Journal” 2002, t. 8, nr 2, s. 290–314.
- Schwartz O., *Untold History of AI: Algorithmic Bias Was Born in the 1980s*, „IEEE Spectrum” 2019. <https://spectrum.ieee.org/tech-talk/tech-history/dawn-of-electronics/untold-history-of-ai-the-birth-of-machine-bias>, dostęp: 17.04.2019.
- Selbst A.D., Powles J., *Meaningful Information and the Right to Explanation*, „International Data Privacy Law” 2017, t. 7, nr 4, s. 233–242.
- Settembri P., *Transparency and the EU Legislator: Let He Who Is without Sin Cast the First Stone*, „Journal of Common Market Studies” 2005, t. 43, nr 3, s. 637–654.
- Sibiga G., Małobęcka-Szwast I., *Relacje prawa do informacji publicznej oraz prawa do ochrony danych osobowych w świetle ogólnego rozporządzenia o ochronie danych (RODO)*, „Monitor Prawniczy” 2019, nr 22 (dodatek specjalny: Polskie przepisy o ochronie danych osobowych), s. 60–73
- Śledzińska-Simon A., *Zasada równości i zasada niedyskryminacji w prawie Unii Europejskiej*, „Studia BAS” 2011, nr 2(26), s. 41–86.
- Staszczyk P., *A Legal Analysis of NGOs and European Civil Society*, Kluwer Law International, Alphen aan den Rijn 2019.
- Suptot A., *Governance by Numbers. The Making of a Legal Model of Allegiance*, tłum. S. Brown, Hart Publishing, Oxford 2017.
- Szpor G. red., *Jawność i jej ograniczenia*, C.H. Beck, Warszawa 2013–2016.
- Szpunar M., *Kilka uwag systematyzujących na temat zakresu zastosowania Karty Praw Podstawowych UE*, „Europejski Przegląd Sądowy” 2015, nr 10, s. 4–10.
- Sztandar-Sztanderska K., Kotnarowski M., Zieleńska M., *Czy algorytmy wprowadzają w błąd? Metaanaliza algorytmu profilowania bezrobotnych stosowanego w Polsce*, „Studia Socjologiczne” 2021, nr 1, s. 89–115.
- Szwarc M., *Zasady wglądu do dokumentów instytucji Wspólnot Europejskich*, „Państwo i Prawo” 2001, z. 11, s. 63–76.
- Temme M., *Algorithms and Transparency in View of the New General Data Protection Regulation*, „European Data Protection Law Review” 2017, t. 3, nr 4, s. 473–485.
- Terwangne C. de, *The work of revision of the Council of Europe Convention 108 for the protection of individuals as regards the automatic processing of personal data*, „International Review of Law, Computers & Technology” 2014, t. 28, nr 2, s. 118–130.
- Tiilikka P., *Access to Information as a Human Right in the Case Law of the European Court of Human Rights*, „Journal of Media Law” 2013, t. 5, nr 1, s. 79–103.
- Tikkinen-Piri Ch., Rohunen A., Markkula J., *EU General Data Protection Regulation: Changes and implications for personal data collecting companies*, „Computer Law & Security Review” 2017, t. 34, nr 1, s. 134–153.
- Tobler Ch., *Equality and Non-Discrimination under the ECHR and EU Law A Comparison Focusing on Discrimination against LGBTI Persons*, „Zeitschrift für ausländisches öffentliches Recht und Völkerrecht” 2014, t. 74, s. 521–561.
- Tosoni L., *The right to object to automated individual decisions: resolving the ambiguity of Article 22(1) of the General Data Protection Regulation*, „International Data Privacy Law” 2021, ipaa024 (online first).

- Veale M., Zuiderveen Borgesius F., *Demystifying the Draft EU Artificial Intelligence Act*, SocArXiv 2021. <https://doi.org/10.31235/osf.io/38p5f>, dostęp: 18.07.2021.
- Wachter S., Mittelstadt B., *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, „Columbia Business Law Review” 2019, nr 2, s. 494–620.
- Wachter S., Mittelstadt B., Floridi L., *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*, „International Data Privacy Law” 2017, t. 7, nr 2, s. 76–99.
- Wachter S., Mittelstadt B., Russel Ch., *Counterfactual Explanations Without Opening the Black Box: Automated Decisions and the GDPR Article*, „Harvard Journal of Law and Technology” 2018, t. 31, nr 2, s. 841–877.
- Wachter S., Mittelstadt B., Russell Ch., *Why Fairness Cannot be Automated: Bridging the gap between EU Non-Discrimination Law and AI*, „Computer Law & Security Review” 2021, t. 41, 105567.
- Wagner J., Benecke A., *National Legislation within the Framework of the GDPR*, „European Data Protection Law Review” 2016, nr 2, s. 353–361.
- Wasilewski A., *Prawo dostępu do dokumentów instytucji Unii Europejskiej*, „Europejski Przegląd Sądowy” 2006, nr 11, s. 4–13.
- Weber R.H., *Socio-Ethical Values and Legal Rules on Automated Platforms: The Quest for a Symbiotic Relationship*, „Computer Law & Security Review” 2020, t. 36, s. 1–8.
- Weiss F., Steiner S., *Transparency as an Element of Good Governance in the Practice of the EU and the WTO: Overview and Comparison*, „Fordham International Law Journal” 2006, t. 30, nr 5, s. 1545–1586.
- Weizenbaum J., *Computer Power and Human Reason: From Judgment to Calculation*, W. H. Freeman and Company, San Francisco 1976.
- Wierczyński G., *Udostępnianie informacji o prawie jako warunek skutecznej działalności prawotwórczej*, Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2015.
- Wiewiórowski W.R., *Prawo do przenoszenia danych w ogólnym rozporządzeniu o ochronie danych osobowych*, „Europejski Przegląd Sądowy” 2017, nr 5, s. 23–30.
- Wong J.C., *The Cambridge Analytica Scandal Changed the World – but It Didn’t Change Facebook*, „The Guardian” 18 marca 2019 r. <https://www.theguardian.com/technology/2019/mar/17/the-cambridge-analytica-scandal-changed-the-world-but-it-didnt-change-facebook>, dostęp: 1.04.2021.
- Wróbel A., red., *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, C.H. Beck, Warszawa 2019.
- Wu T., *When Code Isn’t Law*, „Virginia Law Review” 2003, t. 89, nr 4, s. 679–751.
- Xenidis R., *Tuning EU Equality Law to Algorithmic Discrimination: Three Pathways to Resilience*, „Maastricht Journal of European and Comparative Law” 2020, t. 27, nr 6, s. 736–758.
- Zalnierute M., Moses L.B., Williams G., *The Rule of Law and Automation of Government Decision Making*, „The Modern Law Review” 2019, t. 82, nr 3, s. 425–455.
- Zarsky T.Z., *Transparent Predictions*, „University of Illinois Law Review” 2013, nr 4, s. 1503–1570.
- Zawidzka-Łojek A., *Źródła prawa antydyskryminacyjnego Unii Europejskiej*, [w:] *Prawo antydyskryminacyjne Unii Europejskiej*, red. A. Zawidzka-Łojek, A. Szczerba-Zawada, Instytut Wydawniczy EuroPrawo, Warszawa 2015.
- Zerilli J., Knott A., Maclaurin J., Gavaghan C., *Algorithmic Decision-Making and the Control Problem*, „Minds and Machines” 2019, nr 29, s. 555–578.

- Zięba Ł., *Rozdział IX. Budowanie profili osobowych a wymogi wynikające z nowych przepisów o ochronie danych osobowych*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osiej, C.H. Beck, Warszawa 2017.
- Zuboff S., *Wiek kapitalizmu inwigilacji. Walka o przyszłość ludzkości na nowej granicy władzy*, tłum. A. Unterschuetz, Wydawnictwo Zysk i S-ka, Poznań 2020.
- Zuiderveen Borgesius F.J., *Strengthening Legal Protection against Discrimination by Algorithms and Artificial Intelligence*, „The International Journal of Human Rights” 2020, t. 24, nr 10, s. 1572–1593.
- Zuiderveen Borgesius F., *Discrimination, Artificial Intelligence, and Algorithmic Decision-Making*, Strasburg 2018.

Akty prawne

- American Convention on Human Rights*, „Pact of San Jose”. <https://www.refworld.org/docid/3ae6b36510.html>, dostęp: 1.04.2021 (polska wersja językowa: <http://libr.sejm.gov.pl/tek01/txt/innc/1969a-c1.html>, dostęp: 1.04.2021).
- Convention on the International Right of Correction*, 435 U.N.T.S. 191.
- Council of Europe Convention on Access to Official Documents*, CETS Nr 205.
- Decyzja 93/731/WE w sprawie dostępu do dokumentów Rady, Dz.Urz. WE 1993 L 340, s. 43.
- Decyzja 94/90/EWWG, WE, *Euratom w sprawie dostępu do dokumentów*, Dz.Urz. WE 1994 L 46, s. 58.
- Decyzja Europejskiego Banku Centralnego z dnia 4 marca 2004 r. w sprawie publicznego dostępu do dokumentów Europejskiego Banku Centralnego (EBC/2004/3), Dz.Urz. UE 2004 L 80, s. 42–44.
- Decyzja Komisji z 19 września 1996 zmieniająca decyzję 94/90/EWWG, WE, *Euratom z 8 lutego 1994 w sprawie dostępu do dokumentów (96/657/Euratom, EWWG, WE)*, Dz.Urz. WE 1996 L 247, s. 45.
- Dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego, Dz.Urz. UE 2003 L 345, s. 90–96 (polskie wydanie specjalne: rozdz. 13, t. 32, s. 701–707).
- Dyrektywa 2006/54/WE Parlamentu Europejskiego i Rady z dnia 5 lipca 2006 r. w sprawie wprowadzenia w życie zasady równości szans oraz równego traktowania kobiet i mężczyzn w dziedzinie zatrudnienia i pracy (wersja preredagowana), Dz.Urz. UE 2006 L 204, s. 23–36.
- Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.Urz. WE 1995 L 281, s. 31–50.
- Dyrektywa 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r. w sprawie ochrony prawnej baz danych, Dz.Urz. WE 1996 L 77, s. 20–28.
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłająca decyzję ramową Rady 2008/977/WSiSW, Dz.Urz. UE 2016 L 119, s. 89–131.
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem (Tekst mający znaczenie dla EOG), Dz.Urz. UE 2016 L 157, s. 1–18.

- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego, Dz.Urz. UE 2019 L 172, s. 56–83.
- Dyrektywa Parlamentu Europejskiego i Rady 2008/50/WE z dnia 21 maja 2008 r. w sprawie jakości powietrza i czystszej powietrza dla Europy, Dz.Urz. UE 2008 L 152, s. 1–44.
- Dyrektywa Parlamentu Europejskiego i Rady 2009/24/WE z dnia 23 kwietnia 2009 r. w sprawie ochrony prawnej programów komputerowych (Wersja skodyfikowana) (Tekst mający znaczenie dla EOG), Dz.Urz. UE 2009 L 111, s. 16–22.
- Dyrektywa Parlamentu Europejskiego i Rady 2013/37/UE z dnia 26 czerwca 2013 r. zmieniająca dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego, Dz.Urz. UE 2013 L 175, s. 1–8.
- Dyrektywa Rady 2000/43/WE z dnia 29 czerwca 2000 r. wprowadzająca w życie zasadę równego traktowania osób bez względu na pochodzenie rasowe lub etniczne, Dz.Urz. WE 2000 L 180, s. 22–26 (polskie wydanie specjalne: rozdz. 20, t. 1, s. 23–27).
- Dyrektywa Rady 2000/78/WE z dnia 27 listopada 2000 r. ustanawiająca ogólne warunki ramowe równego traktowania w zakresie zatrudnienia i pracy, Dz.Urz. WE 2000 L 303, s. 16–22 (polskie wydanie specjalne: rozdz. 5, t. 4, s. 79–85).
- Dyrektywa Rady 2004/113/WE z dnia 13 grudnia 2004 r. wprowadzająca w życie zasadę równego traktowania mężczyzn i kobiet w zakresie dostępu do towarów i usług oraz dostarczania towarów i usług, Dz.Urz. UE 2004 L 373, s. 37–43.
- Dyrektywa Rady 82/501/EEC z 24 czerwca 1982 dotycząca zagrożenia poważnymi awariami w odniesieniu do niektórych rodzajów działalności przemysłowej, Dz.Urz. WE 1982 L 230, s. 1–18.
- Dyrektywa Rady z dnia 14 maja 1991 r. w sprawie ochrony prawnej programów komputerowych, Dz.Urz. WE 1991 L 122, s. 42–46.
- Karta praw podstawowych Unii Europejskiej, Dz.Urz. UE 2012 C 326, s. 391–407.
- Konwencja berneńska o ochronie dzieł literackich i artystycznych z dnia 9 września 1886 r., przejrzana w Berlinie dnia 13 listopada 1908 r. i w Rzymie dnia 2 czerwca 1928 r. (ratyfikowana zgodnie z ustawą z dnia 5 marca 1934 r.), Dz.Urz. WE 1935 nr 84 poz. 515.
- Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, sporządzona w Strasburgu dnia 28 stycznia 1981 r., Dz.U. 2003 nr 3 poz. 25 (Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS No. 108).
- Konwencja o cyberbezpieczeństwie i ochronie danych osobowych Unii Afrykańskiej, <https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection>, dostęp: 1.04.2021.
- Konwencja o ochronie praw człowieka i podstawowych wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2, Dz.U. 1993 nr 61 poz. 284.
- Konwencja wiedeńska o prawie traktatów sporządzona w Wiedniu dnia 23 maja 1969 r., Dz.U. 1990 nr 74 poz. 439.
- Loi no. 78-17 du 6. janvier 1978 relative à l'informatique, aux fichiers et aux libertés. <https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006068624/2020-10-09/>, dostęp: 1.04.2021.
- Międzynarodowy pakt praw obywatelskich i politycznych, Dz.U. 1977 nr 38 poz. 167.
- Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No. 223.
- Protocol No. 12 to the Convention for the Protection of Human Rights and Fundamental Freedoms, ETS No. 177.

- Rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji, Dz.Urz. WE 2001 L 145, s. 43–48.
- Rozporządzenie Ministra Sprawiedliwości z dnia 18 czerwca 2019 r. – Regulamin urzędowania sądów powszechnych, Dz.U. 2019 poz. 1141.
- Rozporządzenie Ministra Sprawiedliwości z dnia 28 grudnia 2017 r. zmieniające rozporządzenie – Regulamin urzędowania sądów powszechnych, Dz.U. 2017 poz. 2481.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Tekst mający znaczenie dla EOG), Dz.Urz. UE 2016 L 119, s. 1–88.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002 WE (Tekst mający znaczenie dla EOG), Dz.Urz. UE 2018 L 295, s. 39–98.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/302 z dnia 28 lutego 2018 r. w sprawie nieuzasadnionego blokowania geograficznego oraz innych form dyskryminacji klientów ze względu na przynależność państwową, miejsce zamieszkania lub miejsce prowadzenia działalności na rynku wewnętrznym oraz w sprawie zmiany rozporządzeń (WE) nr 2006/2004 oraz (UE) 2017/2394 i dyrektywy 2009/22/WE (Tekst mający znaczenie dla EOG), Dz.Urz. UE 2018 L 60I, s. 1–15.
- Traktat o funkcjonowaniu Unii Europejskiej, Dz.U. 2012 C 326, s. 47–390.
- Traktat o Unii Europejskiej, Dz.Urz. UE 2012 C 326, s. 13–46.
- Traktat ustanawiający Wspólnotę Europejską (wersja skonsolidowana, Amsterdam), Dz.Urz. UE 2006 C 321E, s. 1–331.
- Traktat z Amsterdamu, Dz.Urz. WE 1997 C 340, s. 1–144.
- Treaty on European Union – Declaration on the right of access to information, Dz.Urz. WE 1992 C 191, s. 4–112.
- Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe, Dz.U. 1997 nr 140 poz. 939
- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, Dz.Urz. WE 1997 nr 133 poz. 883.
- Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, Dz.Urz. WE2010 nr 182 poz. 1228.

Orzecznictwo TSUE

- Wyrok Sądu pierwszej instancji z dnia 12 lipca 2001 r. w sprawie T-204/99, *Olli Mattila przeciwko Radzie Unii Europejskiej i Komisji Wspólnot Europejskich*, ECLI:EU:T:2001:190.
- Wyrok Sądu pierwszej instancji z dnia 17 czerwca 1998 r. w sprawie T-174/95, *Svenska Journalistförbundet przeciwko Radzie Unii Europejskiej*, ECLI:EU:T:1998:127.
- Wyrok Sądu pierwszej instancji z dnia 19 lipca 1999 r. w sprawie T-14/98, *Heidi Hautala przeciwko Radzie Unii Europejskiej*, ECLI:EU:T:1999:157.
- Wyrok Sądu pierwszej instancji z dnia 19 marca 1998 r. w sprawie T-83/96, *Gerard van der Wal przeciwko Komisji Wspólnot Europejskich*, ECLI:EU:T:1998:59.
- Wyrok Sądu pierwszej instancji z dnia 25 kwietnia 2007 r. w sprawie T-264/04, *WWF European Policy Programme przeciwko Radzie Unii Europejskiej*, ECLI:EU:T:2007:114.

- Wyrok Sądu pierwszej instancji z dnia 26 kwietnia 2005 r. w sprawach połączonych T-110/03, T-150/03 oraz T-405/03, *Jose Maria Sison przeciwko Radzie Unii Europejskiej*, ECLI:EU:T:2005:143.
- Wyrok Sądu pierwszej instancji z dnia 6 lutego 1998 r. w sprawie T-124/96, *Interporc Im-und Export GmbH przeciwko Komisji Wspólnot Europejskich*, ECLI:EU:T:1998:25.
- Wyrok Sądu pierwszej instancji z dnia 7 lutego 2002 r. w sprawie T-211/00, *Aldo Kuijer przeciwko Radzie Unii Europejskiej*, ECLI:EU:T:2002:30.
- Wyrok Sądu z dnia 18 września 2015 r. w sprawie T-395/13, *Samuli Miettinen przeciwko Radzie Unii Europejskiej*, ECLI:EU:T:2015:648.
- Wyrok Sądu z dnia 23 stycznia 2017 r. w sprawie T-727/15, *Association Justice & Environment, z.s. przeciwko Komisji Europejskiej*, ECLI:EU:T:2017:18.
- Wyrok Sądu z dnia 26 października 2011 r. w sprawie T-436/09, *Julien Dufour przeciwko Europejskiemu Bankowi Centralnemu*, ECLI:EU:T:2011:634.
- Wyrok Sądu z dnia 27 listopada 2019 r. w sprawie T-31/18, *Luisa Izuzquiza i Arne Semrott przeciwko Europejskiej Agencji Straży Granicznej i Przybrzeżnej (Frontex)*, ECLI:EU:T:2019:815.
- Wyrok Sądu z dnia 28 maja 2020 r. w sprawie T-701/18, *Liam Campbell przeciwko Komisji Europejskiej*, ECLI:EU:T:2020:224.
- Wyrok Sądu z dnia 29 listopada 2012 r. w sprawie T-590/10, *Gabi Thesing i Bloomberg Finance LP przeciwko Europejskiemu Bankowi Centralnemu*, ECLI:EU:T:2012:635.
- Wyrok Sądu z dnia 4 maja 2012 r. w sprawie T-529/09, *Sophie in 't Veld przeciwko Radzie Unii Europejskiej*, ECLI:EU:T:2012:215.
- Wyrok Sądu z dnia 7 lutego 2018 r. w sprawie T-851/16, *Access Info Europe przeciwko Komisji Europejskiej*, ECLI:EU:T:2018:69.
- Wyrok Trybunału z dnia 22 stycznia 2020 r. w sprawie C-178/18 P, *MSD Animal Health Innovation GmbH i Intervet International BV przeciwko Europejskiej Agencji Leków (EMA)*, ECLI:EU:C:2020:873.
- Wyrok Trybunału z dnia 1 lipca 2008 r. w sprawach połączonych C-39/05 P oraz C-52/05 P, *Królestwo Szwecji i Maurizio Turco przeciwko Radzie Unii Europejskiej*, ECLI:EU:C:2008:374.
- Wyrok Trybunału z dnia 1 lutego 2007 r. w sprawie C-266/05 P, *Jose Maria Sison przeciwko Radzie Unii Europejskiej*, ECLI:EU:C:2007:75.
- Wyrok Trybunału z dnia 10 marca 2009 r. w sprawie C-345/06, *Gottfried Heinrich*, ECLI:EU:C:2009:140.
- Wyrok Trybunału z dnia 11 stycznia 2017 r. w sprawie C-491/15 P, *Reiner Typke przeciwko Komisji Europejskiej*, ECLI:EU:C:2017:5.
- Wyrok Trybunału z dnia 13 maja 2014 r. w sprawie połączonych C-131/12, *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi*, ECLI:EU:C:2014:317.
- Wyrok Trybunału z dnia 15 lutego 2016 r. w sprawie C-601/15 PPU, *J.N. przeciwko Staatssecretaris van Veiligheid en Justitie*, ECLI:EU:C:2016:84.
- Wyrok Trybunału z dnia 17 kwietnia 2018 r. w sprawie C-414/16, *Vera Egenberger przeciwko Evangelisches Werk für Diakonie und Entwicklung eV.*, ECLI:EU:C:2018:257.
- Wyrok Trybunału z dnia 17 lipca 2014 r. w sprawach połączonych C-141/12 i C-372/12, *YS przeciwko Minister voor Immigratie, Integratie en Asiel oraz Minister voor Immigratie, Integratie en Asiel przeciwko M i S.*, ECLI:EU:C:2014:2081.
- Wyrok Trybunału z dnia 17 października 2013 r. w sprawie C-280/11 P, *Rada Unii Europejskiej przeciwko Access Info Europe*, ECLI:EU:C:2013:671.

- Wyrok Trybunału z dnia 18 czerwca 2020 r. w sprawie C-78/18, *Komisja Europejska przeciwko Węgrom*, ECLI:EU:C:2020:476.
- Wyrok Trybunału z dnia 18 grudnia 2007 r. w sprawie C-64/05 P, *Królestwo Szwecji przeciwko Komisji Wspólnot Europejskich i innym*, ECLI:EU:C:2007:802.
- Wyrok Trybunału z dnia 18 lipca 2017 r. w sprawie C-213/15 P, *Komisja przeciwko Patriciowi Breyerowi*, ECLI:EU:C:2017:563.
- Wyrok Trybunału z dnia 2 maja 2012 r. w sprawie C-406/10, *SAS Institute Inc. przeciwko World Programming Ltd.*, ECLI:EU:C:2012:259.
- Wyrok Trybunału z dnia 20 grudnia 2017 r. w sprawie C-434/16, *Peter Nowak przeciwko Data Protection Commissioner*. ECLI:EU:C:2017:994.
- Wyrok Trybunału z dnia 21 czerwca 2012 r. w sprawie C-135/11 P, *IFAW Internationaler Tierschutz-Fonds gGmbH przeciwko Komisji Europejskiej*, ECLI:EU:C:2012:376.
- Wyrok Trybunału z dnia 22 grudnia 2008 r. w sprawie C-336/07, *Kabel Deutschland Vertrieb und Service GmbH & Co. KG przeciwko Niedersächsische Landesmedienanstalt für privaten Rundfunk*, ECLI:EU:C:2008:765.
- Wyrok Trybunału z dnia 22 maja 2014 r. w sprawie C-356/12, *Wolfgang Glatzel przeciwko Freistaat Bayern. Case*, ECLI:EU:C:2014:350.
- Wyrok Trybunału z dnia 22 stycznia 2013 r. w sprawie C-283/11, *Sky Österreich GmbH przeciwko Österreichischer Rundfunk*, ECLI:EU:C:2013:28.
- Wyrok Trybunału z dnia 22 stycznia 2019 r. w sprawie C-193/17, *Cresco Investigation GmbH przeciwko Markusowi Achatzemu*, ECLI:EU:C:2019:43.
- Wyrok Trybunału z dnia 22 stycznia 2020 r. w sprawie C-175/18 P, *PTC Therapeutics International Ltd przeciwko Europejska Agencja Leków (EMA)*, ECLI:EU:C:2020:23.
- Wyrok Trybunału z dnia 25 lipca 2018 r. w sprawie C-216/18 PPU, *LM*, ECLI:EU:C:2018:586.
- Wyrok Trybunału z dnia 27 lutego 2018 r. w sprawie C-64/16, *Associação Sindical dos Juízes Portugueses przeciwko Tribunal de Contas*, ECLI:EU:C:2018:117.
- Wyrok Trybunału z dnia 28 lipca 2016 r. w sprawie C-294/16 PPU, *JZ przeciwko Prokuraturze Rejonowej Łódź-Śródmieście*, ECLI:EU:C:2016:610.
- Wyrok Trybunału z dnia 28 listopada 2013 r. w sprawie C-576/12 P, *Ivan Jurašiniović przeciwko Radzie Unii Europejskiej*, ECLI:EU:C:2013:777.
- Wyrok Trybunału z dnia 29 czerwca 2010 r. w sprawie C-139/07 P, *Komisja Europejska przeciwko Technische Glaswerke Ilmenau GmbH*, ECLI:EU:C:2010:376.
- Wyrok Trybunału z dnia 29 czerwca 2010 r. w sprawie C-28/08, *Komisja Europejska przeciwko The Bavarian Lager Co. Ltd.*, ECLI:EU:C:2010:378.
- Wyrok Trybunału z dnia 29 lipca 2010 r. w sprawie C-189/09, *Komisja Europejska przeciwko Republice Austrii*, ECLI:EU:C:2010:455.
- Wyrok Trybunału z dnia 29 października 2020 r. w sprawie C-576/19 P, *Intercept Pharma Ltd i Intercept Pharmaceuticals Inc. przeciwko Europejska Agencja Leków (EMA)*, ECLI:EU:C:2020:873.
- Wyrok Trybunału z dnia 3 lipca 2014 r. w sprawie C-350/12 P, *Rada Unii Europejskiej przeciwko Sophie in 't Veld*, ECLI:EU:C:2014:2039.
- Wyrok Trybunału z dnia 30 kwietnia 1996 r. w sprawie C-58/94, *Królestwo Niderlandów przeciwko Radzie Unii Europejskiej*, ECLI:EU:C:1996:171.
- Wyrok Trybunału z dnia 6 grudnia 2001 r. w sprawie C-353/99 P, *Rada Unii Europejskiej przeciwko Heidi Hautala*, ECLI:EU:C:2001:661.
- Wyrok Trybunału z dnia 6 listopada 2018 r. w sprawach połączonych C-569/16 i C-570/16, *Stadt Wuppertal przeciwko Marii Elisabeth Bauer i Volker Willmeroth przeciwko Martinie Broßonn*, ECLI:EU:C:2018:871.

Wyrok Trybunału z dnia 6 marca 2003 r. w sprawie C-41/00 P, *Interporc Im- und Export GmbH przeciwko Komisji Wspólnot Europejskich*, ECLI:EU:C:2003:125.

Opinie rzeczników generalnych

Opinia rzecznika generalnego Edra Cruza Villalóna przedstawiona w dniu 16 maja 2013 r. w sprawie C-280/11 P, *Rada Unii Europejskiej przeciwko Access Info Europe*, ECLI:EU:C:2013:325.

Opinia rzecznika generalnego Eleanor Sharpston przedstawiona w dniu 12 października 2017 r. w sprawie C-664/15, *Protect Natur-, Arten- und Landschaftschutz Umweltorganisation przeciwko Bezirkshauptmannschaft Gmünd*, ECLI:EU:C:2017:760.

Opinia rzecznika generalnego Juliane Kokott przedstawiona w dniu 8 września 2009 r. w sprawie C-139/07 P, *Komisja Wspólnot Europejskich przeciwko Technische Glaswerke Ilmenau GmbH*, ECLI:EU:C:2009:520.

Opinia rzecznika generalnego Michała Bobeka przedstawiona w dniu 21 grudnia 2016 r. w sprawie C-213/15 P, *Komisja przeciwko Patrickowi Breyerowi*, ECLI:EU:C:2016:994.

Orzecznictwo ETPCz

Wyrok EPTCz z 7 lipca 1989 r. w sprawie *Gaskin przeciwko Zjednoczonemu Królestwu*, skarga nr 10454/83.

Wyrok ETPCz z 10 lipca 2006 r. w sprawie *Sdružení Jihočeské Matky przeciwko Republice Czeskiej*, skarga nr 19101/03.

Wyrok ETPCz z 14 kwietnia 2009 r. w sprawie *Társaság a Szabadságjogokért przeciwko Węgrom*, skarga nr 37374/05.

Wyrok ETPCz z 17 lutego 2015 r. w sprawie *Guseva przeciwko Bułgarii*, skarga nr 6987/07.

Wyrok ETPCz z 19 lutego 1998 r. w sprawie *Guerra i inni przeciwko Włochom*, skarga nr 14967/89.

Wyrok ETPCz z 19 października 2005 r. w sprawie *Roche przeciwko Zjednoczonemu Królestwu*, skarga nr 32555/96.

Wyrok ETPCz z 24 czerwca 2014 r. w sprawie *Roşianu przeciwko Rumunii*, skarga nr 27329/06.

Wyrok ETPCz z 25 czerwca 2013 r. w sprawie *Youth Initiative for Human Rights przeciwko Serbii*, skarga nr 48135/06.

Wyrok ETPCz z 26 maja 2009 r. w sprawie *Kenedi przeciwko Węgrom*, skarga nr 31475/05.

Wyrok ETPCz z 26 marca 1987 r. w sprawie *Leander przeciwko Szwecji*, skarga nr 9248/81.

Wyrok ETPCz z 28 listopada 2013 r. w sprawie *Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung Eines Wirtschaftlich Gesunden Land- und Forst-Wirtschaftlichen Grundbesitzes przeciwko Austrii*, skarga nr 39534/07.

Wyrok ETPCz z 29 stycznia 2019 r. w sprawie *Cangi przeciwko Turcji*, skarga nr 24973/15.

Wyrok ETPCz z 30 stycznia 2020 r. w sprawie *Studio Monitori i inni przeciwko Gruzji*, skarga nr 44920/09 i 8942/10.

Wyrok ETPCz z 31 lipca 2012 r. w sprawie *Shapavalov przeciwko Ukrainie*, skarga nr 5835/05.

Wyrok ETPCz z 7 lutego 2017 r. w sprawie *Bubon przeciwko Rosji*, skarga nr 63898/09.

Wyrok ETPCz z 7 października 2010 r. w sprawie *Karandja przeciwko Bułgarii*, skarga nr 69180/01.

Wyrok ETPCz z 8 listopada 2016 r. w sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*, skarga nr 18030/11.

Orzecznictwo i decyzje innych sądów

- Decyzja austriackiej Komisji do spraw Ochrony Danych z 10 marca 2016 r., App no DSB-D122.322/0001-DSB/2016.
- Komitet Praw Człowieka, Decyzja z dnia 7 kwietnia 1999 r. w sprawie 633/1995 *Gauthier przeciwko Kanadzie*
- Komitet Praw Człowieka, Komunikat z dnia 28 marca 2011 r. w sprawie 1470/2006 *Tok-takunov przeciwko Kirgistanowi*.
- Międzynamerykański Trybunał Praw Człowieka, *Wyrok w sprawie Claude Reyes i inni przeciwko Chile*, 19 września 2006 r., ser. C No. 151.
- Rechtbank Den Haag, *SyRI*, 5.2.2020, C-09-550982 HA ZA 18-388, ECLI:NL:RB-DHA:2020:865. <https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RB-DHA:2020:865>, dostęp: 1.04.2021.
- Urteil des VI. Zivilsenats vom 28.1.2014 – VI ZR 156/13.
- Wyrok NSA, III OSK 836/21, 19 kwietnia 2021 r.
- Wyrok Trybunału Konstytucyjnego, 11 K 53/16, 6 czerwca 2018 r.
- Wyrok WSA w Warszawie, II SAB/Wa 1012/15, 5 kwietnia 2016 r.

Dokumenty, raporty i publikacje organizacji międzynarodowych oraz innych instytucji

- Agencja Praw Podstawowych Unii Europejskiej, *#BigData: Discrimination in data-supported decision making*, Wiedeń 2018.
- Agencja Praw Podstawowych Unii Europejskiej, *Artificial Intelligence, Big Data and Fundamental Rights Country Research Netherlands 2020 Report provided to FRA under contract D-SE-19-T021*, 2020. https://fra.europa.eu/sites/default/files/fra_uploads/fra-ai-project-netherlands-country-research_en.pdf, dostęp: 1.04.2021.
- Agencja Praw Podstawowych Unii Europejskiej, Rada Europy, *Handbook on European non-discrimination law. 2018 edition*, Luksemburg 2018.
- Algo:aware, *State-of-the-Art Report. Algorithmic decision-making*, 2018. <https://platformobservatory.eu/app/uploads/2019/06/AlgoAware-State-of-the-Art-Report.pdf>, dostęp: 1.04.2021.
- AlgorithmWatch, Bertelsmann Stiftung, Open Society Foundations, *Automating Society. Taking Stock of Automated Decision-Making in the EU*, 2019. https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/001-148_AW_EU-ADMreport_2801_2.pdf, dostęp: 1.04.2021.
- Centrum Cyfrowe, Klub Jagielloński, *AlgoPolska. Zautomatyzowane podejmowanie decyzji w służbie społeczeństwu*, 2019. <https://centrumcyfrowe.pl/wp-content/uploads/sites/16/2019/12/Algopolska-raport.pdf>, dostęp: 1.04.2021.
- Code of Conduct concerning public access to Council and Commission documents*, Dz.Urz. WE 1993 L 340, s. 41.
- Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *Application of Convention 108 to the profiling mechanism. Some ideas for the future work of the Consultative Committee*, T-PD (2008) 01.
- European Parliament Research Service, *A governance framework for algorithmic accountability and transparency*, Bruksela 2019.
- European Parliament Research Service, *Understanding algorithmic decision-making: Opportunities and challenges*, Bruksela 2019.
- Fundacja ePaństwo, *alGOVrithms. STATE of PLAY. Report on Algorithms Usage in Government-Citizens Relations in Czechia, Georgia, Hungary, Poland, Serbia and Slovakia*,

2019. <https://epf.org.pl/en/wp-content/uploads/sites/3/2019/05/alGOVrithms-State-of-Play-Report.pdf>, dostęp: 1.04.2021.
- Fundacja Panoptykon (J. Niklas, K. Sztandar-Sztanderska, K. Szymielewicz), *Profiling the Unemployed in Poland: Social and Political Implications of Algorithmic Decision Making*, Warszawa 2015. https://panoptykon.org/sites/default/files/leadimage-biblioteka/panoptykon_profiling_report_final.pdf, dostęp: 1.04.2021.
- Grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji, *Definicja SI: główne funkcje i dyscypliny naukowe*, Bruksela 2019.
- Grupa ekspertów wysokiego szczebla ds. sztucznej inteligencji, *Wytyczne w zakresie etyki dotyczące godnej zaufania sztucznej inteligencji*, Bruksela 2019.
- Grupa Robocza Art. 29, *Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko” do celów rozporządzenia 2016/679*, 4 kwietnia 2017 r., ostatnio zmienione i przyjęte w dniu 4 października 2017 r., 17/PL WP 248 rev.01.
- Grupa Robocza Art. 29, *Wytyczne dotyczące prawa do przeniesienia danych. Przyjęte w dniu 13 grudnia 2016 r.*, 16/EN WP 242.
- Grupa Robocza Art. 29, *Wytyczne w sprawie zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE*, 3 października 2017 r., ostatnio zmienione i przyjęte 6 lutego 2018 r., 17/PL WP 251 rev. 01.
- Komisja Wspólnot Europejskich, *Communication 93/C 156/05 on public access to the institutions' documents*, Dz.Urz. WE 1993 C 156, s. 5.
- Komisja Wspólnot Europejskich, *Communication 93/C 166/04 on openness in the Community*, Dz.Urz. WE 1993 C 166, s. 4.
- Komisja, *Biała księga w sprawie sztucznej inteligencji. Europejskie podejście do doskonałości i zaufania*, COM (2020) 65 final.
- Komisja, *Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security*, COM (90) 314 final – SYN 287.
- Komisja, *Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Coordinated Plan on Artificial Intelligence*, COM (2018) 795 final.
- Komisja, *Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Sztuczna inteligencja dla Europy*, COM (2018) 237 final.
- Komisja, *Wniosek: Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące Sztucznej Inteligencji (Akt w sprawie Sztucznej Inteligencji) i zmieniające niektóre akty ustawodawcze Unii*, COM/2021/206 final
- Komitet Ministrów (Rada Europy), *Recommendation No. R (81) 19 of the Committee of Ministers to Member States on the Access to Information Held by Public Authorities* (Adopted by the Committee of Ministers on 25 November 1981 at the 340th meeting of the Ministers' Deputies). https://www.access-info.org/wp-content/uploads/Recommendation_81_19.pdf, dostęp: 1.04.2021.
- OECD (Directorate for Financial and Enterprise Affairs Competition Committee), *Algorithms and Collusion – Note from the European Union*, DAF/COMP/WD (2017) 12.
- OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980. <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheProtectionofPrivacyandTransborderFlowsOfPersonalData.htm#part2>, dostęp: 1.04.2021.
- OECD, *The OECD Privacy Framework*, 2013. http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, dostęp: 1.04.2021.

- Omidyar Network, Upturn, *Public Scrutiny of Automated Decisions: Early Lessons and Emerging Methods An Upturn and Omidyar Network Report*, 2018. <https://omidyar.com/wp-content/uploads/2020/09/Public-Scrutiny-of-Automated-Decisions.pdf>, dostęp: 1.04.2021.
- Organizacja Narodów Zjednoczonych (Rada Ekonomiczno-Społeczna), *United Nations Conference on Freedom of Information* (7th session, 1948, Geneva), E/RES/152(VII). <https://digitallibrary.un.org/record/212470>, dostęp: 1.04.2021.
- Organizacja Państw Amerykańskich, *Inter-American Program on Access to Public Information (Adopted at the Second Plenary Session, held on June 14, 2016)*, Resolution AG/RES. 2885 (XLVI O/16). http://www.oas.org/en/sla/dil/docs/access_to_information_Inter-American_Program.pdf, dostęp: 1.04.2021.
- Organizacja Państw Amerykańskich, *Principles on the Right of Access to Information*, CJI/RES.147 (LXXIII-O/08). http://www.oas.org/en/sla/dil/docs/CJI-RES_147_LXXIII-O-08_eng.pdf, dostęp: 1.04.2021.
- Powszechna deklaracja praw człowieka*, 10 grudnia 1948, rezolucja Zgromadzenia Ogólnego 217 A (polska wersja językowa: <http://libr.sejm.gov.pl/tek01/txt/onz/1948.html>), dostęp: 1.04.2021).
- Prezes Urzędu Ochrony Danych Osobowych, *Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2018*. <https://uodo.gov.pl/pl/437/1173>, dostęp: 1.04.2021.
- Prezes Urzędu Ochrony Danych Osobowych, *Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2019*. <https://uodo.gov.pl/437>, dostęp: 19.07.2021.
- Rada Europejska, *Conclusions of the Birmingham European Council (A Community close to its citizens)*, Bull. EC 10-1992.
- Rada Europejska, *Conclusions of the Copenhagen European Council (A Community close to its citizens)*, Bull. EC 6-1993.
- Rada Europejska, *Conclusions of the Edinburgh European Council (Openness and Transparency)*, Bull. EC 12-1992.
- Rada Europy (European Commission of Human Rights), *Preparatory work on article 10 of the European Convention on Human Rights*, DH (56) 15 oraz CDH (75) 6. [www.echr.coe.int/LibraryDocs/Travaux/ECHRTravaux-ART10-DH\(56\)15-EN1338895.pdf](http://www.echr.coe.int/LibraryDocs/Travaux/ECHRTravaux-ART10-DH(56)15-EN1338895.pdf), dostęp: 1.04.2021.
- Rada Europy, *Explanatory Report – CETS 223 – Automatic Processing of Personal Data (Amending Protocol)*, 2018. <https://rm.coe.int/cets-223-explanatory-report-to-the-protocol-amending-the-convention-fo/16808ac91a>, dostęp: 1.04.2021.
- Rada Europy, *Explanatory Report to the Council of Europe Convention on Access to Official Documents*, 2009. <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800d3836>, dostęp: 1.04.2021.
- The European Commission's High-Level Expert Group on Artificial Intelligence, *Draft Ethics Guidelines For Trustworthy AI. Working Document for stakeholders' consultation*, Bruksela 2018.
- Uzasadnienie do projektu ustawy z dnia o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego z 29 czerwca 2021 r.*, Druk nr 1338, Warszawa, 29 czerwca 2021 r. <https://orka.sejm.gov.pl/Druki9ka.nsf/0/057A8FFDE2C50C-63C12587040037BD25/%24File/1338.pdf> dostęp: 17.07.2021.
- Zgromadzenie Parlamentarne (Rada Europy), *Recommendation 854 (1979) Access by the public to government records and freedom of information* (Text adopted by the Assembly on 1 February 1979 – 24th Sitting). <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=14888&lang=en>, dostęp: 1.04.2021.

Źródła internetowe

- Ministerstwo Pracy i Polityki Społecznej, *Kwestionariusz do profilowania pomocy dla osób bezrobotnych oraz zasad jego oceniania*. <https://panoptykon.org/wiadomosc/jakie-pytania-zawiera-kwestionariusz-profilowania-bezrobotnych>, dostęp: 1.04.2021.
- Odpowiedź na wniosek o dostęp do informacji publicznej ZO.0143.148.2019.EB (wniosek z dnia 27 maja 2019 r.).
- Office of the Historian: Department of State, *The United States and the United Nations Conference on Freedom of Information*, Genewa 1948. <https://history.state.gov/historicaldocuments/frus1948v01p1/d189>, dostęp: 1.04.2021.
- Oxford Dictionary. https://en.oxforddictionaries.com/definition/artificial_intelligence, dostęp: 1.04.2021.
- Polskie Towarzystwo Prawa Antydyskryminacyjnego: *Protokół Nr 12 do Konwencji o ochronie praw człowieka i podstawowych wolności*. http://www.ptpa.org.pl/site/assets/files/1153/protokol_nr_12_do_kwslwfdk.pdf, dostęp: 1.04.2021.
- Rada Europy. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/223>, dostęp: 1.04.2021.
- Rada Europy. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/205/signatures?p_auth=en0DTgZ8, dostęp: 1.04.2021.
- Rada Europy. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/177/signatures?p_auth=cWKVkrEV, dostęp: 1.04.2021.
- Słownik języka polskiego. <https://sjp.pwn.pl/sjp/sztuczna-inteligencja;2466532.html>, dostęp: 1.04.2021.
- Wikipedia. [https://en.wikipedia.org/wiki/Margaret_Hamilton_\(scientist\)#/media/File:Margaret_Hamilton_-_restoration.jpg](https://en.wikipedia.org/wiki/Margaret_Hamilton_(scientist)#/media/File:Margaret_Hamilton_-_restoration.jpg), dostęp: 1.04.2021.

Summary

The main goal of my analysis is to examine the possibility of treating the algorithms used in automated decision-making as information or official document subjected to the right to access information or the right to access official documents in European law (i.e. the law of the Council of Europe and law of the European Union – EU).

The book is inspired by research which envisions the possibility of considering computer code as law. Automated decision-making is a technique based on algorithms and data analysis, which is used both in the private and in the public sector. In the latter, it can have substantial influence on how law is enforced and can even lead to its modification or creation. Therefore, access to algorithms is important for the transparency of the decision-making process in the public sector, particularly in the light of its discriminatory potential (*algorithmic bias*). The analysis addresses concerns which arise when automated decision-making seems not to be compliant with the prohibition of discrimination in European law.

The existing regulations, adopted in the area of personal data protection, do not address the systemic challenges linked to automated decision-making. They are focused on the situation of a particular individual and the decision made in their case. Both the provisions adopted in the General Data Protection Regulation (GDPR) and the Convention 108+ adopted by the Council of Europe are focused on solutions such as prohibition of automated decision making (limited by a number of exceptions) or providing access to the logic standing behind a particular decision.

However, algorithms used in automated decision-making are not subjected to regulations which would increase their level of transparency. In my book I analyse the extent to which the right to access information based on Art 10 of the European Convention of Human Rights (ECHR) according

to its interpretation by the European Court of Human Rights (ECrHR), can be perceived as an alternative to the rights granted to the individual by data protection laws. As per the ECrHR's case law, the necessary criteria for evoking the right to access information include the purpose of seeking the access, the function of the applicant filing for the access, the readiness and accessibility of information and its significance from the perspective of public interest, however, the state has the possibility to evoke exceptions to the right to access information. These exceptions need to be foreseen in law, protect one of the interests included in Art 10(2) of the ECHR and be necessary in democratic society. The ECrHR's criteria do not exclude the possibility of regarding an algorithm used in the public sector for automated decision-making as information.

The approach to the right to access information in EU law is different. Firstly, the issue was raised as one of the methods of democratization of the EU. Due to this, it came to encompass the right to access official documents of the EU's institutions, bodies and offices and agencies. Secondly, it is called the right to access official documents and as such was included in Art 42 of the Charter of Fundamental Rights (the Charter).

On the basis of the analysis of the term *document* in EU law I conclude that it is possible, in certain circumstances, to consider an algorithm as an official document. However, due to the focus on the right to access official documents (Art 42 of the Charter), EU law lacks the perspective which would link the right to access information with Art 11 of the Charter, corresponding in its content with Art 10 of the ECHR. As a result, the role of recent case law of the ECrHR concerning the right to access information is overlooked in EU law and its potential impact on the interpretation of this right is hindered.

Podziękowania

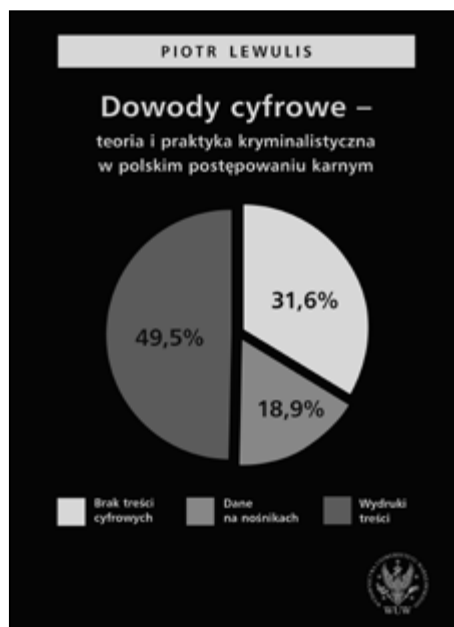
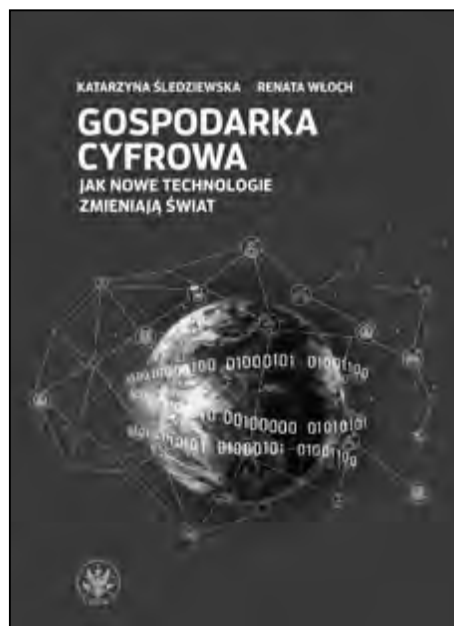
W czasie przygotowywania rozprawy doktorskiej będącej podstawą dla tej książki nieustannym wsparciem była dla mnie opieka prof. dr. hab. Roberta Grzeszczaka oraz dr hab. Magdaleny Słok-Wódkowskiej. Magdzie zawdzięczam ponadto sprowadzenie mnie do DELab UW: gdybym tam nie pracowała, ta książka by nie powstała. Dlatego ogromne podziękowania kieruję również do dyrektora zarządzającego DELabu, dr hab. prof. UW Katarzyny Śledziewskiej, dr hab. prof. UW Renaty Włoch i wszystkich z naszego Zespołu, z którymi praca jest ciągłą przygodą, źródłem radości i inspiracji.

Chciałabym również podziękować osobom pracującym na Wydziale Prawa i Administracji, które przyczyniły się do tego, że skończyłam studia doktoranckie z sukcesem.

Ważnym źródłem przemyśleń prowadzących do poprawiania i uzupełniania książki stały się dla mnie recenzje dr hab. prof. UJ Niny Półtorak oraz dr hab. prof. UG Grzegorza Wierczyńskiego, a także recenzje wydawnicze dr hab. prof. ALK Agnieszki Grzelak oraz dr hab. prof. UŁ Moniki Namysłowskiej, za które bardzo dziękuję.

Last but not least, podziękowania dla moich przyjaciół i bliskich, w tym szczególnie Heli, która jako jedna z niewielu osób niezajmujących się prawem świetnie wie, czym jest TSUE, a czym ETPCz.

Do powstania tej pracy przyczyniły się finansowanie kwerendy badawczej w Oksfordzie ze środków Zintegrowanego Programu Rozwoju Uniwersytetu Warszawskiego (listopad 2019 r.) oraz realizacja grantu Preludium finansowanego ze środków Narodowego Centrum Nauki (nr projektu: 2018/29/N/HS5/00105). Fakt, że książka się ukazuje – i to w formule *open access* – zawdzięczam natomiast środkom z Inicjatywy Doskonałości.



Wydawnictwa Uniwersytetu Warszawskiego
ul. Prosta 69, 00-838 Warszawa
tel. 22 55 31 333
www.wuw.pl

Czy kod komputerowy może być traktowany jako prawo?

Czy stosowany w sektorze publicznym algorytm może być postrzegany jako narzędzie nieprzejrzystego kształtowania sytuacji prawnej jednostki?

I przede wszystkim: czy w związku z rolą, którą algorytmy odgrywają dla jednostek, możliwe jest domaganie się dostępu do nich jako do informacji publicznej?

Analiza przeprowadzona w książce pozwoliła autorce odpowiedzieć na te pytania i pokazać, w jaki sposób prawo dostępu do informacji oraz prawo dostępu do dokumentów urzędowych w prawie europejskim mogą pomóc rozwiązać problemy wynikające z rozwoju technologii stosowanych do zautomatyzowanego podejmowania decyzji.

Joanna Mazur jest absolwentką prawa i Kolegium „Artes Liberales”, w 2021 r. uzyskała tytuł doktora nauk prawnych na Uniwersytecie Warszawskim. Zawodowo związana jest z DELab UW (Digital Economy Lab), gdzie pracuje jako analityczka i zajmuje się prawem nowych technologii. Realizuje grant NCN Preludium „Zautomatyzowane podejmowanie decyzji a zakaz dyskryminacji na gruncie prawa europejskiego” oraz jest wykonawczynią w grantie NCN OPUS „Prawo międzynarodowe gospodarcze w czasie transformacji cyfrowej: trendy, modele regulacyjne oraz szczegółowe rozwiązania w zakresie e-handlu i danych”.

www.wuw.pl



65 LAT
WYDAWNICTWO
UNIWERSYTETU
WARSZAWSKIEGO